iConnect625W User Guide

4-Port ADSL, ADSL 2/2+ Wireless Router

February 2007

Disclaimer
For content and procedures available in this document, OPEN Networks Pty Ltd does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.
Revision: v1.2
Date Released: February, 2007

Table of Contents

1. Introduction

Congratulations on the purchase of your iConnect625W. Fully-featured, it is the perfect high-speed ADSL/ADSL2+ router, specifically designed to connect your PC or LAN to the Internet and connects to your local area network (LAN) via a high speed 10/100 Mbps Ethernet port.

The iConnect625W's extensive routing and bridging functions render it a flexible and scaleable platform for multiple users to access the Internet. Features include port forwarding and VPN pass-through, along with the ability to enable public or private Intranet solutions through a single IP address, using its RIP v 1 / 2 routing engine or NAPT features.

The highest levels of security are implemented in the iConnect625W, including Stateful Packet Inspection firewall support for a full suite of security options against malicious intruders.

The iConnect625W is fully compatible with all computers that support an Ethernet interface and are running a TCP/IP protocol stack. So, plug in the iConnect625W (refer to the Quick Start Guide), configure it, as per your Internet Service Provider's (ISP) instructions and enjoy fast Internet access as never before!

1.1 Features

iConnect625W Features	
Network Support	■ WAN Protocols (PPPoE, DHCP, Static, PPPoA, CLIP, Bridged) ■ Port Mapping / Forwarding ■ PPP on-demand enhancement ■ Secure HTTP Server (HTTPS) ■ IGMP over multiple PVC for video ■ Enhanced QoS architecture (Ingress, Egress, Shaper) and Policy Routing ■ DMZ Support
Address Translation & Security	■ NAT / NAPT for basic Firewall support ■ UPnP Internet Gateway Device (IGD) ■ Application Level Gateways (ALGs) ■ Stateful Packet Inspection (SPI) support ■ Protection Against Denial of Service ■ Packet Filtering Firewall support ■ Password Authentication to modem
Gateway Services	■ DHCP Client / Server / Relay ■ Dynamic DNS Support ■ IGMP Proxy
Element Management	■ Customer-extendible Configuration Manager ■ Web service and Reference Web Pages ■ SNMP Agent and Standard MIB Support ■ Remote Management ■ Telnet, secure shell, TFTP, FTP ■ Diagnostics and Test Capabilities
WLAN Support	■ IEEE 802.11, 802.11b and 802.11g compliant ■ Complies to Wireless Ethernet Compatibility Alliance (WECA), Wireless Fidelity (WI-FI tm) standards ■ Support 802.11b and 802.11g simultaneously ■ Security (WEP, 802.1x, WPA, WPA2) ■ WDS ■ Multiple SSID ■ Operating Range of more than 300 metres (open air)

2. iConnect625W Overview

2.1 Important Safety Instructions

⚠

WARNING!

BEFORE USING YOUR DEVICE, BASIC SAFETY INSTRUCTIONS SHOULD ALWAYS BE FOLLOWED TO REDUCE THE RISK OF FIRE, ELECTRIC SHOCK AND INJURY TO PERSON, INCLUDING THE FOLLOWING:

1. Read and understand all instructions.
2. Follow all warnings and instructions marked on the product.
3. When cleaning this product, do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
4. Do not use this router in high humidity or high temperatures.
5. Do not open or repair the device yourself. If this router is too hot, turn off the power immediately and have it repaired at a qualified service centre.
6. Avoid using this product and all accessories outdoors.
7. Place this router on a stable surface.
8. Only use the power adaptor that comes with the package. Using a different voltage-rating adaptor may damage this router.
9. Slots and openings on the sides and top of the device are provided for ventilation. To protect it from overheating, these openings must not be blocked or covered. The opening should never be blocked by placing the product on the bed, sofa, rug or other similar surface. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
10. Do not allow anything sharp to rest on the cables. Do not locate this product where the cord could be damaged by persons walking on it.
11. Do not overload wall outlet extension cords, as this can result in the risk of fire or electric shock.
12. To reduce the risk of electric shock, do not disassemble this product. Instead, when some repair work is required, take the unit to the place of purchase. Opening or removing covers on the router will void the warranty that comes with the product.
13. Unplug this product from the wall outlet and refer servicing to the place of purchase under the following conditions:
    a. When the power supply cord or plug is damaged or frayed;
    b. If liquid has been spilled onto the product;
    c. If the product has been exposed to rain or water;
    d. If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal operation;
    e. If the product has been dropped or damaged;
    f. If the product exhibits a distinct change in performance.

SAVE THESE INSTRUCTIONS

2.2 System Requirements

2.2.1 Hardware

- Pentium® MMX 233MHz or greater computer;
- CD-ROM drive;
- Network adapter - Ethernet with TCP/IP Protocol (required only if you are connecting to the Ethernet port of your router);

2.2.2 Software

- OS-Independent Ethernet connections.

2.3 Package Contents

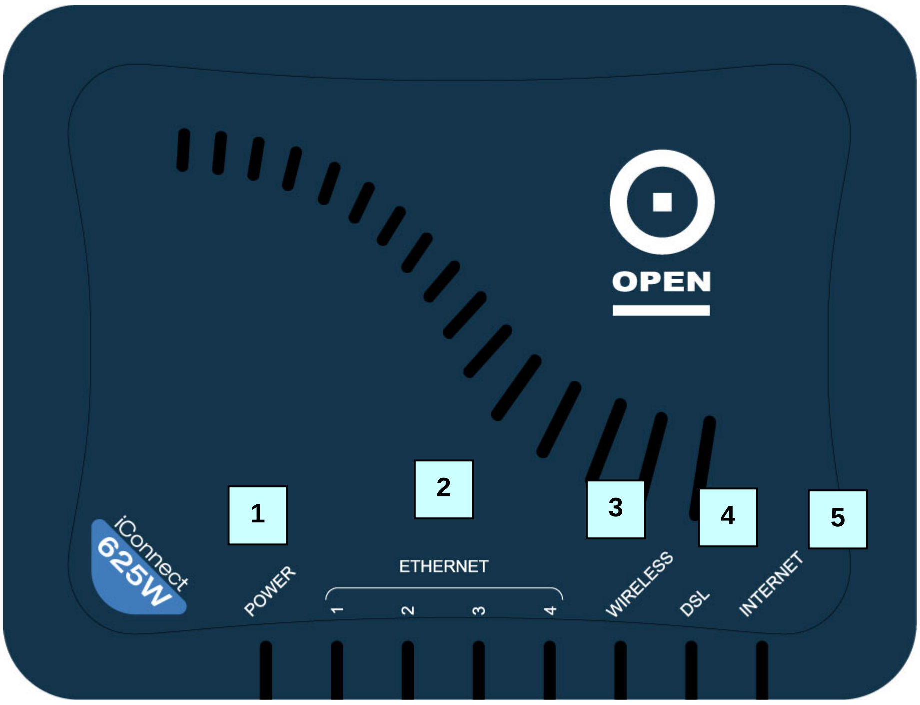
The iConnect625W router contains the following items:

- Wireless 625W router;
- CD-ROM containing the online manual;
- RJ-11 ADSL/telephone Cable;
- Ethernet (CAT-5 LAN) Cable;
- AC-DC power adaptor (9VDC, 1A);
- Quick Start Guide;
- Line Splitter / Filter.

2.4 Appearance

1.4.1 The Front LEDs

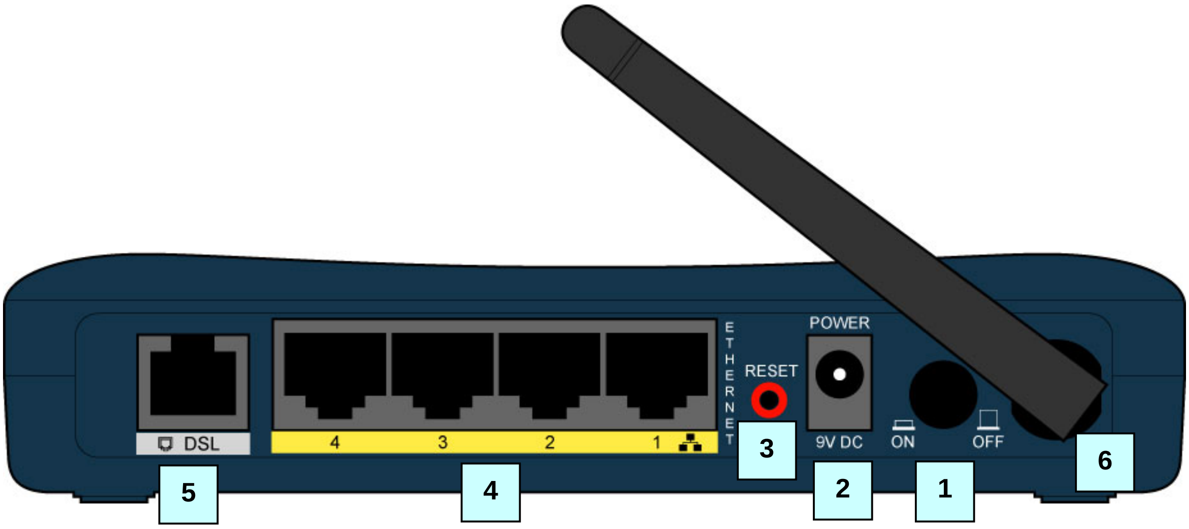
The LED status can help you diagnose problems with the gateway. The LED status definitions are described in the table below.



LED		LED Status	LED Description
1	***POWER***	Steadily Lit Up	Power is supplied to the iConnect625W router.
		Off	No power is supplied to the iConnect625W.
2	***ETHERNET E1 - E4***	Steadily Lit Up	The iConnect625W Ethernet cable is properly connected to the Ethernet port.
		Flickering	The Ethernet is transmitting / receiving data.
		Off	• No power is supplied to the iConnect625W router; • No Ethernet connection; • Wrong type of Ethernet cable used.
3	***WIRELESS***	Steadily Lit Up	The wireless access point is enabled.
		Off	The wireless access point is disabled.
4	***DSL***	Flickering	The iConnect625W is trying to establish connection with the ADSL Service Provider or the iConnect625W router is transmitting / receiving data.
		Steadily Lit Up	ADSL connection is established.
5	***INTERNET***	Steadily Lit Up	The Internet connection is established.
		Off	The Internet connection is not established.

2.4.2 The Rear Ports

The rear panel holds ports that help to power up and connect the iConnect625W router to the network.



LED		Meaning
1	***POWER SWITCH***	Power ON / OFF switch.
2	***POWER***	Connect the supplied power adaptor to this jack. Make sure to observe the proper power requirements.
3	***RESET***	After the device is powered on, press it to reset the device or restore to factory default settings.
4	***Ethernet*** ***1 — 4***	Connect the Ethernet cable to one of the four LAN ports when connecting to a computer or an office/home network of 10Mbps or 100Mbps.
5	***DSL***	Connect the supplied telephone cable to this port when connecting to the ADSL/telephone network.
6	***ANTENNA***	This is the antenna.

3. Setting Up Your iConnect625W Router

The iConnect625W router can be configured with your Web Browser. A Web Browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98 ME/2000/XP/Vista. The product provides a very easy and user-friendly interface for configuration.

Computers must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub. It must also have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router.

The default IP address of the router is *192.168.1.254* and the subnet mask is *255.255.255.0* (i.e. any attached computer must be in the same subnet, and have an IP address in the range of *192.168.1.1* to *192.168.1.253*). The best and easiest way to configure the computer is to get an IP address automatically from the router using DHCP.

If you encounter any problems accessing the router's web interface it may also be advisable to disable any kind of software firewall on your computers, as they can cause problems accessing the *192.168.1.254* IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps provided in the following section to install and configure your computer network environment. Before you begin, it is advisable to check your computer's network components to ensure that the TCP/IP protocol stack and Ethernet network adapter are installed. If they are not installed, please refer to your Windows or other operating system manuals to install them.

3.1 Default Settings

This section will guide you through your iConnect625W router configuration via the web interface. The iConnect625W router is shipped with a standard PPP configuration.

The following table lists the default settings for your iConnect625W router. These settings may change depending on your ISP. Please check with your ISP for more information.

Setting	Default Value	
Login Username	root	
Login Password	**ØP3N** (the first character is a zero: zero-P-3-N)	
WAN	***Username***	<blank> Enter your username as supplied by your ISP.
	Password	<blank> Enter your password as supplied by your ISP.
	Protocol	PPPoE The PPPoE function is *enabled* to automatically get the WAN port from the ISP but you have to set the username and password first for this to happen.
	VPI	8
	VCI	35
DHCP Configuration	DHCP Server function is set to *Enabled*.	
	Start IP	192.168.1.100
	End IP	192.168.1.200
	Lease Time	604800 seconds (or 7 days)
Management IP (LAN)	***IP address***	192.168.1.254
	Subnet Mask	255.255.255.0
	IP addresses for distribution to PCs	101 IP addresses continuing from 192.168.1.100 through 192.168.1.200.

NOTE	**If you ever forget your login password, you may press the RESET button for up to 10 seconds to restore the factory default settings.**

TIP	■ **Ensure that your computer is configured for DHCP mode and that proxies are disabled on your browser.** ■ **You must also ensure that Java Script support is enabled in the browser settings so that the browser does not display a login redirection screen.** ■ **If any screen other than the Login screen appears, you may need to delete your temporary Internet files, i.e. basically flush cached web page(s).**

3.2 Factory Default Settings

You can restore your Factory Defaults by resetting the iConnect625W to the default configuration.

Follow the steps below to restore the *Factory Default Settings*.

Step 1: Ensure that the iConnect625W router has been powered on for a minimum of 10 seconds.

Step 2: Using a blunt implement such as a pencil or paperclip, press the ***Reset*** button for 10 seconds.

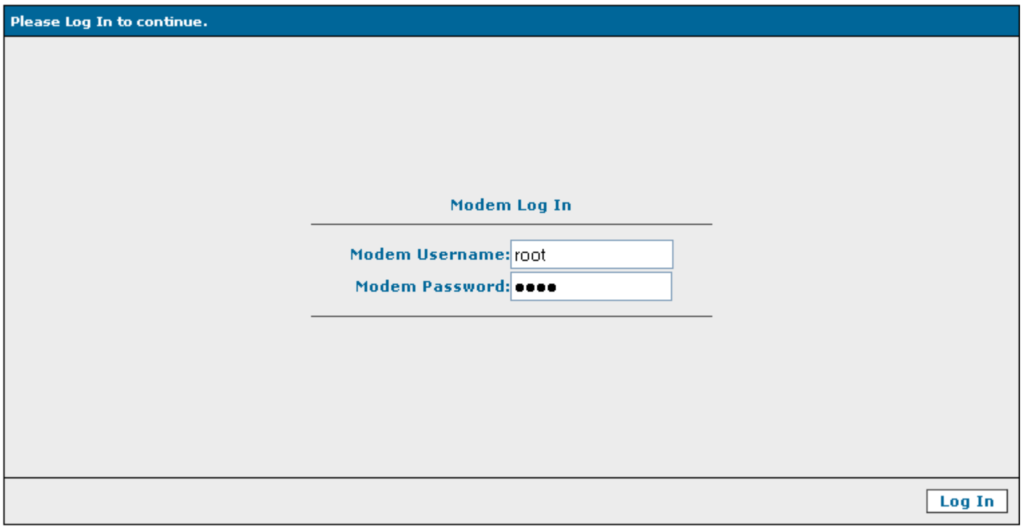
NOTE	**During this time, the reset is in progress. DO NOT power the iConnect625W off whilst it resets.**

Step 3: After 10 seconds, you may release it. The iConnect625W will be reset to its factory defaults once the indicator lights have returned to green (non-blinking).

3.3 Logging Into Your iConnect625W

Use the following procedure to log into your iConnect625W router.

Step 1: Open a web browser, and enter the following address in the *Address* bar: ***http://192.168.1.254***, then click **Go.** The following appears:



Please Log In to continue.

Modem Log In

Modem Username: root

Modem Password: ●●●●

Step 2: Enter the username and password of ***root*** and ***ØP3N*** (zero-P-3-N) in the ***User name*** and ***Password*** fields. These fields are case sensitive .

Step 3: Click the ***Log In*** button.

Congratulations! You have now successfully logged into the iConnect625W router!

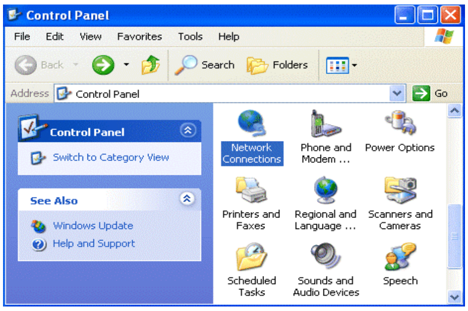
NOTE	**If you have problems logging into the router, please refer to Section 4 to configure your network connection.**

4. PC Network Connection

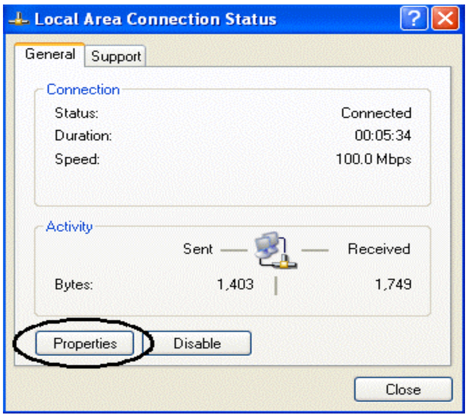
This section demonstrates the steps required to configure your network connections for the DHCP server to obtain an IP address automatically and to activate DNS Configuration, depending on your PC's Operating System (OS).

4.1 Configuring Network Computers Using Windows XP

Step 1: Click ***Start / Control Panel*** (in Classic View). From the *Control Panel* window, double-click ***Network Connections***. The following appears:



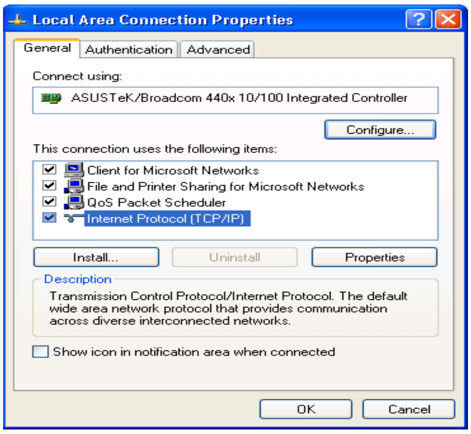
Step 2: Double-click the *Local Area Network* connection name required.



Connection
Status: Connected
Duration: 00:05:34
Speed: 100.0 Mbps

Activity
Sent — — Received
Bytes: 1,403 | 1,749

Step 3: Click ***Properties***. The following appears:


Local Area Connection Properties
General Authentication Advanced
Configure...
Install... Uninstall Properties
OK Cancel

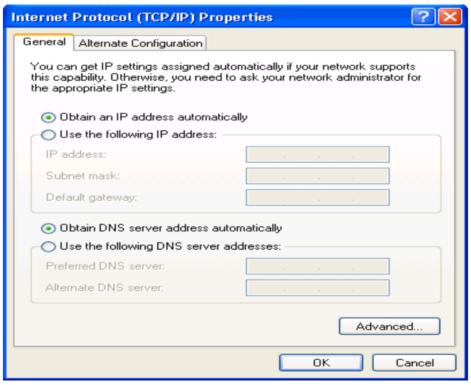
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

Step 4: Ensure the ***General*** tab is active, and highlight *Internet Protocol (TCP/IP),* then click ***Properties.*** The following appears:



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

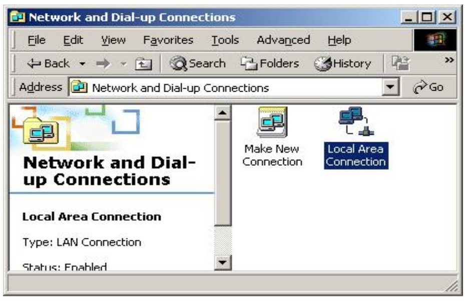
Preferred DNS server: . . .

Alternate DNS server: . . .

Step 5: Highlight the *Obtain an IP address automatically* and the *Obtain DNS server address automatically* radio buttons, then click ***OK*** to complete the configuration.

4.2 Configuring Computers in Windows 2000

Step 1: Click ***Start / Settings / Control Panel****.* From the *Control Panel* window, double-click ***Network and Dial-up Connections****.* The following appears:

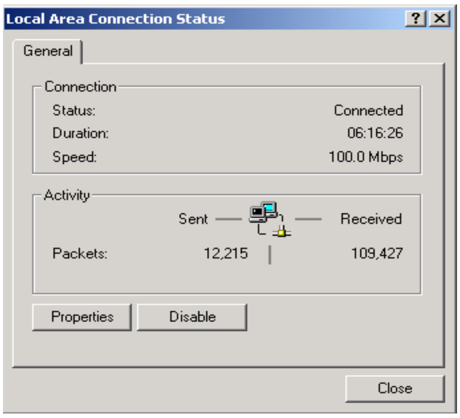

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections Go
Network and Dial-up Connections
Make New Connection
Local Area Connection

Local Area Connection

Type: LAN Connection

Status: Enabled

Step 2: Double-click the ***Local Area Connection*** name as required. The following appears:



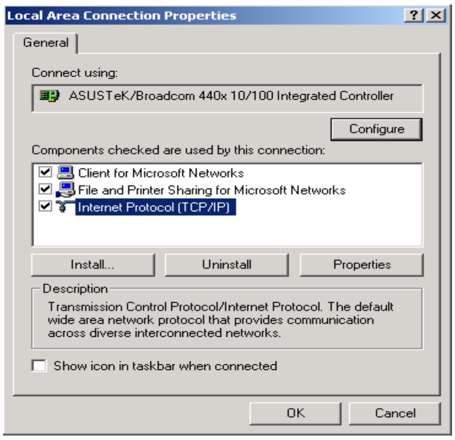
Status: Connected

Duration: 06:16:26

Speed: 100.0 Mbps

Packets: 12,215 | 109,427

Step 3: From the *Local Area Connection Status* window, click ***Properties.*** The following appears:



Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Components checked are used by this connection:

☑ Client for Microsoft Networks

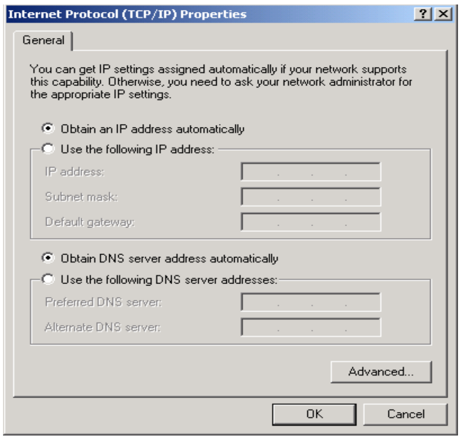
☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

Step 4: Highlight *Internet Protocol (TCP/IP)* and click ***Properties.*** The following appears:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

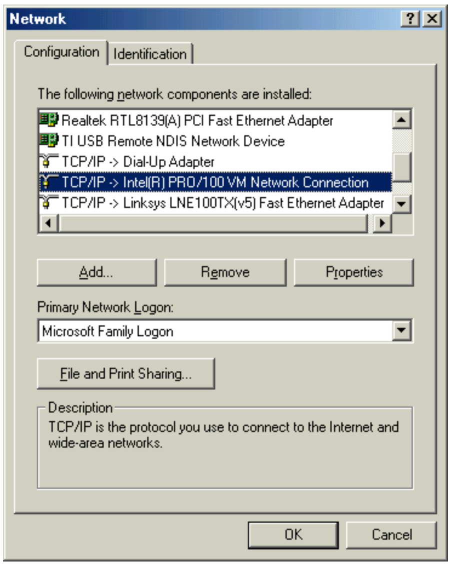
Preferred DNS server:

Alternate DNS server:

Step 5: Highlight the *Obtain an IP address automatically* and the *Obtain DNS server address automatically* radio buttons and click the ***OK*** button to complete the configuration.

4.3 Configuring Computers In Windows 98/ME

Step 1: Click ***Start / Settings / Control Panel****.* From the *Control Panel* window, double-click ***Network*** and highlight the ***Configuration*** tab to make it active. The following appears:



The following network components are installed:

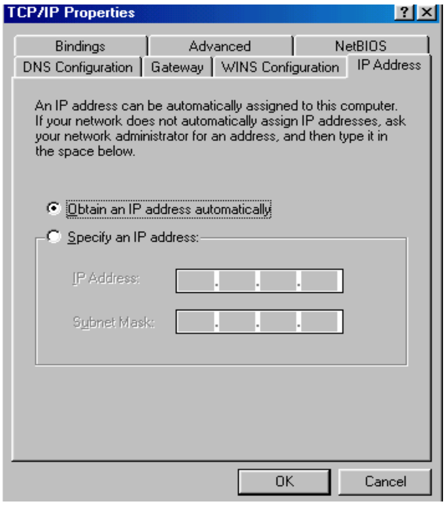
- Realtek RTL8139(A) PCI Fast Ethernet Adapter
- TI USB Remote NDIS Network Device
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Intel(R) PRO/100 VM Network Connection
- TCP/IP -> Linksys LNE100TX(v5) Fast Ethernet Adapter

Primary Network Logon: Microsoft Family Logon

File and Print Sharing...

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Step 2: Highlight ***TCP / IP -> NE2000 Compatible****,* or the name of any Network Interface Card (NIC) in your PC, and click the ***Properties*** button. The following appears:



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

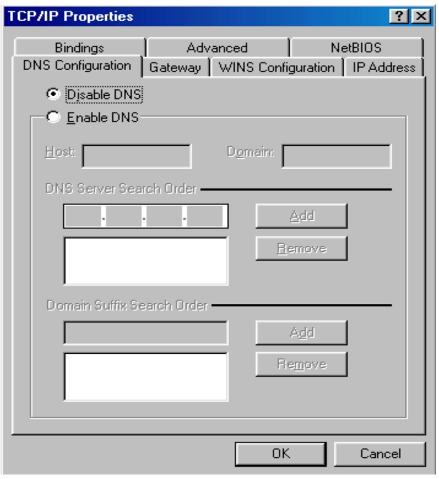
○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Step3: Highlight the ***IP Address*** tab to make it active, then highlight the ***Obtain an IP address automatically*** radio button.

Step 4: Highlight the ***DNS Configuration*** tab to make it active. The following appears:



TCP/IP Properties

Bindings | Advanced | NetBIOS | DNS Configuration | Gateway | WINS Configuration | IP Address

● Disable DNS

○ Enable DNS

Host: Domain:

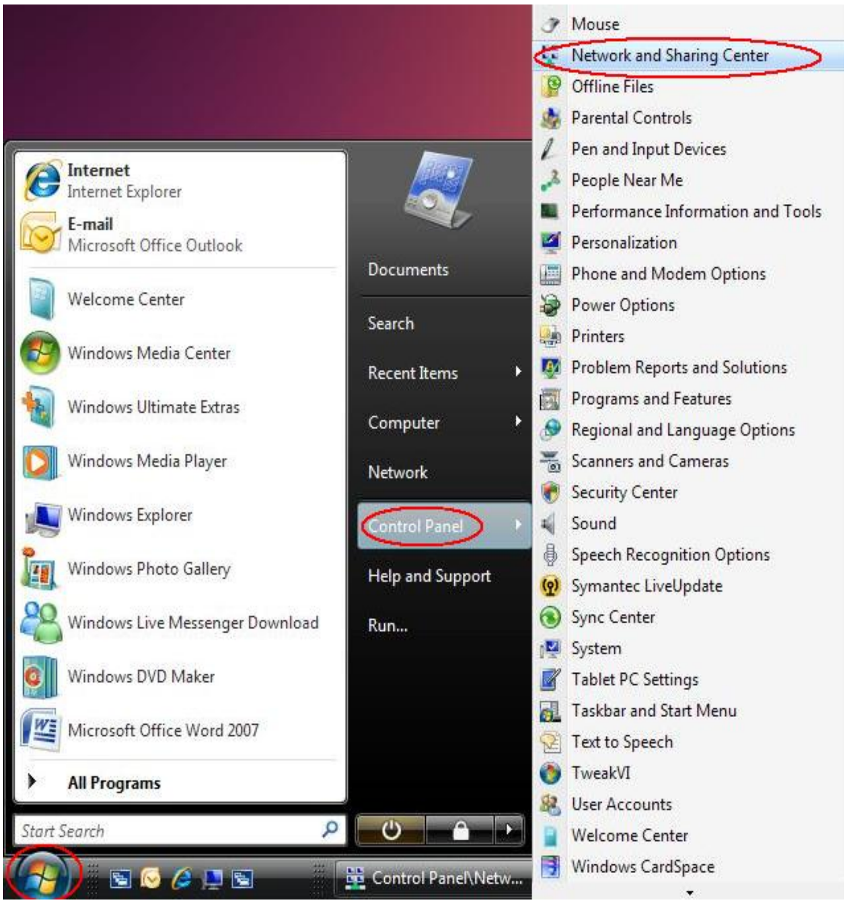
DNS Server Search Order

Domain Suffix Search Order

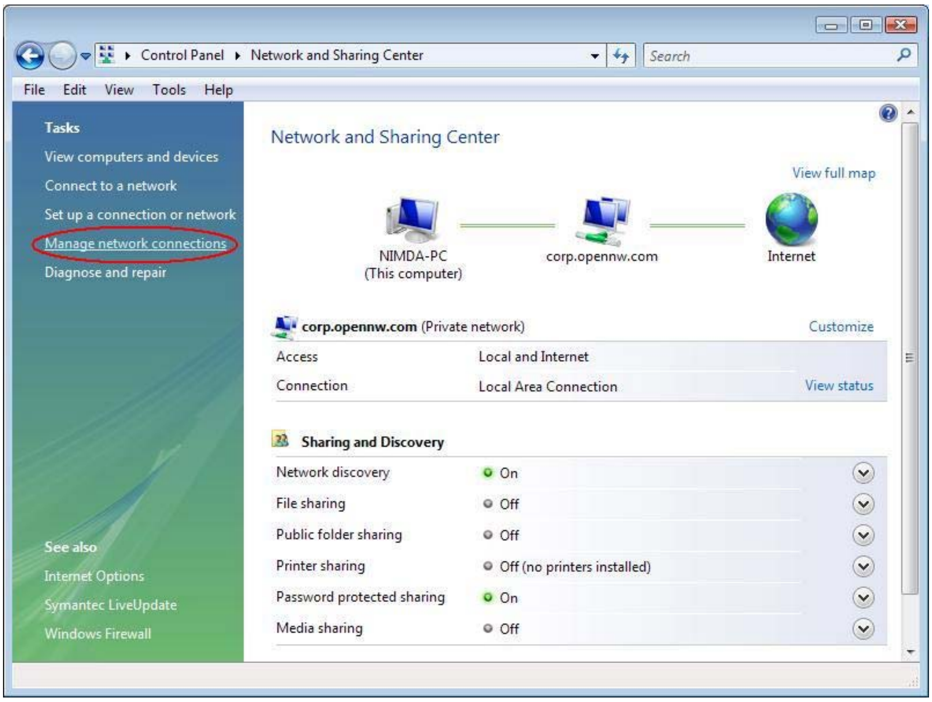
Step 5: Highlight the ***Disable DNS*** radio button, then click the ***OK*** button to complete the configuration.

4.4 Configuring Computers In Windows Vista

Step 1: Click ***Windows logo / Control Panel / Network and Sharing Center*** as shown:



Step 2: The following page appears. Click the ***Manage network connections*** link.



Network and Sharing Center

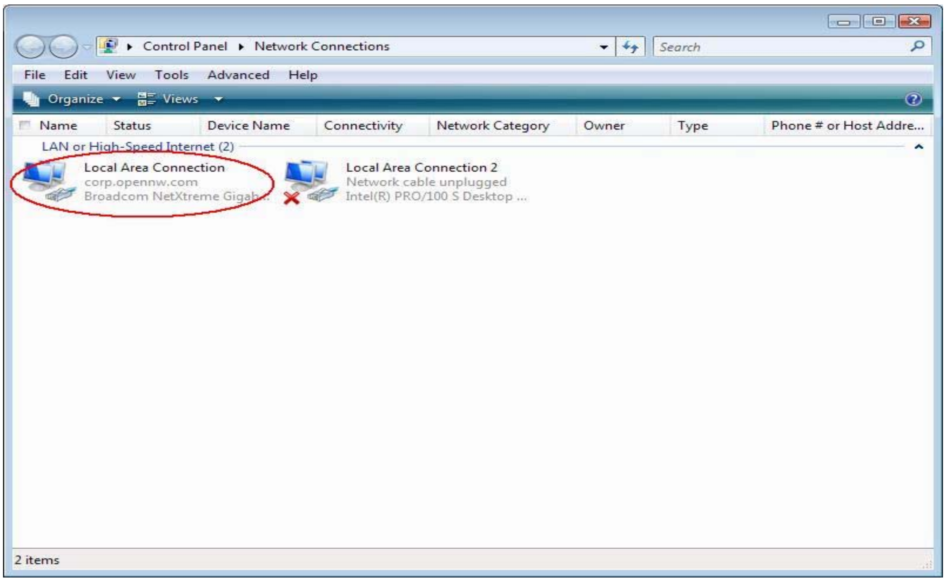
corp.opennw.com (Private network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	● On
File sharing	○ Off
Public folder sharing	○ Off
Printer sharing	○ Off (no printers installed)
Password protected sharing	● On
Media sharing	○ Off

Step 3: The ***Network Connections*** page appears. Double click on the active ***Local Area Connection*** icon.


Control Panel ▸ Network Connections
Search
File Edit View Tools Advanced Help
Organize ▾ Views ▾
Name Status Device Name Connectivity Network Category Owner Type Phone # or Host Addre...

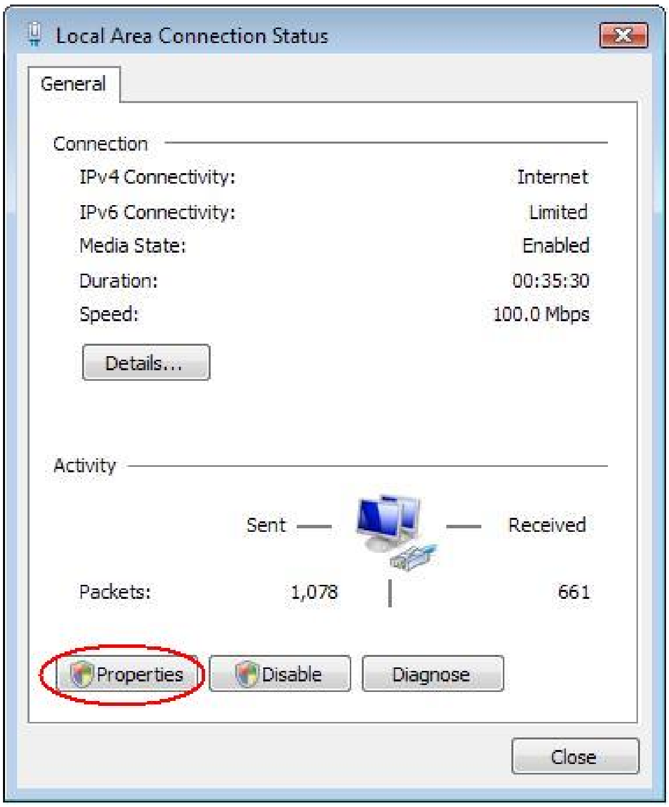
LAN or High-Speed Internet (2)

Local Area Connection
corp.opennw.com
Broadcom NetXtreme Gigab...

Local Area Connection 2
Network cable unplugged
Intel(R) PRO/100 S Desktop ...

2 items

Step 4: The ***Local Area Connection Status*** page appears. Click the ***Properties*** button.


Local Area Connection Status

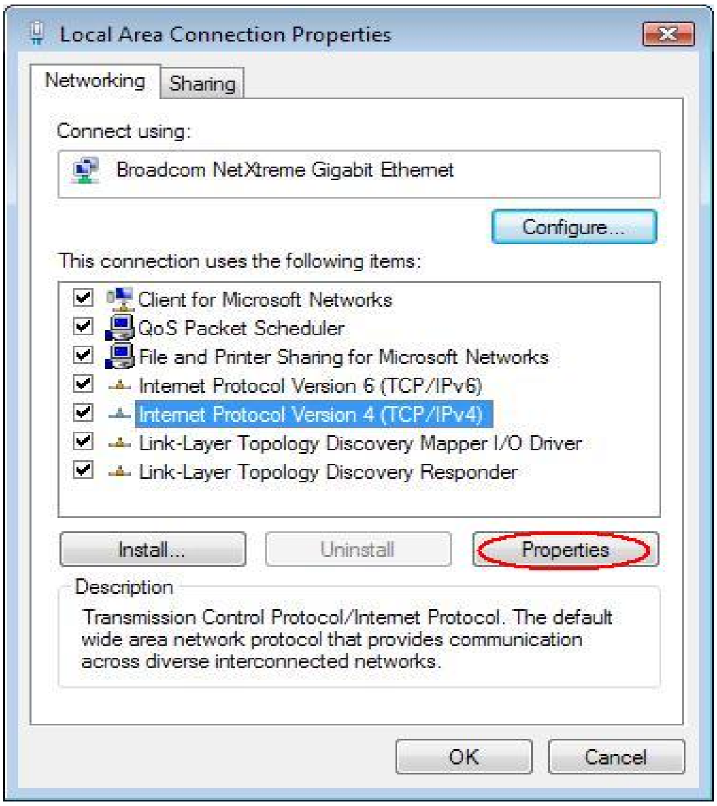
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	Limited
Media State:	Enabled
Duration:	00:35:30
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	1,078	661

Step 5: Under the ***Local Area Connection Properties*** page, highlight ***TCP/IPv4*** and click the ***Properties*** button.



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom NetXtreme Gigabit Ethernet

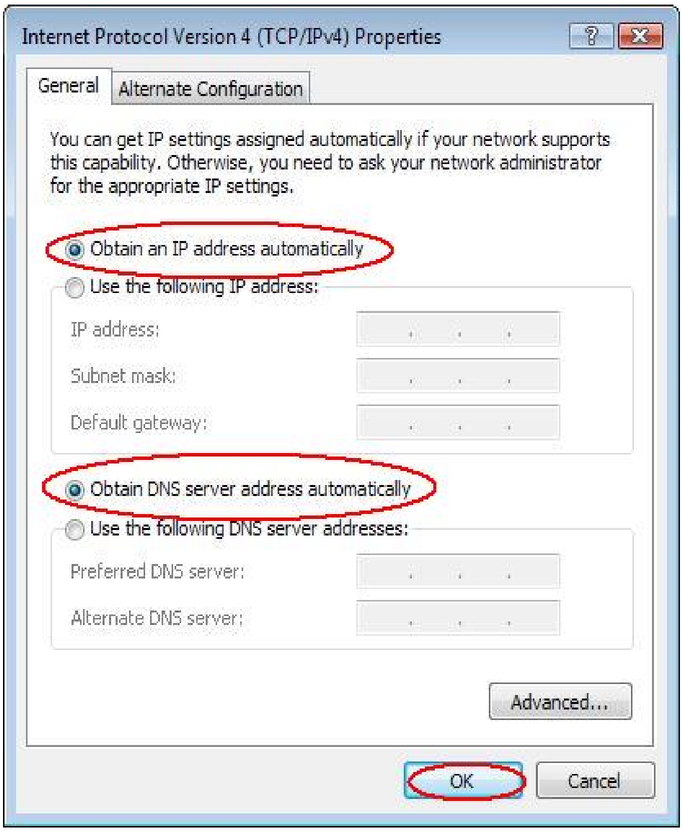
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 6: Highlight the ***Obtain an IP address automatically*** and the ***Obtain DNS server address automatically*** radio buttons and click the ***OK*** button to complete the configuration.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Understanding The Web Interface

5.1 Web Interface Components

The buttons, commands and menus make up the browser-based user interface. Please read the following carefully before you commence configuration of the iConnect625W router.

5.1.1 Buttons

Please take note of the definitions for the buttons as follows:

- ***Apply***
  - Click to implement configuration changes. Clicking the *Apply* button does not save the changes when the router is restarted.
- ***Cancel***
  - Click the *Cancel* button to revert to the last saved configuration.

5.1.2 Menus

At the configuration homepage, the navigation tabs at the top of the screen directs you to the desired configuration page.

There are seven menu items/tabs on the web interface. These include:

- *Home*
- *Setup*
- *Advanced*
- *Wireless*
- *Tools*
- *Status*
- *Help*

The functions for each menu tab are described in detail in the following sections.

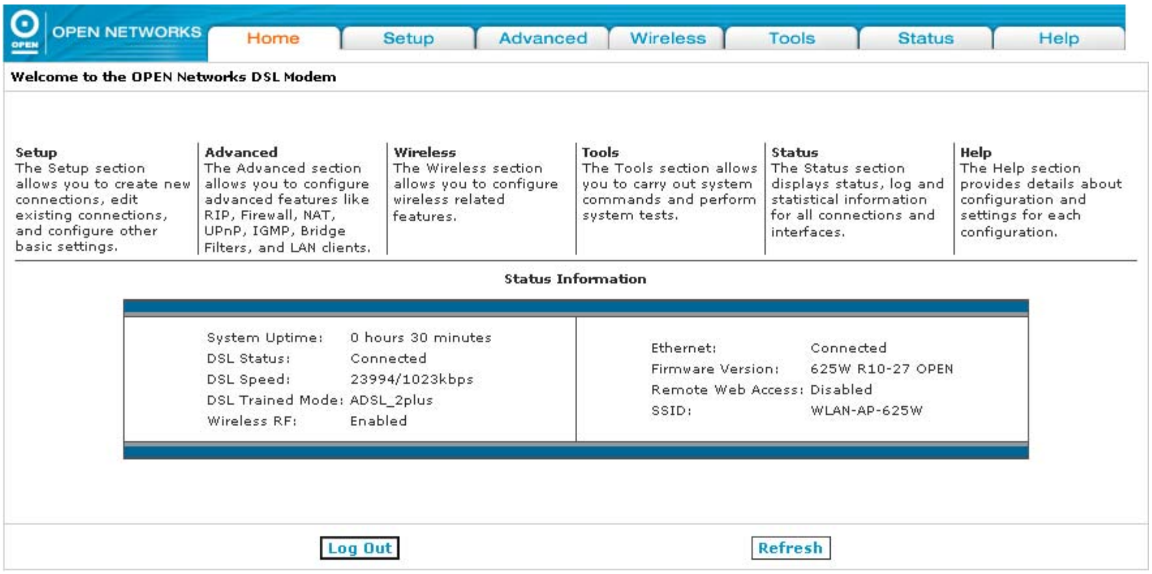
6. Home

The *Home* page allows access to all the menu tabs for iConnect625W configuration. Its basic layout consists of a page selection list of option tabs across the top of the browser window.

The centre part of the screen provides descriptions of the option tabs supported on the web interface pages.

The lower centre part of the page displays the iConnect625W status, connection information, firmware version and other useful information.

Step 1: To access the *Home* page, click the ***Home*** tab at the top of the screen**.** The following appears:



Welcome to the OPEN Networks DSL Modem

Setup
The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

Advanced
The Advanced section allows you to configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.

Wireless
The Wireless section allows you to configure wireless related features.

Tools
The Tools section allows you to carry out system commands and perform system tests.

Status
The Status section displays status, log and statistical information for all connections and interfaces.

Help
The Help section provides details about configuration and settings for each configuration.

Status Information

System Uptime:	0 hours 30 minutes
DSL Status:	Connected
DSL Speed:	23994/1023kbps
DSL Trained Mode:	ADSL_2plus
Wireless RF:	Enabled
Ethernet:	Connected
Firmware Version:	625W R10-27 OPEN
Remote Web Access:	Disabled
SSID:	WLAN-AP-625W

The following table provides a brief description of each of the tabs and their functions.

Tab	Function
Setup	Configuration of new and existing LAN and WAN settings.
Advanced	Configuration of advanced options within the iConnect625W such as SNTP, routing and filtering.
Wireless	Configuration of wireless features.
Tools	Access tools and diagnostics to assist in debugging.
Status	Status views of the modem network to all connections and interfaces.
Help	View the extensive online Help topics.
Buttons	**Function**
Log Out	Click on this button to log out of the router.
Refresh	Clicking on this button refreshes the details on the screen.

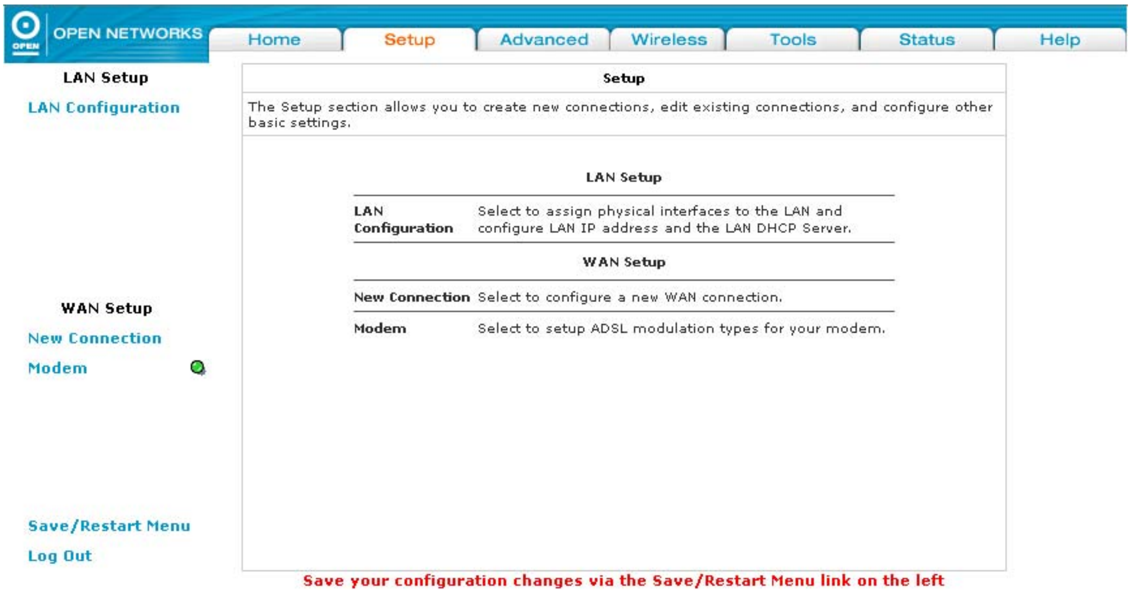
7. Setup

The ***Setup*** page consists of two subsections: *LAN Setup* and *WAN Setup*. Using the appropriate links provided on the left menu, you can configure these settings as required.

The *LAN Setup* consists of LAN configuration. This is where local hosts are connected. The iConnect625W router is configured to automatically provide all the hosts on the LAN network with IP addresses.

The *WAN Setup* consists of the setup of various connection types: PPPoA, PPPoE, Static, DHCP, Bridged connection, CLIP connection and modem setups. The WAN interface is also referred to as a broadband connection. It is different for every WAN service provider used.

Step 1: To access the setup page, click the ***Setup*** tab on the top navigation panel. The following page appears:



Setup

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

LAN Setup

LAN Configuration	Select to assign physical interfaces to the LAN and configure LAN IP address and the LAN DHCP Server.

WAN Setup

New Connection	Select to configure a new WAN connection.
Modem	Select to setup ADSL modulation types for your modem.

Save your configuration changes via the Save/Restart Menu link on the left

Refer to the following sections on how to configure LAN and WAN Setups.

7.1 LAN Setup

By default, your iConnect625W has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of them. If you connect a second DHCP server into the network, you will experience network errors and the network will not function normally.

7.1.1 LAN Configuration

The LAN Group Configuration allows you to configure settings for each defined LAN group. You can view the status of advanced services that can be applied to this LAN group. A green status indicates that the services have been enabled, while a red status indicates that the service is currently disabled.

The iConnect625W provides *LAN Configuration* for multiple LAN groups. Up to five LAN Groups are supported:

- LAN Group 1
- LAN Group 2
- LAN Group 3
- LAN Group 4
- LAN Group 5

The LAN interfaces include the following:

- Ethernet1;
- WLAN (Primary SSID);
- SSID1;
- SSID2;
- SSID3

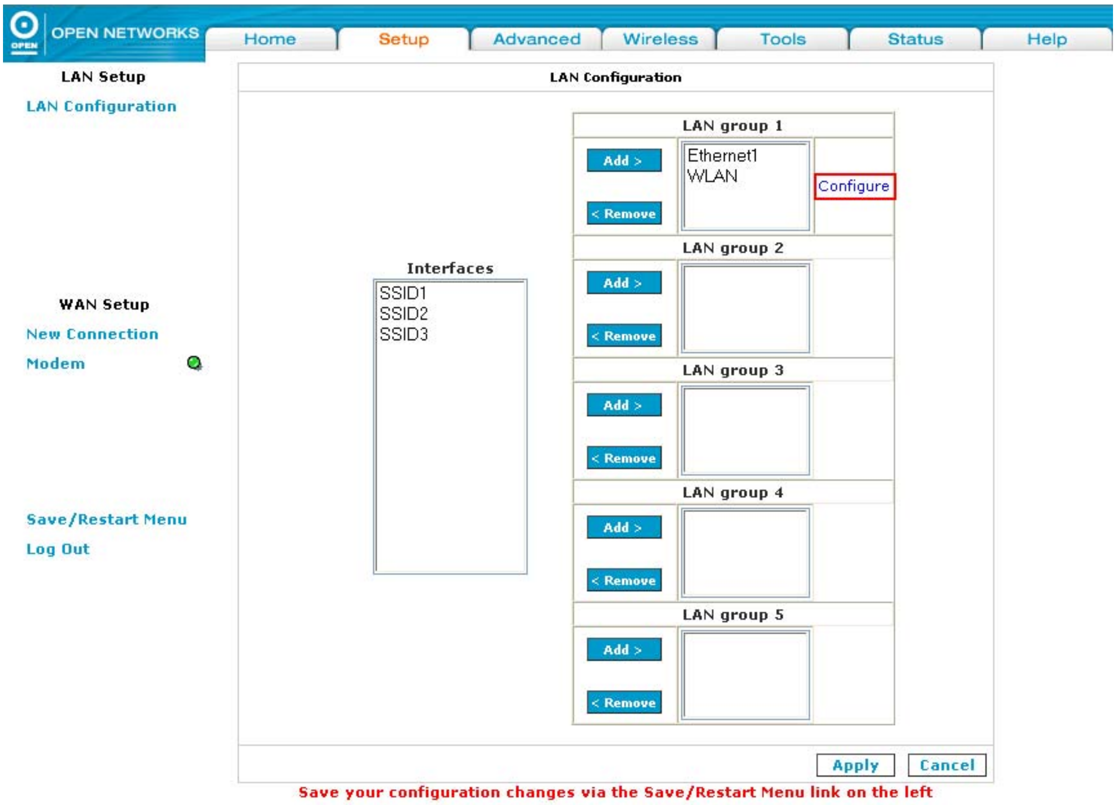
It is possible to assign any LAN interface to any bridge group but the Ethernet interface needs to be in *LAN Group 1.*

NOTE	**The following interfaces are not valid until multiple SSID is enabled and the secondary SSIDs are configured:** ❑ **SSID1 (corresponds to the first secondary SSID)** ❑ **SSID2 (corresponds to the second secondary SSID)** ❑ **SSID3 (corresponds to the third secondary SSID)**

To setup *LAN Configuration*, follow the steps below.

Step 1: From the top menu, click the ***Setup*** tab.

Step 2: Click the ***LAN Configuration*** link on the left menu. The following appears:



LAN Configuration

Interfaces: SSID1, SSID2, SSID3

LAN group 1: Ethernet1, WLAN

LAN group 2

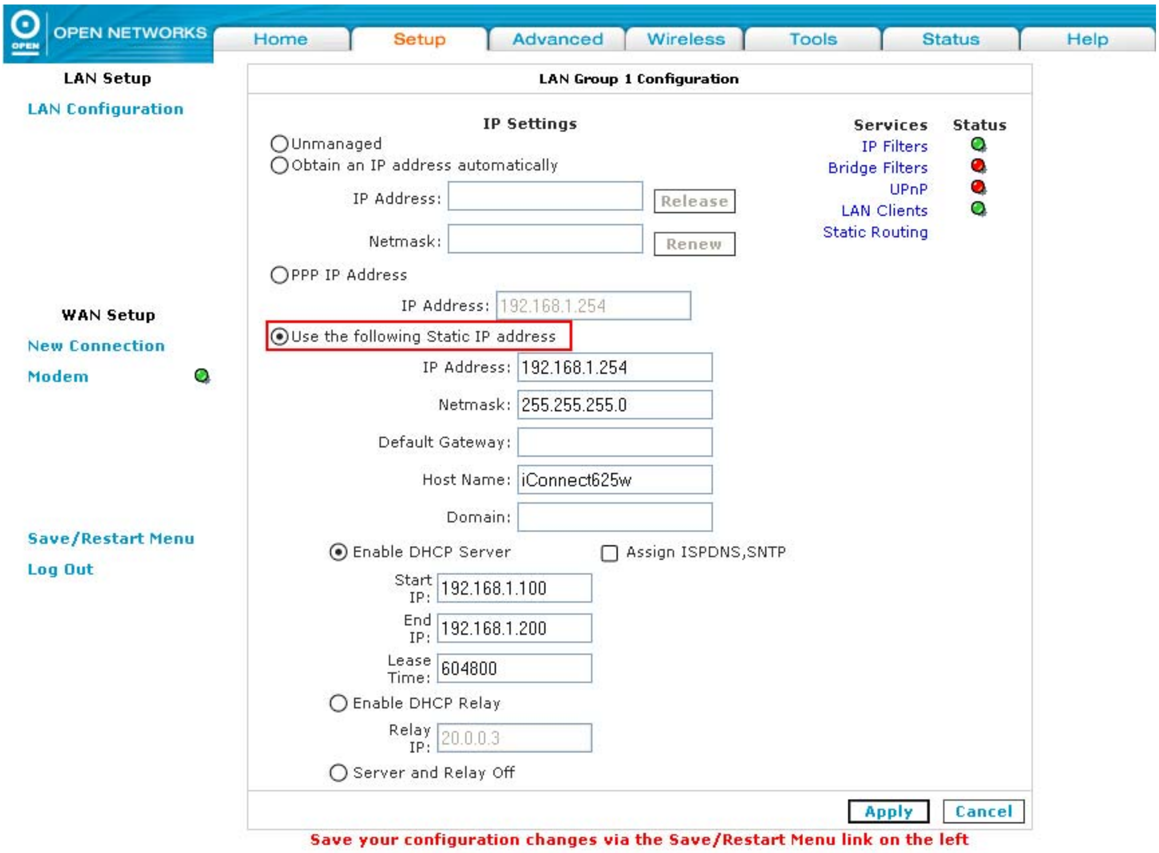
LAN group 3

LAN group 4

LAN group 5

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The *Ethernet* interface is defaulted to *LAN Group 1* and should always remain in this group. Click the ***Configure*** link within the *LAN Group 1* box. The *LAN Group 1 Configuration* page appears:



LAN Group 1 Configuration

IP Settings

○ Unmanaged

○ Obtain an IP address automatically

IP Address:

Netmask:

○ PPP IP Address

IP Address: 192.168.1.254

● Use the following Static IP address

IP Address: 192.168.1.254

Netmask: 255.255.255.0

Default Gateway:

Host Name: iConnect625w

Domain:

● Enable DHCP Server □ Assign ISPDNS,SNTP

Start IP: 192.168.1.100

End IP: 192.168.1.200

Lease Time: 604800

○ Enable DHCP Relay

Relay IP: 20.0.0.3

○ Server and Relay Off

Services	Status
IP Filters	🟩
Bridge Filters	🟥
UPnP	🟥
LAN Clients	🟩
Static Routing	

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: The ***Use the following Static IP address*** radio button is highlighted by default. The default ***IP Address*** field is set to: *192.168.1.254.* Change this field to a different IP Address, if required.

Step 4: The default ***Netmask*** field is set to: *255.255.255.0*.

Step 5: The ***Enable DHCP Server*** radio button is highlighted by default. Enter a different ***Start IP*** in the field if the default value: *192.168.1.100* does not apply. This address is the beginning of the range from which the DHCP Server starts issuing IP addresses.

Step 6: Enter the ***End IP*** field if the default value: *192.1.168.200* does not apply. This address is the end of the range from which the DHCP Server issues IP addresses.

Step 7: The ***Lease Time*** field is defaulted to 604800 seconds (or 7 days).

Step 8: Click the ***Apply*** button.

Step 9: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

The following table lists the *LAN Group Configuration* fields and their definitions.

Field	Definition	
Unmanaged	*Unmanaged* is a state when the LAN group is not configured and no IP address has been assigned to the bridge.	
Obtain an IP Address Automatically	Highlight the radio button to select this option if the iConnect625W router is acting as a DHCP client. When this option is enabled, your iConnect625W router will request an IP address from the DHCP server on the LAN side.	
	IP Address	You can retrieve or renew an IP address from the DHCP server using the *Release* and *Renew* buttons.
	Netmask	This is the subnet mask of your iConnect625W router.
PPP IP Address	Check this checkbox if PPP is providing addressing. The IP address should be different from, but in the same netmask as the WAN-side IP address.	
Use the Following Static IP Address	This is the default setting. It enables you to change the IP address of the iConnect625W router.	
	IP Address	Enter a static IP address. The default IP address for the iConnect625W router is *192.168.1.254.*
	Netmask	Enter the static subnet mask. The default Netmask for the iConnect625W router is 255.255.255.0. This subnet allows the router to support 254 users. If you want to support a larger number of users, you can change the subnet mask.
	Default Gateway	The default gateway is the routing device used to forward all traffic that is addressed to a station within the local subnet. Enter the default gateway as specified by your ISP. Otherwise leave this field blank and it will be automatically populated when an ISP connection is made.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify your iConnect625W router. The hostname can be any alphanumeric character that does not contain spaces.
	Domain	The domain name is used in conjunction with the host name to uniquely identify the iConnect625W.
Enable DHCP Server	Highlighting this option turns on the DHCP server. This needs to be disabled if a DHCP server is already running on the LAN. The DHCP server (LAN side) is defaulted to *Enabled*.	

Field	Definition	
	Assign ISPDNS, SNTP	Enables/disables the *Assign ISPDNS, SNTP* feature. The default is set to disabled.
	Start IP	This address is the beginning of the range from which the DHCP server starts issuing IP addresses. You need to ensure the iConnect625W *Management IP Address* and any statistically defined addresses are not within the DHCP start and end address ranges. The default *Start IP* address is *192.168.1.100.*
	End IP	This is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 253. This means that the maximum value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the *End IP* addresses (to the limit of 254) or reduce the lease time.
	Lease Time	The *Lease Time* is the amount of time that a network user is allowed to maintain a network connection to the router using the dynamic IP address. The client will automatically renew the address after this time has elapsed or a new IP address is issued. If the LAN computer does not renew the address after the lease period, the lease information will be removed from the DHCP database. This database can be viewed under *Tools>DHCP Clients*. The lease time is in units of seconds. The default value is set to *604800* seconds (or 7 days).
Enable DHCP Relay	Highlighting this option configures the iConnect625W to forward the DHCP request to a remote DHCP server. Enter the remote DHCP server address in the *Relay IP* field.	
	Relay IP	The IP address of the DHCP relay server.
Server and Relay Off	This will disable the iConnect625W's DHCP server and relay functionality.	

7.2 Setting Up a WAN Connection

A new WAN connection is a virtual connection over the physical DSL connection. Your iConnect625W can support up to 8 different (unique) virtual connections. If you have multiple different virtual connections, you may need to use the static and dynamic routing capabilities of your iConnect625W to pass data correctly.

Before the router can pass any data between the LAN and WAN interfaces, the *WAN Setup* must be configured and you must ensure that you have a DSL connection.

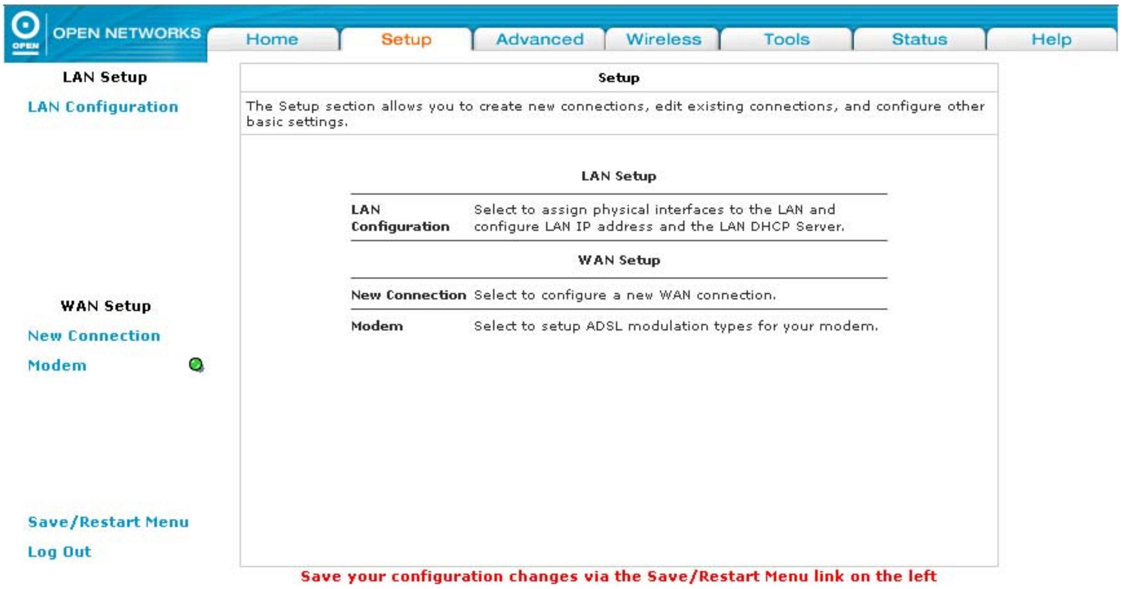
Depending on your ISP, you will need some or all of the information outlined below before you can properly configure the *WAN Setup*.

The iConnect625W supports the following connection types:

- PPPoE
- PPPoA
- Bridged
- Static
- DHCP
- CLIP

Follow the steps to access the Setup page.

Step 1: To access the *WAN Setup*, click the **Setup tab**. The following page appears:



Setup

The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.

LAN Setup

LAN Configuration	Select to assign physical interfaces to the LAN and configure LAN IP address and the LAN DHCP Server.

WAN Setup

New Connection	Select to configure a new WAN connection.
Modem	Select to setup ADSL modulation types for your modem.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Click on **New Connection** or **Modem** to setup your WAN configuration.

The following sections will provide steps on how to configure each connection type.

7.2.1 PPPoE Connection Setup

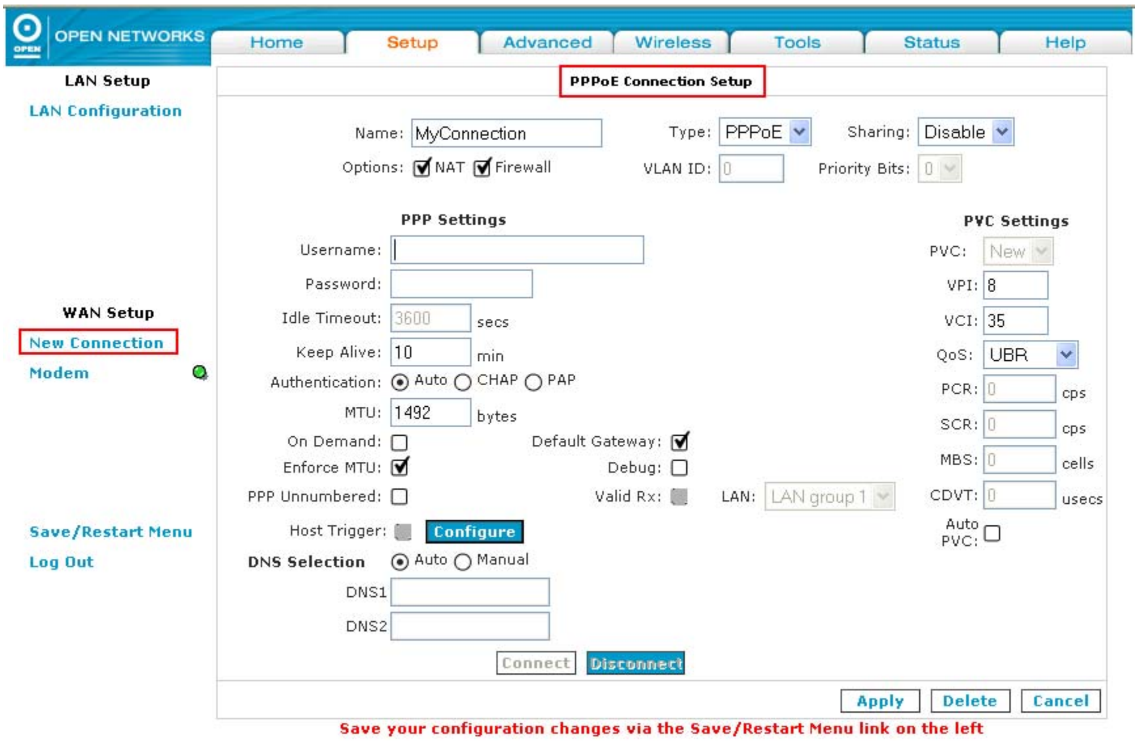
PPP, or Point-to-Point Protocol, is a method of establishing a network connection/session between network hosts. It provides secure login, and traffic metering among other advanced features.

PPPoE (PPP over Ethernet) is a protocol for encapsulating PPP frames in Ethernet frames. It provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator.

It was designed to bring the security and metering benefits of PPP to Ethernet connections such as DSL. PPPoE allows ADSL users to be authenticated by the ISP's systems. Most broadband connections are Ethernet, hence PPP over Ethernet. It also allows for ISPs to provide multiple services over multiple PPP sessions, i.e., rated services, broadband specific content (movies, etc.), metered services, etc.

To configure *PPPoE* connection, follow the steps provided below.

Step 1: To begin, click the **Setup tab** on the top menu. Click the **New Connection** link. The default *PPPoE Connection Setup* page appears:



PPPoE Connection Setup

Name: MyConnection Type: PPPoE Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Username:

Password:

Idle Timeout: 3600 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Enforce MTU: ☑ Debug: □

PPP Unnumbered: □ Valid Rx: □ LAN: LAN group 1

Host Trigger: □ Configure

DNS Selection ● Auto ○ Manual

DNS1

DNS2

PVC Settings

PVC: New

VPI: 8

VCI: 35

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: ***MyConnection*** is the default name displayed in the ***Name*** field. Enter a unique name for your *PPPoE* connection. The name must not have spaces and cannot begin with numbers.

Step 3: From the ***Type*** drop-down list, ***PPPoE*** is the default setting.

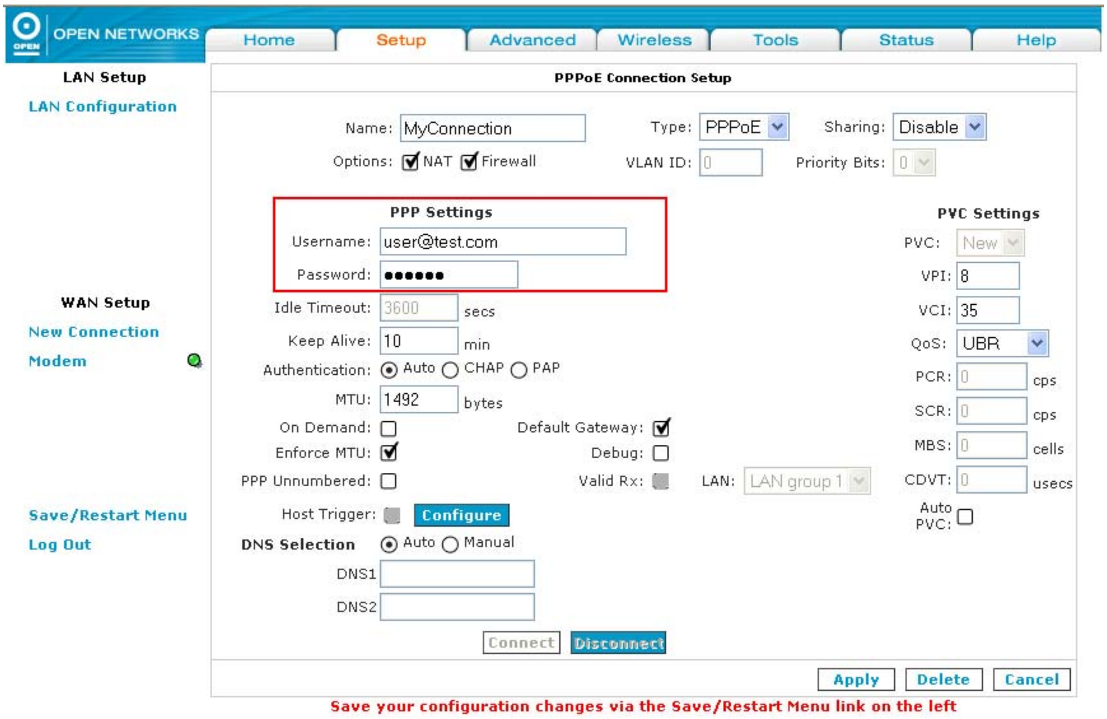
Step 4: The ***NAT*** and ***Firewall*** checkboxes are enabled by default under the ***Options*** field. Leave these in the default mode.

NOTE	NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you cannot access the Internet.

Step 5: If you want to enable VLAN, refer to the table at the end of this section as a reference to configure the following fields:

- ***Sharing***: Select ***VLAN*** to enable the ***VLAN ID*** and ***Priority Bits*** fields.
- ***VLAN ID***: Enter the ***VLAN ID.***
- ***Priority Bits***: Select the ***Priority Bits*** of the VLAN.

Step 6: Enter your ***Username*** and ***Password*** in the respective fields under the *PPP Settings* section as shown, as provided by your ISP.



PPPoE Connection Setup

Name: MyConnection
Type: PPPoE
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings
Username: user@test.com
Password: ●●●●●●
Idle Timeout: 3600 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □
PPP Unnumbered: □
Valid Rx: □
LAN: LAN group 1
Host Trigger: □ Configure
DNS Selection ● Auto ○ Manual
DNS1
DNS2

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

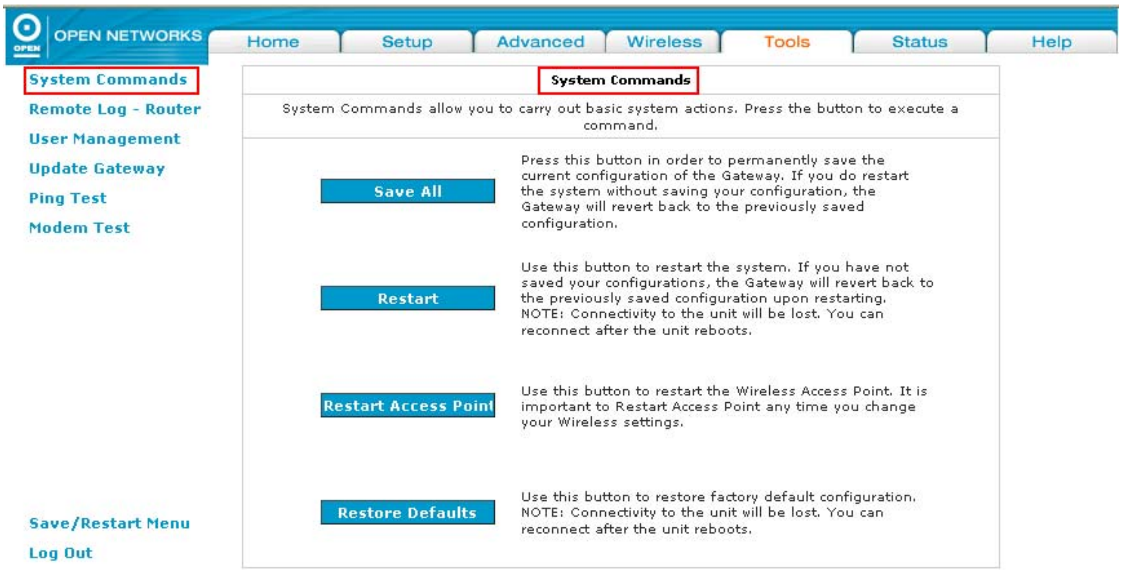
Save your configuration changes via the Save/Restart Menu link on the left

Step 7: In the *PVC Settings* section, enter the values for the ***VPI*** and ***VCI*** if they differ from the default values: *8* and *35* respectively, as provided by your ISP.

NOTE	If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.

Step 8: Select the ***Quality of Service (QOS)***. Leave the default value as is if you are unsure or if the ISP did not provide this information.

Step 9: Click the ***Apply*** button and the ***Save / Restart Menu*** link on the left menu. The following screen appears:



System Commands

System Commands allow you to carry out basic system actions. Press the button to execute a command.

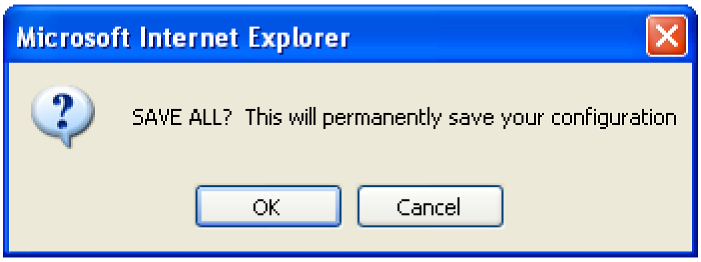
Save All — Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.

Restart — Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Restart Access Point — Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.

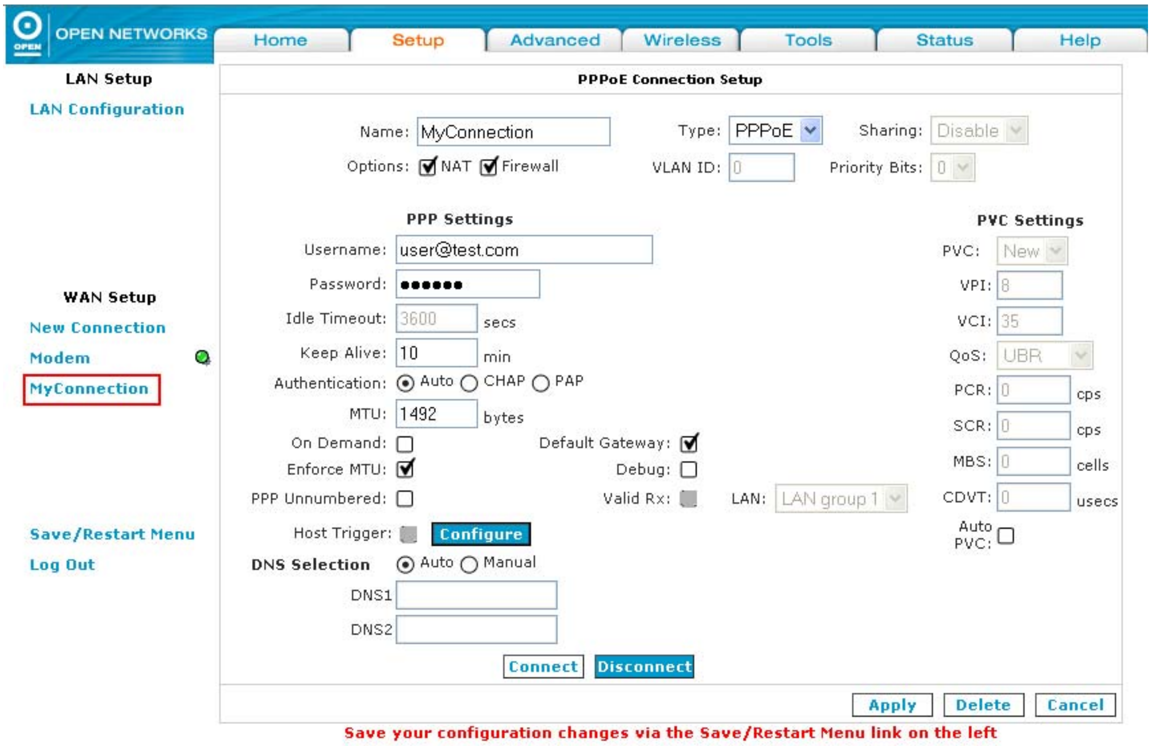
Restore Defaults — Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Step 10: Click the ***Save All*** button. The following screen appears. Click the ***OK*** button to save the settings.



SAVE ALL? This will permanently save your configuration

Step 11: ***MyConnection*** has been created for this connection in the left-hand menu. You can connect, disconnect, apply, delete or cancel this connection using the buttons at the bottom of the *MyConnection* page.



PPPoE Connection Setup

Name: MyConnection Type: PPPoE Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Username: user@test.com

Password: ●●●●●●

Idle Timeout: 3600 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Enforce MTU: ☑ Debug: □

PPP Unnumbered: □ Valid Rx: □ LAN: LAN group 1

Host Trigger: □

DNS Selection ● Auto ○ Manual

DNS1

DNS2

PVC Settings

PVC: New

VPI: 8

VCI: 35

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

The following table lists the *PPPoE Connection Setup* page fields and describes each of the options:

Field	Description	
NAT	*Network Address Translation* is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.	
Firewall	This is set to *Enabled* by default for standard operation.	
VLAN Settings	***Sharing***	The following options are available: • ***Disable:*** Disables connection sharing; • ***Enable:*** Enables connection sharing; • ***VLAN:*** The ***VLAN ID*** and ***Priority Bits*** fields are activated when *VLAN* is selected, which enables you to create VLAN.
	VLAN ID	Multiple connections over the same PVC are supported, which requires the WAN network to have VLAN support and for the DSLAMS and routers on the ISP to handle VLAN Tags. Extended support is also available, which allows multiple connections to be placed over the single PVC without VLAN support (VLAN Tag of *0* in this special case). In this mode of operation, a received packet is flooded on all the connections that reside over it.
	Priority Bits	Priority is given to a VLAN connection from *0-7.* All packets sent over the VLAN connection have the priority bits set to the configured level.
PPP Settings	Each of the fields for *PPP Settings* is described as follows.	
	Username	Your user name for the PPPoE access provided by your ISP. This field is alphanumeric and the maximum limit is 64 characters. It cannot start with a number.
	Password	Your password for the PPPoE access provided by your ISP. This field is alphanumeric and the maximum number of characters allowed is 128 characters. It cannot start with a number.

Field	Description		
	Idle Timeout	Specifies that the PPPoE connection should disconnect if the link has no activity detected for *n* seconds. This field is in conjunction with the *On-Demand* feature and is enabled only when the ***On Demand*** checkbox is checked. To ensure that the link is always active, enter a *0* in this field. You can also enter a value larger than *10* (secs).	
	Keep Alive	When the *On Demand* option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a *0* in this field. You can also enter any positive integer values into this field.	
	Authentication	This defines the authentication protocol for your ISP. This is set to *Auto* by default.	
		Auto	The authentication is automatic.
		CHAP	Stands for *Challenge Handshake Authentication Protocol.*
		PAP	Stands for *Password Authentication Protocol.*
	MTU	This is the *Maximum Transmission Unit* that the DSL connection can transmit. It is a negotiated value that packets no more than *n* bytes can be sent to the service provider. The PPPoE interface default is *1492 (max)* and PPPoA is *1500 (max).* The minimum MTU value is *64*.	
	On-Demand	If selected, this enables on-demand connectivity to the Internet. Your Internet connection is activated when traffic is generated from LAN clients. The connection disconnects if no activity is detected after the specified timeout value. When checked, this field enables the following fields: • Idle Timeout; • Host Trigger; • Valid Rx.	
	Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.	

Field	Description	
	Enforce MTU	This feature is enabled by default. It forces all TCP traffic to conform with the PPP MTU by changing the TCP maximum segment size to the PPP MTU. If it is disabled, you may have issues accessing some Internet sites.
	Debug	Check this checkbox to enable PPPoE connection debugging facilities.
	PPP Unnumbered	*PPP Unnumbered* is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is essentially like a bridged connection.
	Valid Rx	This field is used in conjunction with the On-Demand feature and is enabled only when the *On Demand* field is checked. When the *On-Demand* feature is enabled and *Valid Rx* is unchecked, only packets going from the LAN side to the WAN side keep the link active. After the iConnect625W times out, no packets can be received from the WAN side to the LAN side. If *Valid Rx* is checked, the incoming packets can keep the PPPoE WAN connection active. There is one condition: these incoming packets should belong to a connection initiated from a LAN-side device.

Field	Description	
	Host Trigger	This field is used in conjunction with the On-Demand feature and is enabled only when the *On Demand* field is checked. There are 3 types of packets: • ***LAN packets (Type 1):*** packets are generated by the iConnect625W from the LAN to the WAN. • ***Proxied packets (Type 2):*** packets are generated by the iConnect625W after receiving packets from the LAN side, such as DNS Proxy. • ***Locally generally packets (Type 3):*** packets are generated by the iConnect625W such as Voice, SNMP, etc. When the *On-Demand* feature is enabled and *Host Trigger* is unchecked, only the flow of *Type 1* packets keeps the link active, i.e. if the iConnect625W has not received *Type 1* packets for x amount of time (as specified in the *Timeout* field), the connection times out. If *Host Trigger* is checked, *Type 2* and *Type 3* packets can keep the link active as well. You can configure the packets using the *Trigger Traffic* page, which is accessed by clicking the *Configure* button next to *Host Trigger*. The following fields can be used to identify the traffic of *Type 2* and/or *Type 3* packets that will keep the link alive: • ***Source Port*** (the character * is used to denote any port); • ***Destination Port*** (the character * is used to denote any port); • ***Protocol*** (*TCP, UDP, ICMP*, or *Specify* the protocol number)
	LAN	The *LAN* field is associated with the *PPP Unnumbered* field and is enabled when the latter field is checked. You can specify the LAN group the packets need to go to when the *PPP Unnumbered* feature is activated.

Field	Description		
PVC Settings	The *Permanent Virtual Circuit* is a fixed virtual circuit between two users. It is the public data network equivalent to a leased line. No call setup or clearing of procedures are needed.		
	VPI	The VPI (Virtual Path Identifier) defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be based on the information provided by your ISP.	
	VCI	The VCI (Virtual Channel Identifier) defines the virtual channel settings for the ADSL connection between you and your ISP. The VCI value entered here must be based on the information provided by your ISP.	
	QoS	QoS is a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The 3 QoS options are: • *UBR, CBR and VBR*. The QoS selected must be based on the information provided by your ISP. This is set to *UBR* by default.	
		UBR	UBR is the bandwidth allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is often used when transmitting data that can tolerate delays.
		CBR	CBR is the bandwidth service that requires the user to determine a fixed bandwidth requirement at the time the connection is set up so that the data can be sent in a steady stream. CBR service is often used when transmitting fixed-rate uncompressed video.

Field	Description		
		VBR	VBR is the bandwidth service that allows users to specify a throughput capacity (i.e., a peak rate) and a sustained rate but data is not sent evenly. VBR is often used when transmitting compressed packetized voice and video data, such as video conferencing.
	PCR	The *Peak Cell Rate,* measured in cells/sec, is the cell rate that the source may never exceed.	
	SCR	*Sustained Cell Rate,* measured in cells/sec, is the average cell rate over the duration of the connection.	
	MBS	The *Maximum Burst Size* is a traffic parameter that specifies the maximum number of cells that can be transmitted at the *PCR.*	
	CDVT	The *Cell Delay Variation Tolerance* is the maximum amount of cell delay variation that can be accommodated. Cell delay variation measures the random inter-arrival times of cells within an ATM connection due to cell transfer delay caused by buffering, multiplexing and so on.	

Field	Description	
	Auto PVC	The overall operation of the auto-sensing PVC feature relies on end-to-end OAM pings to defined PVCs. There are two groups of PVCs: • Customer default PVCs - defined by the ISP and the backup PVCs. It must have 0/35 as the first default PVC. • Backup list of PVCs - it must be of the following VPI/VCI: *0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51* and *8/59.* These are defined in XLM and are configurable. The Auto-sensing PVC feature itself is also configurable in that the auto-search mechanism can be disabled. Upon DSL synchronization, end-to-end OAM pings will be conducted for every defined PVC. The result of the pings will be recorded in an array for later use to determine the usability of the particular PVC for connectivity. This list helps the PVC to manage the available PVC for use, and needs to be synchronised with connections made without auto-sensing PVC. Once the connection is established, the PVC is stored in flash as the default PVC. Therefore upon reboot, this PVC is automatically chosen as the PVC for that connection. The list of default PVCs and backup PVCs need to be global for the management of all connections, non auto-sensing PVC connection and auto-sensing connections. These lists allow end users to establish connectivity without keeping track of the PVC used.
Connect	Click *Connect* to authenticate to your ISP via PPPoE and connect to the Internet.	
Disconnect	Click *Disconnect* to break your Internet connection.	
Apply	Applies the changes made to the connection.	
Delete	Deletes the connection.	
Cancel	Cancels the changes made to the connection.	

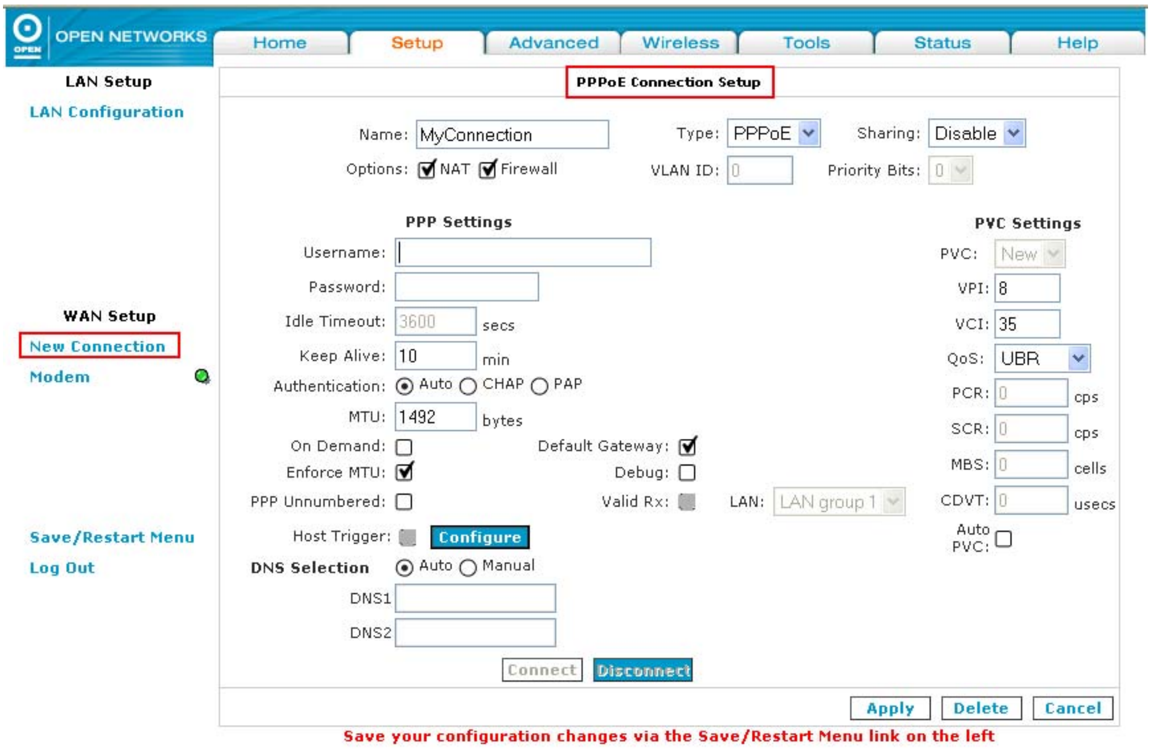
7.2.2 PPPoA Connection Setup

PPPoA (Point-to-Point Protocol over ATM) is a network protocol for encapsulating PPP packets in ATM cells that are carried over the DSL line. It is used mainly with ADSL services and is compliant with RFC 2364.

PPP is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. *Logical Link Control* (LLC) and *Virtual Circuit* (VC) are two different methods of encapsulating the PPP packet. Contact your ISP to determine which encapsulation is being used on your DSL connection.

To configure *PPPoA* connection, follow the steps below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***New Connection*** link. The default *PPPoE Connection Setup* page appears:



PPPoE Connection Setup

Name: MyConnection
Type: PPPoE
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

PPP Settings

Username:
Password:
Idle Timeout: 3600 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □
Default Gateway: ☑
Enforce MTU: ☑
Debug: □
PPP Unnumbered: □
Valid Rx: □
LAN: LAN group 1
Host Trigger: □
DNS Selection ● Auto ○ Manual
DNS1
DNS2

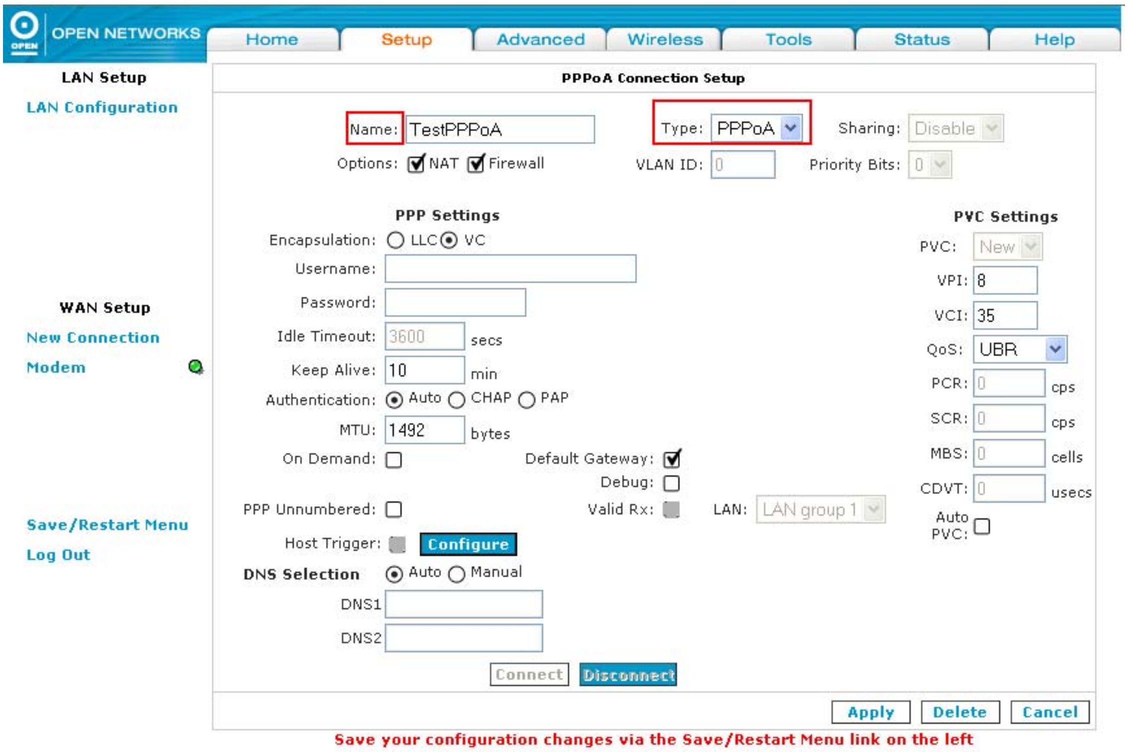
PVC Settings

PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Enter a unique name for your *PPPoA* connection in the ***Name*** field. The name must not have spaces and cannot begin with numbers.

Step 3: From the ***Type*** drop-down list, select ***PPPoA***. The default *PPPoA* page appears:



PPPoA Connection Setup

Name: TestPPPoA Type: PPPoA Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Encapsulation: ○ LLC ● VC

Username:

Password:

Idle Timeout: 3600 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Debug: □

PPP Unnumbered: □ Valid Rx: □ LAN: LAN group 1

Host Trigger: □

DNS Selection ● Auto ○ Manual

DNS1

DNS2

PVC Settings

PVC: New

VPI: 8

VCI: 35

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

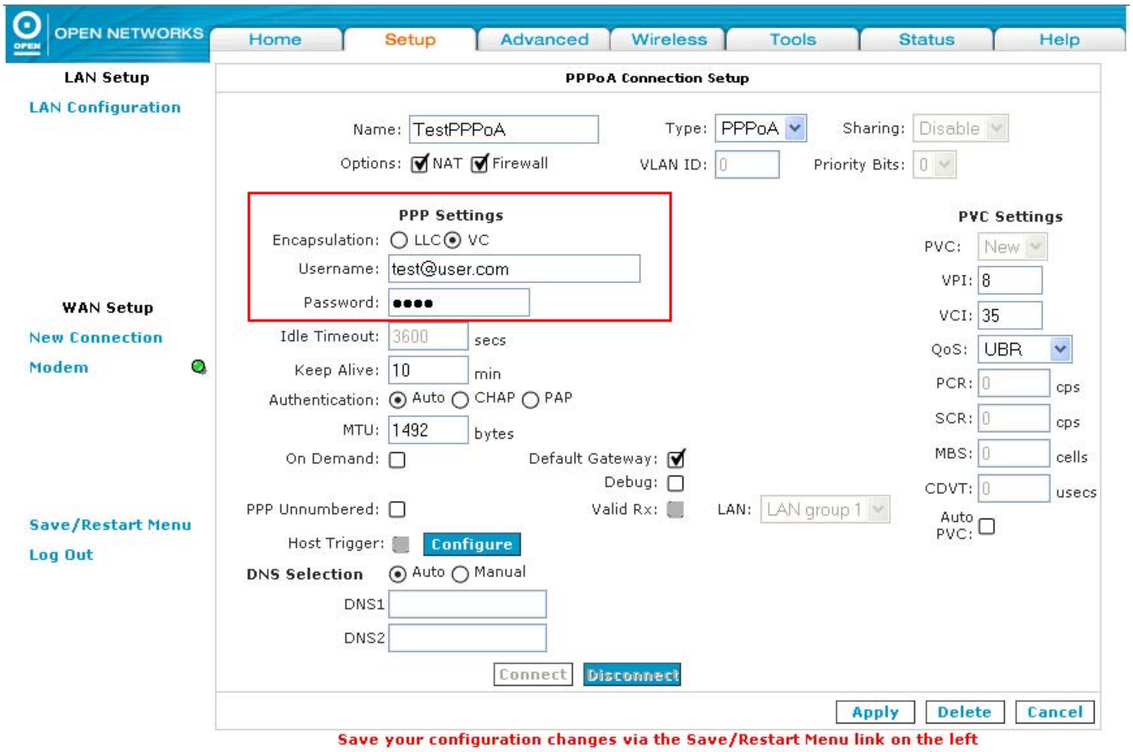
Step 4: The ***NAT*** and ***Firewall*** checkboxes are checked by default under the ***Options*** field. Leave these in the default mode.

Step 5: If you want to enable VLAN, refer to the table at the end of this section as a reference to configure the following fields:

- ***Sharing***: Select ***VLAN*** to enable the ***VLAN ID*** and ***Priority Bits*** fields.
- ***VLAN ID***: Enter the ***VLAN ID.***
- ***Priority Bits***: Select the ***Priority Bits*** of the VLAN.

Step 6: In the *PPP Settings* section, select the ***Encapsulation Type*** (LLC or VC) by highlighting the appropriate radio button. The default is set to *VC*. Your ISP should be providing the *Encapsulation Type*. If you are unsure, maintain the default mode.

Step 7: Enter your ***Username*** and ***Password*** in the respective fields as shown below, as provided by your ISP.



PPPoA Connection Setup

Name: TestPPPoA Type: PPPoA Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Encapsulation: ○ LLC ● VC

Username: test@user.com

Password: ●●●●

Idle Timeout: 3600 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Debug: □

PPP Unnumbered: □ Valid Rx: ▨ LAN: LAN group 1

Host Trigger: ▨

DNS Selection ● Auto ○ Manual

DNS1

DNS2

PVC Settings

PVC: New

VPI: 8

VCI: 35

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

CDVT: 0 usecs

Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 8: In the *PVC Settings* section, enter the ***VPI*** and ***VCI*** values, as provided by your ISP. These are defaulted to '8' and '35', respectively,

NOTE	**If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.**

Step 9: Select the ***QoS***. Leave the default value if you are unsure or if the ISP did not provide this information.

Step 10: Click the ***Apply*** button.

Step 11: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *PPPoA Connection Setup* screen fields and describes each of the options:

Field	Description	
NAT	*Network Address Translation* is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.	
Firewall	Select to enable security for this connection. This is set to *Enabled* by default for standard operation.	
PPP Settings	Each of the fields for *PPP Settings* is described as follows.	
	Encapsulation	Encapsulation is the technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. Two options are provided: *LLC* and *VC*.

Field	Description		
		LLC	With *LLC* encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM VC.
		VC	With *VC m*ultiplexing, .no link control header is needed as the ATM VC is assumed to be carrying a single protocol.
	Username	Your user name for the PPPoA access provided by your ISP. This field is alphanumeric and the maximum length is 64 characters. It cannot start with a number.	
	Password	Your password for the PPPoA access provided by your ISP. This field is alphanumeric and the maximum length is 128 characters. It cannot start with a number.	
	Idle Timeout	Specifies that the PPPoA connection should disconnect if the link has no activity detected for *n* seconds. This field is in conjunction with the *On-Demand* feature and is enabled only when the ***On Demand*** checkbox is checked. To ensure that the link is always active, enter a *0* in this field. You can also enter a value larger than *10* (secs).	
	Keep Alive	When the *On Demand* option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a *0* in this field. You can also enter any positive integer value in this field.	
	Authentication	This defines the authentication protocol for your ISP. This is set to *Auto* by default.	
		Auto	The authentication is automatic.
		CHAP	Stands for *Challenge Handshake Authentication Protocol.*
		PAP	Stands for *Password Authentication Protocol.*
	MTU	This is the *Maximum Transmission Unit* that the DSL connection can transmit. It is a negotiated value that packets no more than *n* bytes can be sent to the service provider. The PPPoE interface default is *1492 (max)* and PPPoA is *1500 (max).* The minimum MTU value is *64*.	
	On-Demand	If selected, this enables on-demand mode. The connection disconnects if no activity is detected after the specified timeout value.	
	Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.	

Field	Description	
	Debug	Check this checkbox to enable PPP connection debugging facilities.
	PPP Unnumbered	*PPP Unnumbered* is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is essentially like a bridged connection.
	LAN	The *LAN* field is associated with the *PPP Unnumbered* field. The packets need to go through a specific LAN group when the *PPP Unnumbered* feature is activated.
PVC Settings	The *PVC Settings* are not mandatory except for the *VPI* and *VCI* fields.	
	VPI	The VPI defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be based on the information provided by your ISP.
	VCI	The VCI (Virtual Channel Identifier) defines the virtual channel settings for the ADSL connection between you and your ISP. The VCI value entered here must be based on the information provided by your ISP.
	QoS	This field defines QoS at the ATM layer. Three different Quality Of Service options are available in the iConnect625W: *UBR, CBR and VBR* (refer to the previous section under the PPPoE table for the definitions). The QoS selected here must be based on the information provided by your ISP. This is set to *UBR* by default.
Connect	Click *Connect* to authenticate to your ISP via PPPoA and connect to the Internet.	
Disconnect	Click *Disconnect* to break your Internet connection.	
Apply	Applies the changes made to the connection.	
Delete	Deletes the connection.	
Cancel	Cancels the changes made to the connection.	

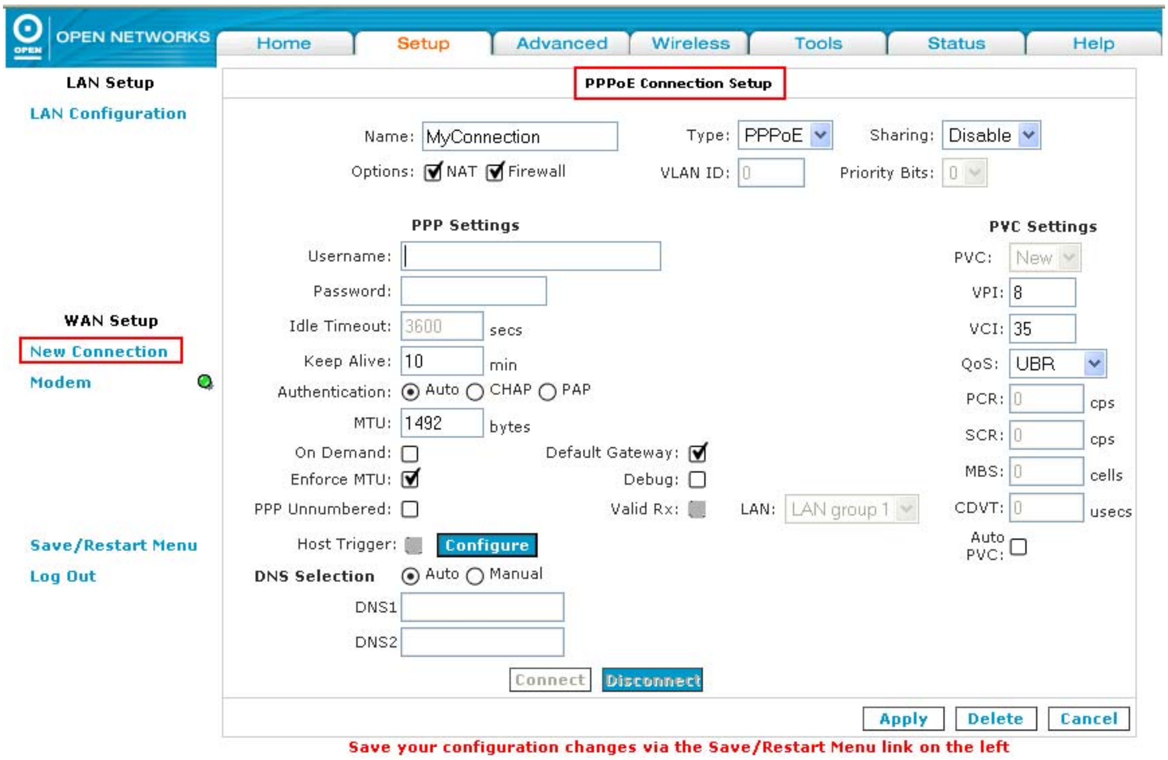
NOTE	**For VLAN and PVC field descriptions, please refer to the table under PPPoE section.**

7.2.3 Static Connection Setup

A Static Connection type is used whenever an ISP provides a Static IP address. Your ISP should provide the information for the Subnet Mask and the Gateway. Up to three *Domain Name Server* (DNS) addresses can be identified. These servers would enable you to have access to other web servers using the host name.

To configure *Static* connection, follow the steps provided below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***New Connection*** link. The default *PPPoE Connection Setup* page appears:



PPPoE Connection Setup

Name: MyConnection Type: PPPoE Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Username:
Password:
Idle Timeout: 3600 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □ Default Gateway: ☑
Enforce MTU: ☑ Debug: □
PPP Unnumbered: □ Valid Rx: ▨ LAN: LAN group 1
Host Trigger: ▨ Configure
DNS Selection ● Auto ○ Manual
DNS1
DNS2
Connect Disconnect

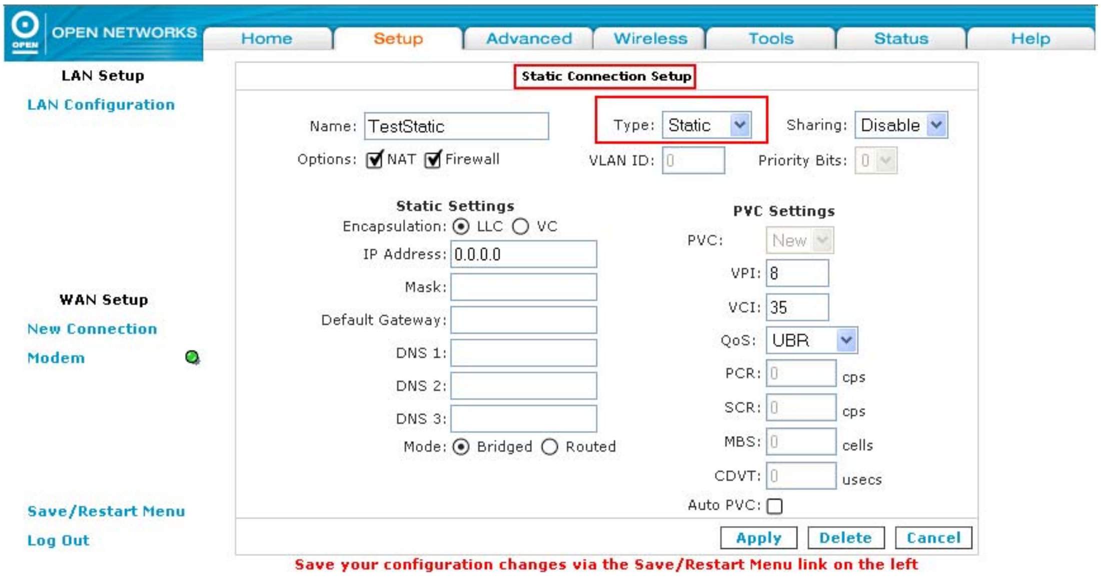
PVC Settings

PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Apply Delete Cancel

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Type*** drop-down list, select ***Static.*** The following page appears:



Static Connection Setup

Name: TestStatic Type: Static Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

Static Settings

Encapsulation: ● LLC ○ VC
IP Address: 0.0.0.0
Mask:
Default Gateway:
DNS 1:
DNS 2:
DNS 3:
Mode: ● Bridged ○ Routed

PVC Settings

PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Apply Delete Cancel

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter a unique name for your *Static* connection in the ***Name*** field. The name must not have spaces and cannot begin with numbers.

Step 4: The ***NAT*** and ***Firewall*** checkboxes are checked by default under the ***Options*** field. Leave these in the default mode.

Step 5: Select the ***Encapsulation Type*** (LLC or VC) by highlighting the appropriate radio button. The default is set to *LLC*. If you are unsure about the option, leave the default setting as it is.

Step 6: In the ***IP Addres***s field, enter your assigned IP address based on the information provided by your ISP.

Step 7: In the ***Mask*** field, enter the Subnet Mask based on the information provided by your ISP.

Step 8: In the ***Default Gateway*** field, enter the *Default Gateway* based on the information provided by your ISP.

Step 9: In the ***DNS1, DNS2*** and ***DNS3*** fields, enter the Domain Name Services values based on the information provided by your ISP.

Step 10: For the static configuration in the ***Mode*** option, the default mode is set to ***Bridged***. You can select the ***Routed*** connection, if this is applicable.

Step 11: In the *PVC Settings* section, the ***VPI*** and ***VCI*** are defaulted to *8* and *35*, respectively. Make the changes in these fields, as provided by your ISP, if required.

NOTE	***If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.***

Step 12: Select the ***QoS***. Leave the default value if you are unsure or if the ISP did not provide this information. The PCR, SCR, MBS and CDVT fields are enabled / disabled based depending on the selection for QoS. Your ISP should provide these values.

Step 13: Click the ***Apply*** button.

Step 14: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

The following table lists the *Static Connection Setup* screen fields and their definitions:

Field	Description		
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.		
Firewall	Select to enable security for this connection. This is set to *Enabled* by default for standard operation.		
Static Settings	Each of the fields for *Static Settings* is described as follows.		
	Encapsulation	*LLC* or *VC* and two different methods of encapsulating multiple sessions. The default is set to *LLC*.	
		LLC	With *LLC* encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit (VC).
		VC	With *VC m*ultiplexing, no link control header is needed as the ATM VC is assumed to be carrying a single protocol.
	IP Address	This is the static IP address that will be assigned to the WAN interface of the iConnect625W router. The information is based on the details provided by your ISP.	
	Mask	A *Mask* is used to determine which subnet an IP address belongs to. This is the *Subnet Mask* that will be assigned to the WAN interface of the iConnect625W router. The information is based on the details provided by your ISP.	
	Default Gateway	The *Default Gateway* is the host to which local computers send data that is destined for a non-local machine. On the iConnect625W router, configure the default gateway to reach all computers that are not in the same local IP subnet.	
	DNS 1 - DNS 3	DNS service is used to translate a *Domain Name* into a corresponding IP address. The DNS server name should be obtained from your ISP.	
	Mode	Select either the *Routed* or *Bridged* mode option.	
Apply	Applies the changes made to the connection.		
Delete	Deletes the connection.		
Cancel	Cancels the changes made to the connection.		

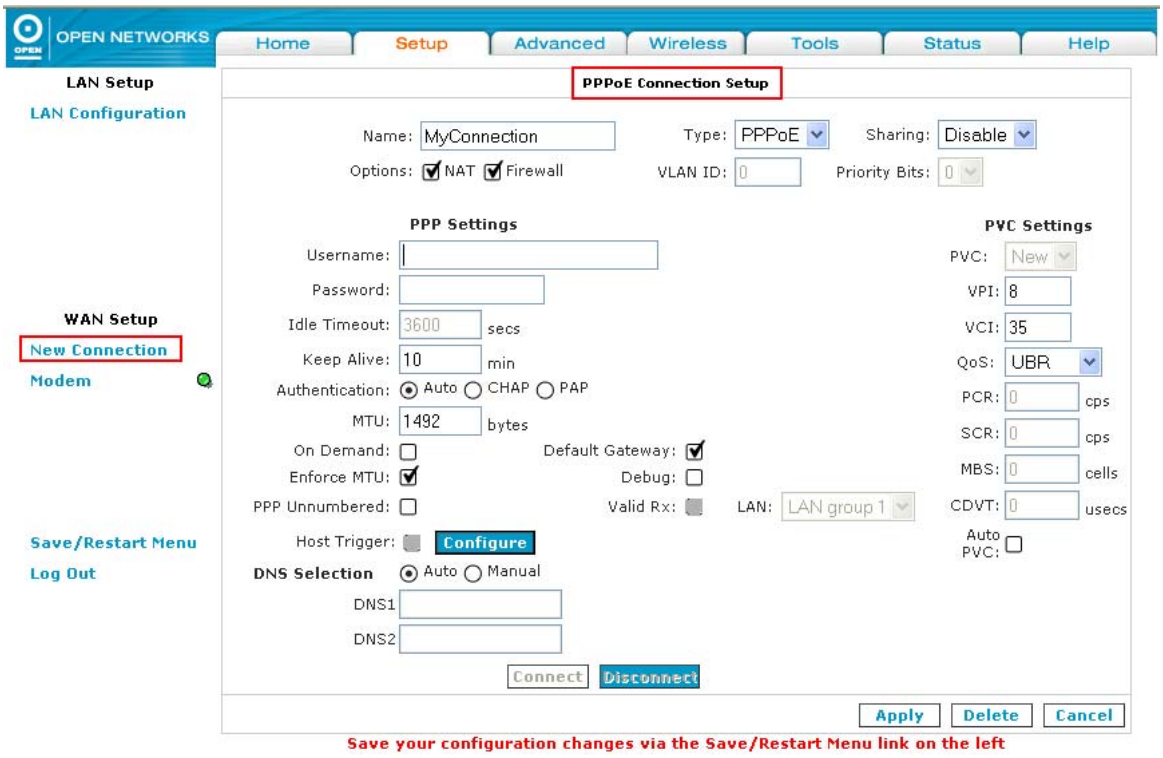
NOTE	**For VLAN and PVC field descriptions, please refer to the table under PPPoE section.**

7.2.4 DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the iConnect625W to obtain an IP address automatically from the server. With dynamic addressing, a device may have a different IP address every time it connects to the network. Before configuration begins, please check with your ISP to ensure that this mode is supported.

To configure *DHCP* connection, follow the steps provided below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***New Connection*** link. The default *PPPoE Connection Setup* page appears:



PPPoE Connection Setup

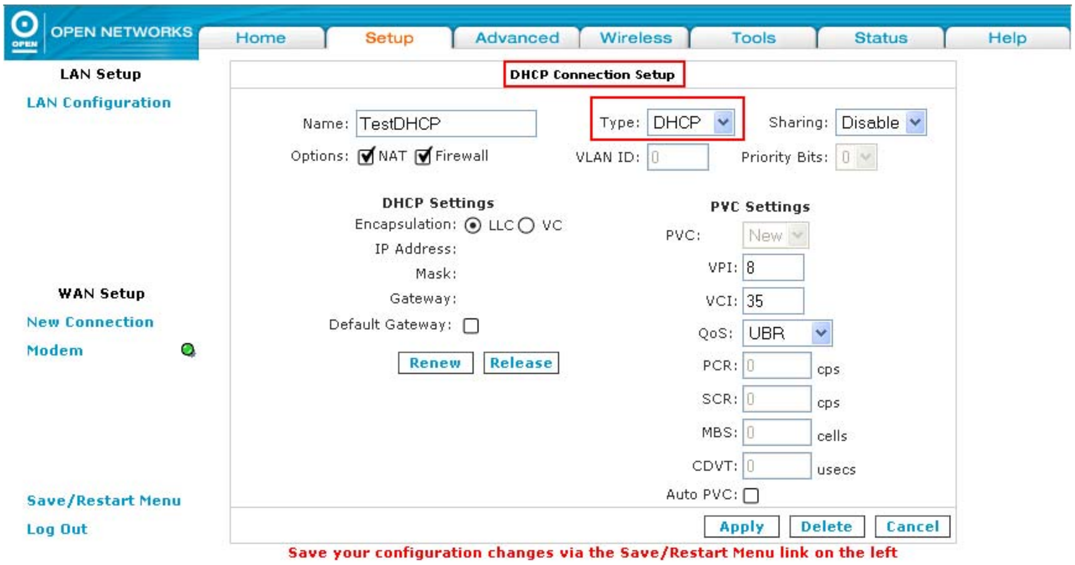
Name: MyConnection Type: PPPoE Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings
Username:
Password:
Idle Timeout: 3600 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □ Default Gateway: ☑
Enforce MTU: ☑ Debug: □
PPP Unnumbered: □ Valid Rx: ▨ LAN: LAN group 1
Host Trigger: ▨
DNS Selection ● Auto ○ Manual
DNS1
DNS2

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Type*** drop-down list, select ***DHCP.*** The following page appears:



DHCP Connection Setup

Name: TestDHCP Type: DHCP Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

DHCP Settings
Encapsulation: ● LLC ○ VC
IP Address:
Mask:
Gateway:
Default Gateway: □

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter a unique name for your *DHCP* connection in the ***Name*** field. The name must not have spaces and cannot begin with numbers.

Step 4: The ***NAT*** and ***Firewall*** checkboxes are checked by default under the ***Options*** field. Leave these in the default mode.

Step 5: Select the ***Encapsulation Type*** (LLC or VC) by highlighting the appropriate radio button. The default is set to *LLC*. If you are unsure about the option, leave the default setting as it is.

Step 6: If your DSL line is connected and your ISP supports DHCP, click the ***Renew*** button to retrieve an *IP address, Subnet Mask* and *Default Gateway* address. Alternatively, you can click the ***Release*** button at any time to release the DHCP address.

NOTE	**You can renew the DHCP address at any time by clicking the Renew button. This is not required in most cases as the process runs automatically.**

Step 7: From the *PVC Settings* section, the ***VPI*** and ***VCI*** are defaulted to *8* and *35*, respectively. Make the changes in these fields, if required, based on the information from your ISP.

NOTE	**If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.**

Step 8: Select the ***QoS***. Leave the default value if you are unsure or if the ISP did not provide this information.

The ***PCR, SCR, MBS*** and ***CDVT*** fields could be enabled/disabled depending on the ***QoS*** section. Your ISP should provide these values.

Step 9: Click the ***Apply*** button.

Step 10: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

The following table lists the *DHCP Connection Setup* screen fields and their definitions:

Field	Description		
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.		
Firewall	Select to enable security for this connection. This is set to *Enabled* by default for standard operation.		
DHCP Settings	Each of the fields for *DHCP Settings* is described as follows.		
	Encapsulation	*LLC* and *VC* are two different methods of encapsulating multiple sessions. The default is set to *LLC*.	
		LLC	With *LLC* encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit (VC).
		VC	With *VC m*ultiplexing, no link control header is needed as the ATM VC is assumed to be carrying a single protocol.
	IP Address	This is the static IP address assigned by the DHCP server.	
	Mask	A *Mask* is used to determine which subnet an IP address belongs to. This is the *Subnet Mask* that will be assigned to the WAN interface of the iConnect625W router. The information is based on the details provided by your ISP.	
	Gateway	The *Gateway* is the IP address of your gateway.	
	Default Gateway	If this field is enabled/checked, this WAN connection will act as the default gateway to the Internet.	
Renew	It may be necessary on occasion to get a new IP address or to update the DHCP options sent by your ISP's DHCP server. Pressing this button renews the DHCP lease.		
Release	Clicking this button releases the current network settings from the iConnectAccess264W router.		
Apply	Applies the changes made to the connection.		
Delete	Deletes the connection.		
Cancel	Cancels the changes made to the connection.		

NOTE	**For VLAN and PVC field descriptions, please refer to the table under PPPoE section.**

7.2.5 Bridged Connection Setup

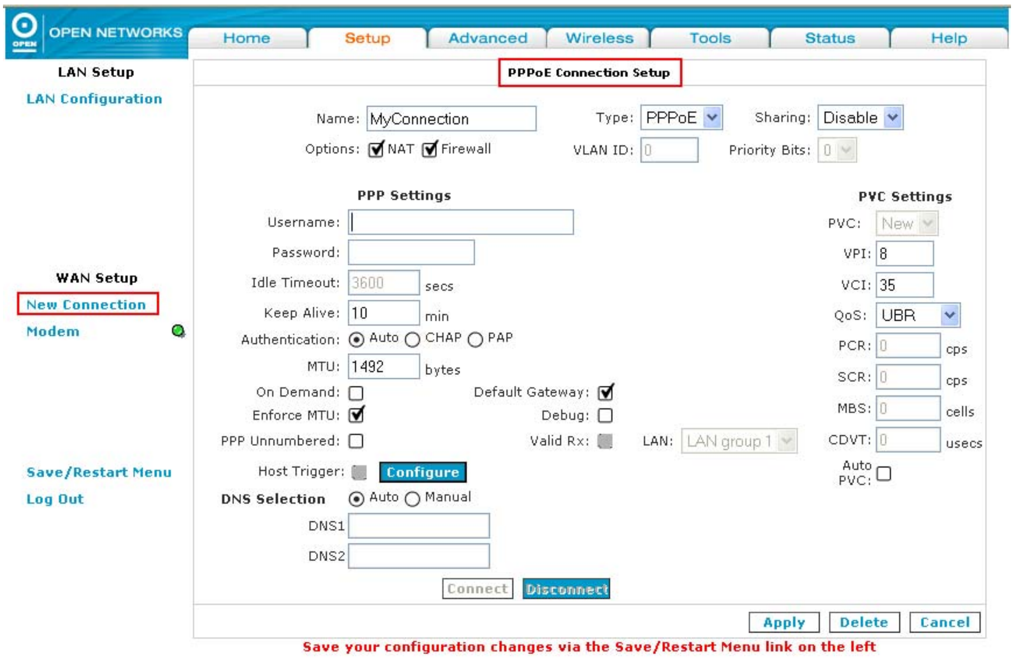
In *Bridge* mode, Ethernet frames are bridged over ATM VC. The Ethernet frames are encapsulated using either *LLC Encapsulation* or *VC Multiplexing*. Since the Ethernet packets are bridged, the router's only functionality is to pass the Ethernet packets to and from the ISP and the local network.

Your ISP assigns the IP addresses of the local network, either statically or dynamically. If your ISP provides bridged service, you may select the *Bridged* connection type.

In this setting, the NAT and firewall rules are disabled. This connection method makes the iConnect625W act as a transparent hub and passes packets across from the WAN interface to the LAN interface transparently.

To configure *Bridge* connection, follow the steps provided below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***New Connection*** link. The default *PPPoE Connection Setup* page appears:



PPPoE Connection Setup

Name: MyConnection Type: PPPoE Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Username:

Password:

Idle Timeout: 3600 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1492 bytes

On Demand: □ Default Gateway: ☑

Enforce MTU: ☑ Debug: □

PPP Unnumbered: □ Valid Rx: ▨ LAN: LAN group 1

Host Trigger: ▨ Configure

DNS Selection ● Auto ○ Manual

DNS1

DNS2

Connect Disconnect

PVC Settings

PVC: New

VPI: 8

VCI: 35

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

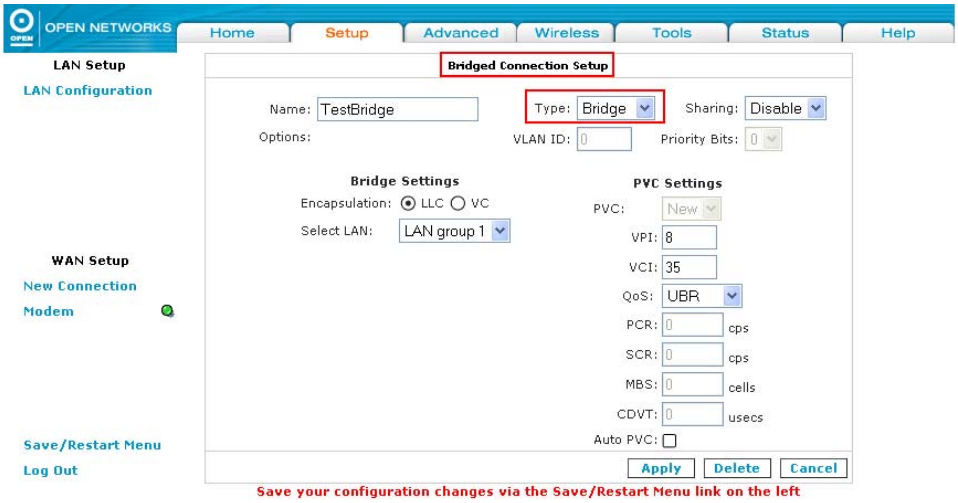
CDVT: 0 usecs

Auto PVC: □

Apply Delete Cancel

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Type*** drop-down list, select ***Bridge.*** The following page appears:



Bridged Connection Setup

Name: TestBridge
Type: Bridge
Sharing: Disable
Options:
VLAN ID: 0
Priority Bits: 0

Bridge Settings
Encapsulation: ● LLC ○ VC
Select LAN: LAN group 1

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter a unique name for your *Bridged* connection in the ***Name*** field. The name must not have spaces and cannot begin with numbers.

Step 4: Select the ***Encapsulation Type*** (LLC or VC) by highlighting the appropriate radio button. The default is set to *LLC*. If you are unsure about the option, leave the default setting as it is.

Step 5: In the ***Select LAN*** field, select the appropriate *LAN Group* you wish to configure for *Bridge* mode.

Step 6: The ***VPI*** and ***VCI*** values are defaulted to *8* and *35*, respectively. Make the changes in these fields as provided by your ISP, if required.

NOTE	**If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.**

Step 7: Select the ***QoS***. Leave the default value if you are unsure or if the ISP did not provide this information.

The ***PCR, SCR, MBS*** and ***CDVT*** fields could be enabled/disabled depending on the ***QoS*** section. Your ISP should provide these values.

Step 8: Click the ***Apply*** button.

Step 9: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Bridge Connection Setup* screen and their definitions:

Field	Description		
Bridge Settings	Each of the fields for *Bridge Settings* is described as follows.		
	Encapsulation	*LLC and VC* are two different methods of encapsulating multiple sessions. The default is set to *LLC*.	
		LLC	With *LLC* encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit (VC).
		VC	With *VC m*ultiplexing, .no link control header is needed as the ATM VC is assumed to be carrying a single protocol.
	Select LAN	Select the LAN Group (as defined in the *LAN Configuration* screen) for the bridged connection. The options are: • LAN Group 1 • LAN Group 2 • LAN Group 3 • LAN Group 4 • LAN Group 5 • None The *Bridge* connection is added to the LAN Group configuration, unless you have selected the option: *None.* In this case, the connection will be added to the *Interfaces* box instead.	
Apply	Applies the changes made to the connection.		
Delete	Deletes the connection.		
Cancel	Cancels the changes made to the connection.		

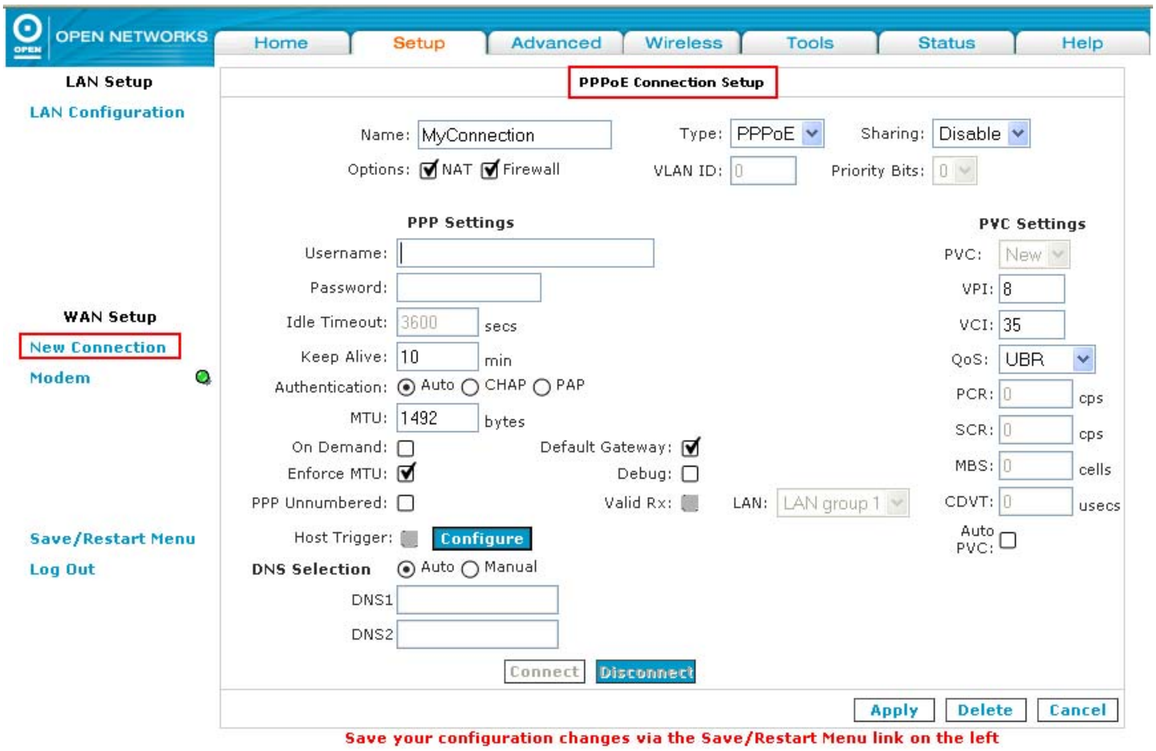
NOTE	**For VLAN and PVC field descriptions, please refer to the table under PPPoE section.**

7.2.6 CLIP Connection Setup

Classical IP Over ATM as defined in RFC1577 provides the ability to transmit IP packets over an ATM network. CLIP support encapsulates IP in an AAL5 Packet Data Unit (PDU) frame using RFC 1577 and it sends out an ARP request to a CLIP-enable ARP server, which returns the ATM address.

To configure *CLIP* connection, follow the steps provided below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***New Connection*** link. The following page appears if no prior connection has been configured:



PPPoE Connection Setup

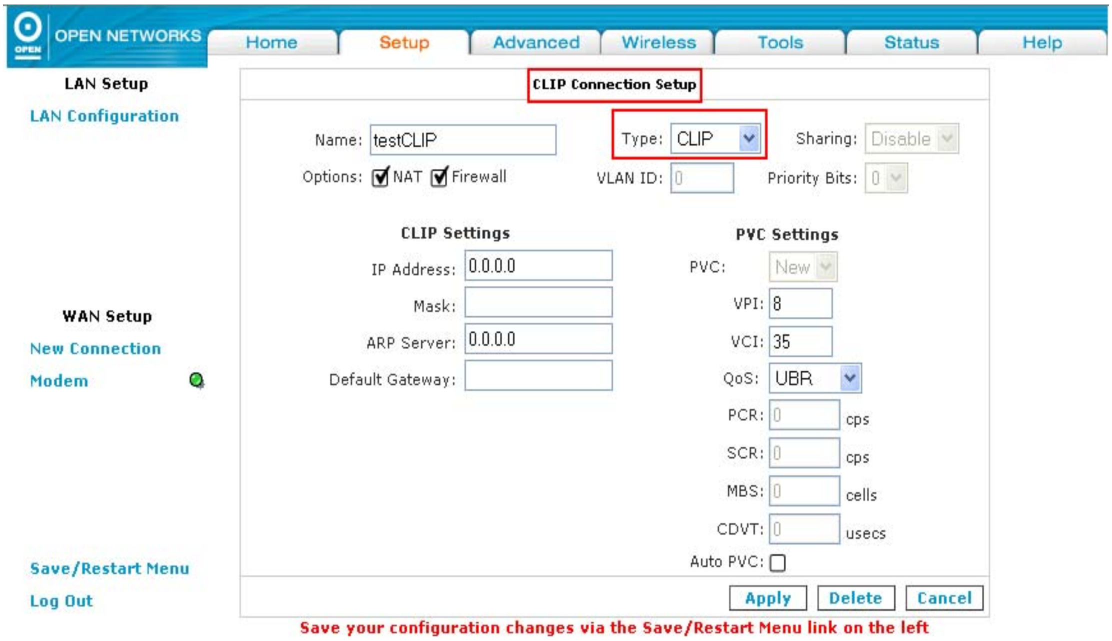
Name: MyConnection Type: PPPoE Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings
Username:
Password:
Idle Timeout: 3600 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □ Default Gateway: ☑
Enforce MTU: ☑ Debug: □
PPP Unnumbered: □ Valid Rx: ▨ LAN: LAN group 1
Host Trigger: ▨ Configure
DNS Selection ● Auto ○ Manual
DNS1
DNS2

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Type*** drop-down list, select ***CLIP.*** The following page appears:



CLIP Connection Setup

Name: testCLIP Type: CLIP Sharing: Disable
Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

CLIP Settings
IP Address: 0.0.0.0
Mask:
ARP Server: 0.0.0.0
Default Gateway:

PVC Settings
PVC: New
VPI: 8
VCI: 35
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter a unique name for your *Bridged* connection in the ***Name*** field. The name must not have spaces and cannot begin with numbers.

Step 4: The ***NAT*** and ***Firewall*** checkboxes are checked by default under the ***Options*** field. Leave these in the default mode.

Step 5: In the ***IP Address*** field, enter your assigned IP address based on the information provided by your ISP.

Step 6: In the ***Mask*** field, enter the Subnet Mask based on the information provided by your ISP.

Step 7: In the ***ARP Server*** field, enter the *ARP Server* address based on the information provided by your ISP.

Step 8: In the ***Default Gateway*** field, the *Default Gateway* is blank. Enter this field based on the information provided by your ISP.

Step 9: In the *PVC Settings* section, the ***VPI*** and ***VCI*** values are defaulted to *8* and *35*, respectively. Make the changes in these fields, as provided by your ISP, if required.

NOTE	***If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the settings. It is not possible to have more than one connection using the same VPI/VCI values.***

Step 10: Select the ***QoS***. Leave the default value if you are unsure or if the ISP did not provide this information.

The ***PCR, SCR, MBS*** and ***CDVT*** fields could be enabled/disabled depending on the ***QoS*** section. Your ISP should provide these values.

Step 11: Click the ***Apply*** button.

Step 12: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

The following table lists the *CLIP Connection Setup* screen and their definitions:

Field	Description		
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.		
Firewall	Select to enable security for this connection. This is set to *Enabled* by default for standard operation.		
CLIP Settings	Each of the fields for *CLIP Settings* is described as follows.		
	Encapsulation	*LLC and VC* are two different methods of encapsulating multiple sessions. The default is set to *LLC*.	
		LLC	With *LLC* encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit (VC).
		VC	With *VC m*ultiplexing, .no link control header is needed as the ATM VC is assumed to be carrying a single protocol.
	IP Address		The CLIP Server IP Address provided by your ISP.
	Mask		The CLIP Server Subnet Mask provided by your ISP.
	ARP Server		The Address Resolution Protocol (ARP) Server IP Address provided by your ISP.
	Default Gateway		If checked, this WAN connection acts as the default gateway to the Internet.
Apply	Applies the changes made to the connection.		
Delete	Deletes the connection.		
Cancel	Cancels the changes made to the connection.		

NOTE	**For VLAN and PVC field descriptions, please refer to the table under PPPoE section.**

7.2.7 Modify an Existing Connection

Follow the steps below to modify an existing connection.

Step 1: To begin, click the ***Setup tab*** on the top menu, and click the connection you wish to modify from the left hand menu.

Step 2: Edit as applicable on the individual connection page.

Step 3: Click the ***Apply*** button.

Step 4: To save your configuration, please refer to the section under ***Save / Restart Menu***.

7.2.8 Delete an Existing Connection

Follow the steps below to delete a WAN connection.

Step 1: To begin, click the ***Setup tab*** on the top menu, and click the connection you wish to delete from the left hand menu.

Step 2: Click the ***Delete*** button on the applicable connection you wish to remove.

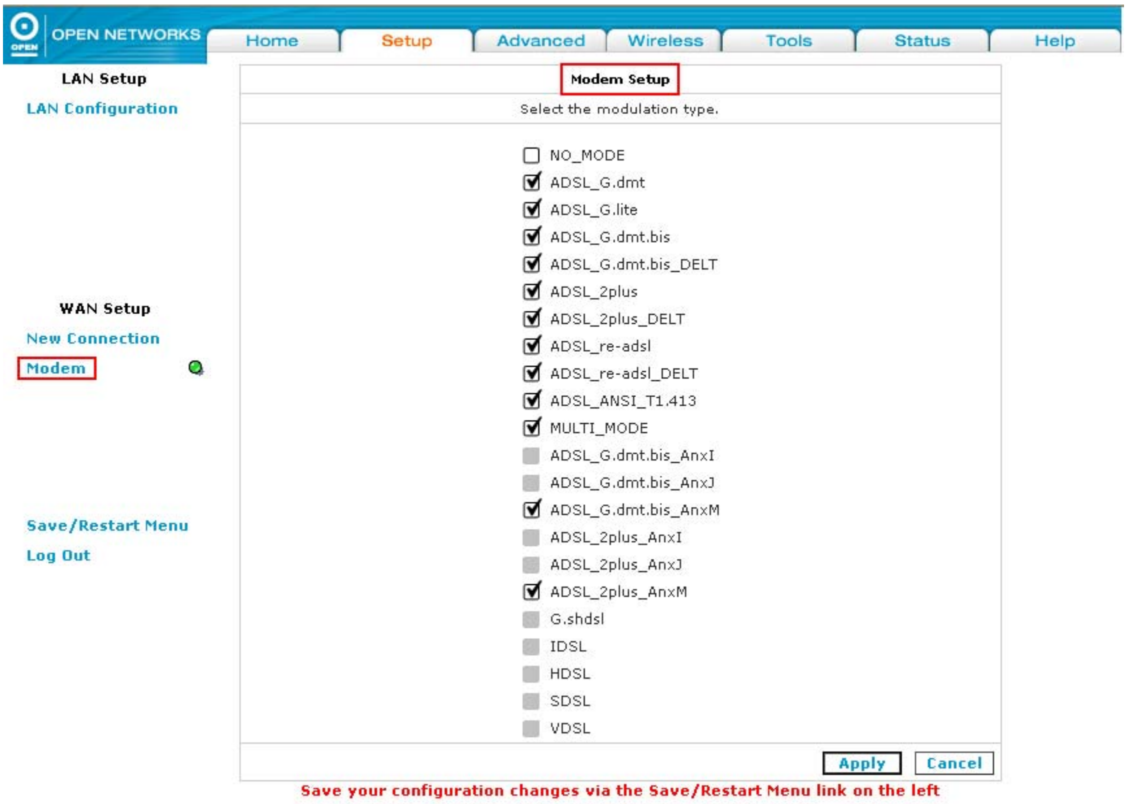
NOTE	*The changes take effect when you click Delete. However, if the iConnect625W router configuration is not saved, these changes will be lost when you reboot the iConnect625W router.*

Step 3: To save your configuration, please refer to the section under ***Save / Restart Menu***.

7.2.9 Modem Setup

To configure the ADSL modulation types, follow the steps below.

Step 1: To begin, click the ***Setup tab*** on the top menu. Click the ***Modem*** link. The following page appears:



Modem Setup

Select the modulation type.

□ NO_MODE
☑ ADSL_G.dmt
☑ ADSL_G.lite
☑ ADSL_G.dmt.bis
☑ ADSL_G.dmt.bis_DELT
☑ ADSL_2plus
☑ ADSL_2plus_DELT
☑ ADSL_re-adsl
☑ ADSL_re-adsl_DELT
☑ ADSL_ANSI_T1.413
☑ MULTI_MODE
□ ADSL_G.dmt.bis_AnxI
□ ADSL_G.dmt.bis_AnxJ
☑ ADSL_G.dmt.bis_AnxM
□ ADSL_2plus_AnxI
□ ADSL_2plus_AnxJ
☑ ADSL_2plus_AnxM
□ G.shdsl
□ IDSL
□ HDSL
□ SDSL
□ VDSL

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The ***Modulation Type*** checkboxes are defaulted to the above settings as shown. It is recommended that the default settings remain.

NOTE	**The iConnect625W router is pre-configured to detect the ADSL modulation type automatically. In most cases, this screen should not be modified.**

Step 3: If any modulation type has been amended, click the ***Apply*** button.

Step 4: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Modem* screen fields and their definitions:

Field	Description
There are multiple combinations of ADSL modulation modes to be selected.	
No Mode	No mode is defaulted to disabled.
ADSL_G.dmt	G.dmt stands for G Discrete Multi-Tone. It supports ITU-U ADSL over POTS (G.992.1).
ADSL_G.lite	It support ITU-T ADSL over POTS (G.992.2)
ADSL_G.dmt.bis	It supports ITU-T ADSL 2 over POTS (G.992.3)
ADSL_G.dmt.bis.DELT	It supports ADSL G.DMT.bis DELT
ADSL_2plus	It supports ITU-T ADSL 2+ over POTS (G.992.5) and speeds up to 24Mbps.
ADSL_2plus_DELT	It supports ADSL 2+ and speeds up to 24Mbps.
ADSL re-adsl	It supports ITU-T RE-ADSL 2 over POTS (G.992.3).
ADSL re-adsl DELT	It supports ADSL re-adsl DELT.
ADSL_ANSI_T1.413	This applies to ANSI T1.413-1998.
MULTI_MODE	*Multi-Mode* is automatically detected.
ADSL_G.dmt.bis_AnxM	It supports ITU-T ADSL 2 G.992.3 Annex M.
ADSL2plus_AnxM	It supports ITU-T ADSL 2+ G.992.5 Annex M.

8. Advanced

The iConnect625W supports a host of advanced networking and routing features including the setup of your LAN and WAN interfaces, security, port configuration, user management, restarting the router and plug and play capability.

In addition, it allows you to performance advanced configuration functions for existing connection such as enabling and disabling voice, voice provision, UPnP, SNTP, SNMP and so on.

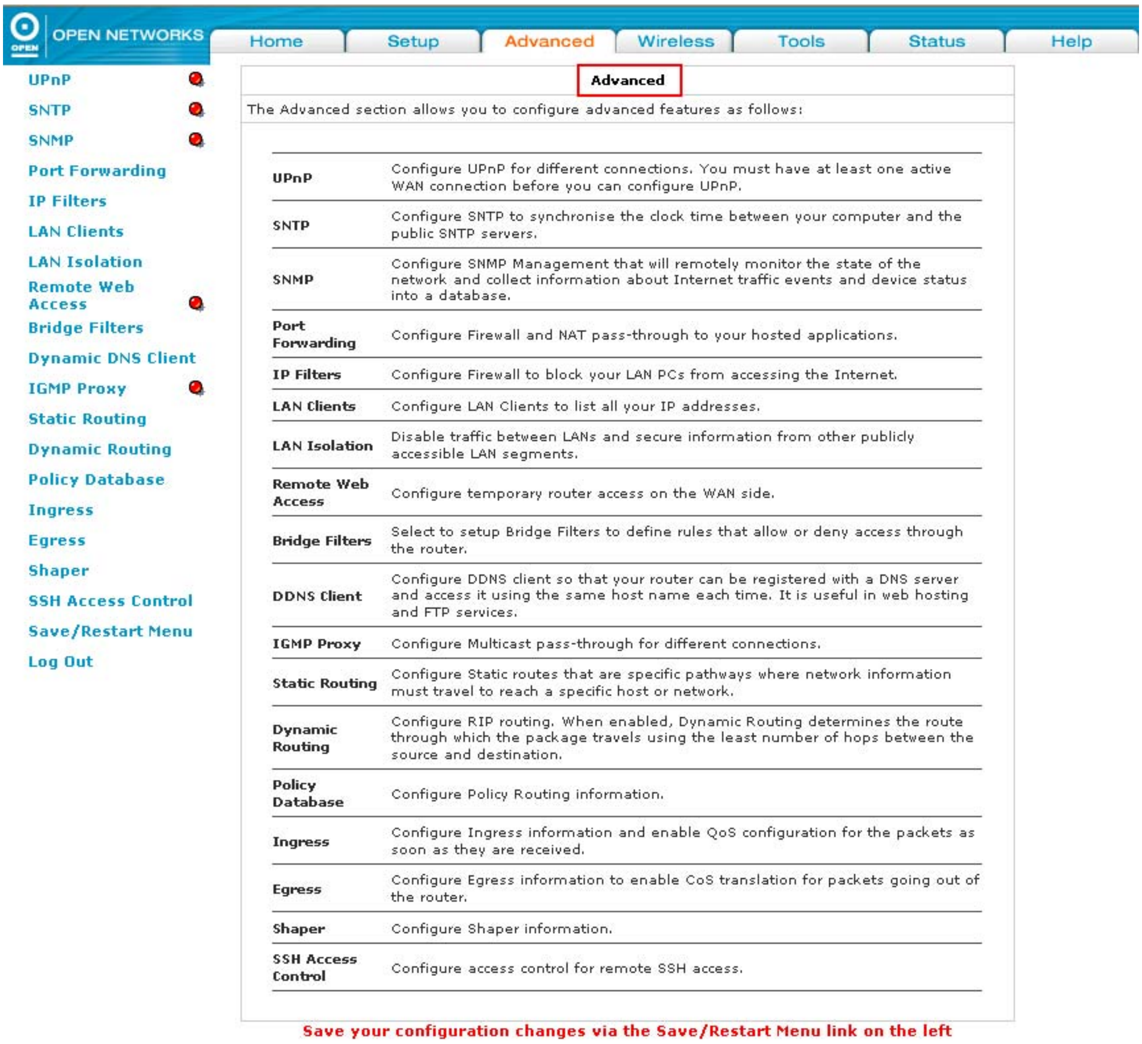
There should be at least one WAN connection configured before implementing advanced WAN configuration features. Similarly, at least one LAN group must be defined before advanced LAN configuration features can be implemented.

The features include:

- Universal Plug and Play (UPnP)
- Simple Networking Timing Protocol (SNTP)
- Simple Network Management Protocol (SNMP)
- Port Forwarding
- IP Filters
- LAN Clients
- LAN Isolation between LAN groups
- Remote Web Access
- Bridge Filters
- Dynamic DNS Client
- Internet Group Management Protocol (IGMP) Proxy
- Static Routing
- Dynamic Routing
- Policy Database
- Ingress
- Egress
- Shaper
- SSH Access Control

To access the *Advanced* configuration screen, follow the steps below.

Step 1: Click the ***Advanced*** tab to access the advanced configuration features. The following page appears:



Advanced

The Advanced section allows you to configure advanced features as follows:

UPnP	Configure UPnP for different connections. You must have at least one active WAN connection before you can configure UPnP.
SNTP	Configure SNTP to synchronise the clock time between your computer and the public SNTP servers.
SNMP	Configure SNMP Management that will remotely monitor the state of the network and collect information about Internet traffic events and device status into a database.
Port Forwarding	Configure Firewall and NAT pass-through to your hosted applications.
IP Filters	Configure Firewall to block your LAN PCs from accessing the Internet.
LAN Clients	Configure LAN Clients to list all your IP addresses.
LAN Isolation	Disable traffic between LANs and secure information from other publicly accessible LAN segments.
Remote Web Access	Configure temporary router access on the WAN side.
Bridge Filters	Select to setup Bridge Filters to define rules that allow or deny access through the router.
DDNS Client	Configure DDNS client so that your router can be registered with a DNS server and access it using the same host name each time. It is useful in web hosting and FTP services.
IGMP Proxy	Configure Multicast pass-through for different connections.
Static Routing	Configure Static routes that are specific pathways where network information must travel to reach a specific host or network.
Dynamic Routing	Configure RIP routing. When enabled, Dynamic Routing determines the route through which the package travels using the least number of hops between the source and destination.
Policy Database	Configure Policy Routing information.
Ingress	Configure Ingress information and enable QoS configuration for the packets as soon as they are received.
Egress	Configure Egress information to enable CoS translation for packets going out of the router.
Shaper	Configure Shaper information.
SSH Access Control	Configure access control for remote SSH access.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Please refer to the sections below on how to configure the advanced features.

8.1 UPnP

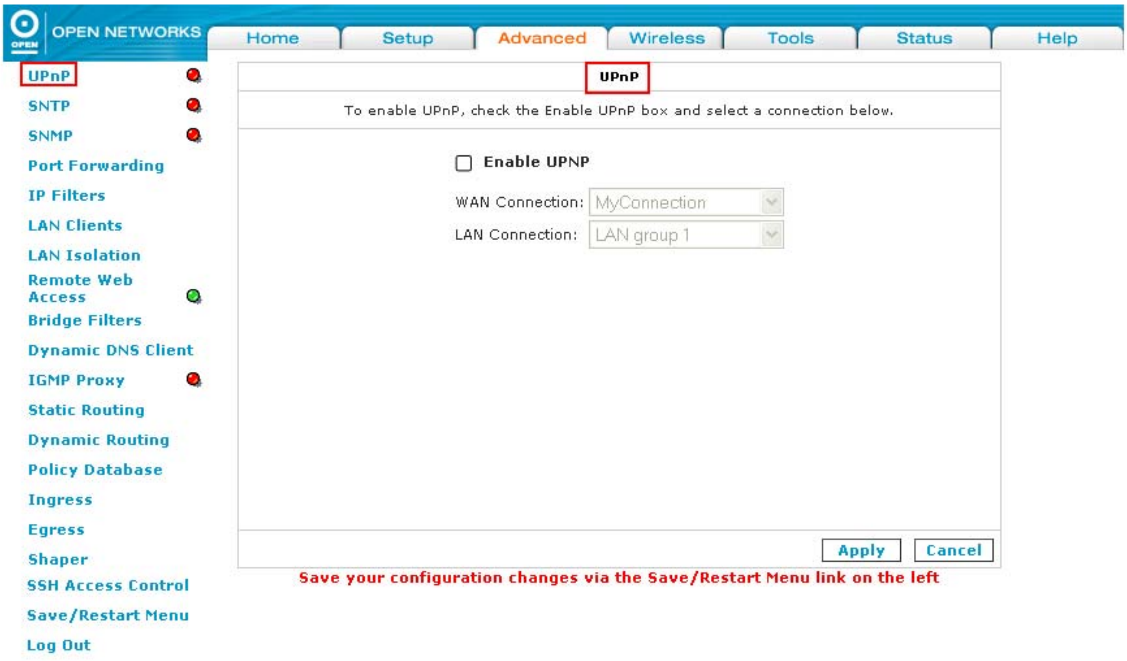
UPnP is a networking architecture that provides compatibility among networking equipment, software and peripherals such as game consoles, digital cameras and other systems that connect by TCP/IP. It can be supported on any operating system, and boasts device-driver independence and zero-configuration networking.

UPnP is a standard that uses Internet and Web protocols to enable the iConnect625W to plug into a network and automatically recognise each other. This feature is set to *Disabled* by default in the iConnect625W.

This feature requires one active WAN connection. In the presence of multiple WAN connections, select a connection on which the incoming traffic is present, for example, the default WAN connection.

Follow the steps below to enable *UPnP*.

Step 1: From the ***Advanced*** tab, click the ***UPnP*** link on the left menu. The following page appears:



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

□ Enable UPNP

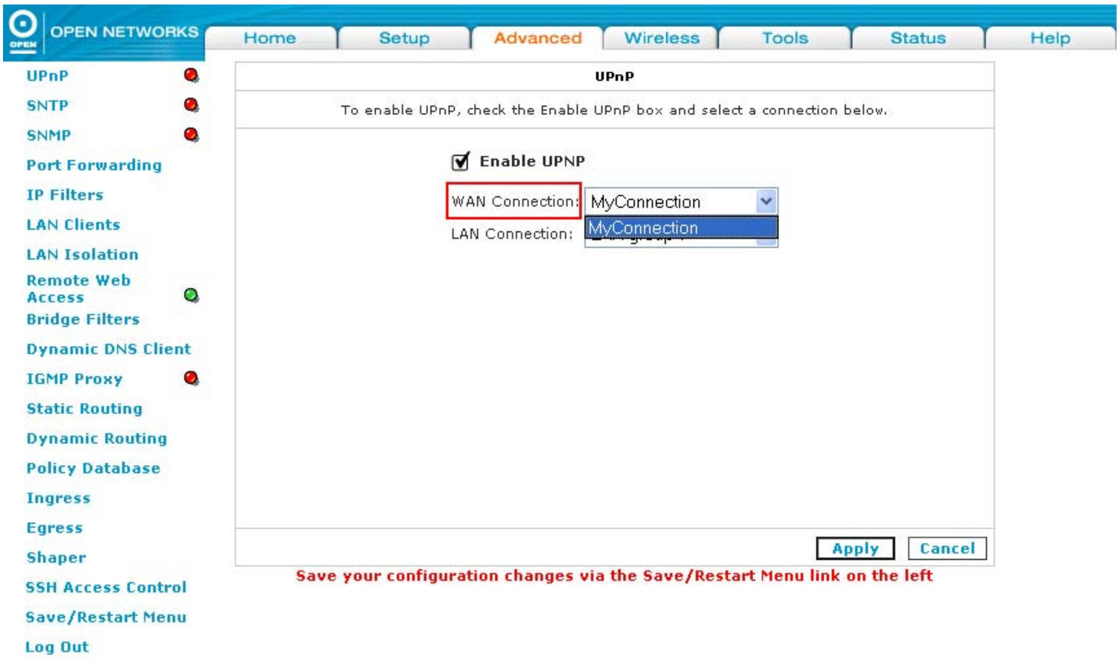
WAN Connection: MyConnection

LAN Connection: LAN group 1

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable UPnP*** checkbox. This enables the WAN connection and LAN connection fields.

Step 3: Select the required ***WAN Connection*** that will use *UPnP* by highlighting the appropriate item from the drop-down list.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

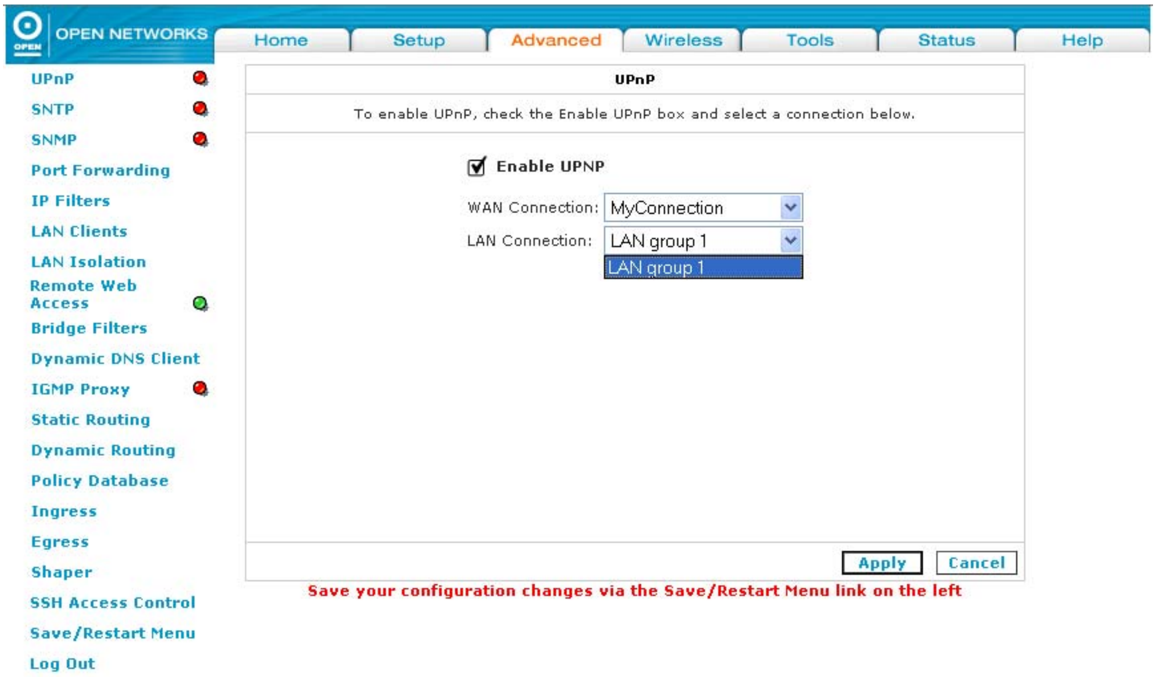
☑ Enable UPNP

WAN Connection: MyConnection

LAN Connection: MyConnection

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Select the ***LAN Connection*** that will use *UPnP* by highlighting the appropriate item from the drop-down list.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

☑ Enable UPNP

WAN Connection: MyConnection

LAN Connection: LAN group 1

LAN group 1

Save your configuration changes via the Save/Restart Menu link on the left

Step 5: Click the ***Apply*** button to apply the settings.

Step 6: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.2 SNTP

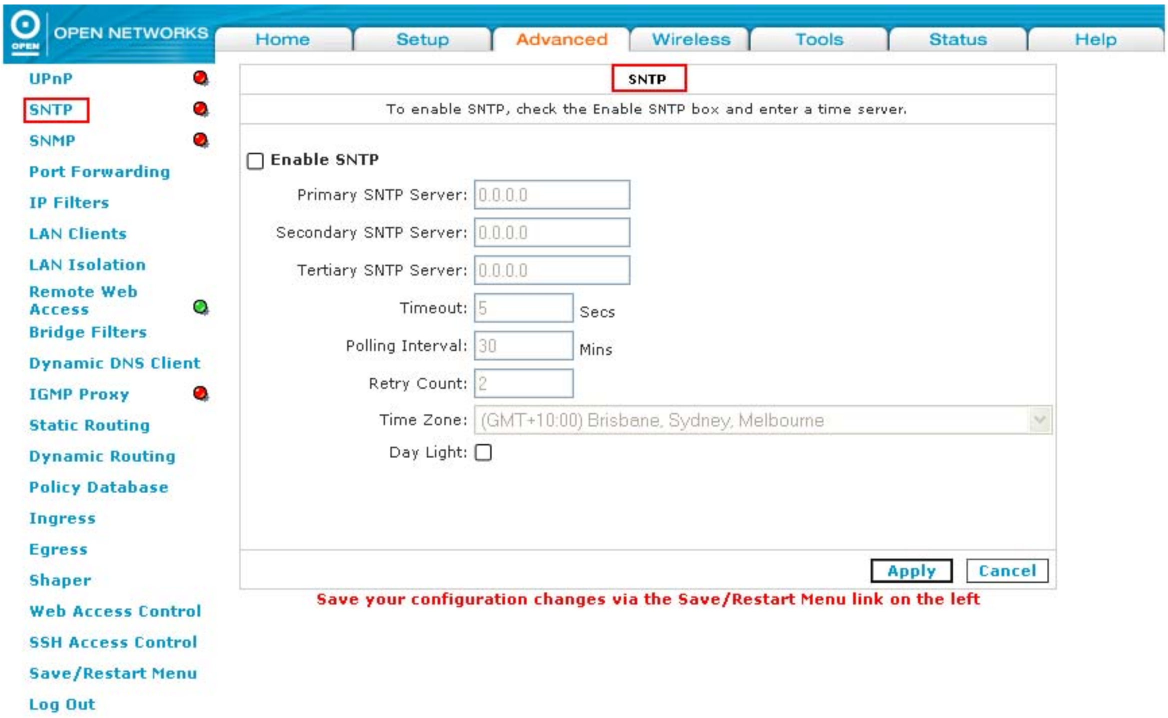
SNTP ensures that the computer clock time can be synchronised in a network of computers to the millisecond to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers.

When the SNTP feature is enabled, your iConnect625W starts verifying the time clock information from the primary SNTP server. If it does not get a valid response within the *Timeout* period, it makes additional attempts based on the number on the value of the *Retry Count* field before it moves to the Secondary SNTP server. If there is no valid response either for this server, it moves on to the Tertiary SNTP server. If it does not get a valid response from all the servers, the program stops.

When it does receive a valid response from one of the servers, the program goes to sleep for a few minutes as specified in the *Polling Interval* field before starting the whole process again.

Follow the steps below to configure *SNTP.*

Step 1: From the ***Advanced*** tab, click the ***SNTP*** link on the left menu. The following page appears:



SNTP

To enable SNTP, check the Enable SNTP box and enter a time server.

□ Enable SNTP

Primary SNTP Server: 0.0.0.0

Secondary SNTP Server: 0.0.0.0

Tertiary SNTP Server: 0.0.0.0

Timeout: 5 Secs

Polling Interval: 30 Mins

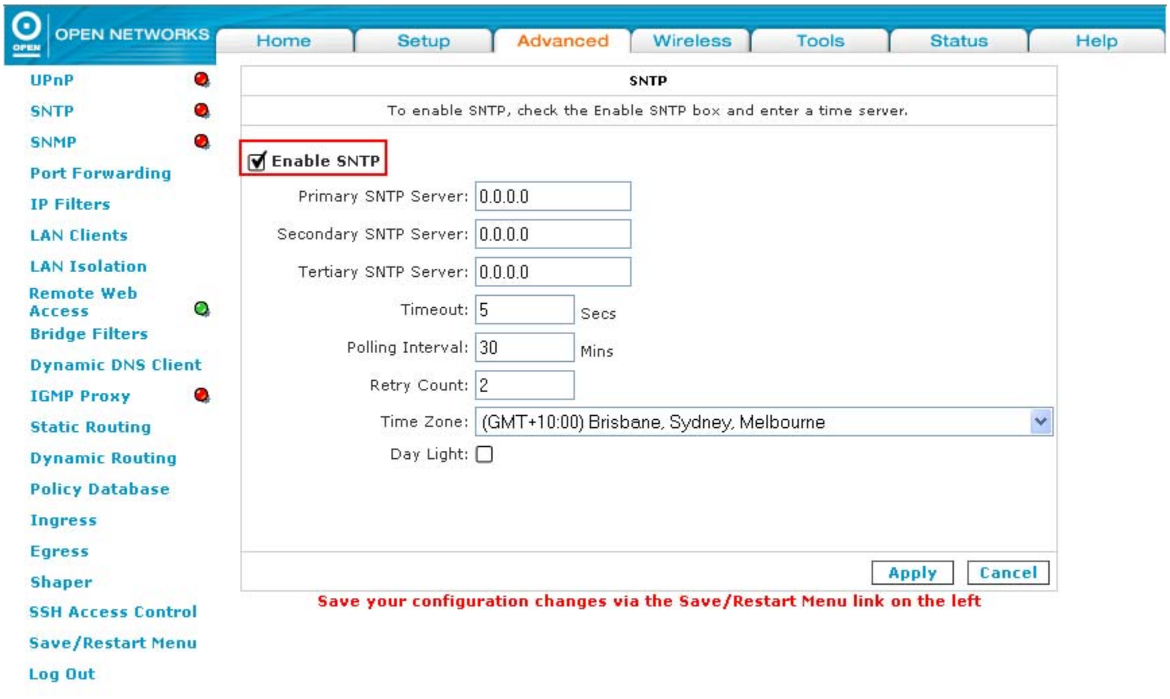
Retry Count: 2

Time Zone: (GMT+10:00) Brisbane, Sydney, Melbourne

Day Light: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable SNTP*** checkbox as shown below.



SNTP

To enable SNTP, check the Enable SNTP box and enter a time server.

☑ Enable SNTP

Primary SNTP Server: 0.0.0.0

Secondary SNTP Server: 0.0.0.0

Tertiary SNTP Server: 0.0.0.0

Timeout: 5 Secs

Polling Interval: 30 Mins

Retry Count: 2

Time Zone: (GMT+10:00) Brisbane, Sydney, Melbourne

Day Light: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter the *Primary SNTP Server* address as required in the ***Primary SNTP Server*** field.

Step 4: Enter the *Secondary SNTP Server* address as required in the ***Secondary SNTP Server*** field.

Step 5: Enter the *Tertiary SNTP Server* address as required in the ***Tertiary SNTP*** field.

Step 6: Enter a *Timeout limit* (in seconds) into the ***Timeout*** field. The default is set to *5sec.*

Step 7: Enter a time (in minutes) in the ***Polling Interval*** field. The default is set to *30mins.*

Step 8: Enter the number of times to retry connecting to the server in the ***Retry Count*** field. The default value is 2.

Step 9: Select the ***Time Zone*** from the drop-down list. The time zone refers to the location where the router is operating.

Step 10: Check the ***Day Light*** checkbox to activate daylight saving time (DST), if it is applicable.

Step 11: Click the ***Apply*** button to save the settings.

Step 12: To save your configuration, please refer to the section under ***Save / Restart Menu***.

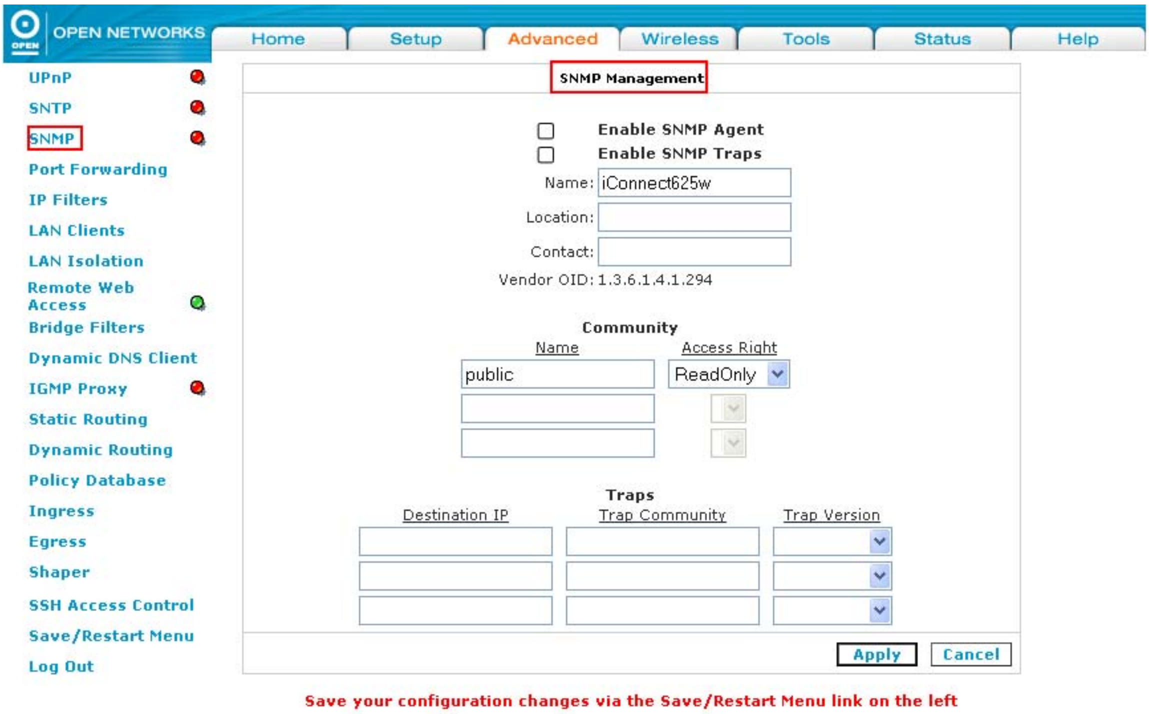
The following table lists the *SNTP* screen fields and their definitions:

Field	Description
Enable SNTP	Check this checkbox to enable the iConnect625W to synchronise the system time to the public SNTP servers.
Primary SNTP Server	The IP address or the host name of the primary SNTP server. Refer to your ISP for this information. The default setting is *0.0.0.0*.
Secondary SNTP Server	The IP address or host name of the secondary SNTP server. Refer to your ISP for this information. The default setting is *0.0.0.0.*
Tertiary SNTP Server	The IP address or host name of the tertiary SNTP server. Refer to your ISP for this information. The default setting is *0.0.0.0.*
Timeout	The time in seconds that the iConnect625W will wait for an SNTP server to respond. If the router fails to connect to an SNTP server within the timeout period, it retries the connection. The default is set to *5* seconds.
Polling Interval	The amount of time (in minutes) that the iConnect625W checks the time between a successful connection with an SNTP server and a new attempt to connect to an SNTP server. The default setting is *30* minutes.
Retry Count	The number of retries before a backup server is polled, i.e. the number of times the router tries to connect to an SNTP server before it tries to connect to the next server in line. The default setting is set to *2*.
Time Zone	The time zone where the router resides.
Daylight	Select this option to enable daylight saving time (DST). DST is not automatically enabled or disabled. This function needs to be enabled manually.

8.3 SNMP

SNMP is used to remotely monitor the state of the network and collect information about Internet traffic events and device status into a database. It is a troubleshooting and management tool that uses UDP protocol on Port 161 to communicate between clients and servers. For example, SNMP can be used to monitor the amount of traffic passing through the network.

Step 1: From the ***Advanced*** tab, click the ***SNMP*** link on the left menu. The *SNMP Management* page appears:



SNMP Management

□ Enable SNMP Agent

□ Enable SNMP Traps

Name: iConnect625w

Location:

Contact:

Vendor OID: 1.3.6.1.4.1.294

Community

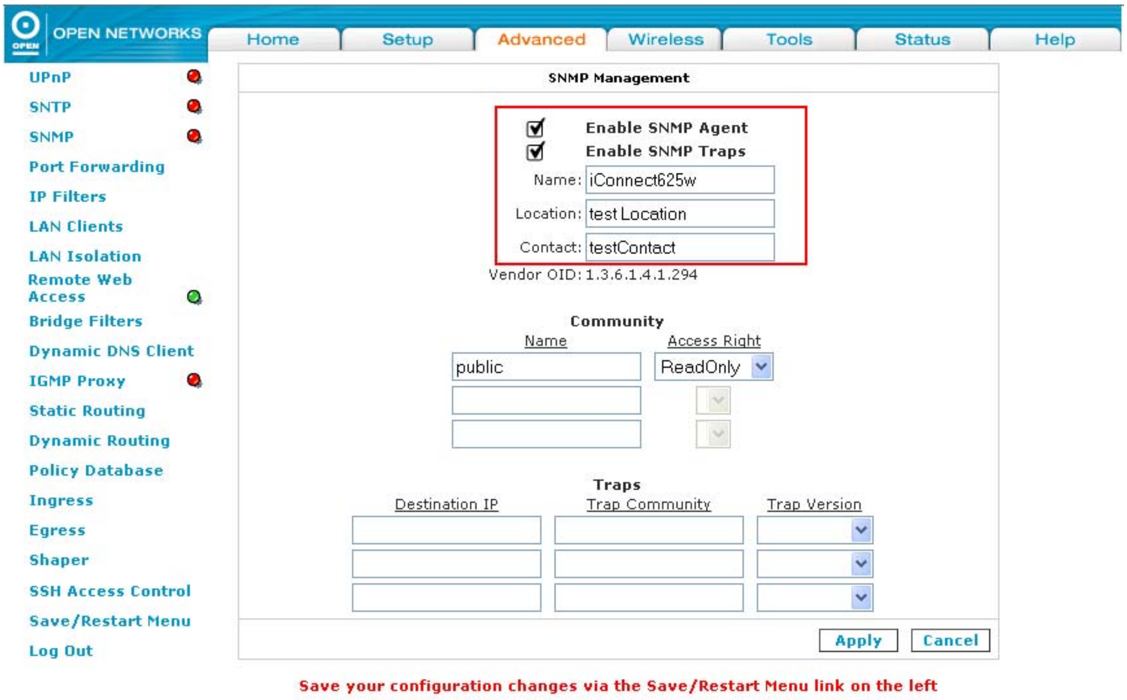
Name	Access Right
public	ReadOnly

Traps

Destination IP	Trap Community	Trap Version

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable SNMP Agent*** and ***Enable SNMP Traps*** checkboxes to enable this feature as shown.



SNMP Management

☑ Enable SNMP Agent

☑ Enable SNMP Traps

Name: iConnect625w

Location: test Location

Contact: testContact

Vendor OID: 1.3.6.1.4.1.294

Community

Name	Access Right
public	ReadOnly

Traps

Destination IP	Trap Community	Trap Version

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter an administrative name for the device in the ***Name*** field.

Step 4: Enter the physical location of the iConnect625W router in the ***Location*** field.

Step 5: Enter a contact for the iConnect625W in the ***Contact*** field.

Step 6: Enter a community name in the ***Name*** field under the *Community* section. The default is set to *Public*.

Step 7: The ***Access Right*** is defaulted to the *ReadOnly* option. The alternative option is the *ReadWrite* option from the drop-down list.

Step 8: Enter the *Trap Community name* in the ***Trap Community*** field. This should match the ***Community Name*** on the server receiving the traps.

Step 9: Select the ***Trap Version*** of the SNMP to use from the drop-down list.

Step 10: Click the ***Apply*** button to apply the settings.

Step 11: ***T***o save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *SNMP* screen fields and their definitions:

<table>
<tr><th>Field</th><th colspan="3">Description</th></tr>
<tr><td>***Enable SNMP Agent***</td><td colspan="3">Check this checkbox to enable SNMP on this device. Enter the SNMP settings in the *Community* section of the screen.</td></tr>
<tr><td>***Enable SNMP Traps***</td><td colspan="3">Check this checkbox to enable SNMP trap service. Enter the SNMP trap settings in the *Traps* section of the screen.</td></tr>
<tr><td>***Name***</td><td colspan="3">This is an administrative name that is assigned for the iConnect625W router.</td></tr>
<tr><td>***Location***</td><td colspan="3">This is the physical location of the iConnect625W router.</td></tr>
<tr><td>***Contact***</td><td colspan="3">This is the contact person and/or contact information for the iConnect625W router.</td></tr>
<tr><td rowspan="4">***Community***</td><td colspan="3">SNMP defines a community as a relationship between an SNMP agent and one or more SNMP managers.</td></tr>
<tr><td>***Name***</td><td colspan="2">The default community name is set to *Public* with *read-only* access mode created in the configuration file. SNMP supports up to 3 communities including the default community name *Public*.</td></tr>
<tr><td rowspan="2">***Access Rights***</td><td>***Read Only***</td><td>The SNMP *Read Only Community* string is like a user ID or password that allows access to the router's statistics.</td></tr>
<tr><td>***Read Write***</td><td>The SNMP *Read Write Community* string allows a remote device to read information from a device and to modify the settings on that device.</td></tr>
<tr><td rowspan="4">***Traps***</td><td colspan="3">Trap is an event notification. There are 4 standard traps that are supported in the iConnect625W router:
• WarmStartTrap;
• LinkUpTrap;
• LinkDownTrap;
• AuthenticationFailureTrap.</td></tr>
<tr><td colspan="2">***Destination IP***</td><td>This is the Destination IP Address of the host to receive the SNMP traps.</td></tr>
<tr><td colspan="2">***Trap Community***</td><td>This is the community name of the trap. It should match the community name on the server receiving the traps.</td></tr>
<tr><td colspan="2">***Trap Version***</td><td>Select the version of the SNMP to use from the drop-down list:
• SNMP v1
• SNMP v2</td></tr>
</table>

8.4 Port Forwarding

Port Forwarding allows you to provide local services (for example, web hosting) for users on the Internet or to play Internet games. When users send this type of request to your network via the Internet, the iConnect625W router forwards these requests to the appropriate computer. Hence, it allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol.

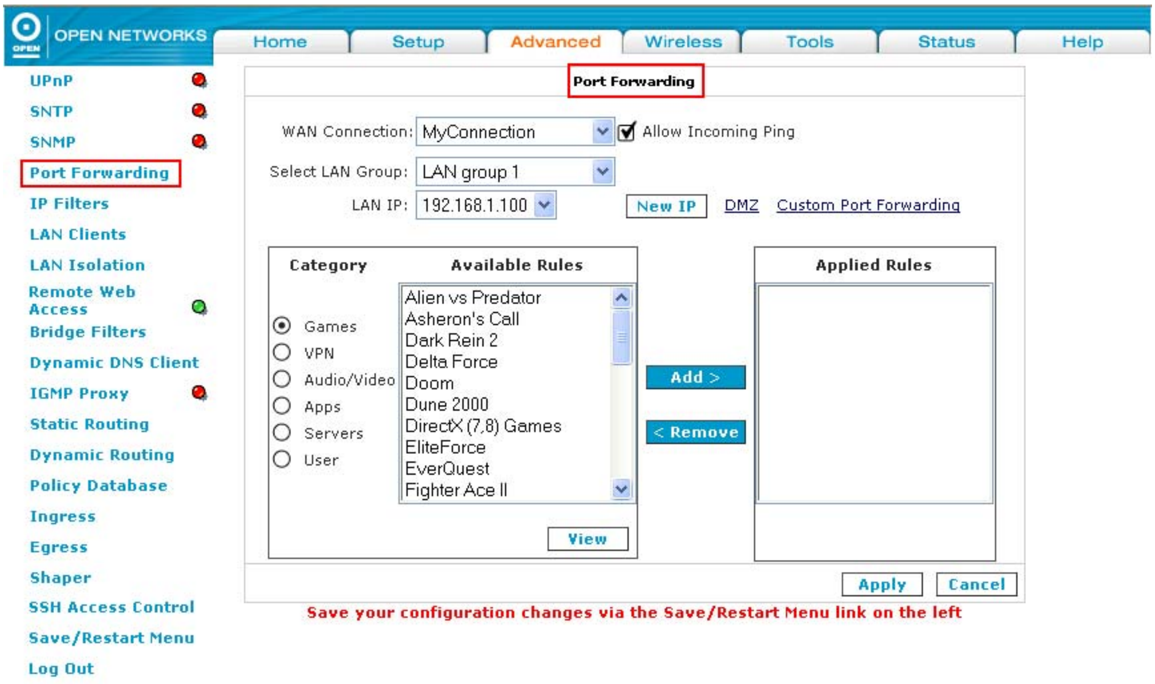
Port Forwarding can be used with dynamic DHCP-assigned addresses and is configurable per LAN group. For example, if you were configuring a Netmeeting server, you would want to assign this server to a static IP address so that the IP address is not re-assigned.

If Internet users are trying to access an Internet application, they must use the WAN IP address. Port Forwarding translates the WAN IP address into a LAN IP address.

Before Port Forwarding can be configured, you must ensure that you have a LAN IP Address configured in *LAN Clients*.

To configure Port Forwarding, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Port Forwarding*** link on the left menu. The following page appears:



Port Forwarding

WAN Connection: MyConnection ☑ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

Category: ● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User

Available Rules: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, Fighter Ace II

Applied Rules:

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***WAN Connection*** drop-down list, select the connection type for which you wish to which port forwarding is applied.

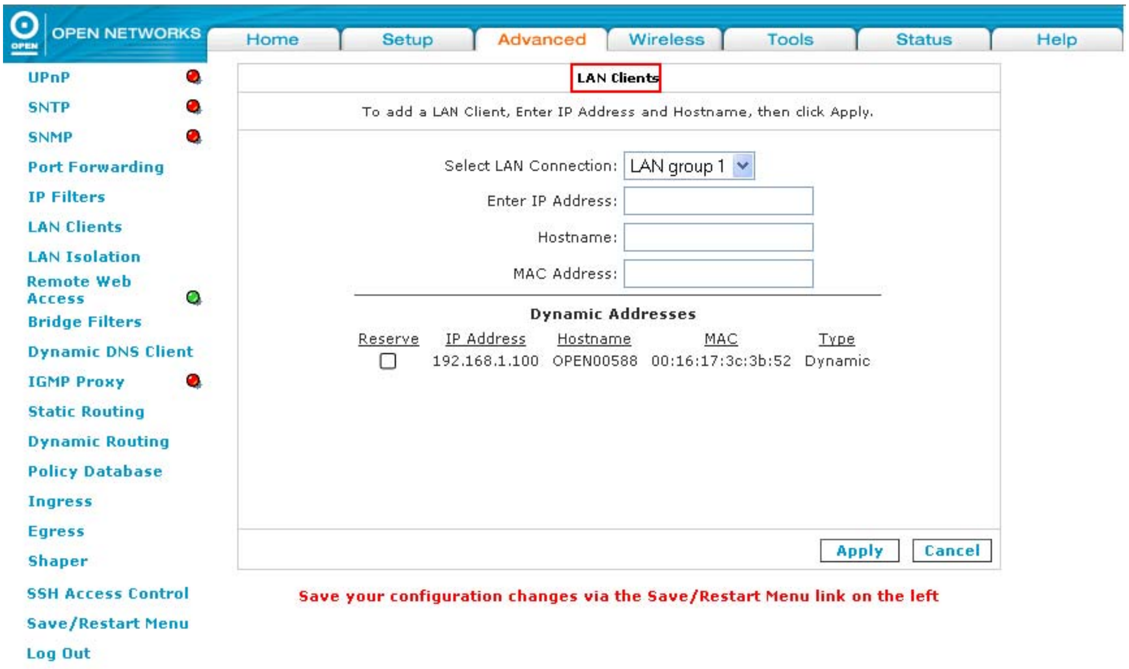
Step 3: Check the ***Allow Incoming Ping*** (ICMP) checkbox if you wish to monitor the connectivity between the IP devices. This is optional.

Step 4: From the ***Select LAN Group*** drop-down list, *LAN group 1* is the default setting that was previously configured under *Setup>LAN Configuration.*

Step 5: For the ***LAN IP*** drop-down list, select the IP address for which you wish to host the service.

NOTE	It is recommended that the Static IP Addresses rather than the DHCP IP Addresses be used for Port Forwarding.

Step 6: If you wish to add a new LAN IP address, click the ***New IP*** button. The *LAN Clients* page appears:



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

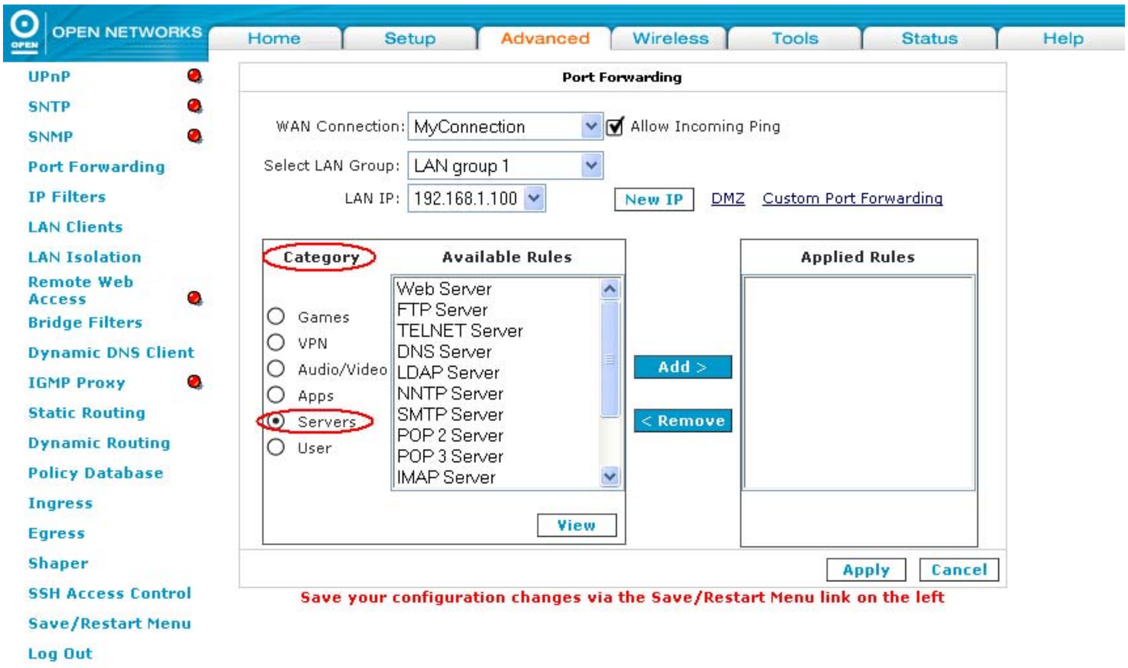
Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
□	192.168.1.100	OPEN00588	00:16:17:3c:3b:52	Dynamic

Save your configuration changes via the Save/Restart Menu link on the left

Step 7: Follow the instructions under the ***LAN Clients*** section for details on entering the fields.

Step 8: To add a new rule for this connection, highlight the appropriate category radio button for your configuration in the ***Category*** section, for example, *Servers*.



Port Forwarding

WAN Connection: MyConnection ☑ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

Category

○ Games
○ VPN
○ Audio/Video
○ Apps
● Servers
○ User

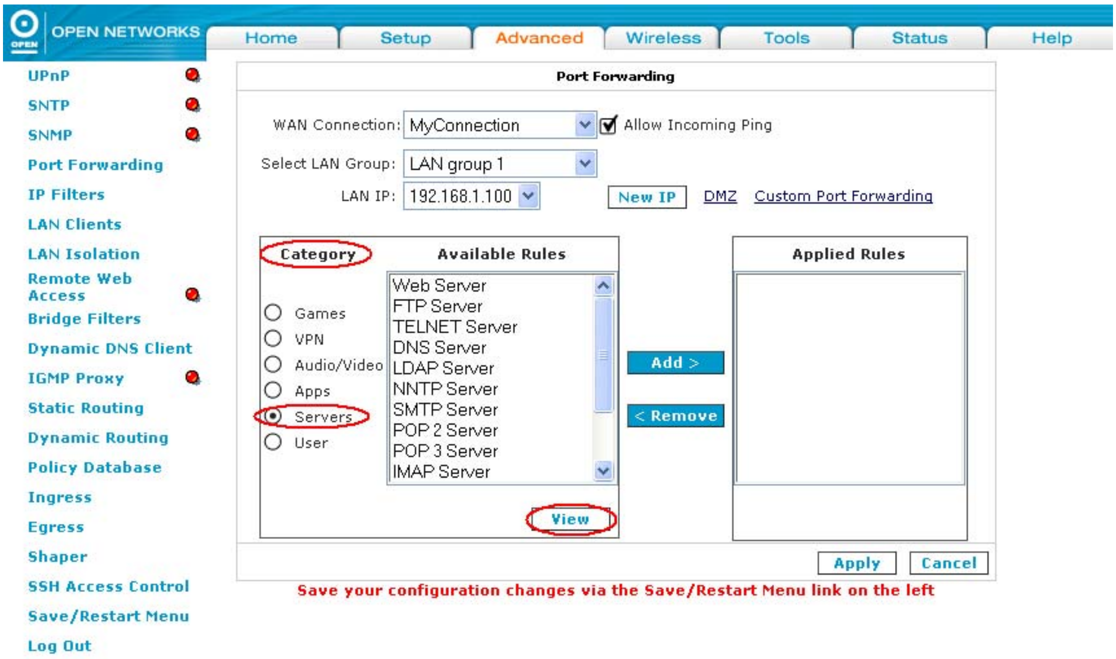
Available Rules

Web Server
FTP Server
TELNET Server
DNS Server
LDAP Server
NNTP Server
SMTP Server
POP 2 Server
POP 3 Server
IMAP Server

Applied Rules

Save your configuration changes via the Save/Restart Menu link on the left

Step 9: Select the ***Available Rules*** for a given category. The *Available Rules* window displays the common Internet services within the selected category. Rules for each service can be viewed by clicking the ***View*** button.



Port Forwarding

WAN Connection: MyConnection ☑ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

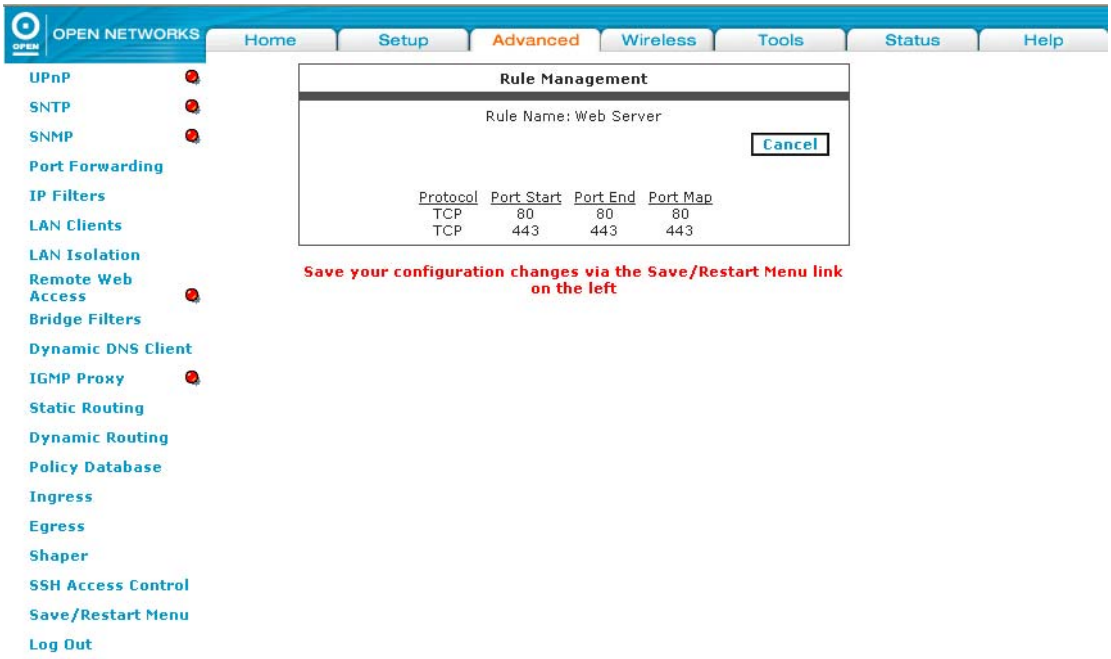
Category: ○ Games ○ VPN ○ Audio/Video ○ Apps ● Servers ○ User

Available Rules:
Web Server
FTP Server
TELNET Server
DNS Server
LDAP Server
NNTP Server
SMTP Server
POP 2 Server
POP 3 Server
IMAP Server

Applied Rules

Save your configuration changes via the Save/Restart Menu link on the left

The *Rule Management* page appears:



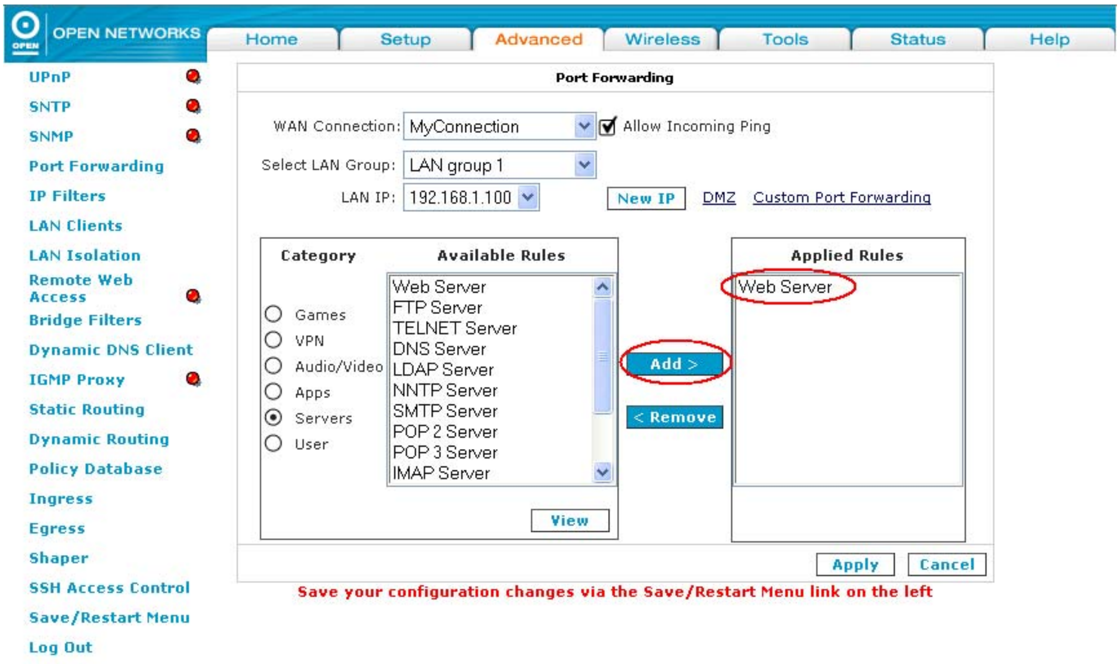
Rule Management

Rule Name: Web Server

Protocol	Port Start	Port End	Port Map
TCP	80	80	80
TCP	443	443	443

Save your configuration changes via the Save/Restart Menu link on the left

Step 10: Click the ***Add*** button. The rule then appears in the ***Applied Rules*** section of the screen. Continue to add rules as they apply from each category.



WAN Connection: MyConnection ☑ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

○ Games
○ VPN
○ Audio/Video
○ Apps
● Servers
○ User

Available Rules: Web Server, FTP Server, TELNET Server, DNS Server, LDAP Server, NNTP Server, SMTP Server, POP 2 Server, POP 3 Server, IMAP Server

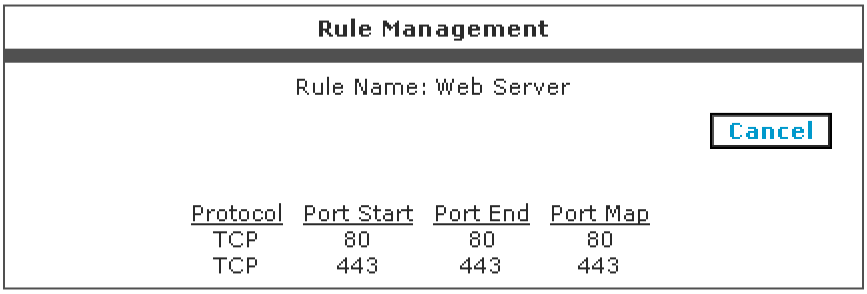
Applied Rules: Web Server

Save your configuration changes via the Save/Restart Menu link on the left

Step 11: Click the ***Apply*** button to apply the settings.

Step 12: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Port Forwarding* screen fields and their definitions:

Field	Description
WAN Connection	Select a defined WAN connection.
Allow Incoming Ping	*Ping* is a protocol used mainly for monitoring the connectivity between IP devices. Enabling this function allows remote devices to use ping to check connectivity to your device. Enable this function for monitoring purposes.
Select LAN Group	Select the *LAN Group* where the computer of the port to be forwarded to is a member. LAN Groups can be managed or created under *Setup>LAN Configuration*.
LAN IP	This is the IP address to which the selected ports are forwarded. It is recommended that a static IP address be used. This should be defined under the *LAN Clients* screen.
New IP	Clicking on this link leads to the *LAN Client* screen. Static addresses not listed under the *LAN IP* drop-down list can be added here.
DMZ	This links to the *Demilitarised (DMZ)* screen. Please refer to the section on *DMZ* for details on this function.
Custom Port Forwarding	Clicking on this link leads to the *Custom Port Forwarding* screen. Please refer to the section on *Custom Port Forwarding* for details on this function.
Category	With Port Forwarding, you can provide local services (for example web hosting) for users on the Internet or play Internet games. This is the *Category* section of the *Port Forwarding* screen. To configure a service or game, select the external connection (for e.g. the Internet connection), select the computer hosting the service and add the corresponding firewall rule. A number of pre-defined categories and rules are available here. These are *Games, VPN, Audio/Video, Apps, Servers* and *Users*. E.g. Web servers specify the following port forwarding profile.  Rule Management Rule Name: Web Server Protocol · Port Start · Port End · Port Map TCP · 80 · 80 · 80 TCP · 443 · 443 · 443 The categories available for Port Forwarding include: Games, VPN, Audio/Video, Apps (or applications), Servers and Users.

Field	Description	
	Games	Internet users are able to play Internet games when this function is configured. Examples of the games list include Aliens and Predators, Doom, Dune 2000, etc.
	VPN	The default VPN settings are: IPSEC L2TP and PPTP.
	Audio/Video	Net2Phone, Netmeeting and Quick Time 4 Server can be configured for Audio/Video services.
	Apps	Various applications are set as defaults under this category, including: VNC, Win2K terminals, PcAnywhere, etc.
	Servers	The default servers include: Web Servers, FTP server, Telnet Server, and so on.
	Users	New user rules can be added here.
Available Rules	Each category has *Available Rules* that are pre-defined or user-defined. Default rules such as Netmeeting is available under the *Audio/Video* category and Web Server is an available rule under the *Servers* category.	
View	To view the profile allocated for each category and available rule, click the *View* button.	
Add	The *Add* button allows users to add the applied rule as required.	
Remove	To delete an existing applied rule, click the *Remove* button.	
Applied Rules	This specifies the applied *Port Forwarding* rule for the selected WAN Connection and the LAN IP.	

8.4.1 Allow Incoming Ping

Enabling the *Incoming Internet Control Message Protocol (ICMP) Ping* will allow Echo requests to come into the gateway. The gateway will respond with an ICMP Echo response message. The option allows the DSL provider or ISP to determine the following:

- The status of the network;
- Tracking and isolating hardware and software problems;
- Testing, measuring and managing networks.

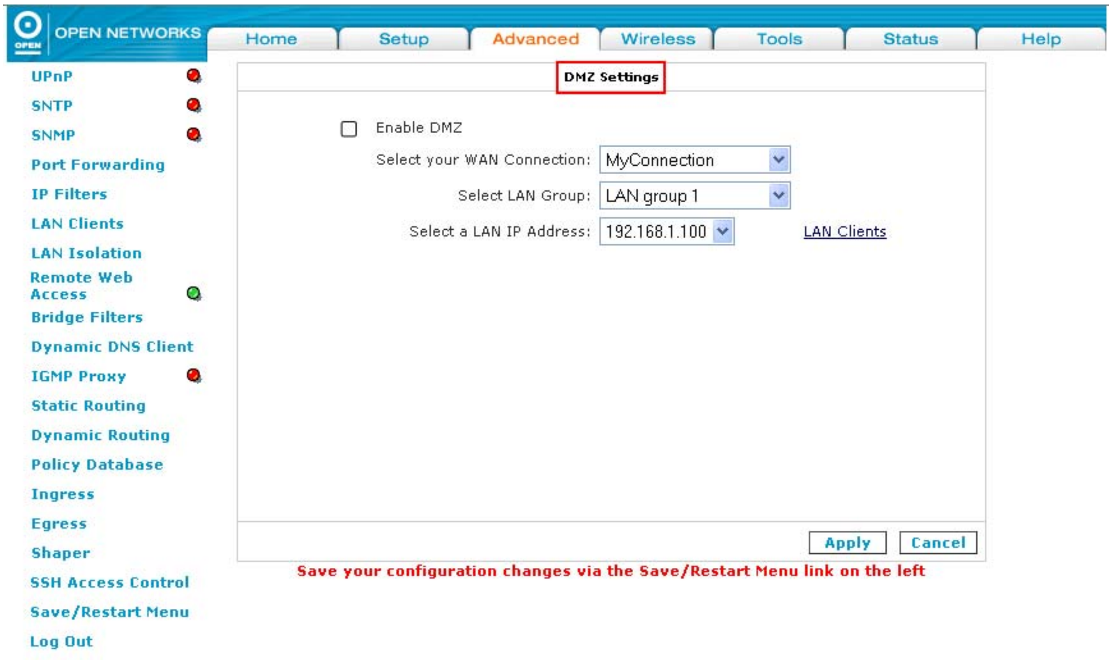
8.4.2 DMZ

Setting a computer on your local network as DMZ forwards any network traffic that is not redirected to another computer via the *Port Forwarding* feature to the computer's IP address. This opens access to the DMZ computer from the Internet.

The DMZ feature is disabled by default.

Follow the steps below to enable *DMZ*.

Step 1: From the ***Port Forwarding*** screen, click the *DMZ* link next to the New IP button. The following page appears:



DMZ Settings

□ Enable DMZ

Select your WAN Connection: MyConnection

Select LAN Group: LAN group 1

Select a LAN IP Address: 192.168.1.100

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable DMZ*** checkbox. This is configurable per LAN segment.

Step 3: From the ***Select Your WAN Connection*** drop-down list, select the connection type for which you wish to add the *DMZ*.

Step 4: From the ***Select LAN Group*** drop-down list, select the LAN group for which you wish to enable the *DMZ*.

NOTE	***It is recommended that the Static IP Addresses rather than the DHCP IP Addresses be used for the DMZ host.***

Step 5: Select the DMZ Host IP Address from the ***Select a LAN IP Address*** drop-down list. If your IP Address is not listed, click the *LAN Clients* link provided and follow the instructions under the *LAN Clients* screen.

Step 6: Click the ***Apply*** button to apply the settings.

Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *DMZ Settings* screen fields and their definitions:

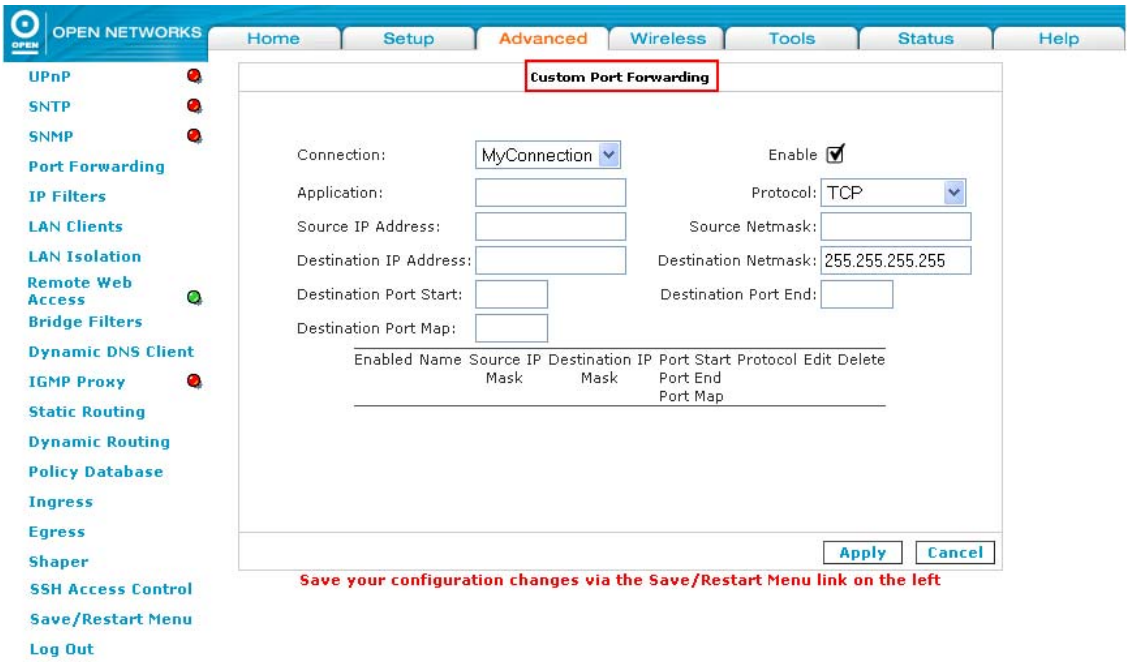
Field	Description
Enable DMZ	Enables/Disables the DMZ feature. The default is set to disabled.
Select your WAN Connection	List of WAN connections defined in the WAN Setup for which the DMZ feature is applied.
Select LAN Group	Select the *LAN Group* for which you wish to enable the DMZ from the drop-down list.
Select a LAN IP Address	This option refers to the Host computer to act as the DMZ.
LAN Clients	This link leads to the *LAN Client* page. Static addresses that are not listed under the LAN IP drop-down list can be added here.

8.4.3 Custom Port Forwarding

The *Custom Port Forwarding* feature is only required when specifying IP Subnets or IP Addresses not listed under *LAN Clients*. This feature allows you to create up to 15 custom Port Forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

To configure *Custom Port Forwarding*, follow the steps below.

Step 1: From the ***Port Forwarding*** screen, click the ***Custom Port Forwarding*** link provided. The following page appears:



Custom Port Forwarding

Connection: MyConnection — Enable ☑

Application: — Protocol: TCP

Source IP Address: — Source Netmask:

Destination IP Address: — Destination Netmask: 255.255.255.255

Destination Port Start: — Destination Port End:

Destination Port Map:

Enabled	Name	Source IP Mask	Destination IP Mask	Port Start Port End Port Map	Protocol	Edit	Delete

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Connection*** drop-down list, select the connection name for which you wish to configure port forwarding.

Step 3: Enter a unique name for the rule in the ***Application*** field.

Step 4: Select the protocol from the ***Protocol*** drop-down list. The options are: *TCP, UDP, TCP and UDP*.

Step 5: Identify the traffic by entering the ***Source IP Address*** and ***Source Netmask***.

Step 6: Enter the ***Destination IP Address*** and ***Destination Netmask*** of the server to which the traffic is being forwarded.

Step 7: Enter the ***Destination Port Start*** and ***Destination Port End*** fields.

Step 8: Enter the Destination Port on which the server will respond, in the ***Destination Port Map*** field.

Step 9: Click the ***Apply*** button to apply the settings.

Step 10: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Custom Port Forwarding* screen fields and their definitions:

Field	Description
Connection	The name of the WAN connection on which you wish to customise *Port Forwarding*.
Enable	This checkbox is enabled by default.
Application	Enter a unique name of the application for which your ports must be opened.
Protocol	Select the protocol for your traffic. The options are: *TCP, UDP* or *TCP and UDP*.
Source IP Address	This is the IP address from which the incoming traffic is allowed. You may enter *0.0.0.0* for all.
Source Netmask	The Network Mask of the interface forwarding the traffic or *0.0.0.0* for all.
Destination IP	This is the LAN-side IP address of the device that is receiving the traffic.
Destination Netmask	The LAN-side destination network mask of the device that is receiving the traffic.
Destination Port Start	The starting destination port number that is made open for this application.
Destination Port End	The ending destination port number that is made open for this application.
Destination Port Map	The destination port number to which traffic is forwarded on the LAN-side. There are two types of port mapping: • ***One-to-One*** where one port is mapped to another; • ***Multiple-to-One*** where multiple ports are mapped to one port.

NOTE	**Wildcard (*) entries are allowed for IP Address/Netmask and Port range fields.**

8.5 IP Filters

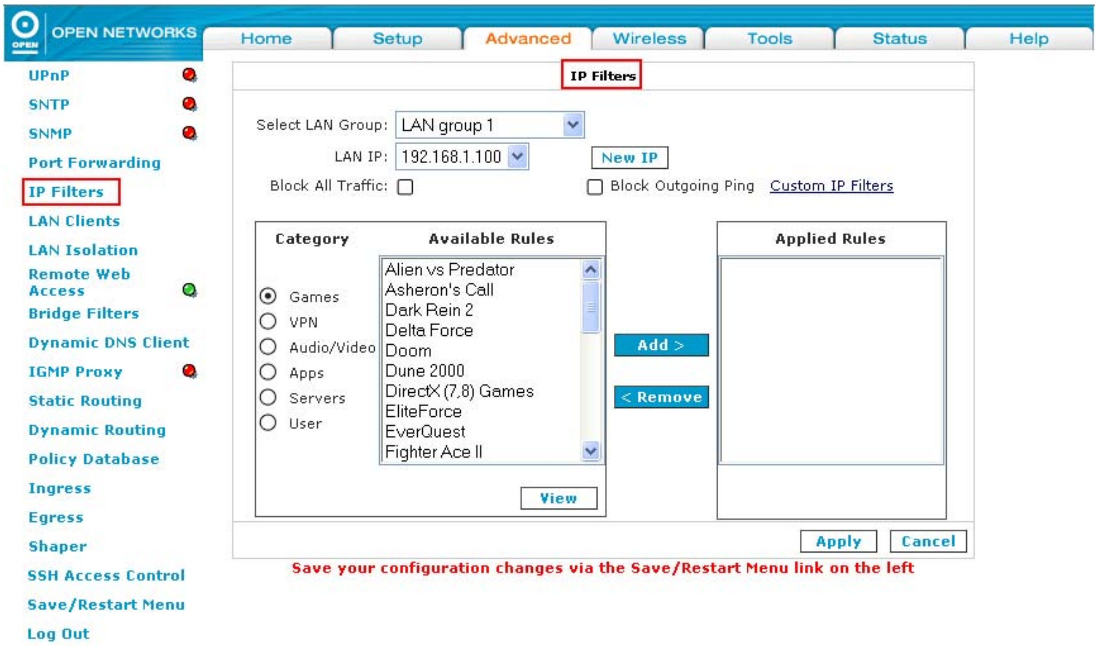
IP Filters allows you to block network access based on a user's computer IP Address on the local LAN. You can use this option to block specific traffic (for e.g., block web access) or any traffic from a computer on your local network.

If the *Block All Traffic* checkbox is checked, all network traffic from that computer will be blocked. You can also add, edit or delete IP Filter rules without using the pre-defined rules.

You will need to use *Custom IP Filters* when specifying IP subnets or IP address that is not listed under *LAN Clients*. Otherwise, new filters can be defined in the *User Category* of the *Available Rules*, and then mapped to the appropriate WAN connection and LAN IP.

To configure *IP Filters*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***IP Filters*** link provided. The following page appears:



Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

Block All Traffic: □

□ Block Outgoing Ping

● Games
○ VPN
○ Audio/Video
○ Apps
○ Servers
○ User

Alien vs Predator
Asheron's Call
Dark Rein 2
Delta Force
Doom
Dune 2000
DirectX (7,8) Games
EliteForce
EverQuest
Fighter Ace II

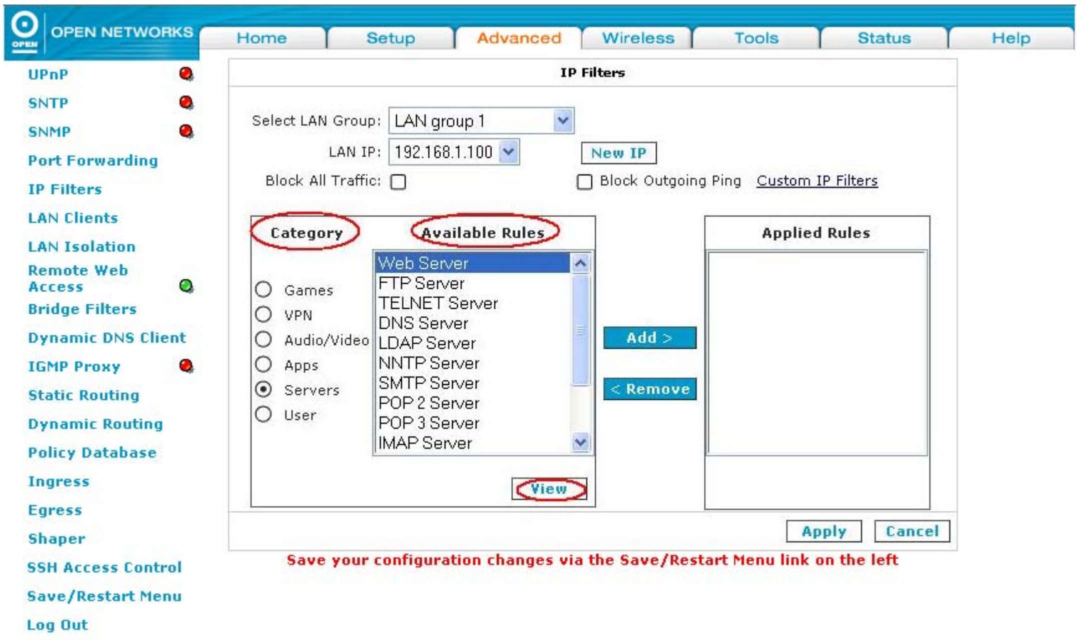
Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Select LAN Group*** drop-down list, select the LAN Group for which you wish to add the rule.

Step 3: From the ***LAN IP*** drop-down list, select the IP address for which you wish to apply the rule. If your IP address is not listed, click the ***New IP*** button and follow the instructions under the *LAN Clients* screen.

NOTE	***It is recommended that Static IP Addresses rather than DHCP IP Addresses be used for IP Filtering.***

Step 4: In the ***Category*** area of the screen, highlight the appropriate radio button for the category. The ***Available Rules*** area displays common Internet services within the category selected. Rules for each service can be viewed by clicking the ***View*** button.



IP Filters

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

Block All Traffic: □ □ Block Outgoing Ping

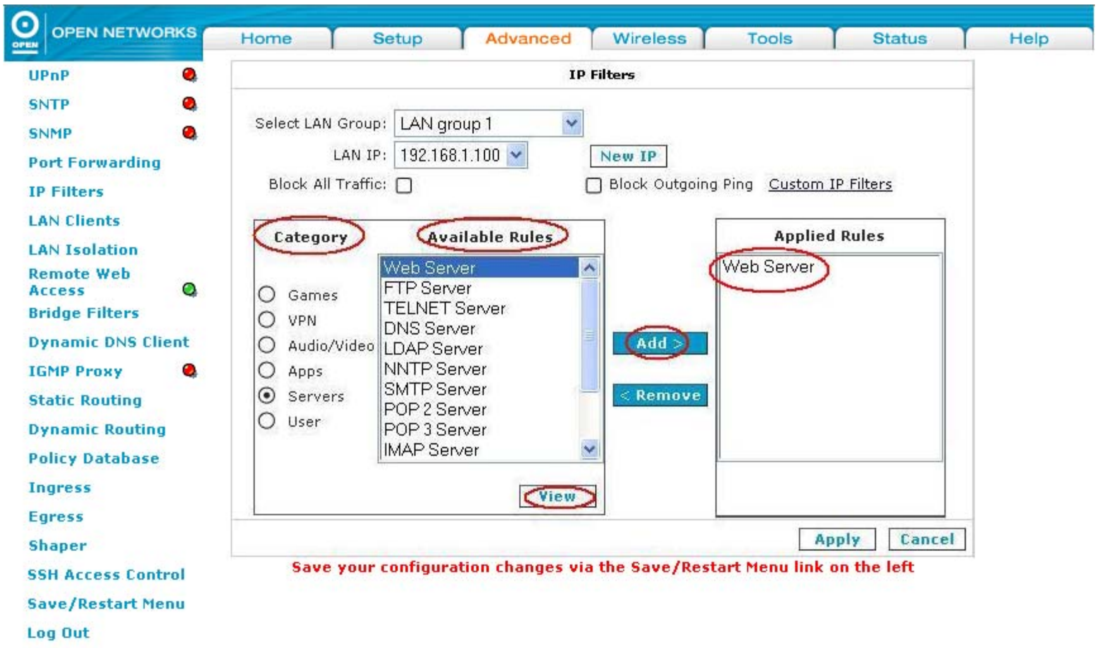
Category: ○ Games ○ VPN ○ Audio/Video ○ Apps ● Servers ○ User

Available Rules: Web Server, FTP Server, TELNET Server, DNS Server, LDAP Server, NNTP Server, SMTP Server, POP 2 Server, POP 3 Server, IMAP Server

Applied Rules

Save your configuration changes via the Save/Restart Menu link on the left

Step 5: To add a rule for this connection, highlight the service or application from the ***Available Rules*** window and click the ***Add*** button. The rule will appear in the ***Applied Rules*** area of the screen.



IP Filters

Select LAN Group: LAN group 1

LAN IP: 192.168.1.100

Block All Traffic: □ □ Block Outgoing Ping

Category: ○ Games ○ VPN ○ Audio/Video ○ Apps ● Servers ○ User

Available Rules: Web Server, FTP Server, TELNET Server, DNS Server, LDAP Server, NNTP Server, SMTP Server, POP 2 Server, POP 3 Server, IMAP Server

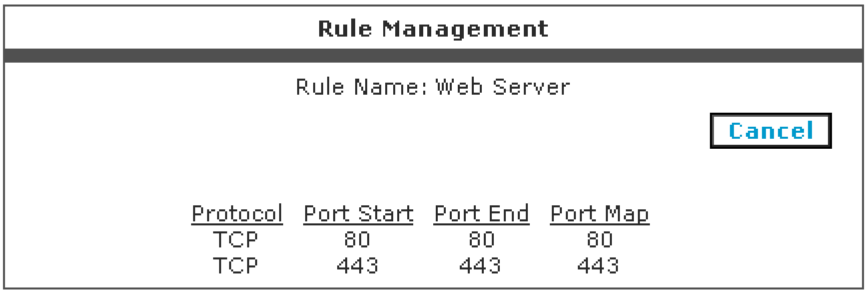
Applied Rules: Web Server

Save your configuration changes via the Save/Restart Menu link on the left

Step 6: Click the ***Apply*** button to apply the settings.

Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *IP Filters* screen fields and their definitions:

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td><b><i>Select LAN Group</i></b></td><td colspan="2">Select the <i>LAN Group</i> where the computer of the port to be forwarded to is a member. LAN Groups can be managed or created under <i>Setup&gt;LAN Configuration</i>.</td></tr>
<tr><td><b><i>LAN IP</i></b></td><td colspan="2">This is the IP address to which the selected ports are filtered. It is recommended that a static IP address be used. This should be defined under the <i>LAN Clients</i> screen.</td></tr>
<tr><td><b><i>New IP</i></b></td><td colspan="2">Clicking on this link leads to the <i>LAN Client</i> screen. Static addresses not listed under the <i>LAN IP</i> drop-down list can be added here.</td></tr>
<tr><td><b><i>Block All Traffic</i></b></td><td colspan="2">Checking this checkbox blocks all IP traffic from the specified LAN IP Address.</td></tr>
<tr><td><b><i>Block Outgoing Ping</i></b></td><td colspan="2">Highlighting this option blocks all ICMP traffic from the specified LAN IP Address. This feature can be used if you host has a virus that attempts a Ping-Of-Death Denial of Service attack.</td></tr>
<tr><td><b><i>Custom IP Filters</i></b></td><td colspan="2">Use this link to create filtering rules that are not pre-defined.</td></tr>
<tr><td rowspan="4"><b><i>Category</i></b></td><td colspan="2">A database of pre-defined IP Filters allow you to apply one or more filtering rules to one or more defined LAN groups. The categories and rules available include: <i>Games, VPN, Audio/Video, Apps, Servers</i> and <i>Users</i>.
E.g. Web servers specify the following profile.
Rule Management
Rule Name: Web Server

<table><tr><th>Protocol</th><th>Port Start</th><th>Port End</th><th>Port Map</th></tr><tr><td>TCP</td><td>80</td><td>80</td><td>80</td></tr><tr><td>TCP</td><td>443</td><td>443</td><td>443</td></tr></table>
The categories available for IP Filters include: Games, VPN, Audio/Video, Apps (or applications), Servers and Users.</td></tr>
<tr><td><b><i>Games</i></b></td><td>Internet users are able to play Internet games when this function is configured. Examples of the games list include Aliens and Predators, Doom, Dune 2000, etc.</td></tr>
<tr><td><b><i>VPN</i></b></td><td>The default VPN settings are: IPSEC L2TP and PPTP.</td></tr>
<tr><td><b><i>Audio/Video</i></b></td><td>Net2Phone, Netmeeting and Quick Time 4 Server can be configured for Audio/Video services.</td></tr>
</table>

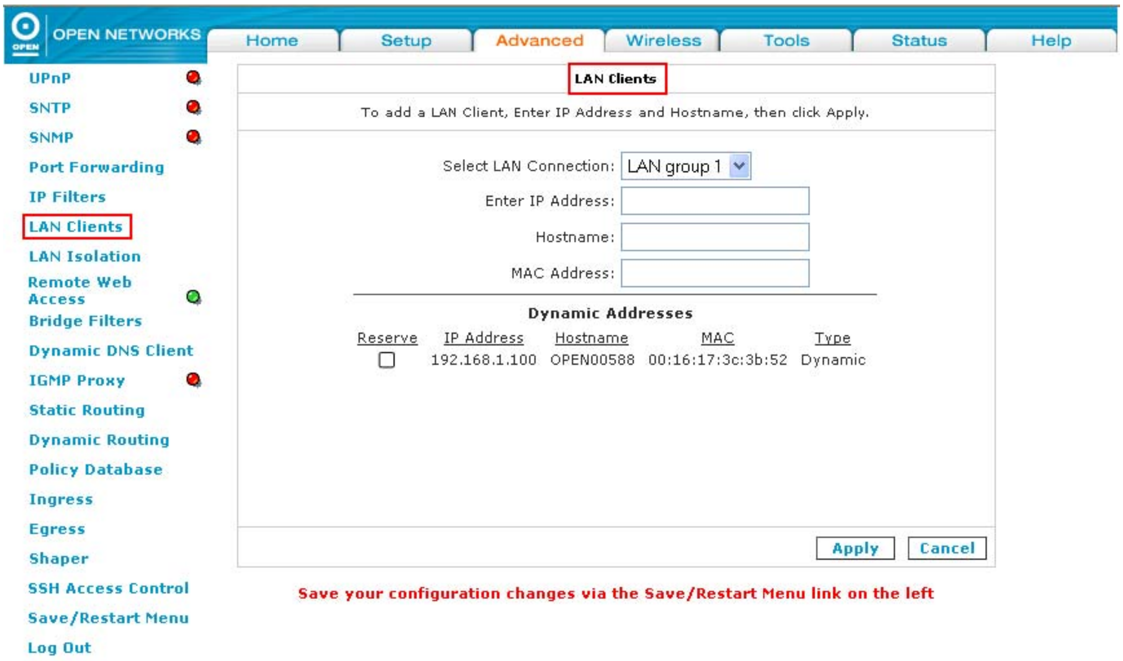
Field	Description	
	Apps	Various applications are set as defaults under this category, including: VNC, Win2K terminal, PcAnywhere, etc.
	Servers	The default servers include: Web Servers, FTP server, Telnet Server, and so on.
	Users	New user rules can be added here.
Available Rules	Each category has *Available Rules* that are pre-defined. Default rules such as Netmeeting is available under the *Audio/Video* category and Web Server is an available rule under the *Servers* category.	
Applied Rules	This specifies the applied IP filtering for the selected LAN IP Address.	

8.6 LAN Clients

All current DHCP clients are automatically registered in the LAN Client database as a dynamic address if DHCP is used. If a static IP address is used on a LAN device and you wish to apply IP rules to this address, you must add the IP address to the LAN Clients list. Once the IP address has been added, Port Forwarding and Access Control rules can be added to this IP address.

To configure *LAN Clients*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***LAN Clients*** link provided. The following page appears:



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

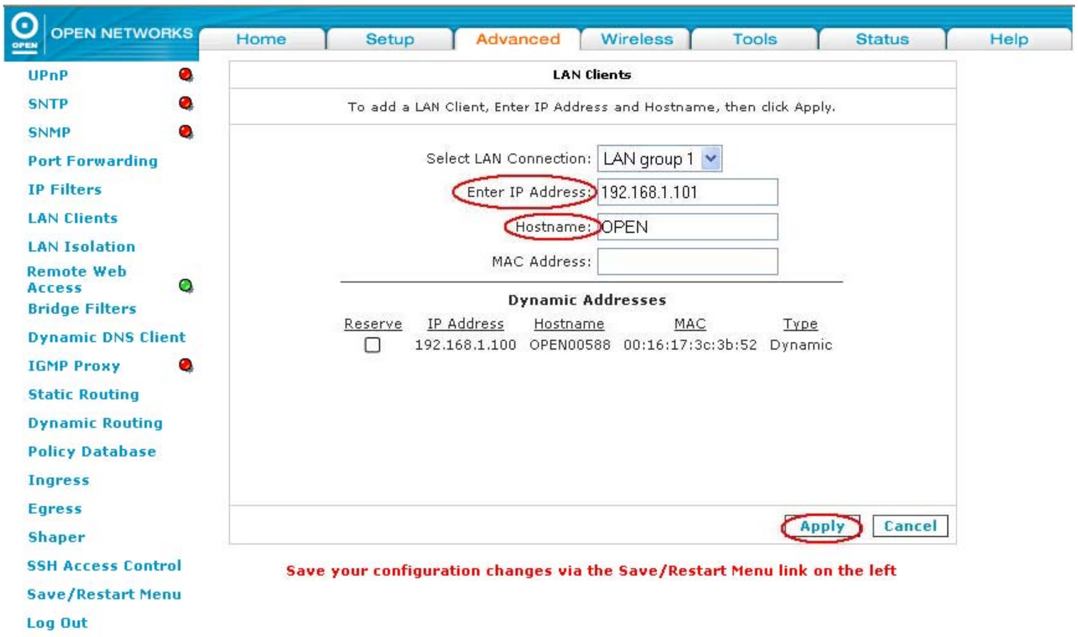
Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
☐	192.168.1.100	OPEN00588	00:16:17:3c:3b:52	Dynamic

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Select LAN Connection*** drop-down list, select the LAN group for which you wish to apply the LAN Client.

Step 3: To add the LAN Client Address, enter the LAN IP Address in the ***Enter IP Address*** field, e.g. *192.168.1.101.*



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address: 192.168.1.101

Hostname: OPEN

MAC Address:

Dynamic Addresses

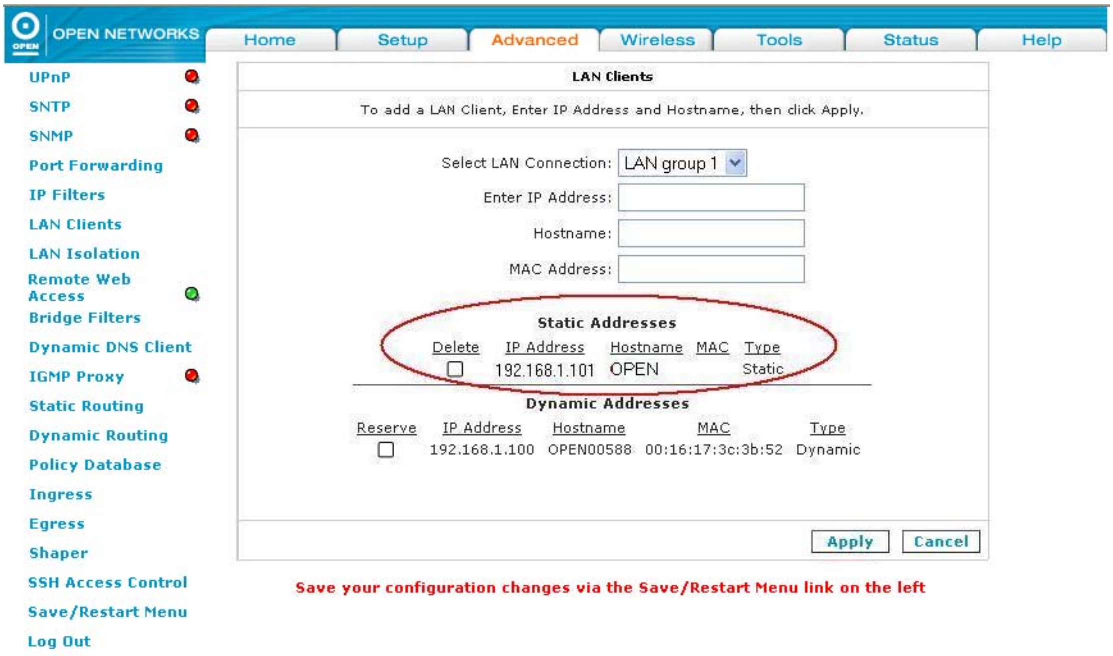
Reserve	IP Address	Hostname	MAC	Type
☐	192.168.1.100	OPEN00588	00:16:17:3c:3b:52	Dynamic

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Enter the LAN's host name in the ***Host Name*** field if required. This is an optional field.

Step 5: Enter the MAC address of the LAN Client in the ***MAC Address*** field.

Step 6: Click the ***Apply*** button to apply the settings. The IP address is allocated and it shows up in the list of LAN clients as a *Static Type*.



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Static Addresses

Delete	IP Address	Hostname	MAC	Type
☐	192.168.1.101	OPEN		Static

Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
☐	192.168.1.100	OPEN00588	00:16:17:3c:3b:52	Dynamic

Save your configuration changes via the Save/Restart Menu link on the left

Step 7: To reserve an IP entry, check the ***Reserve*** checkbox.

Step 8: Click the ***Apply*** button to apply the amended settings.

Step 9 To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *LAN Clients* screen fields and their definitions:

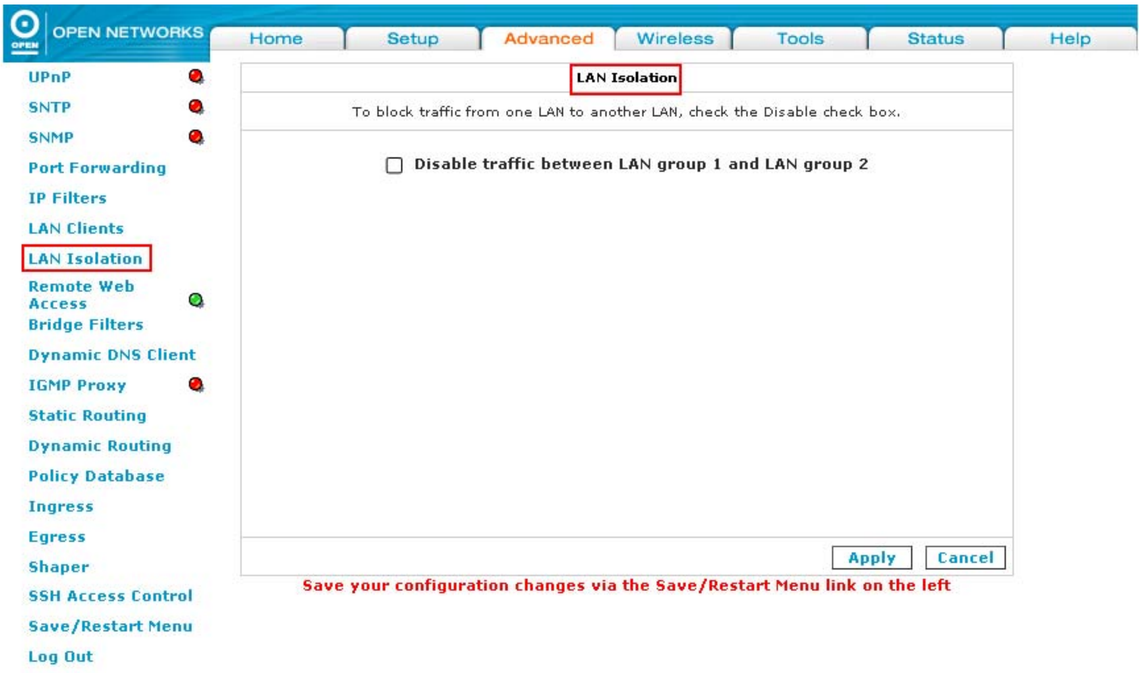
Field	Description
Select LAN Connection	Select the *LAN Group* to which you are adding the new LAN client.
Enter IP Address	The IP address of the server / host that you want to use for Port Forwarding or Access Control must be defined here.
Hostname	An optional hostname can be assigned to the above address.
MAC Address	All MAC addresses of the host can be assigned here.

8.7 LAN Isolation

LAN Isolation allows you to disable the flow of packets between two LAN groups. This allows you to secure information in the private portions of the LAN from other publicly accessible LAN segments.

Follow the steps below to block traffic from one LAN to another using *LAN Isolation.*

Step 1: From the ***Advanced*** tab, click the ***LAN Isolation*** link provided. The following page appears:



LAN Isolation

To block traffic from one LAN to another LAN, check the Disable check box.

□ Disable traffic between LAN group 1 and LAN group 2

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: If you wish to disable traffic between LAN groups, check the ***Disable traffic between LAN group 1 and LAN group 2*** checkbox as required.

Step 3: Click the ***Apply*** button to apply the settings.

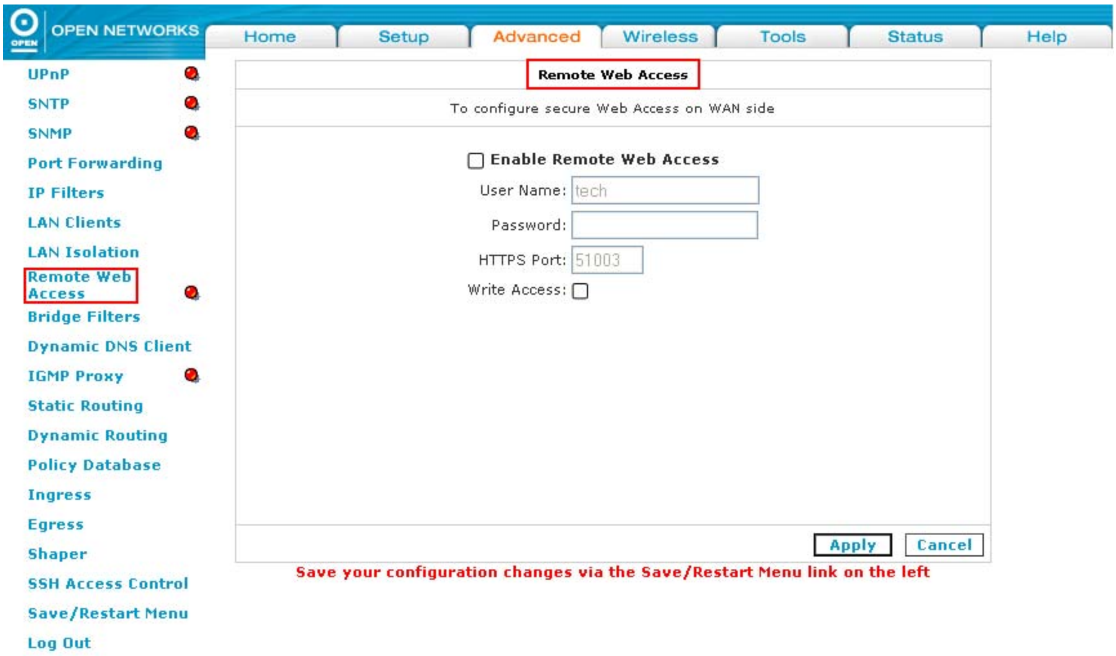
Step 4: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.8 Remote Web Access

The Remote Web Access page allows you to give temporary permission to a user to access your router from the WAN side. From the moment the account is enabled, the user is expected to log in within 20 minutes or the account expires. Once the user is logged in, an inactive session of more than 20 minutes will log the user out and the account expires.

To enable a temporary user account for remote access, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Remote Web Access*** link provided. The following page appears:



Remote Web Access

To configure secure Web Access on WAN side

□ Enable Remote Web Access

User Name: tech

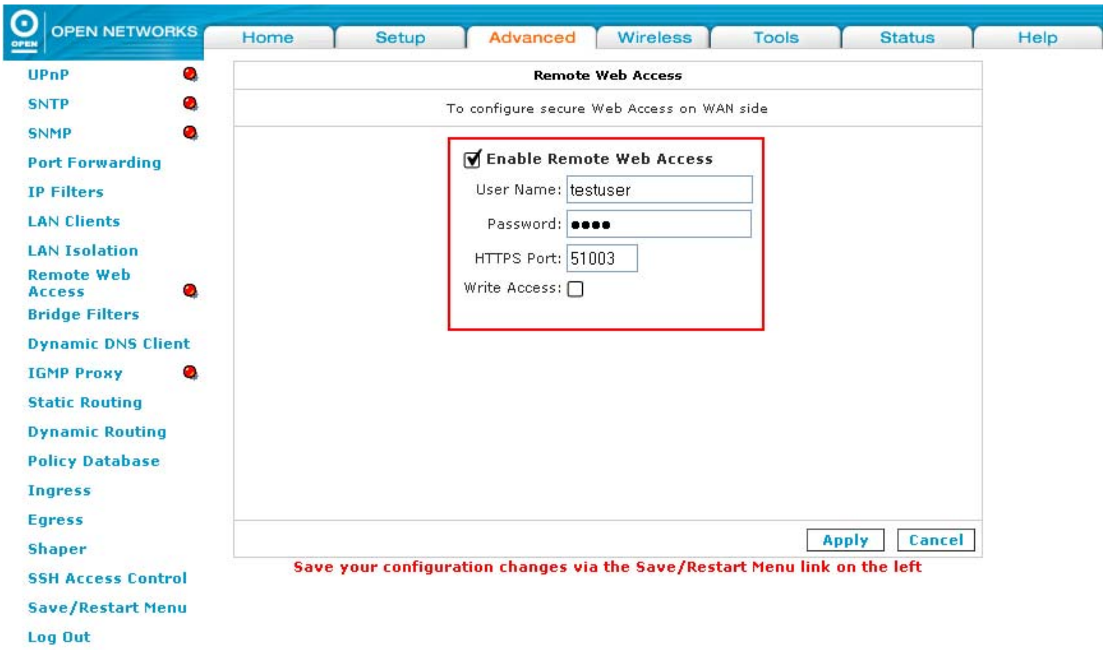
Password:

HTTPS Port: 51003

Write Access: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable Remote Web Access*** checkbox to give the account read and write access to the iConnect625W router.



Remote Web Access

To configure secure Web Access on WAN side

☑ Enable Remote Web Access

User Name: testuser

Password: ●●●●

HTTPS Port: 51003

Write Access: □

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter a unique user name in the ***User Name*** field for the WAN access account as shown above.

Step 4: Enter the user password in the ***Password*** field for the WAN access account as shown above.

Step 5: The default port number in the ***Port*** field is *51003*. This is the port number to be opened for the temporary WAN access.

Step 6: Click the ***Apply*** button to apply the settings.

Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

8.9 Bridge Filters

The Bridge filtering mechanism enables users to define rules which allow/deny access through the iConnect625W, via the hardware (MAC Address) of network devices.

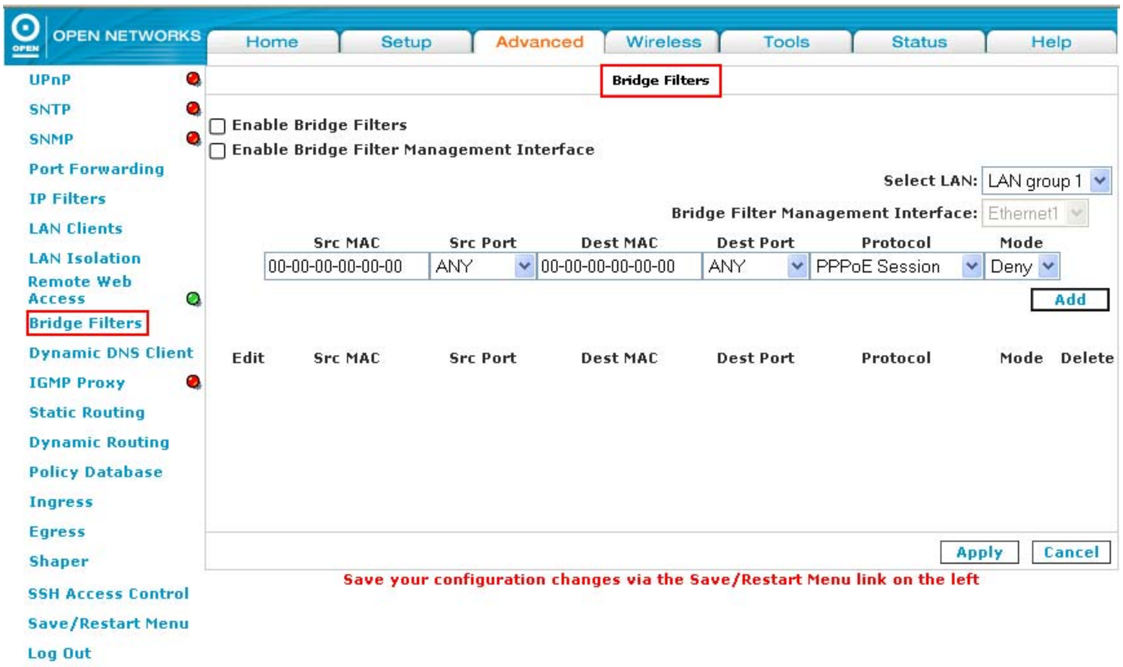
The User Interface for *Bridge Filter* allows the following functionality:

- Enabling filter rules;
- Adding / Editing / Deleting filter rules.

When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow/deny) is performed.

To enable *Bridge Filters*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Bridge Filters*** link provided. The following page appears:



Bridge Filters

☐ Enable Bridge Filters
☐ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

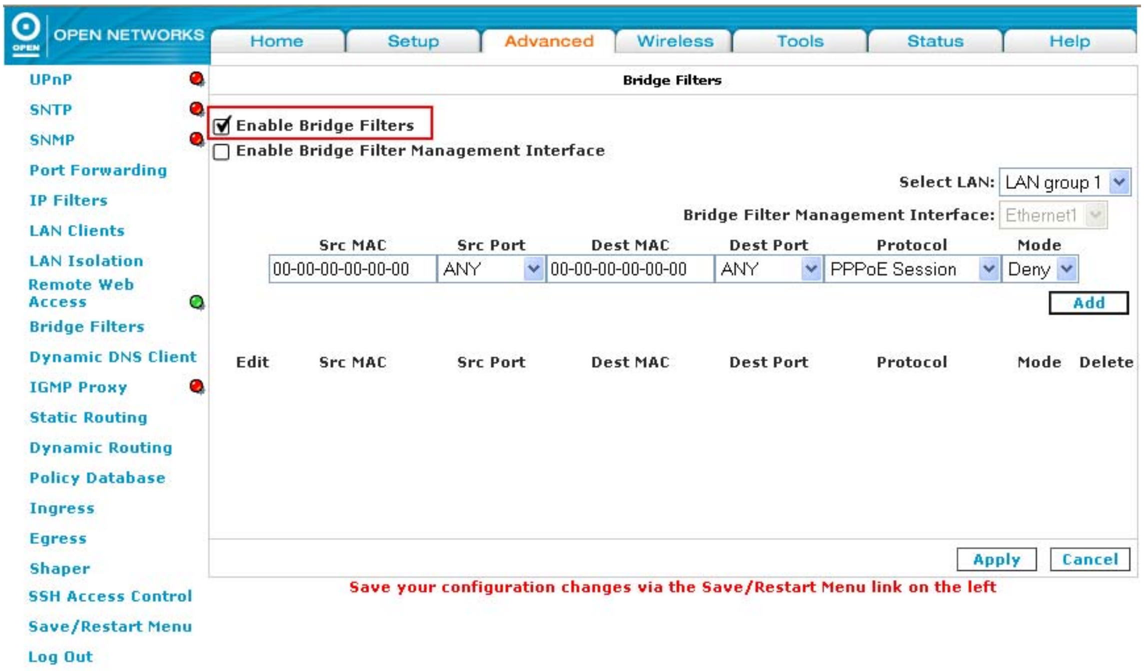
Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable Bridge Filters*** checkbox to enable this feature as shown and click the ***Apply*** button.



Bridge Filters

☑ Enable Bridge Filters

□ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

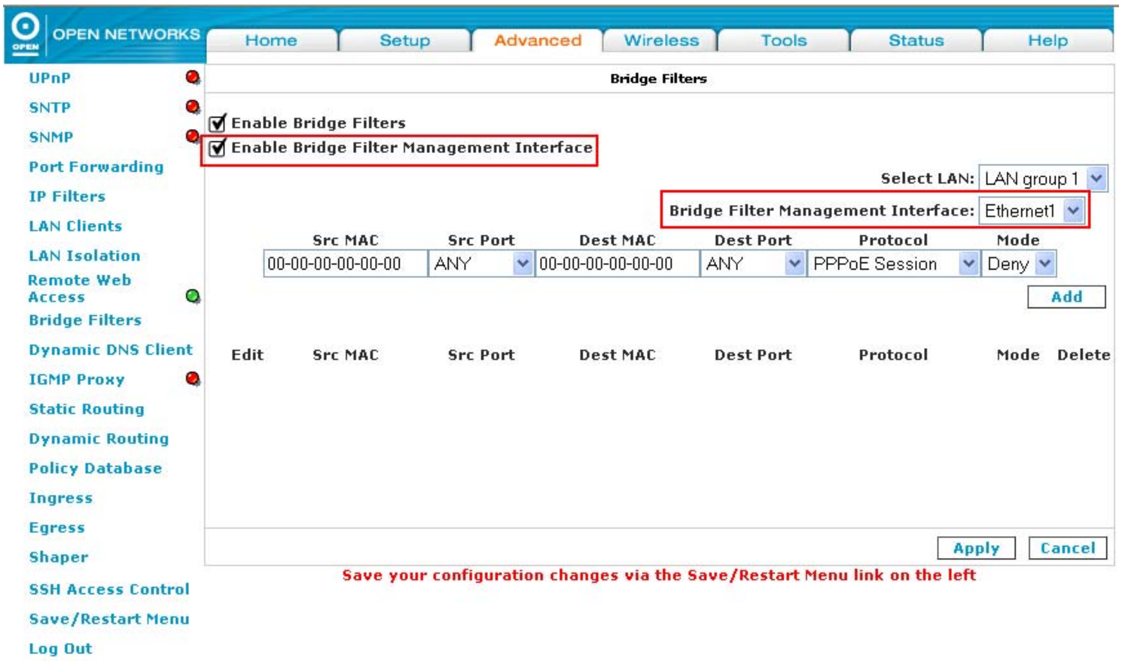
Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Check the ***Bridge Filter Management Interface*** checkbox as shown below to enable the *Bridge Filter Management Interface* field. This ensures that you do not get locked out of the iConnect625W on the interface of the LAN group specified in the next two fields.



Bridge Filters

☑ Enable Bridge Filters

☑ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Select the LAN group from the ***Select LAN*** drop-down list.

Step 5: Enter the source MAC address in the ***SRC MAC*** field. It must be in *xx-xx-xx-xx-xx-xx* format.

Step 6: Select the source port from the ***SRC Port*** drop-down list. You can choose from *Any, Ethernet, WLAN or WAN Bridge Connection Port* for the particular bridge, if available.

Step 7: Enter the destination MAC address in the ***Dest MAC*** field.

Step 8: Select the destination port from the ***Dest Port*** drop-down list.

NOTE	**Entering 00-00-00-00-00-00 in the Source or Destination MAC fields means that ALL MAC addresses are matched.**

Step 9: Select the protocol to be filtered from the ***Protocol*** drop-down list. You can choose from the following options: *PPPoE Session, PPPoE Discovery, IPX-Ethernet II, RARP, IPv6, IPv4* and *Any.*

Step 10: Select the mode from the ***Mode*** drop-down list. The options are *Allow* or *Deny.*

Step 11: Click the ***Add*** button.

NOTE	**A maximum of 20 MAC filter rules can be supported with bridge filtering.**

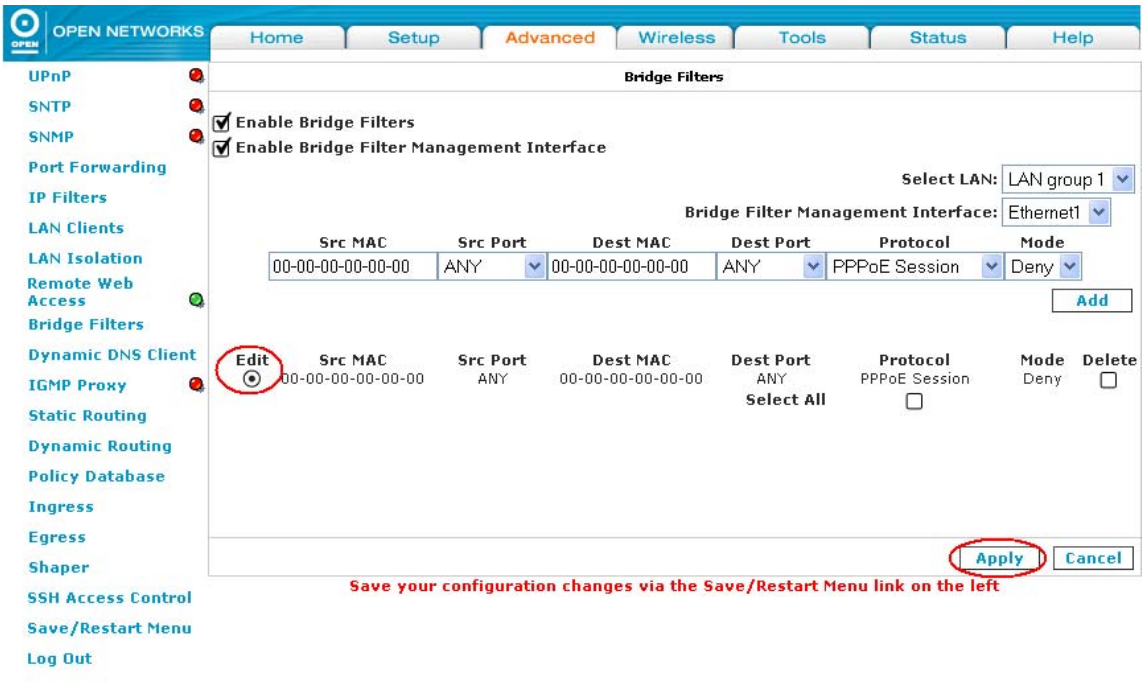
Step 11: Click the ***Apply*** button to apply the settings.

Step 12: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.9.1 Editing Bridge Filters

Follow the steps below to edit an existing bridge filter.

Step 1: From the ***Bridge Filter*** screen, highlight the ***Edit*** radio button from existing filter rules and edit the rule, as shown below.



Bridge Filters

☑ Enable Bridge Filters

☑ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete
●	00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny	□

Select All □

Save your configuration changes via the Save/Restart Menu link on the left

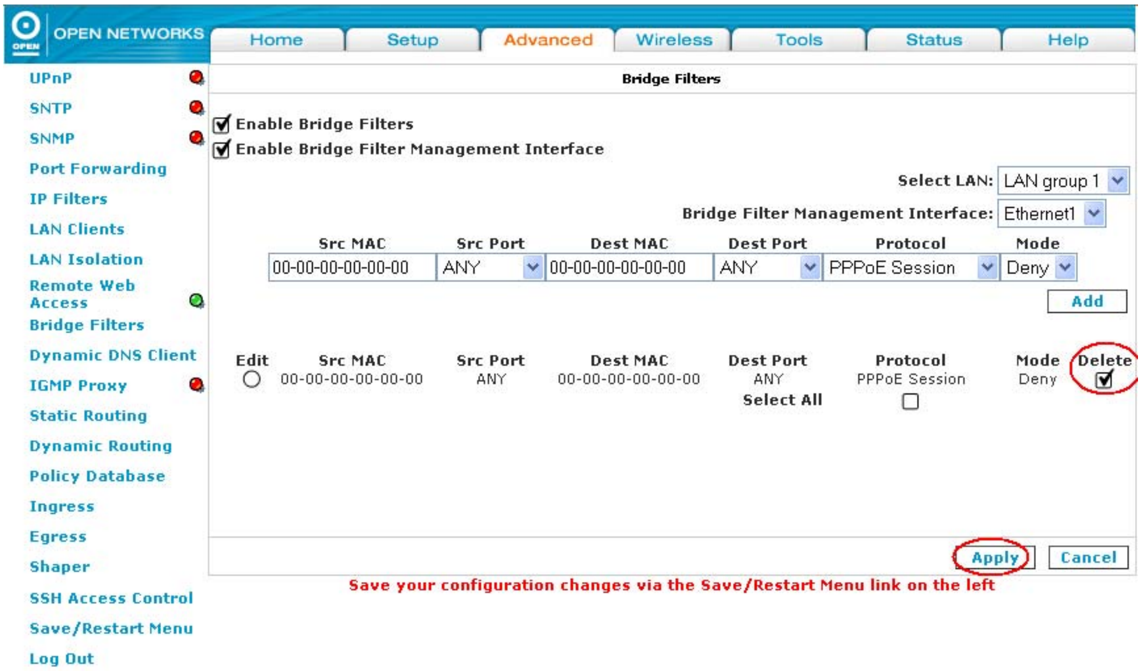
Step 2: Make the required changes to the ***MAC Address***, ***Protocol*** and ***Mode*** options and click the ***Apply*** button to apply the settings.

Step 3: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.9.2 Deleting Filter Rules

Follow the steps below to delete an existing bridge filter.

Step 1: From the ***Bridge Filter*** screen, check the ***Delete*** checkbox for the rule to be removed as shown in the image below.



Bridge Filters

☑ Enable Bridge Filters

☑ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete
○	00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny	☑
				Select All	□		

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Click the ***Apply*** button to apply the settings.

Step 3: To save your configuration, please refer to the section under ***Save / Restart Menu***.

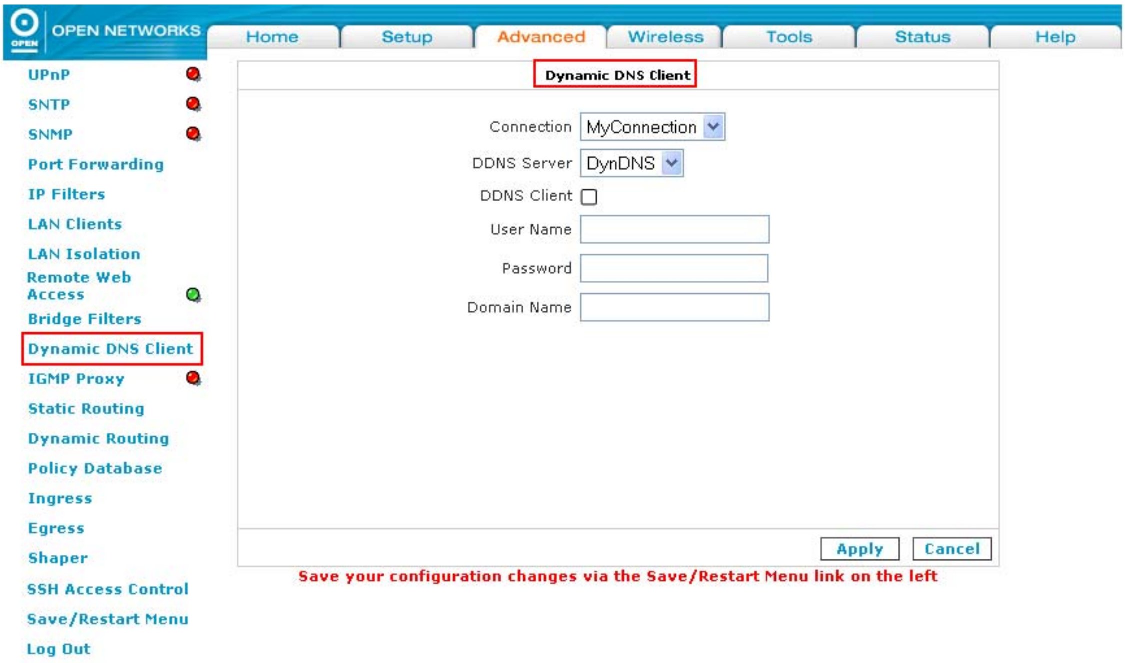
8.10 Dynamic DNS Client

Dynamic DNS allows you to register with a Dynamic DNS provider. Each time you connect to the Internet, your ISP assigns a different IP address to your iConnect625W router.

The Dynamic DNS feature allows you to register your iConnect625W router with a DNS server and access it each time using the same host name. It is useful in web hosting and FTP services.

To enable *Dynamic DNS Client*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Dynamic DNS Client*** link provided. The following page appears:



Dynamic DNS Client

Connection MyConnection

DDNS Server DynDNS

DDNS Client □

User Name

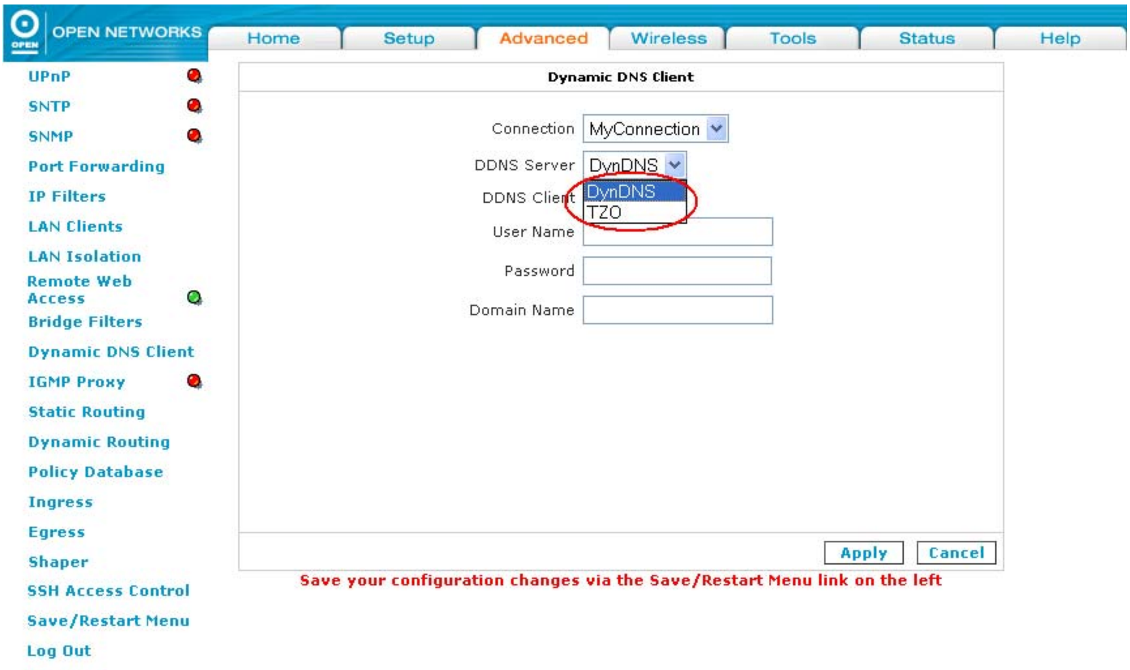
Password

Domain Name

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The ***Connection*** field is defaulted to the iConnect625W's WAN connection over which your router will be accessed. Select another connection from the ***Connection*** drop-down list.

Step 3: Select the *DynDNS* for the ***DDNS Server*** option. If there are different DDNS service providers, select the other options provided as shown below.



Connection: MyConnection
DDNS Server: DynDNS
DDNS Client
User Name
Password
Domain Name

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Check the ***DDNS Client*** checkbox to enable the DDNS client feature for the WAN connection.

Step 5: Enter your ***User Name*** and ***Password*** fields using the same user name and password you have specified during the registration of the DNS hostname. These fields are mandatory.

Step 6: Enter the domain name of the DNS server into the ***Domain Name*** field.

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save/Restart Menu***.

8.11 IGMP Proxy

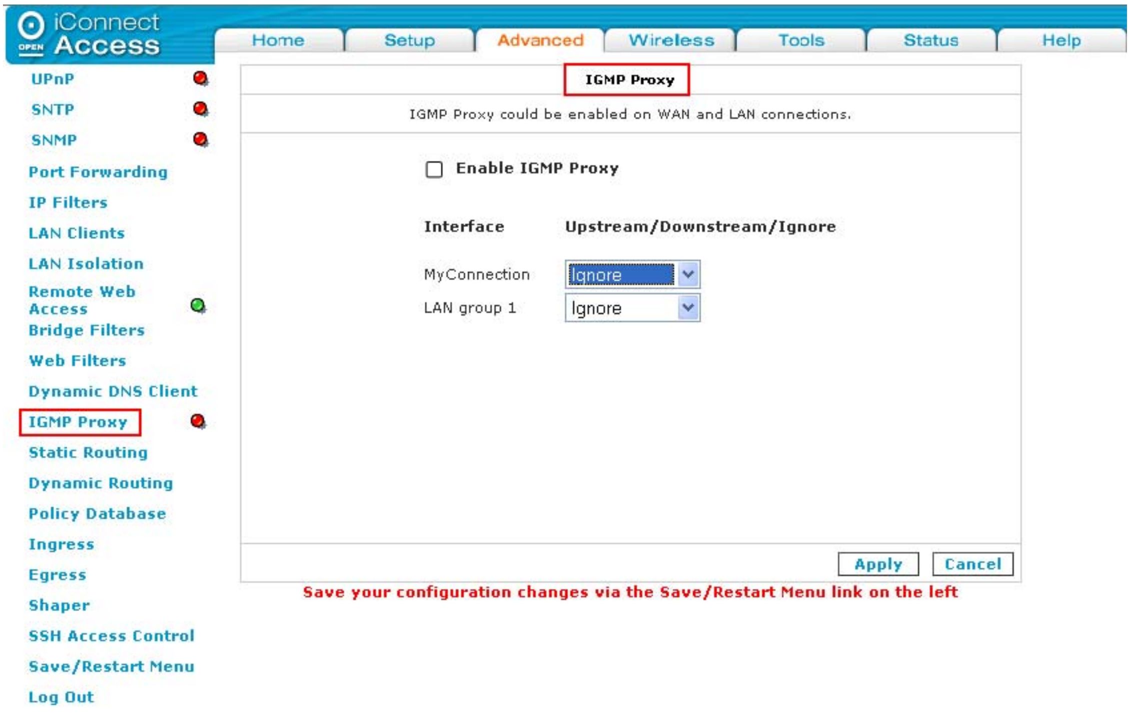
The iConnect625W router supports IGMP Proxy that handles IGMP messages. When enabled, the iConnect625W acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side. Multicasting is useful when the same data needs to be sent to more than one device.

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a "host group". A host group is a set of one or more hosts identified by the same destination IP address. The following statements apply to host groups:

- Anyone can join or leave a host group at will;
- There are no restrictions on a host's location;
- There are no restrictions on the number of members that may belong to a host group;
- Non-group members may send UDP datagrams to the host group.

To enable *IGMP Proxy*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***IGMP Proxy*** link provided. The following page appears:



IGMP Proxy

IGMP Proxy could be enabled on WAN and LAN connections.

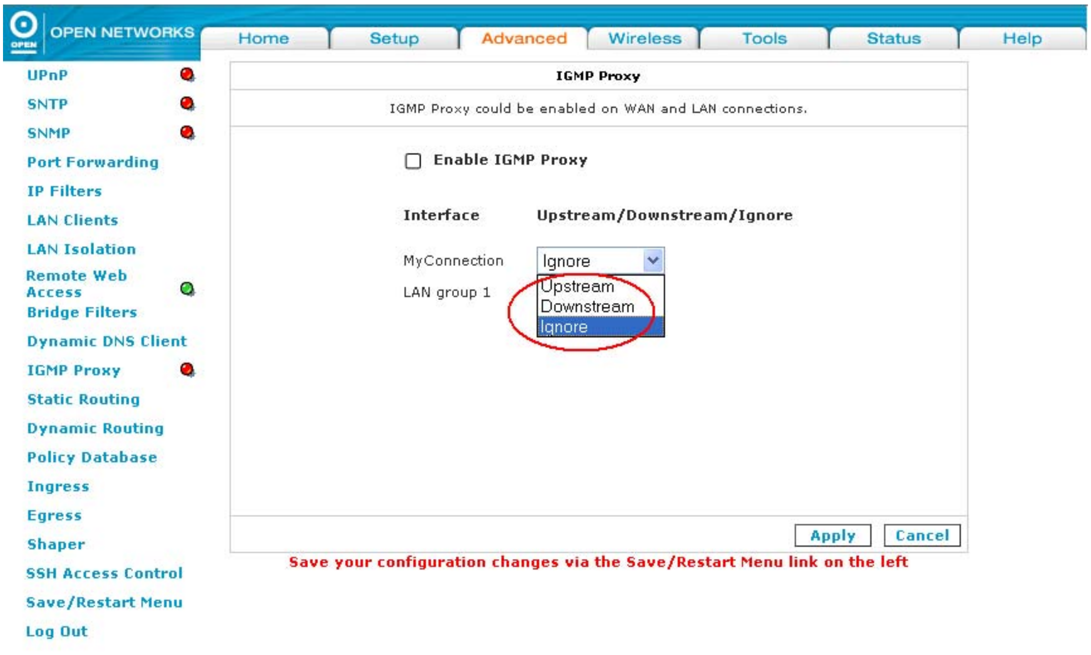
□ Enable IGMP Proxy

Interface	Upstream/Downstream/Ignore
MyConnection	Ignore
LAN group 1	Ignore

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable IGMP Proxy*** checkbox to enable IGMP proxy.

Step 3: Configure the ***MyConnection*** and ***LAN Group 1*** interfaces using the *Upstream*, *Downstream* or *Ignore* options as shown below.



IGMP Proxy

IGMP Proxy could be enabled on WAN and LAN connections.

□ Enable IGMP Proxy

Interface	Upstream/Downstream/Ignore
MyConnection	Ignore
LAN group 1	

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Click the ***Apply*** button to apply the settings.

Step 5: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *IGMP Proxy* screen fields and their definitions:

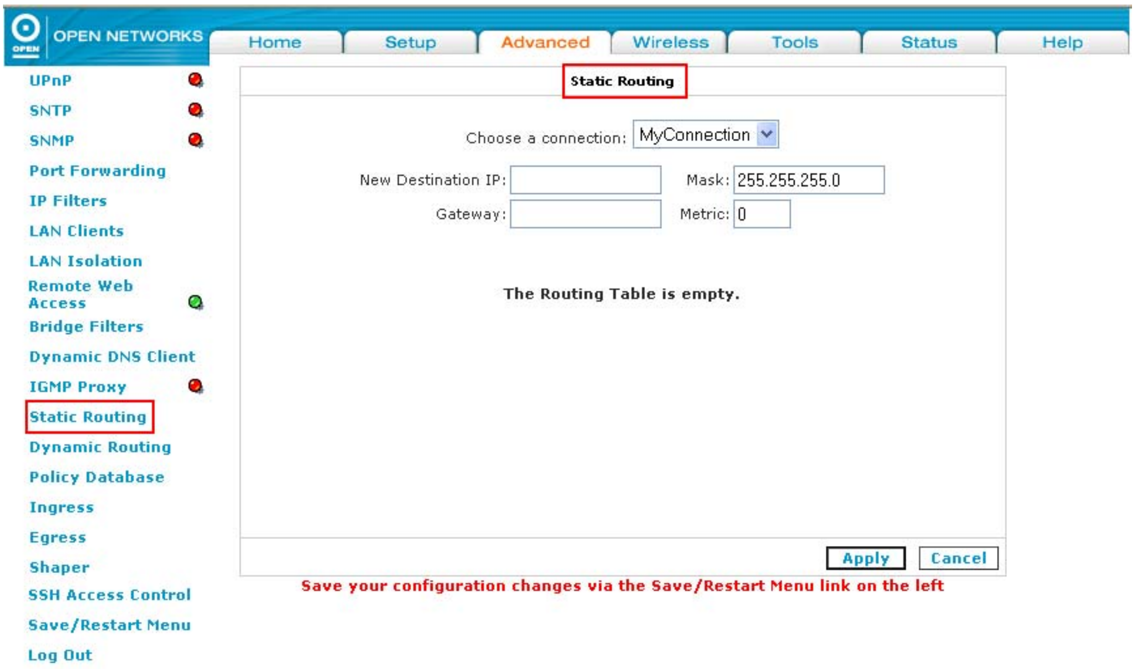
Field	Description	
Enable IGMP Proxy	Checking the *Enable IGMP Proxy* checkbox allows you to enable the iConnect625W router to receive multicast traffic for your available WAN and LAN connections. Multicast delivers IP packets to a group of hosts on the network. IGMP is a session layer (Layer 3) protocol used to establish membership in a Multicast group.	
Interface	You can configure one of the following options for each WAN or LAN interface.	
	Upstream	The interface that IGMP requests from the hosts is sent to the multicast router.
	Downstream	The interface data from the multicast router are sent to hosts in the multicast group database.
	Ignore	No IGMP request nor data multicast are forwarded when you select this option.
MyConnection	Configure using one of the 3 options for your WAN connection: *Upstream, Downstream* or *Ignore* options.	
LAN Group 1	Configure using one of the 3 options for your LAN connection: *Upstream, Downstream* or *Ignore* options.	

8.12 Static Routing

If the iConnect625W is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway down which network information must travel to reach a specific host or network.

To enable *Static Routing*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Static Routing*** link provided. The following page appears:



Static Routing

Choose a connection: MyConnection

New Destination IP:

Mask: 255.255.255.0

Gateway:

Metric: 0

The Routing Table is empty.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select a connection type from the ***Choose a Connection*** drop-down list.

Step 3: Enter the new destination IP for the remote LAN network or host to which you wish to assign a static route in the ***New Destination IP*** field.

Step 4: Enter a subnet mask in the ***Mask*** field or leave the default value *255.255.255.0* as it is.

Step 5: Enter the IP address of the new device to connect to the remote network or host in the ***Gateway*** field.

Step 6: Enter a metric in the ***Metric*** field or leave the default value *0* as it is.

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Static Routing* screen fields and their definitions:

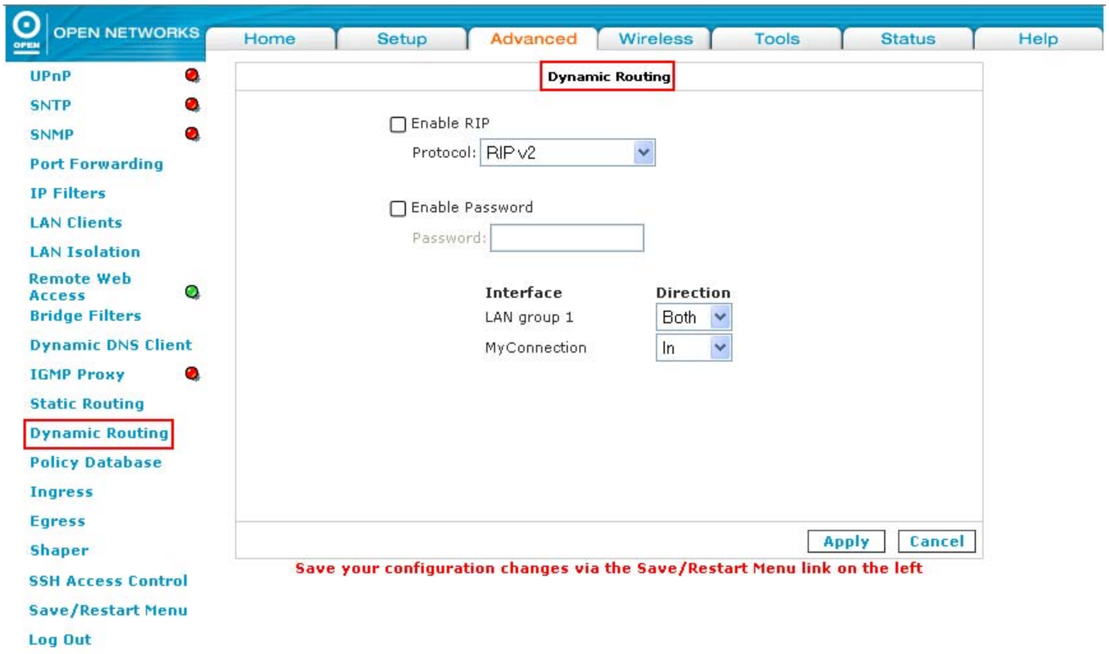
Field	Description
Choose a Connection	Choose the connection profile from the drop-down list provided.
New Destination IP	The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route.
Mask	Enter the subnet mask for the destination network. Use 255.255.255.255 for a host route. The subnet mask identifies which portion of an IP address is the network portion, and which portion of an IP address is the host portion.
Gateway	The Gateway IP address should be the IP address of the gateway device that allows for contact between the gateway and the remote network or host. The iConnect625W examines the destination address in the packet header and passes the packet along to this gateway if the address is within the specified range. A packet may go through 30 or more routers in its travels from one host computer to another.
Metric	This field defines the number of hops between network nodes that data packets travel. Enter the metric value to be assigned to this static route. If you are unsure, leave the default value of *0* as it is.

8.13 Dynamic Routing

Dynamic Routing allows the iConnect625W router to automatically adjust to physical changes in the network. It determines the route through which the package travels based on the least number of hops between the source and the destination. RIP protocol regularly broadcasts routing information to other routers on the network.

To enable *Dynamic Routing*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Dynamic Routing*** link provided. The following page appears:



Dynamic Routing

□ Enable RIP

Protocol: RIP v2

□ Enable Password

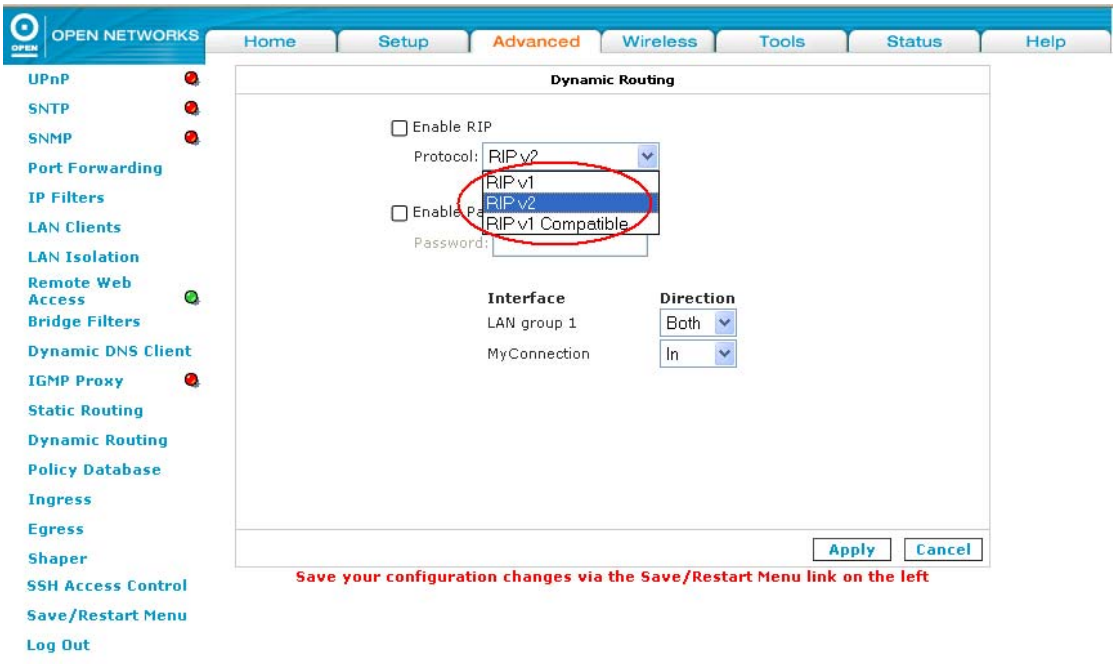
Password:

Interface	Direction
LAN group 1	Both
MyConnection	In

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable RIP*** checkbox.

Step 3: From the ***Protocol*** drop-down list, select the RIP version as appropriate. The versions provided are: *RIPv1, RIPv2* and *RIPv1 Compatible*, as shown below.



□ Enable RIP

Protocol: RIP v2

RIP v1
RIP v2
RIP v1 Compatible

□ Enable Pa

Password:

Interface	Direction
LAN group 1	Both
MyConnection	In

Save your configuration changes via the Save/Restart Menu link on the left

NOTE	**The same RIP protocol should be used to enable dynamic routing on all routers on the network.**

Step 4: Check the ***Enable Password*** checkbox as appropriate.

Step 5: If you have checked ***Enable Password*** checkbox, enter a password in the ***Password*** field. This is an optional field for additional security purposes.

Step 6: Select the ***Direction*** for the LAN Group 1 and *MyConnection* interfaces from the drop-down list. The options are: *None, In, Out* and *Both*.

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Dynamic Routing* screen fields and their definitions:

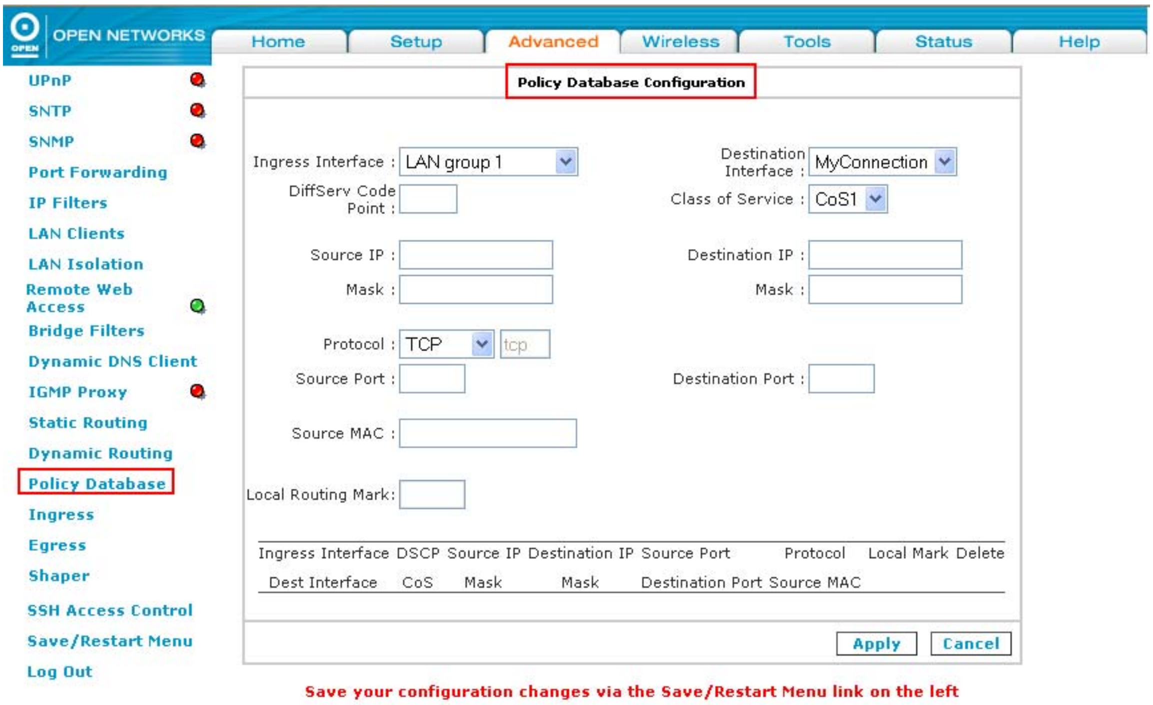
<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td><b><i>Enable RIP</i></b></td><td colspan="2">This enables RIP routing on the iConnect625W router.</td></tr>
<tr><td><b><i>Protocol</i></b></td><td colspan="2">There are three versions of RIP:
1. RIP v1 (UDP Protocol)
2. RIP v2 (multicast protocol)
3. RIP v1-Compatible (UDP Protocol with multicast format)
Routers using RIP v1 or RIP v1-Compatible protocol can talk to each other, but not to routers using RIP v2 protocol.</td></tr>
<tr><td rowspan="5"><b><i>Direction</i></b></td><td colspan="2">Direction determines the means through which RIP routers will be updated. Select one of the options below.</td></tr>
<tr><td><b><i>In</i></b></td><td>Selecting <i>In</i> means that the iConnect625W router will only incorporate received RIP information.</td></tr>
<tr><td><b><i>Out</i></b></td><td>Selecting <i>Out</i> means that the iConnect625W router will only send out RIP information.</td></tr>
<tr><td><b><i>Both</i></b></td><td>Selecting <i>Both</i> means that the iConnect625W router will incorporate received RIP information and send out updated RIP information.</td></tr>
<tr><td><b><i>None</i></b></td><td>Select this option if the function is not required.</td></tr>
<tr><td><b><i>Enable Password</i></b></td><td colspan="2">Simple password authentication for RIP v2 was defined in RFC 1723. If you intend to use password authentication, you must enable your password here.</td></tr>
<tr><td><b><i>Password</i></b></td><td colspan="2">Type the RIPv2 authentication password here. Ensure that all routers are configured with this password for RIPv2 to work.</td></tr>
</table>

8.14 Policy Database

The Policy Database page enables you to configure policy routing and QoS. Policy Database involves routing packets on the basis of various fields in the packet. For example, the current routing algorithms make decisions based on the destination address, i.e. only the Destination IP Address and subnet mask are supported.

To configure *Policy Database*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Policy Database*** link provided. The following page appears:



Policy Database Configuration

Ingress Interface : LAN group 1

Destination Interface : MyConnection

DiffServ Code Point :

Class of Service : CoS1

Source IP :

Destination IP :

Mask :

Mask :

Protocol : TCP tcp

Source Port :

Destination Port :

Source MAC :

Local Routing Mark:

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete
Dest Interface	CoS	Mask	Mask	Destination Port	Source MAC		

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the incoming traffic interface from the ***Ingress Interface*** drop-down list. The options are: *LAN Interfaces, WAN Interfaces, Locally generated* and *Not Applicable (N/A*).

Step 3: Select the outgoing connection from the ***Destination Interface*** drop-down list.

Step 4: Enter the ***DiffServ Code Point*** in the field provided. This has to be configured in conjunction with other fields like the *Source MAC, IP* and *Ingress Interface*.

Step 5: Enter the Source IP and netmask addresses in the ***Source IP*** and ***Mask*** fields.

Step 6: Select the protocol for the interface from the ***Protocol*** drop-down list. The options are: *TCP, UDP, ICMP, None* or *Specify*.

Step 7: If you have selected the option: *Specify* in the previous step, you have to enter the protocol number in the box next to ***Protocol***.

Step 8: Enter the ***Source*** and ***Destination ports*** in the respective fields.

Step 9: Enter the source MAC address into the ***Source MAC*** field.

Step 10: Enter the ***Local Routing Mark*** field if *Locally Generated Ingress Interface* was previously selected.

Step 11: Select the ***Class of Service*** from the drop-down list. The options range from *CoS1* to *CoS6*.

Step 12: Enter the Destination IP and netmask addresses in the ***Destination IP*** and ***Mask*** fields.

Step 13: Click the ***Apply*** button to apply the settings.

Step 14: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Policy Database* screen fields and their definitions:

Field	Description
Source Information	
Ingress Interface	The incoming traffic interface for a Policy Database rule. The options include *LAN Interfaces, WAN Interfaces, Locally generated* (traffic), and *Not Applicable*.
DiffServ Code Point	The DiffServ Code Point or DSCP value ranges from *1* to *255*. This field cannot be configured alone. Additional fields like *IP, Source MAC* and/or *Ingress Interface* should be configured at the same time.
Source IP	The IP address of the traffic source,
Mask	This is the Source IP netmask. This field is mandatory if the Source IP has been entered.
Protocol	The selections are: *TCP, UDP, ICMP, Specify* and *None*. If you choose *Specify,* you need to enter the protocol number in the box next to the *Protocol* field. This field cannot be configured alone. It has to be configured along with fields such as the *IP, Source MAC* and/or *Ingress Interface*. In addition, this field is also mandatory if the *Source Port* or *Destination Port* has been entered.
Source Port	This is the source protocol port. You cannot configure this field without entering the protocol first.
Source MAC	This is the MAC address of the traffic source.

Field	Description
Local Routing Mark	This field is enabled only when *Locally generated* is selected in the *Ingress Interface* field. The mark for DNS traffic generated by different applications are described below: ❑ Dynamic DNS: 0xE1 ❑ Dynamic Proxy: 0xE2 ❑ Web Server: 0xE3 ❑ MSNTP: 0xE4 ❑ DHCP Server: 0xE5 ❑ IP tables Utility: 0xE6 ❑ PPP Daemon: 0xE7 ❑ IP Route: 0xE8 ❑ ATM Library: 0xE9 ❑ Net Tools: 0xEA ❑ RIP: 0xEB ❑ RIP v2: 0xEC ❑ UPnP: 0xEE ❑ Busybox Utility: 0xEF ❑ Configuration Manager: 0xF0 ❑ DropBear Utility: 0xF1 ❑ Voice: 0
Destination Information	
Destination Interface	The outgoing traffic interfaces for a Policy Database rule. The options include *LAN Interfaces* and *WAN Interfaces*.
Class of Service	The selections for CoS in order of descending priority are: *CoS1, CoS2, CoS3, CoS4, CoS5, CoS6* and *N/A,* where CoS6 has the lowest priority.
Destination IP	The IP address of the traffic destination.
Mask	The netmask for the destination. This field is required if the destination IP field has been populated.
Destination Port	This is the destination protocol or port range. Similar to the source port, you cannot configure this field without entering the protocol first.

8.15 Ingress

Ingress enables you to configure QoS for packets as soon as they come into the router. The domain mappings are converted to CoS (Class of Service) so that priority marking is carried over.

There are four Ingress modes:

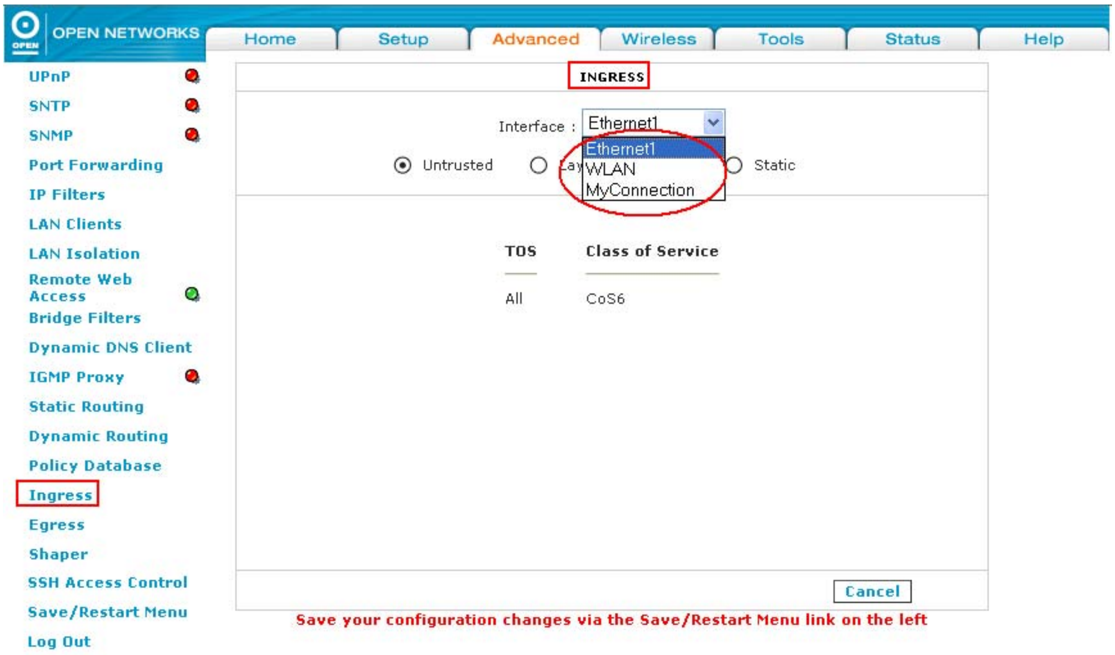
- Untrusted mode
- Layer 2
- Layer 3
- Static

8.15.1 Untrusted Mode

Untrusted mode is the default Ingress page setting for all interfaces. In this mode, all packets are treated as CoS6 (best effort).

To access and configure Untrusted Mode, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Ingress*** link provided. The following page appears:



INGRESS

Interface : Ethernet1

● Untrusted ○ Lay ○ Static

TOS	Class of Service
All	CoS6

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the connection from the ***Interface*** drop-down list. The options will differ depending on the connections you have created.

Step 3: The *Ingress* ***Untrusted Mode*** is the default setting for all the interfaces.

NOTE	**All interfaces that are not configured has the default Untrusted Mode.**

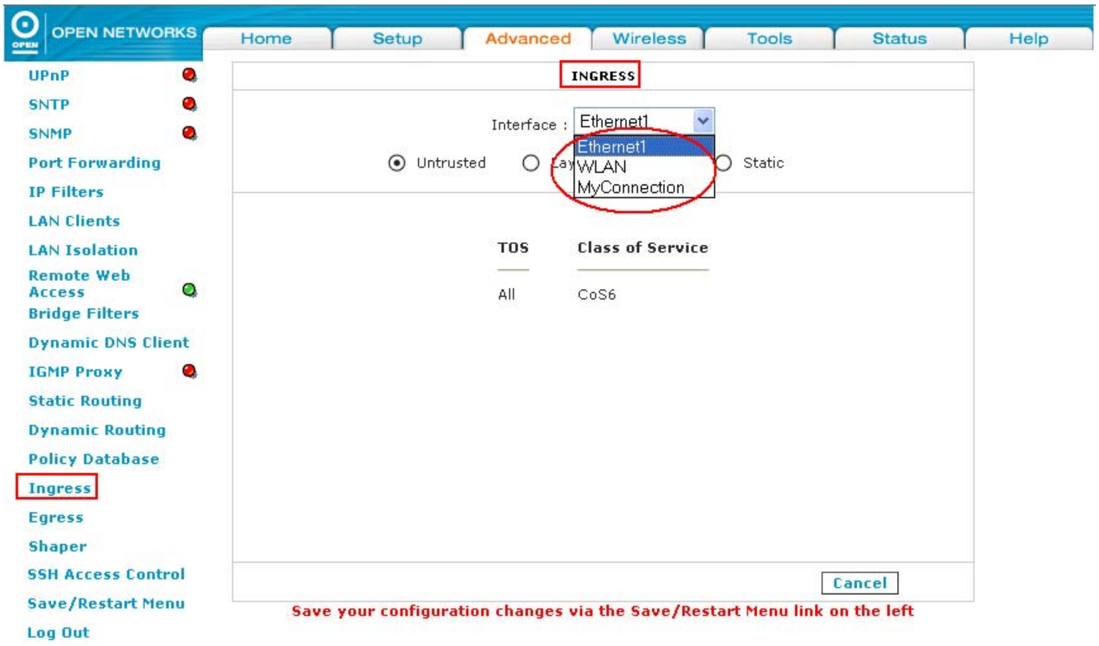
Step 4: If you wish to change from Layer 2 or Layer 3 modes to Untrusted Mode, select the appropriate radio button and refer to the ***Save / Restart Menu*** section to save the changes made.

8.15.2 Ingress Layer 2

Layer 2 enables you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side.

To configure *Layer 2*, follow the steps below.

Step 1: From the ***Ingress*** screen, select the *WAN Interface* to configure the CoS incoming traffic from the ***Interface*** drop-down list as shown below.



Interface : Ethernet1

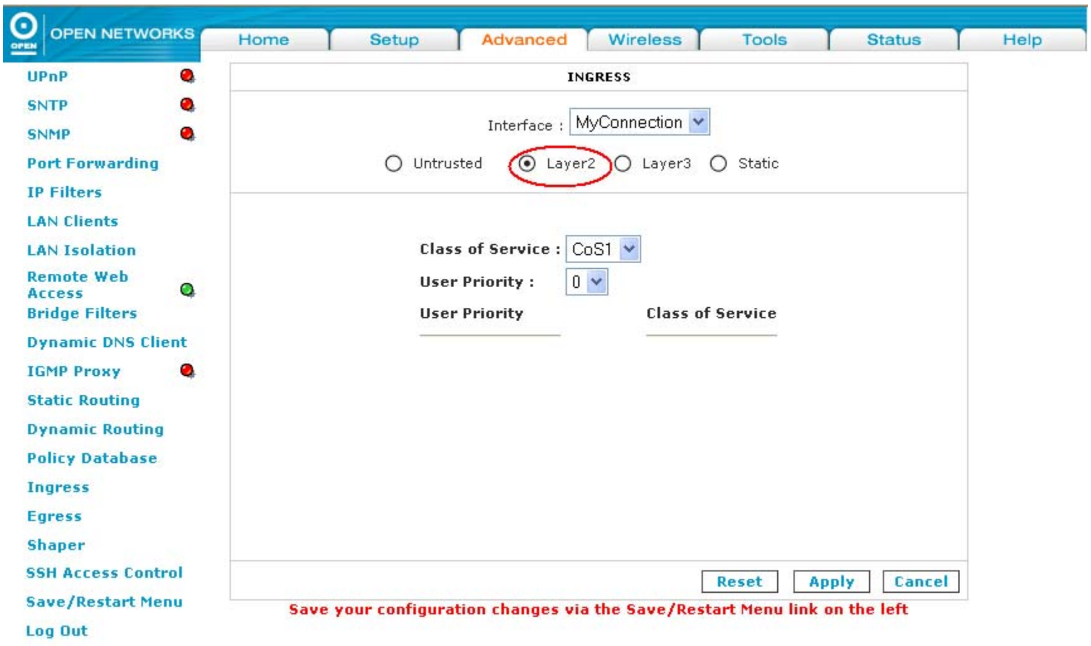
● Untrusted ○ Lay ○ Static

TOS	Class of Service
All	CoS6

Save your configuration changes via the Save/Restart Menu link on the left

NOTE	***A maximum of 8 rules can be configured for each interface.***

Step 2: Highlight the ***Layer 2*** radio option. The following page appears:



INGRESS

Interface : MyConnection

○ Untrusted ● Layer2 ○ Layer3 ○ Static

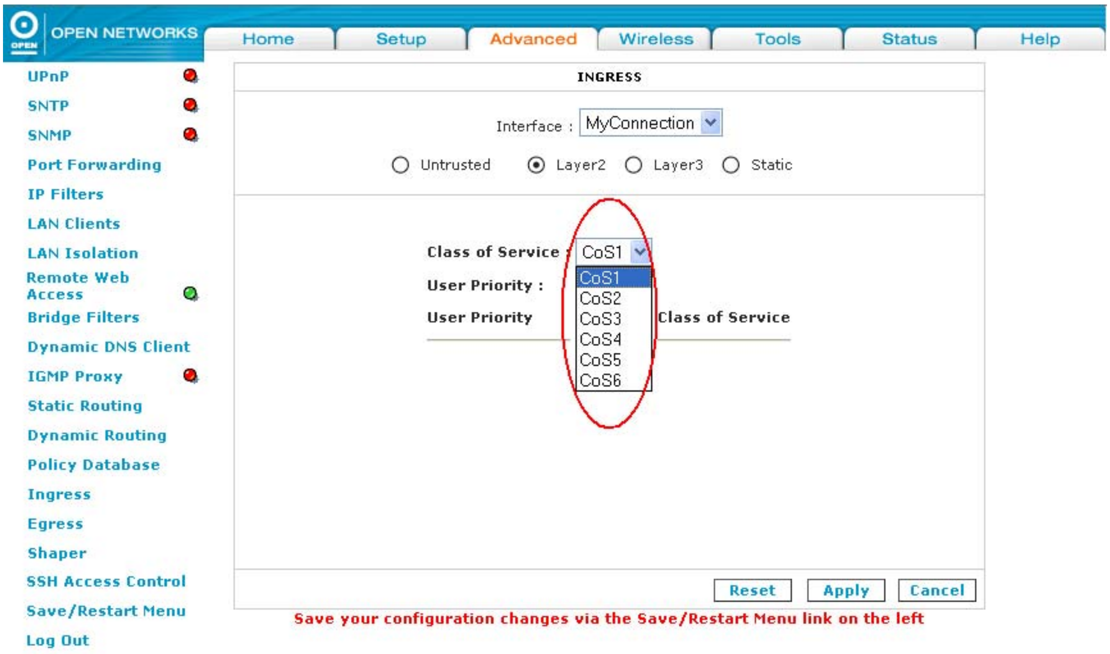
Class of Service : CoS1

User Priority : 0

User Priority   Class of Service

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Select the *CoS* options from the ***Class of Service*** drop-down list as shown. The selections are in order of **descending** priority, i.e. CoS6 has the lowest priority.



INGRESS

Interface : MyConnection

○ Untrusted ● Layer2 ○ Layer3 ○ Static

Class of Service : CoS1

User Priority :

User Priority   Class of Service

Save your configuration changes via the Save/Restart Menu link on the left

For example, if you select *CoS1* for *Class of Service* field and *5* for *Priority Bits* field, this means that any packets that have a *User Priority* bit of *5* is mapped to *CoS1* - the highest priority. This is given to the high priority packets such as video.

Alternatively, if you select *CoS2* in the *Class of Service* field and *1* in the *Priority Bits* field, this meant that any packets that have a *User Priority* of 1 is mapped to *CoS2*, the second highest priority. This is normally given to voice packets.

Step 4: Select the priority from the ***User Priority*** drop-down list. The selections are from *0* to *7.*

☞ NOTE	***Any User Priority bits that have not been mapped to a CoS is defaulted to CoS6, the lowest priority.***

Step 5: Click the ***Apply*** button to apply the settings.

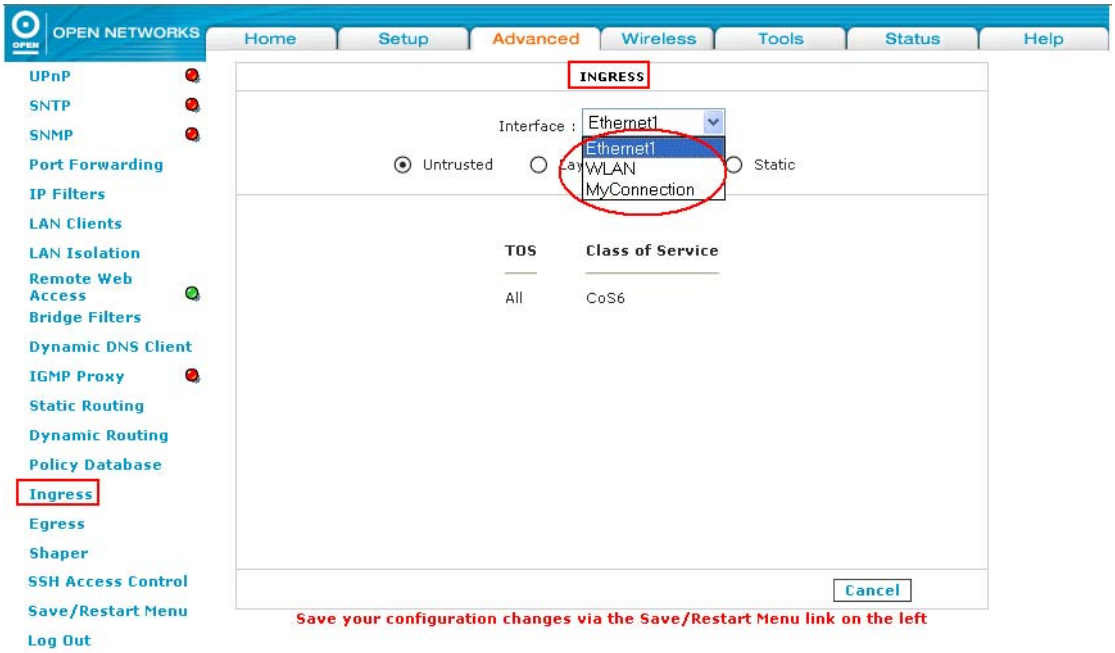
Step 6: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

8.15.3 Ingress Layer 3

The Layer 3 page allows you to map ToS (type of service) bits of incoming packets from the IP network to CoS for each WAN/LAN interface.

To configure *Layer 3*, follow the steps below.

Step 1: From the ***Ingress*** screen, select a *LAN Interface* from the ***Interface*** drop-down list as shown on the screen below.



INGRESS

Interface : Ethernet1

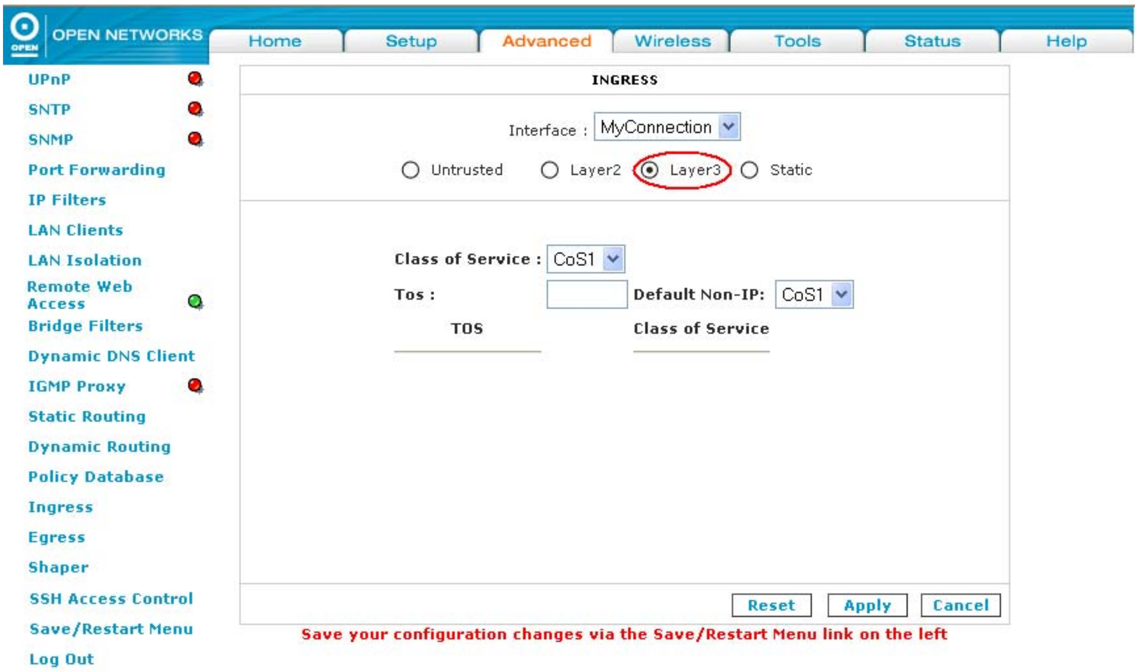
Ethernet1
WLAN
MyConnection

● Untrusted ○ Lay ○ Static

TOS	Class of Service
All	CoS6

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Highlight the ***Layer 3*** radio option. The following page appears:



INGRESS

Interface : MyConnection

○ Untrusted ○ Layer2 ● Layer3 ○ Static

Class of Service : CoS1

Tos : Default Non-IP: CoS1

TOS	Class of Service

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Select the *CoS1* from the ***Class of Service*** drop-down list. The selections are in order of **descending** priority, i.e. CoS6 has the lowest priority.

Step 4: In the ***ToS*** field, if you enter *22* for instance, this means that any incoming packet from the selected *Interface* in *Step 1* (Layer 3) with a ToS of *22* is mapped to *CoS1*, the highest priority. This is normally given to voice packets.

Step 5: Leave the default value *CoS1* option in the ***Default Non-IP*** drop-down list. This is the highest priority.

Step 6: Click the ***Apply*** button to apply the settings.

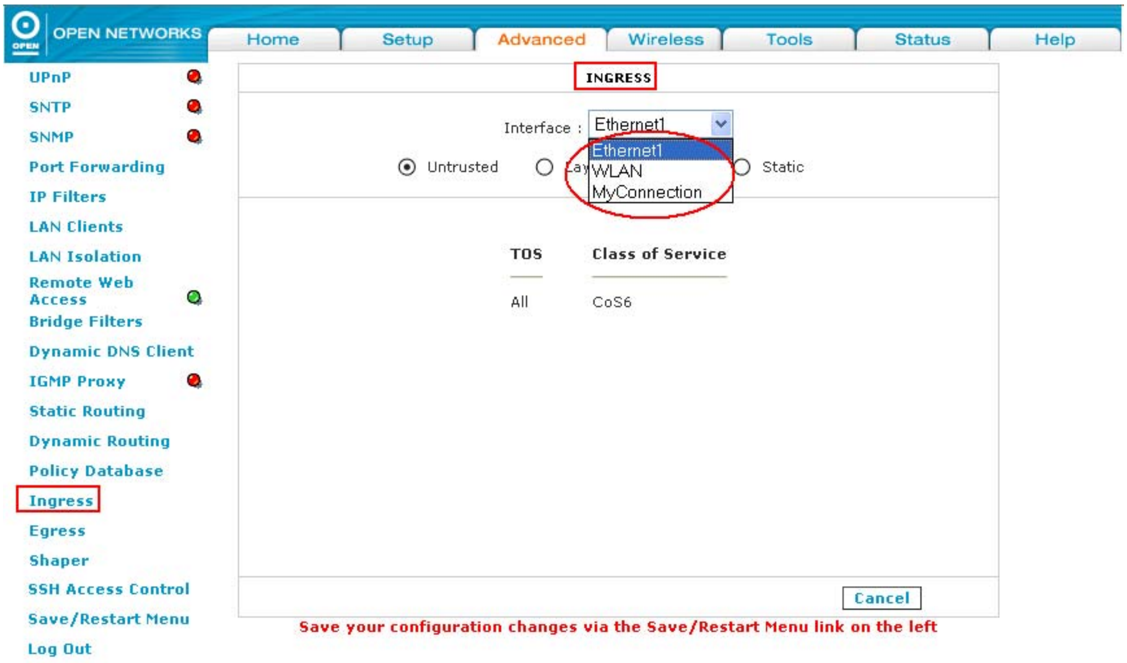
Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

8.15.4 Static Configuration

The Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.

To configure *Static*, follow the steps below.

Step 1: From the ***Ingress*** screen, select a *LAN* or *WAN Interface* from the ***Interface*** drop-down list as shown on the screen below.



INGRESS

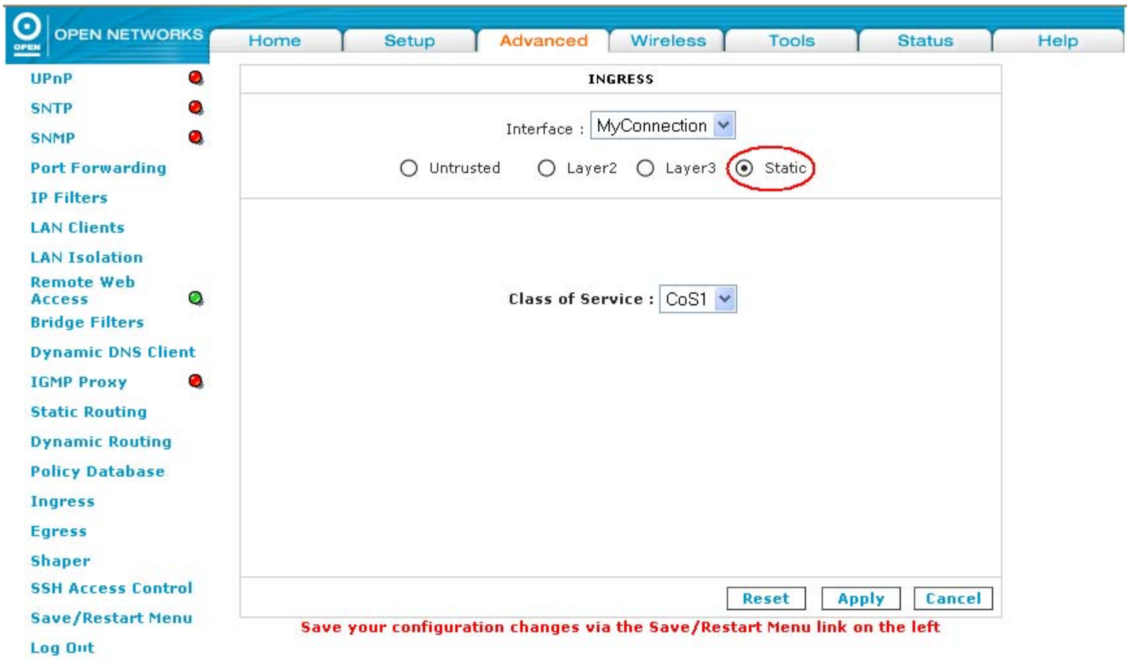
Interface : Ethernet1

● Untrusted ○ Lay ○ Static

TOS	Class of Service
All	CoS6

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Highlight the ***Static*** radio option. The following page appears:



INGRESS

Interface : MyConnection

○ Untrusted ○ Layer2 ○ Layer3 ● Static

Class of Service : CoS1

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Select the ***Class of Service*** from the drop-down list.

Step 4: Click the ***Apply*** button to apply the settings.

Step 5: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.16 Egress

For packets going out of the router, the markings (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using Egress.

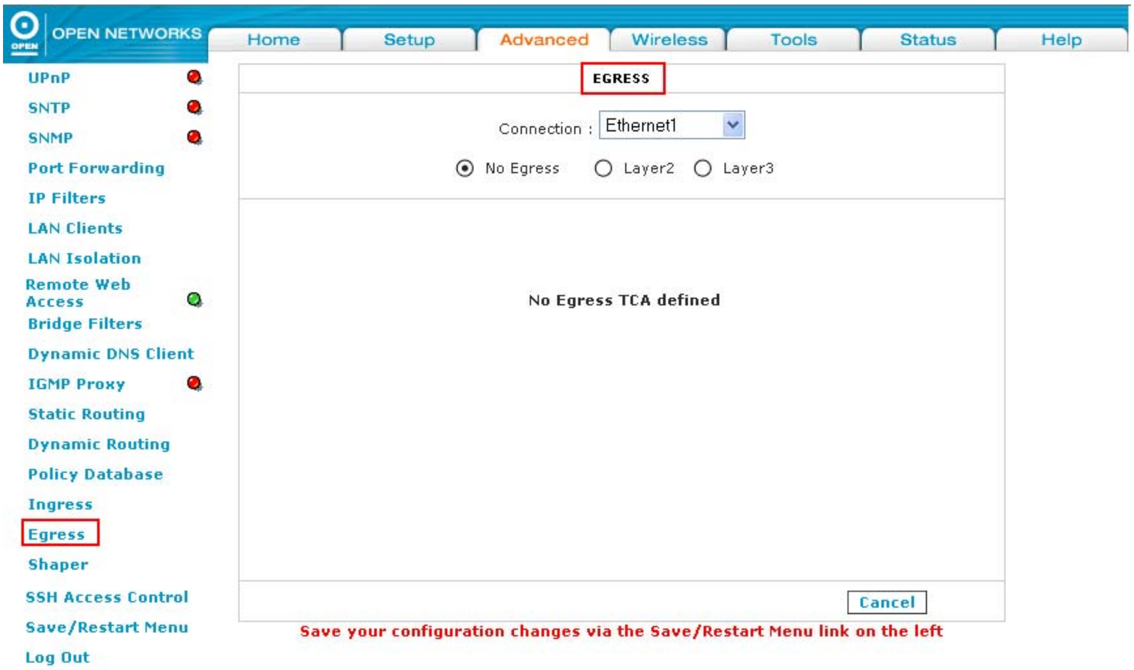
There are 3 Egress modes:

- No Egress
- Layer 2 - not supported for this version.
- Layer 3

8.16.1 No Egress

To access *No Egress*, follow the step below.

Step 1: From the ***Advanced*** tab, click the ***Egress*** link provided. The following page appears:



EGRESS

Connection : Ethernet1

● No Egress ○ Layer2 ○ Layer3

No Egress TCA defined

Save your configuration changes via the Save/Restart Menu link on the left

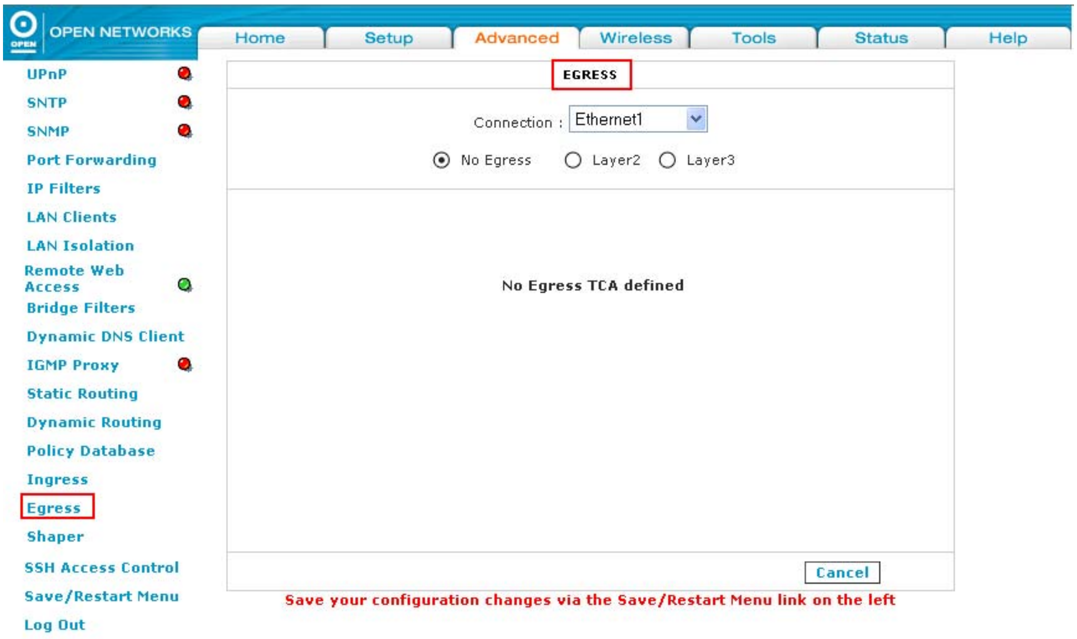
NOTE	**The No Egress mode is the default setting for all interfaces. In this mode, the domain mappings of the packets are untouched.**

8.16.2 Egress Layer 3

The Egress Layer 3 page enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.

To configure Egress Layer 3, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Egress*** link provided. The following page appears:



EGRESS

Connection : Ethernet1

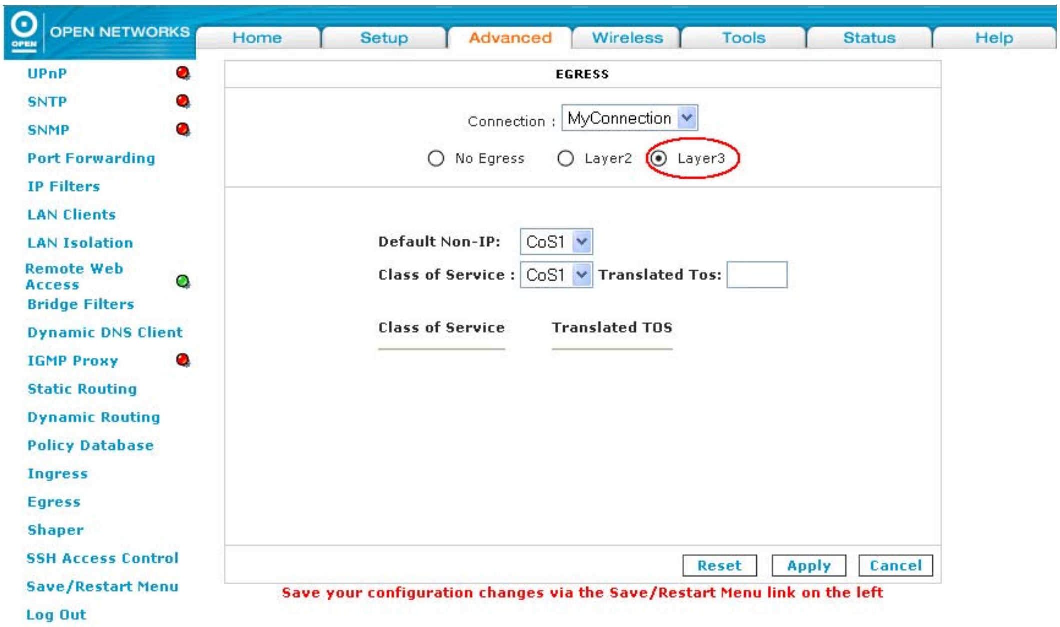
● No Egress ○ Layer2 ○ Layer3

No Egress TCA defined

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the interface from the ***Connection*** drop-down list to configure QoS for outgoing traffic to the IP network.

Step 3: Highlight the ***Layer 3*** radio option. The following page appears:



EGRESS

Connection : MyConnection

○ No Egress ○ Layer2 ● Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service	Translated TOS

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Select the CoS value for all unclassified outgoing packets on Layer 3 from the ***Default Non-IP*** drop-down list. The options are between CoS1 to CoS6 and are in descending order of priority. The default value is CoS1 (recommended).

NOTE	**Some locally generated packets may not have been classified and therefore do not have a CoS value, such as ARP packets.**

Step 5: Select the CoS from the ***Class of Service*** drop-down list. The options are in descending order of priority.

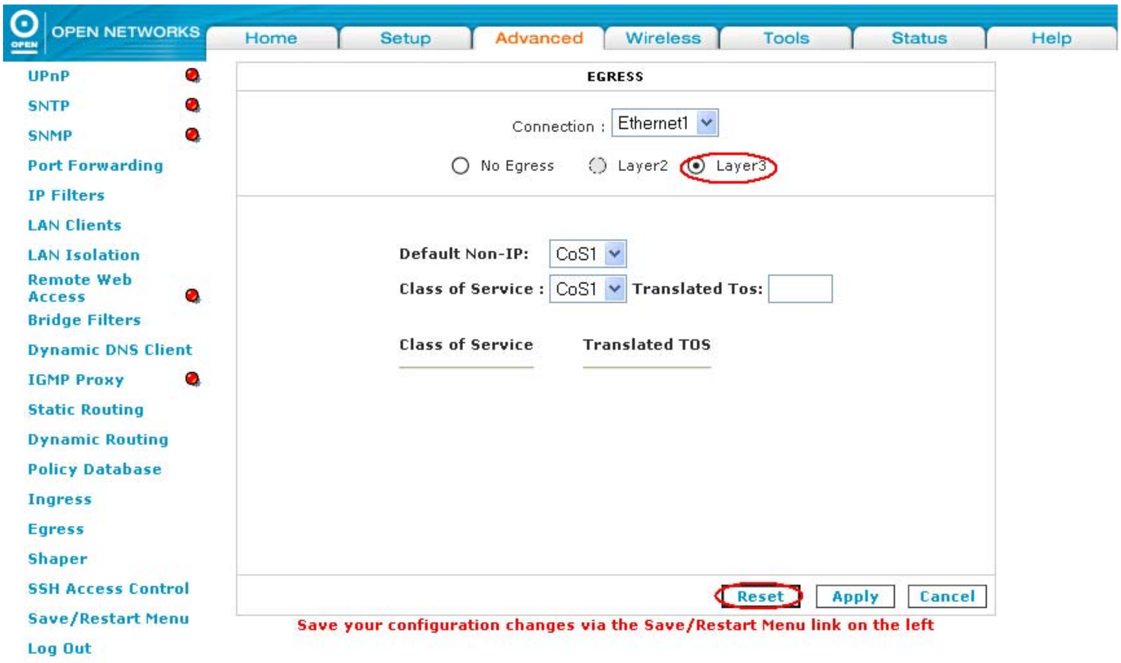
Step 6: Enter the ToS value into the ***Translated ToS*** field. The type of service takes value from *1* to *255*.

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.16.3 Resetting Egress Mode

Step 1: If you are making changes from *Layer 3* modes to *No Egress* mode, click the ***Reset*** button as shown below.



EGRESS

Connection : Ethernet1

○ No Egress ○ Layer2 ● Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service	Translated TOS

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Refer to the ***Save / Restart Menu*** section to save your configuration.

8.17 Shaper

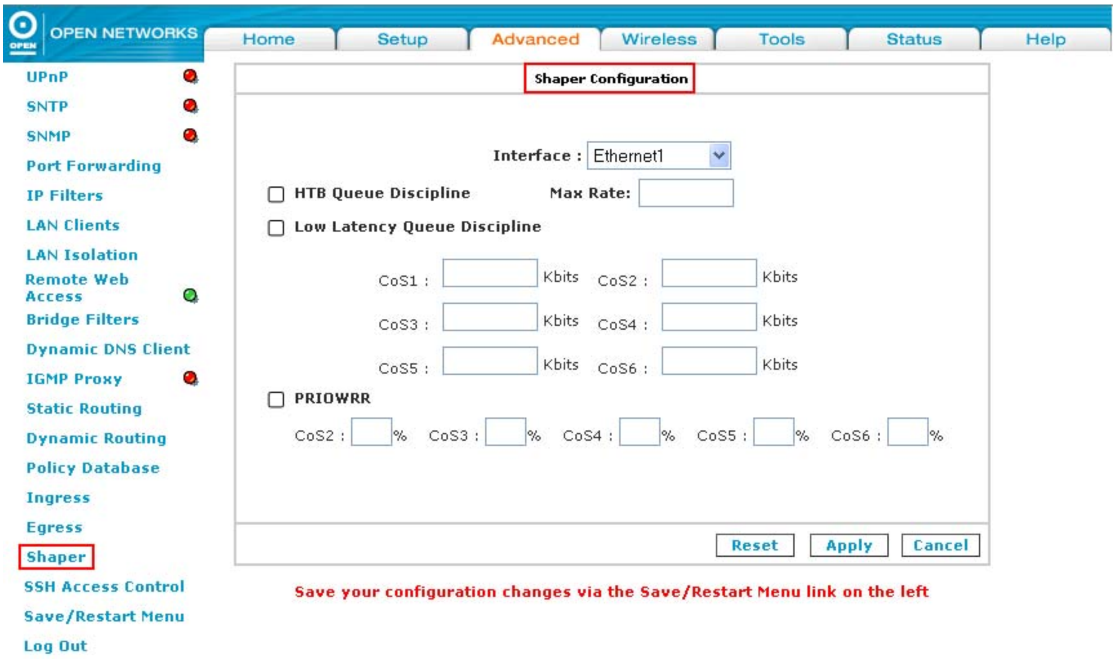
Three Shaper algorithms are supported:

- HTB Queue Discipline
- Low Latency Queue Discipline
- PRIOWRR

8.17.1 HTB Queue Discipline

To enable *HTB Queue Discipline*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Shaper*** link provided. The following page appears:



Shaper Configuration

Interface : Ethernet1

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

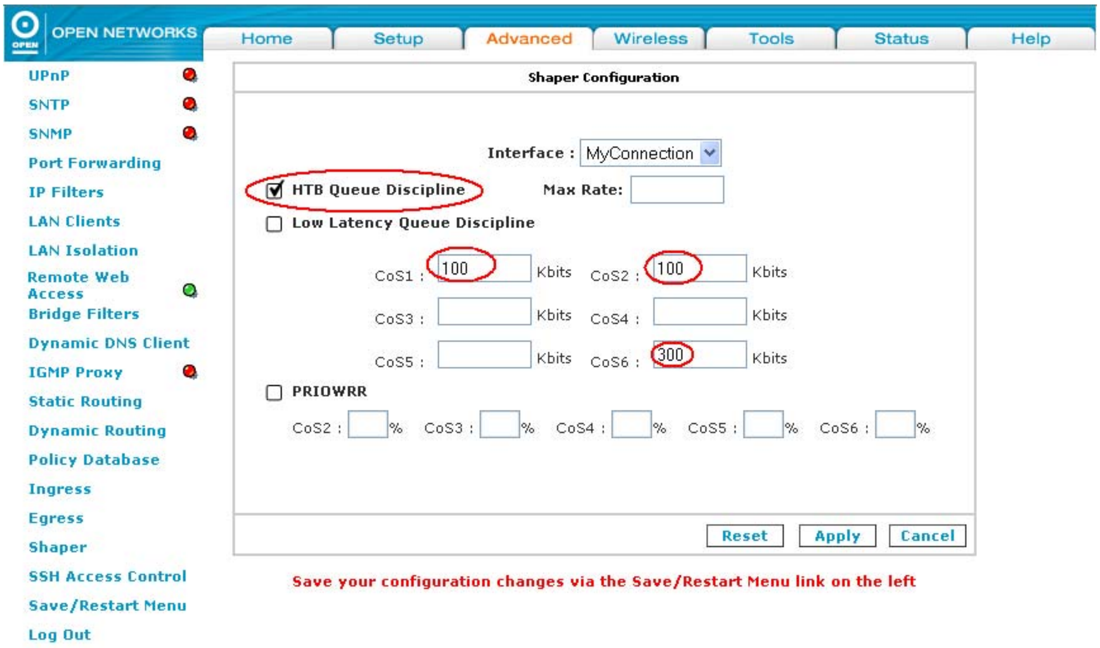
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the interface from the ***Interface*** drop-down list.

Step 3: Check the ***HTB Queue Discipline*** checkbox to enable this feature. In the example below, the *MyConnection* has a total of 300 kbits of bandwidth, of which 100 kbits is given to CoS1 and another 100 kbits is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 kbits of bandwidth.



Shaper Configuration

Interface : MyConnection

☑ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : 100 Kbits CoS2 : 100 Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : 300 Kbits

□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Click the ***Apply*** button to apply the settings.

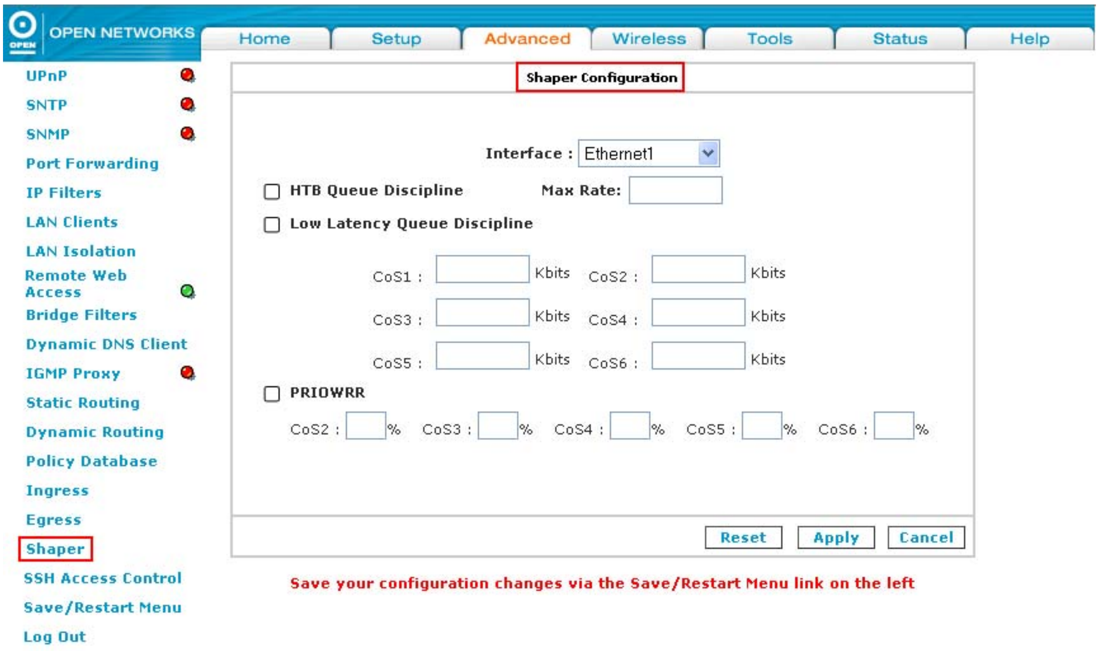
Step 5: To save your configuration, please refer to the section under ***Save / Restart Menu***.

:

8.17.2 Low Latency Queue Discipline

To enable *Low Latency Queue Discipline*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Shaper*** link provided. The following page appears:



Shaper Configuration

Interface : Ethernet1

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

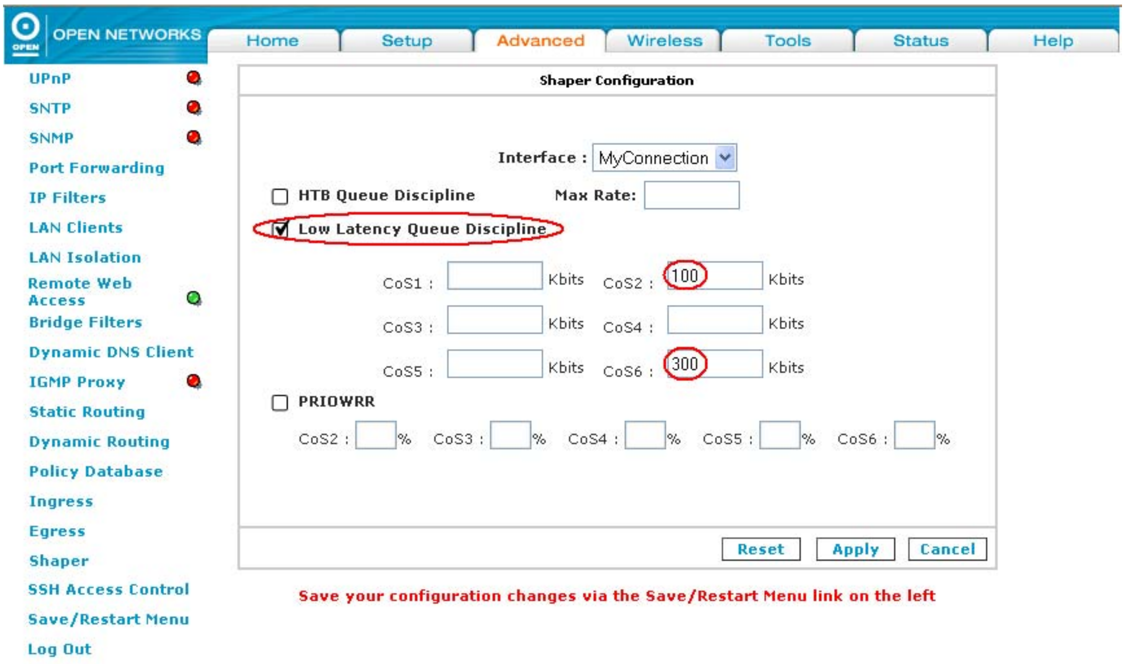
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the interface from the ***Interface*** drop-down list.

Step 3: Check the ***Low Latency Queue Discipline*** checkbox. The *MyConnection* example below has a total of 300 kbits of bandwidth, of which 100 kbits is given to CoS2 when there is no CoS1 packets. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 kbits of bandwidth.



Shaper Configuration

Interface : MyConnection

□ HTB Queue Discipline Max Rate:

☑ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : 100 Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : 300 Kbits

□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

NOTE	*CoS1 is not rate-controlled so the field is disabled.*

Step 4: Click the ***Apply*** button to apply the settings.

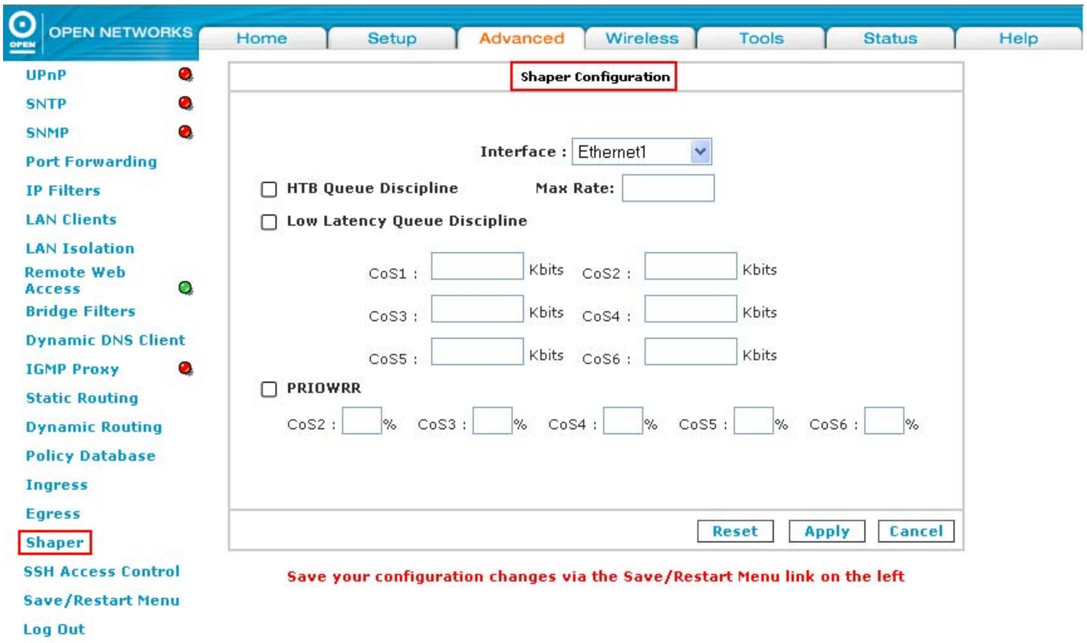
Step 5: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.17.3 PRIOWRR

PRIOWRR stands for Priority Weighted Round Robin.

To enable *PRIOWRR*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***Shaper*** link provided. The following page appears:



Shaper Configuration

Interface : Ethernet1

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

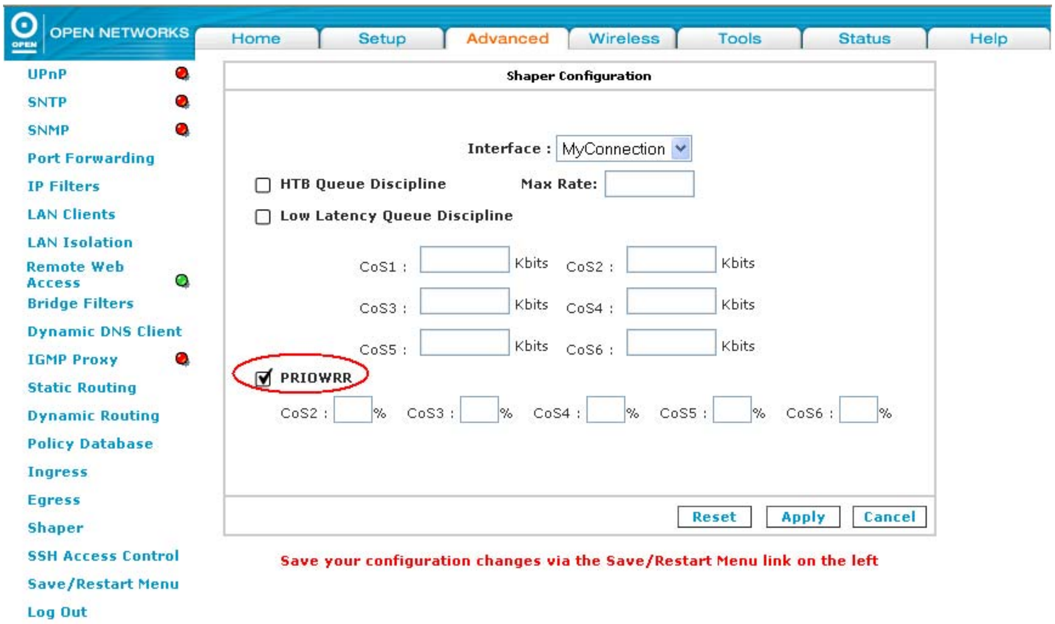
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the interface from the ***Connection*** drop-down list.

Step 3: Check the ***PRIOWRR*** checkbox to enable it, as shown.



Shaper Configuration

Interface : MyConnection

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

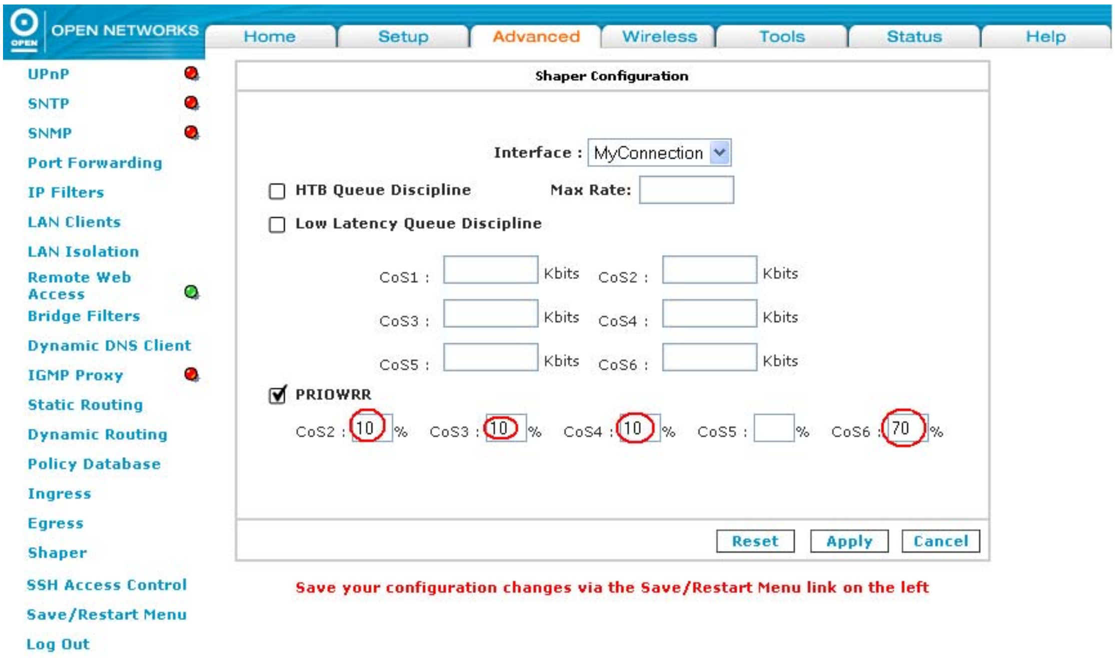
☑ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: PRIOWRR operates only on the number of packets being transmitted, so the ***Max Rate*** field has been disabled.

Step 5: Only percentages can be assigned to ***CoS2 - CoS6*** fields. In the *MyConnection* example below, when there are no CoS1 packets, CoS2, CoS3 and CoS4 each have 10% and CoS6 has 70% as shown in the screen image below. This is similar to the *Low Latency Queue Discipline*, except that *PRIOWRR* is packet-based and the other is rate-based.



Shaper Configuration

Interface : MyConnection

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

☑ PRIOWRR

CoS2 : 10 % CoS3 : 10 % CoS4 : 10 % CoS5 : % CoS6 : 70 %

Save your configuration changes via the Save/Restart Menu link on the left

Step 6: Click the ***Apply*** button to apply the settings.

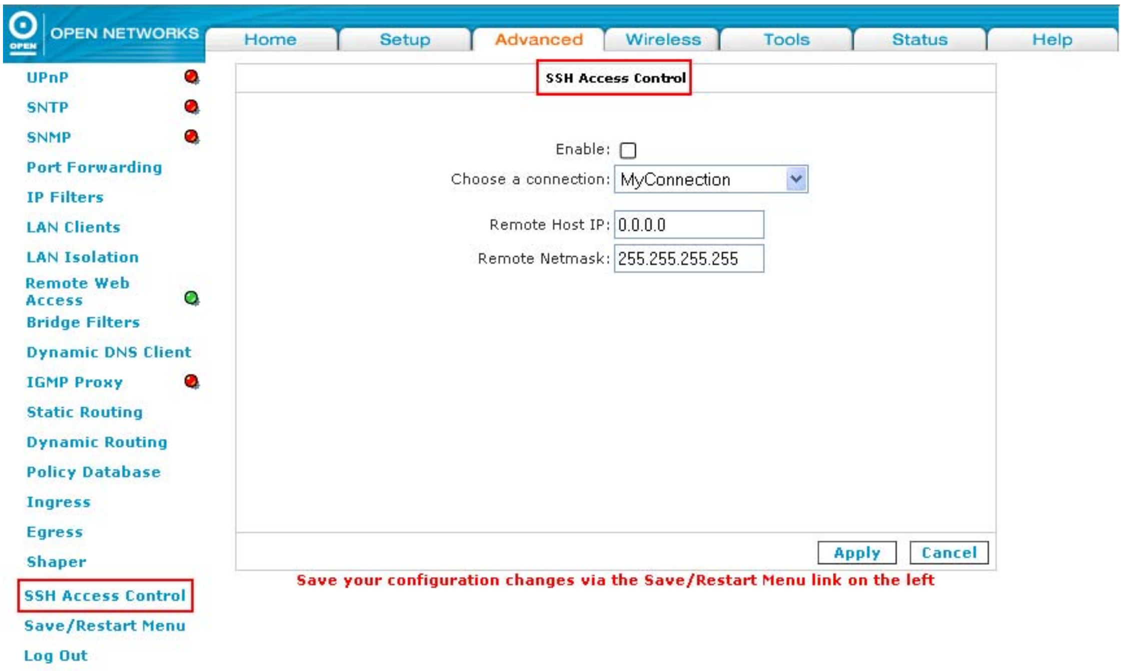
Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

8.18 SSH Access Control

The SSH Access Control feature allows you to access the iConnect625W remotely via SSH from the WAN side.

To configure *SSH Access Control*, follow the steps below.

Step 1: From the ***Advanced*** tab, click the ***SSH Access Control*** link provided. The following page appears:



SSH Access Control

Enable: □

Choose a connection: MyConnection

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable*** checkbox.

Step 3: In the ***Choose a Connection*** field, leave the default WAN connection selected.

Step 4: In the ***Remote Host IP*** field, enter the WAN-side IP address that you will use to access the iConnect625W router. The default setting is 0.0.0.0.

Step 5: In the ***Remote Netmask*** field, enter the netmask of your WAN-side IP address.

Step 6: Click the ***Apply*** button to apply the settings.

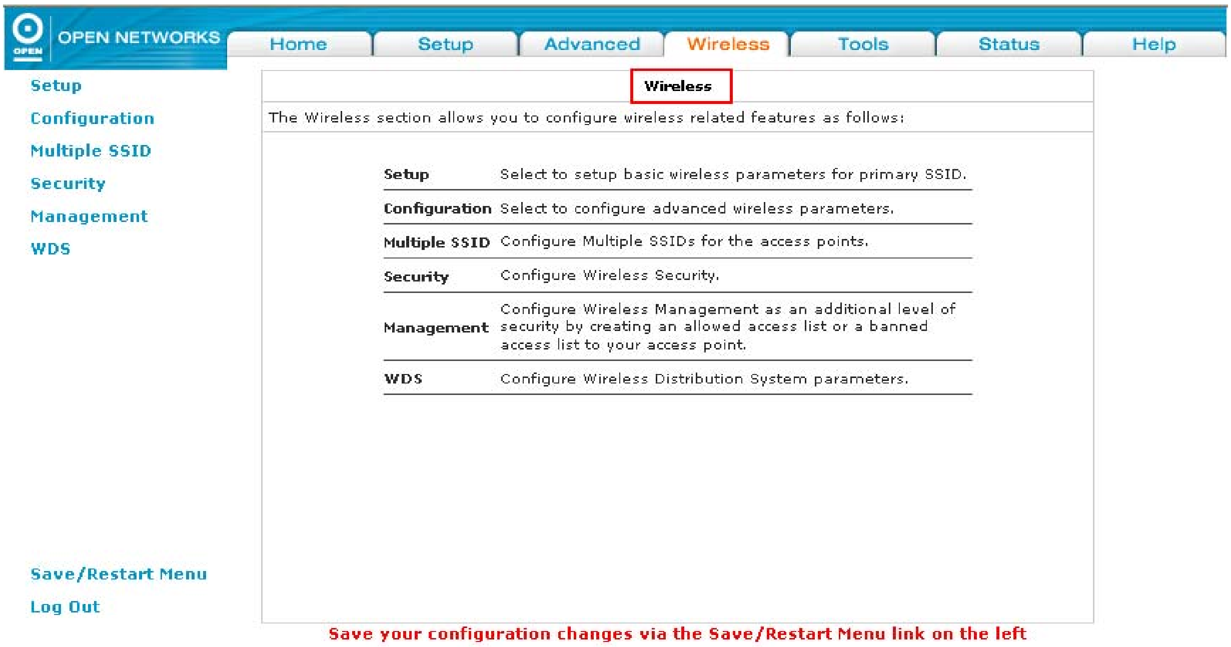
Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

9. Wireless

The Wireless main page provides access to the following features:

- Setup
- Configuration
- Multiple SSID
- Security
- Management
- WDS

To access the *Wireless Main* page, click the ***Wireless*** tab as shown on the screen below.



Wireless

The Wireless section allows you to configure wireless related features as follows:

Setup	Select to setup basic wireless parameters for primary SSID.
Configuration	Select to configure advanced wireless parameters.
Multiple SSID	Configure Multiple SSIDs for the access points.
Security	Configure Wireless Security.
Management	Configure Wireless Management as an additional level of security by creating an allowed access list or a banned access list to your access point.
WDS	Configure Wireless Distribution System parameters.

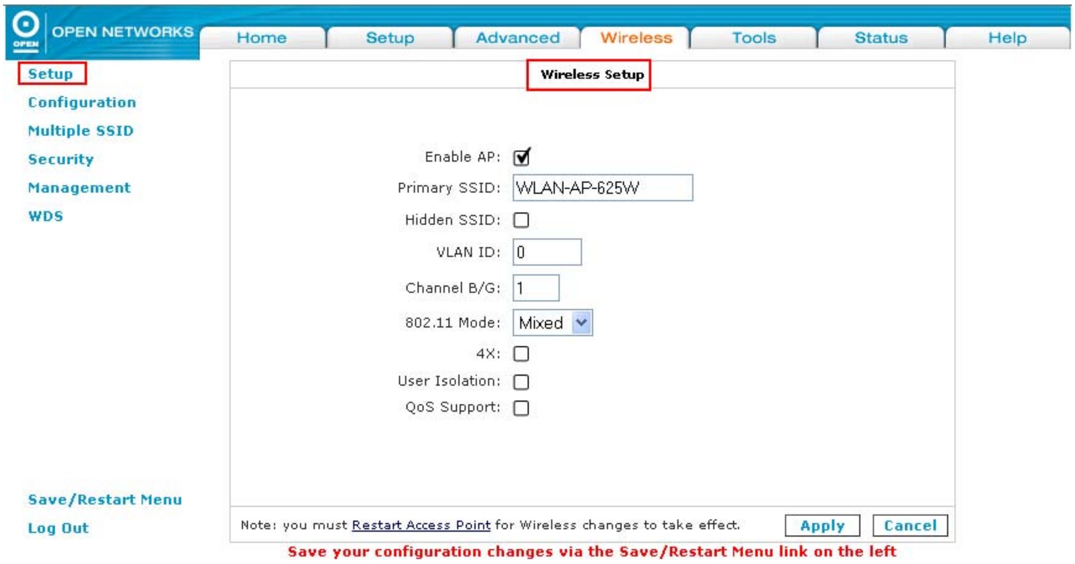
Save your configuration changes via the Save/Restart Menu link on the left

Each of the features on the left menu is described in the following sections.

9.1 Setup

To configure Setup, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Setup*** link provided. The following page appears:



Wireless Setup

Enable AP: ☑
Primary SSID: WLAN-AP-625W
Hidden SSID: □
VLAN ID: 0
Channel B/G: 1
802.11 Mode: Mixed
4X: □
User Isolation: □
QoS Support: □

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The ***Enable*** checkbox is enabled by default for the access point (AP).

Step 3: The default setting for the ***Primary SSID*** field is *WLAN-AP-625W* and you can assign a unique SSID to your AP, if required.

NOTE	**The maximum number of characters for the SSID field is 32 characters.**

Step 4: The ***Hidden SSID*** checkbox is used to enable/disable this feature. When the hidden SSID is enabled, the SSID is removed from the beacon frames that the AP transmits. This hides the AP from being seen by any other station.

Step 5: The ***VLAN ID*** applies to the primary SSID. The default value is *0.* Enter the VLAN ID as required.

Step 6: Next, enter the ***Channel B/G*** field. The default channel is *1* but different domains have different ranges of channels. For example, the FCC default channel in 2.4 GHz is *11*.

Step 7: Select the ***802.11 Mode*** from the drop-down list. The options are: *Mixed mode, 11b only Mode, 11b+ Mode* and 1*1g only Mode*.

Step 8: Check the ***User Isolation*** checkbox if you wish to prevent wireless users from directly accessing other wireless users.

Step 9: Check the QoS Support checkbox to enable QoS configuration. The QoS settings can be found in the table provided below.

Step 10: Click the ***Apply*** button to apply the settings.

Step 11: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Setup* screen fields and their definitions:

Field	Description
Enable AP	Enables / Disables the access point (AP).
Primary SSID	The primary SSID is the primary service set identifier of the AP. The SSID field allows up to a maximum field length of 32 characters.
Hidden SSID	Enables / Disables the *Hidden SSID* feature. When the SSID is removed from the beacon frames that the AP transmits. The AP will no longer be seen by any other station.
VLAN ID	This is the *VLAN ID* for the *Primary SSID*. By default, multiple SSID is disabled and the VLAN of the primary SSID is *0.* When you enable multiple SSID, you are prompted to change the VLAN ID of the primary SSID to a unique value between *1 and 4095*.
Channel B/G	This is the channel on which the AP and the wireless stations communicate.
802.11 Mode	You can select from the following modes: • **Mixed Mode** o Both 802.11b and g modes are supported. The legacy supported rates information element (SR IE) contains the 802.11b legacy supported rates and the additional OFDM supported rates. Extended SR IE contains the extended support rates, if present. • **11b Only Mode** o The legacy SR IE contains only the 802.11b legacy supported rates. The extended SR IE is not present. • **11b+ Mode** o Similar to the 802.1b-only mode except that **22Mbps** PBCC rate/modulation is included. • **11g Only Mode** o The legacy SR IE contains only the OFDM additional supported rates. The extended SR IE contains the extended rates, if present.
4x	Enables / Disables the 4x feature. This function is TI (Texas Instruments) proprietary and is only available when both TI wireless station card and TI RG are used.

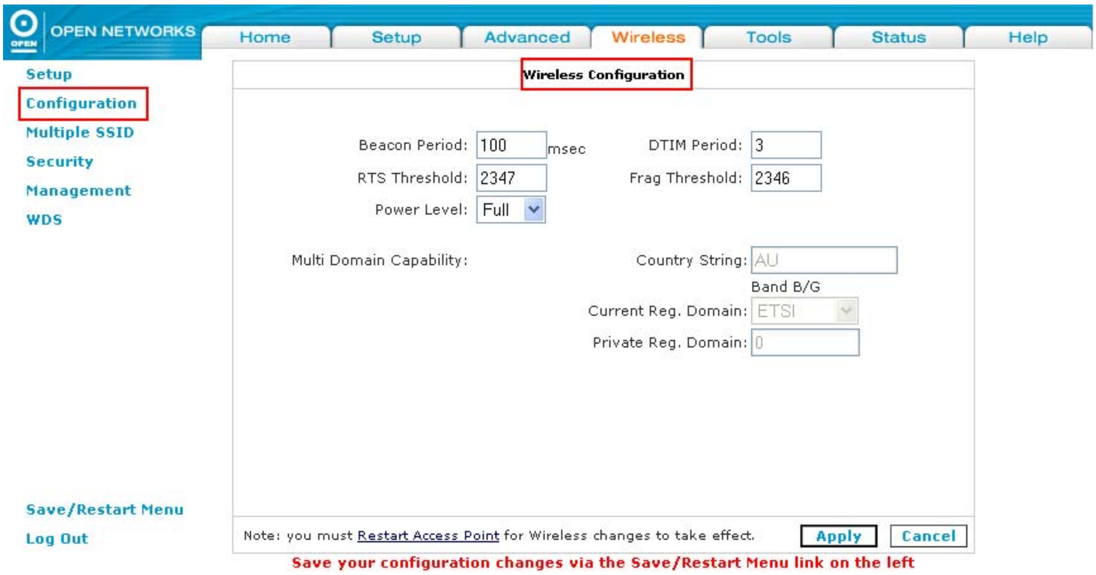
Field	Description
User Isolation	When checked, wireless users will not be able to directly access other wireless users. Access can be controlled by the AP. The 3 states of enabling User Isolation feature are: 1. *AP disabled basic set (BSS) bridging***:** Before user isolation is enabled, the stations can exchange data via the AP. This is disabled when user isolation is enabled. 2. All data is sent to the *WAN*. 3. *Enable / Disable flag*: No station has direct access to other stations as a result of user isolation.
QoS Support	Please refer to the QoS Settings table provided below.

9.2 Configuration

The Wireless Configuration page provides the advanced wireless network parameter settings.

To access and enable *Configuration*, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Configuration*** link provided. The following page appears:



Wireless Configuration

Beacon Period: 100 msec

DTIM Period: 3

RTS Threshold: 2347

Frag Threshold: 2346

Power Level: Full

Multi Domain Capability:

Country String: AU

Band B/G

Current Reg. Domain: ETSI

Private Reg. Domain: 0

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The default value for the time interval between beacon frame transmissions in the ***Beacon Period*** field is set to *100* milliseconds. Modify this value, if required.

Step 3: The default value for the *Delivery Traffic Identification Map* period in the ***DTIM*** field is set to *3.* Modify this value, if required.

Step 4: Enter the *Request to Send* threshold in the ***RTS Threshold*** field. The defaulted value is *2347*.

Step 5: Enter the *Fragmentation Threshold* in the ***Frag Threshold*** field. The defaulted value is *2346*.

Step 6: Select the ***Power Level*** from the drop-down list. The options are: *Full, 75%, 50%, 25% and 6%.*

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *Configuration* screen fields and their definitions:

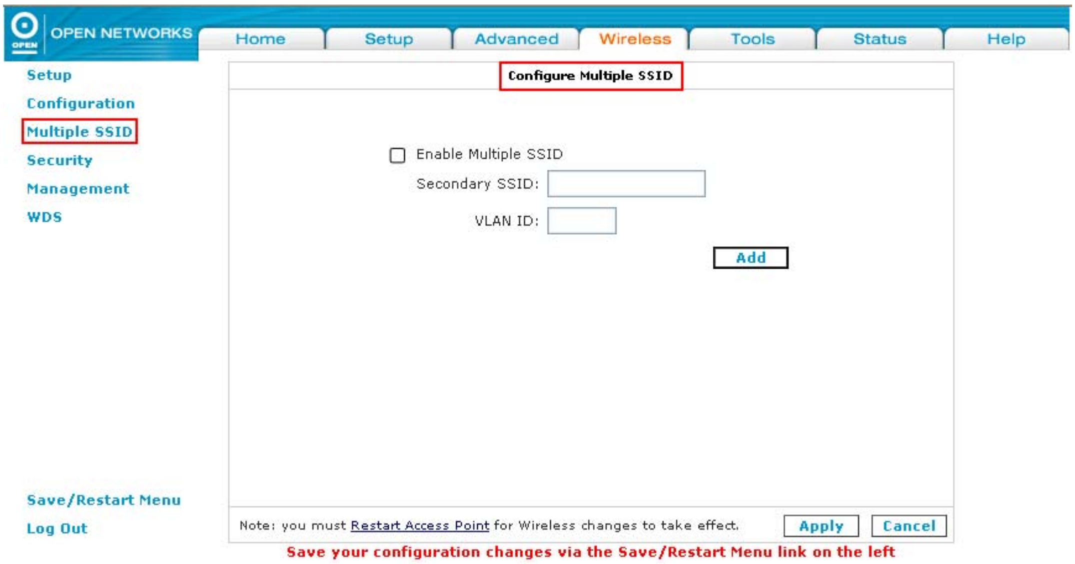
Field	Description
Beacon Period	This refers to the time interval between beacon frame transmissions, ranging from *0 - 65535* milliseconds (msec). The default value of this field is 1*00* msec.
DTIM Period	DTIM stands for *Delivery Traffic Identification Method* period. The number of beacon frame transmissions before frames are targeted for stations operating in low-power mode will be transmitted. The default value of this field is 3.
RTS Threshold	RTS stands for *Request to Send* threshold. It refers to the number of bytes in a MAC protocol data unit (MPDU) below which an RTS / CTS handshake will not be performed. The default value is *2347.* However, when *4x* is enabled on the *Setup* page, the RTS threshold value changes to *4096.*
Fragmentation Threshold	This refers to the minimum length of a frame that will be fragmented. The default value is *2346.* However, when *4x* is enabled on the *Setup* page, the fragmentation threshold value changes to *4096.*
Multi Domain Capability	Not Applicable for end users.

9.3 Multiple SSID

This feature allows you to create multiple SSIDs for the AP. The Multiple SSID features support up to two SSID classes - one primary and one secondary.

To configure *Multiple SSID,* follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Multiple SSID*** link provided. The following page appears:



Configure Multiple SSID

□ Enable Multiple SSID

Secondary SSID:

VLAN ID:

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable Multiple SSID*** checkbox to enable this feature.

Step 3: Enter the secondary SSID in the ***Secondary SSID*** field.

NOTE	***The maximum number of Secondary SSIDs that are supported is 3, in addition to the Primary SSID.*** ***The maximum number of characters for the Secondary SSID is 32 characters and it is unique from the Primary SSID.***

Step 4: Enter the ***VLAN ID*** in the field provided.

Step 5: Click the ***Add*** button. The *Available Secondary SSIDS(s)* section appears.

Step 6: Click the *Setup* link and change the ***VLAN ID*** of the primary SSID to a number between *1* and *4095*.

Step 7: To delete an SSID, check the applicable SSID, and click ***Delete*** button in the pop-up window.

Step 8: To delete all the SSIDs, check the ***Delete All*** checkbox.

Step 9: Click the ***Apply*** button to apply the settings.

Step 10: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

9.4 Security

The Security provides 4 wireless network security options for configuration. These include:

- None
- WEP
- 802.1x
- WPA

These options will be described in detail as follows.

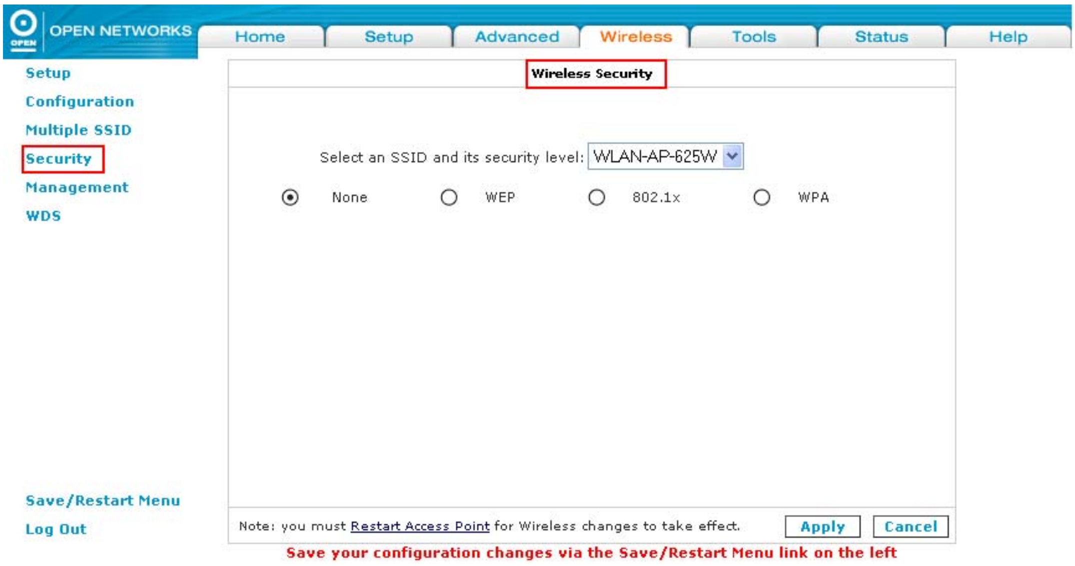
If you have *Multiple SSID* enabled, you can assign security to each SSID. There are a few rules / limitations that you should follow:

- WEP cannot be assigned to more than one SSID;
- 802.1x cannot be assigned to more than one SSID;
- WEP and 802.1x cannot both be assigned concurrently to different SSID;
- When more than one SSID exists with security enabled, the Authentication type for WEP cannot be *Shared.*

9.4.1 No security

To access the wireless *Security*, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Security*** link provided. The following page appears:



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The default ***SSID*** is *WLAN-AP-625W*. Select a different SSID as required.

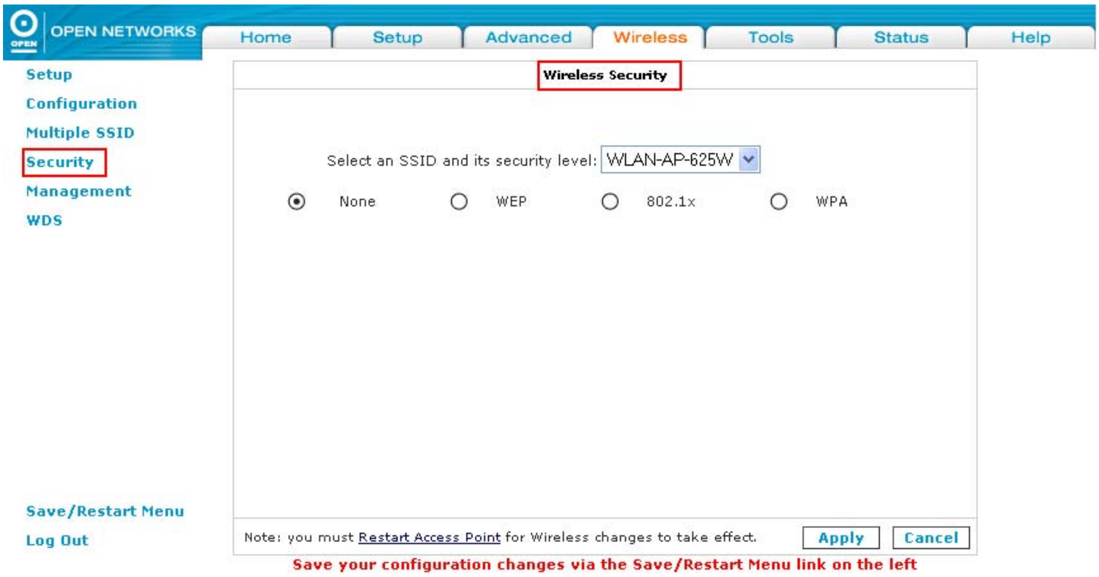
Step 3: The default wireless network security option is set to ***None.*** This means that no security is used.

9.4.2 WEP

WEP is a security protocol for WLAN. WEP provides security by encrypting data that is sent over the WLAN.

To configure wireless security for *WEP*, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Security*** link provided. The following page appears:



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

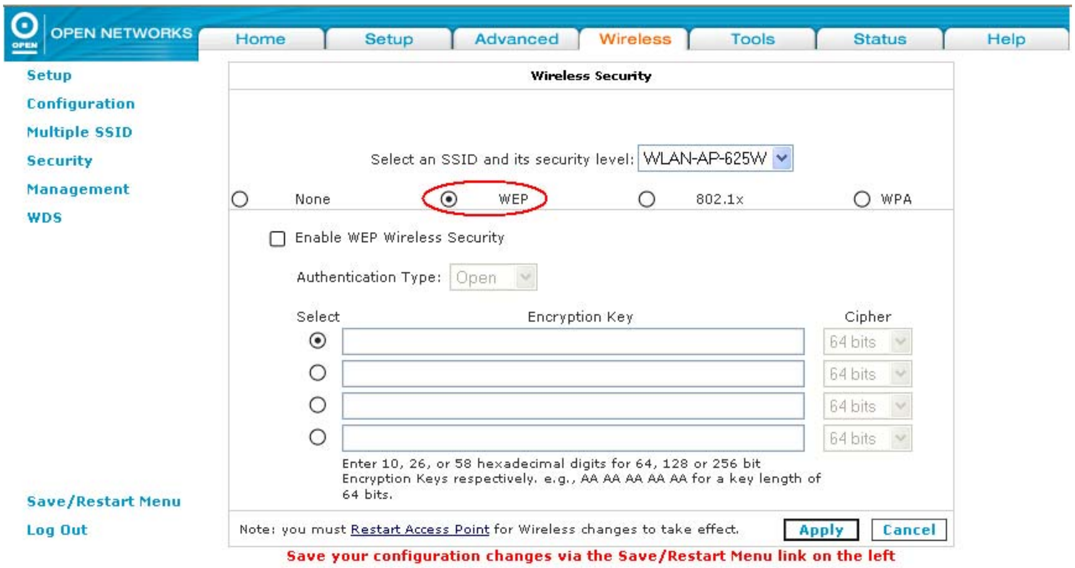
● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: If there are multiple SSIDs used, select the ***Select an SSID and its security level*** from the drop-down menu.

Step 3: Select the ***WEP*** protocol from the security options provided. The following page appears:



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

○ None ● WEP ○ 802.1x ○ WPA

□ Enable WEP Wireless Security

Authentication Type: Open

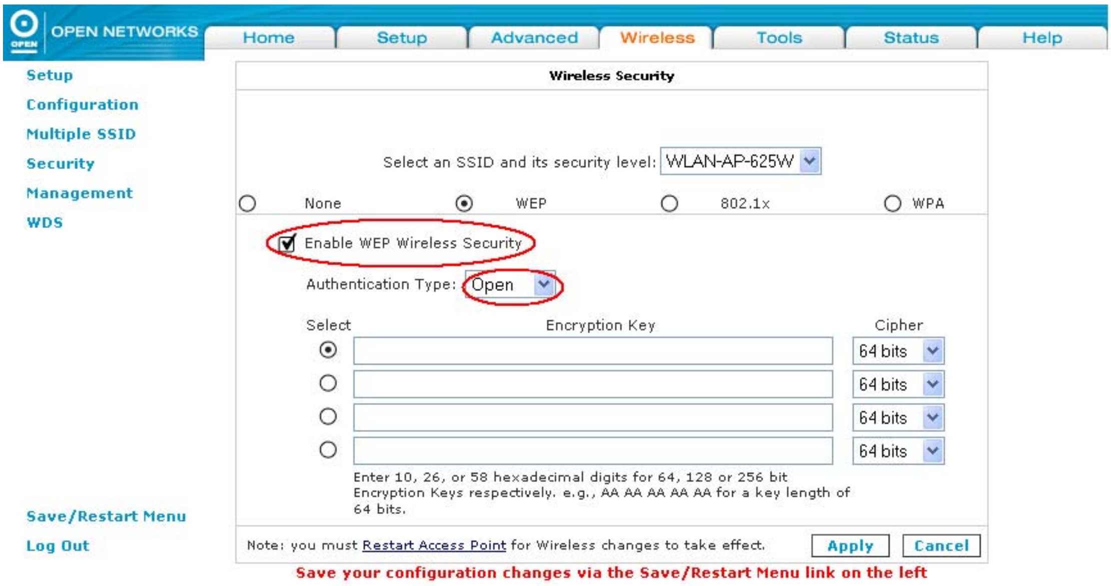
Select	Encryption Key	Cipher
●		64 bits
○		64 bits
○		64 bits
○		64 bits

Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 4: Check the ***Enable WEP Wireless Security*** checkbox to enable WEP wireless security for the selected SSID, as shown.



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

○ None ● WEP ○ 802.1x ○ WPA

☑ Enable WEP Wireless Security

Authentication Type: Open

Select	Encryption Key	Cipher
●		64 bits
○		64 bits
○		64 bits
○		64 bits

Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 5: Select the ***Authentication Type:*** *Open*, *Shared* or *Both*. The default setting is *OPEN*.

Step 6: Select the ***Encryption Key*** and select ***Cipher*** in bits. You will need to enter the same key for the first time configuration of each station.

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table lists the *WEP* wireless security screen fields and their definitions:

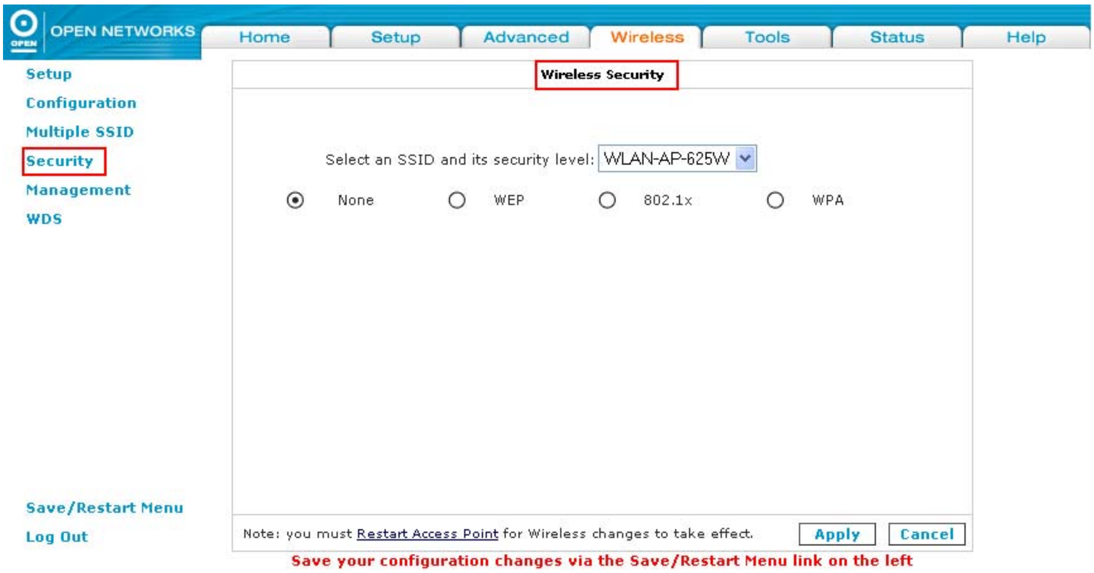
Field	Description
Select an SSID and its Security Level	If multiple SSID is enabled, use the drop-down menu to select the SSID that you want to apply wireless security to.
Enable WEP Wireless Security	Check this field to enable WEP wireless security on the selected SSID.
Authentication Type	This refers to the authentication algorithm to use when the security configuration is set to *Legacy.* This field is enabled when the WEP security field is checked. There are 3 options: • ***Open*** (default): In open-system authentication, the access point accepts any station without verifying its identity. • ***Shared***: Shared key authentication requires a shared key (WEP encryption key) be distributed to the stations before attempting authentication. • ***Both:*** If *Both* is selected, the access point will perform shared-key authentication, then open-system authentication.
Encryption Key	This field is enabled when the WEP security is checked to identify the key value that is used when the security configuration is set to WEP. The key length must match the WEP cipher.
WEP Cipher	This field is enabled when the WEP security is checked. You can select from *64 bits, 128 bits,* and *256 bits* - these are the WEP cipher that is used when the security configuration is set to *WEP*. This field is not used when the security configuration is set to *802.1x* and *WPA.*

9.4.3 802.1x

802.1x is a security protocol for WLAN. It is a port-based network access control that keeps the network disconnected until authentication is completed. 802.1x is based on extensible authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the remote authentication dial-in user server (RADIUS) protocol.

To configure wireless security for *802.1x*, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Security*** link provided. The following page appears:



Wireless Security

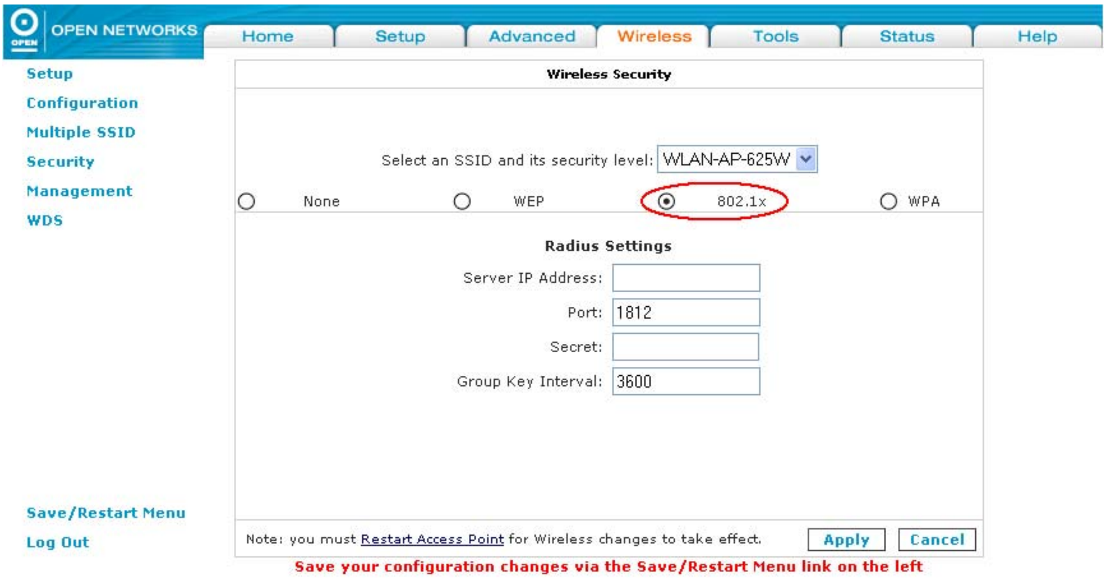
Select an SSID and its security level: WLAN-AP-625W

● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the ***802.1x*** protocol from the security options provided. The following page appears:



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

○ None ○ WEP ● 802.1x ○ WPA

Radius Settings

Server IP Address:

Port: 1812

Secret:

Group Key Interval: 3600

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Enter the IP address of the server under the ***Server IP Address*** field.

Step 4: The default ***Port*** is set to *1812*. Enter a different port number if required.

Step 5: Enter the secret that the AP shares with the RADIUS server in the ***Secret*** field.

Step 6: Enter the group key interval in seconds in the ***Group Key Interval*** field. The default value is set to *3600.*

Step 7: Click the ***Apply*** button to apply the settings.

Step 8: To save your configuration, please refer to the section under ***Save / Restart Menu****.*

The following table lists the *WEP* wireless security screen fields and their definitions:

Field	Description
Select an SSID and its Security Level	If multiple SSID is enabled, use the drop-down menu to select the SSID that you want to apply wireless security to.
Server IP Address	The IP address of the RADIUS server. This is used for authentication purposes.
Port	This is the protocol port of the RADIUS server.
Secret	This is the secret that the AP shares with the RADIUS server. You can enter up to 63 alphanumeric characters.
Group Key Interval	The group key interval that is used to distribute the group key to 802.1x and WPA stations. The default value of this field is *3600* seconds.

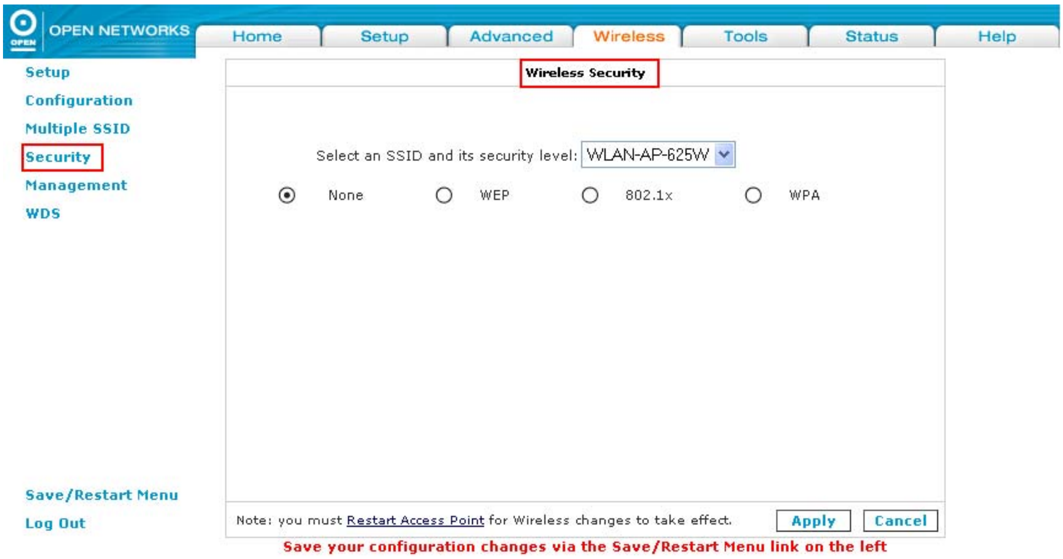
9.4.4 WPA

WPA is a security protocol for WLAN. WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an AP. Protocols including 802.1X, EAP, and RADIUS are used for strong authentication.

Like WEP, keys can still be entered manually (pre-shared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. WPA uses temporal key integrity protocol (TKIP) for data encryption. WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol for data encryption.

To configure *WPA* wireless security, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Security*** link provided. The following page appears:



Wireless Security

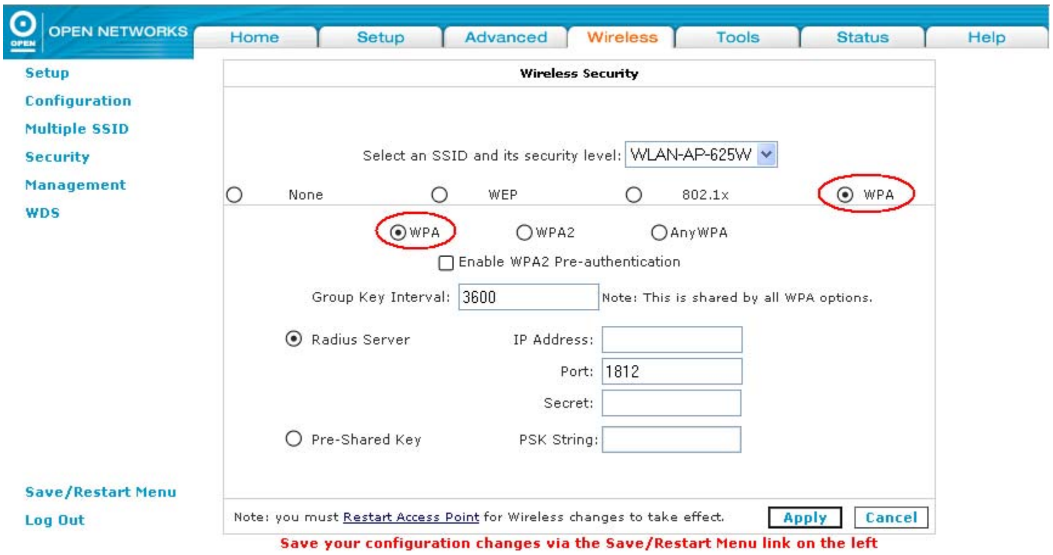
Select an SSID and its security level: WLAN-AP-625W

● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the ***WPA*** protocol from the security options provided. The following page appears:



Wireless Security

Select an SSID and its security level: WLAN-AP-625W

○ None ○ WEP ○ 802.1x ● WPA

● WPA ○ WPA2 ○ AnyWPA

□ Enable WPA2 Pre-authentication

Group Key Interval: 3600 Note: This is shared by all WPA options.

● Radius Server IP Address:

Port: 1812

Secret:

○ Pre-Shared Key PSK String:

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: The ***WPA*** radio option is highlighted by default as shown above. You may select from 2 other options provided as applicable: *WPA2, AnyWPA*.

Step 4: The default ***Group Key Interval*** field is set to *3600* seconds. Enter a different interval time if required.

Step 5: The ***Radius Server*** is the default radio option selected. Select ***Pre-Shared Key*** radio option if a pre-shared secret with the AP is used instead.

Step 6: Enter the IP address of the Radius Server in the ***IP Address*** field.

Step 7: The default port number is set to *1812*. Enter a different port number in the ***Port*** field if required.

Step 8: Enter the ***Secret*** field.

Step 9: Click the ***Apply*** button to apply the settings.

Step 10: To save your configuration, please refer to the section under **Save / Restart Menu**.

The following table lists the *WPA* wireless security screen fields and their definitions:

Field	Description	
Select an SSID and its Security Level	If multiple SSID is enabled, use the drop-down menu to select the SSID that you want to apply wireless security to.	
WPA Options	***WPA***	Enables stations that support WPA v.1 to connect to the AP.
	WPA2	Enables stations that support WPA v.2 to connect to the AP.
	Any WPA	Enables stations that support WPA v.1 and WPA v.2 to connect to the AP.
Enable WPA2 Pre-Authentication	Enables / Disables WPA2 pre-authentication. This field is only activated when *WPA2* or *AnyWPA* is enabled.	
Group Key Interval	This value is measured in seconds. The default value is *3600* seconds.	
Radius Server	When selected, the WPA stations authenticate with the RADIUS server using extensible authentication protocol - transport layer security (EAP-TLS) over 802.1x.	
	IP Address	The IP address of the RADIUS server.
	Port	The protocol port of the RADIUS server.
	Secret	This is the secret that the AP shares with the RADIUS server. You can enter up to 63 alphanumeric characters into this field.
Pre-Shared Key	When selected, the WPA stations do not authenticate with the RADIUS server using EAP-TLS. Instead, they share a pre-shared key secret with the AP (ASCII format).	
	PSK String	PSK stands for the pre-shared key string. The PSK string needs to be entered in the first time configuration of each station. You can enter *8 - 63* alphanumeric characters in this field.

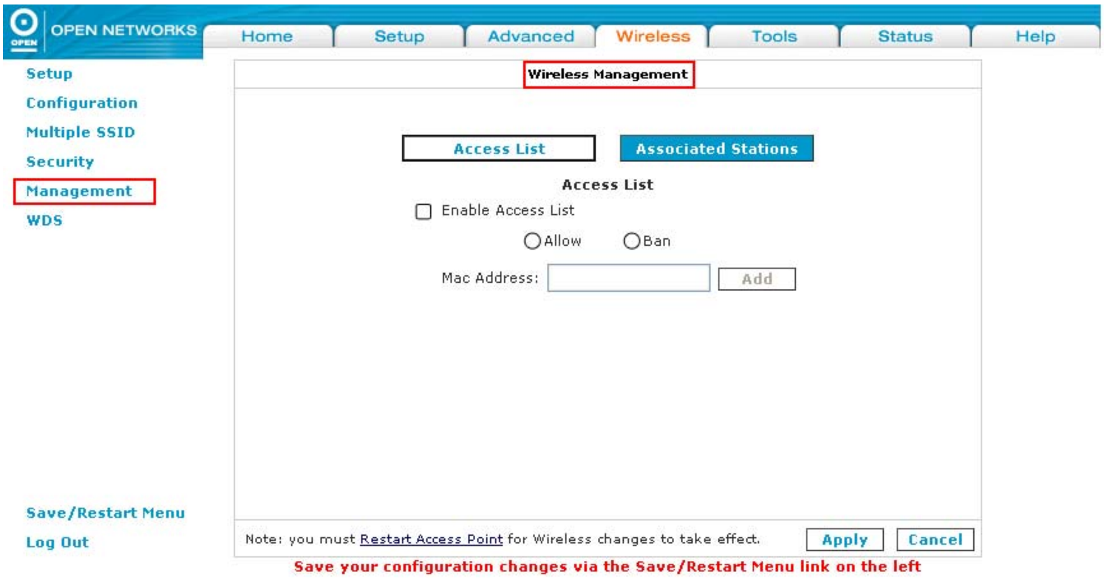
9.5 Management

The wireless Management function gives another level of security to your AP. It allows you to create either an allowed access list or a banned access list and view a list of stations associated with your access point.

The Associated Stations page allows you to see a list of all the stations associated with the AP. From this screen, you can ban any station if required.

To configure *Management* and access *Associated Stations*, please follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***Management*** link provided. The following page appears:



Wireless Management

Access List

□ Enable Access List

○ Allow ○ Ban

Mac Address:

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Check the ***Enable Access List*** checkbox.

Step 3: Highlight the ***Allow*** radio button to create an allowed access list or ***Ban*** radio button to create a banned list.

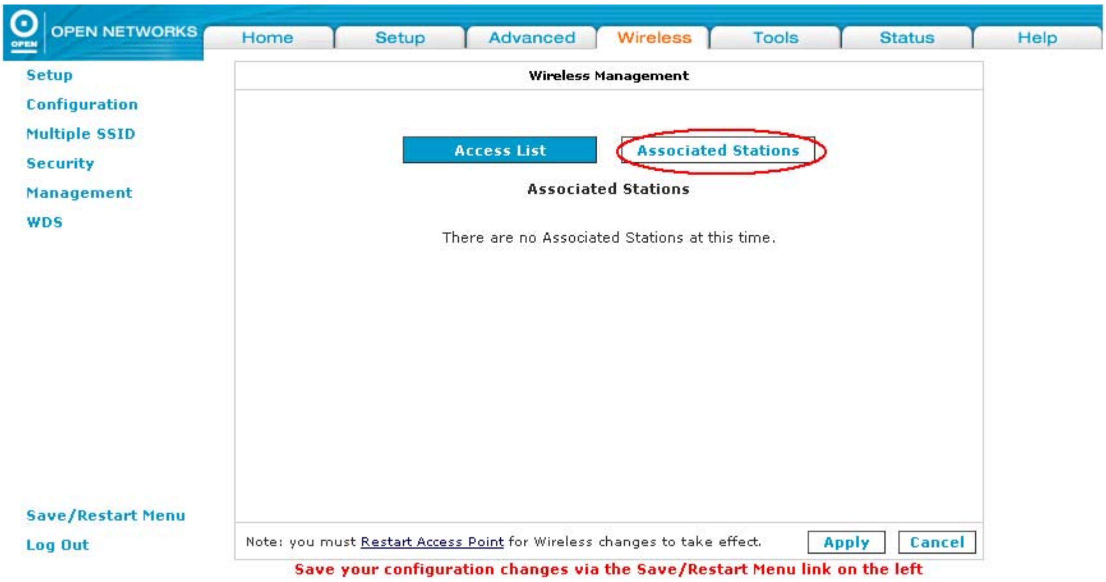
NOTE	***You cannot select both Allow and Ban; you can only select one option.***

Step 4: Enter a MAC address of an allowed or banned station in the ***MAC Address*** field.

Step 5: Click the ***Add*** button.

Step 6: Repeat this step for each station you want to add to your access list.

Step 7: To view associated stations, click the ***Associated Stations*** button. The following page appears:



Wireless Management

Associated Stations

There are no Associated Stations at this time.

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 8: Click the ***Apply*** button to apply the settings.

Step 9: To save your configuration, please refer to the section under ***Save / Restart Menu***.

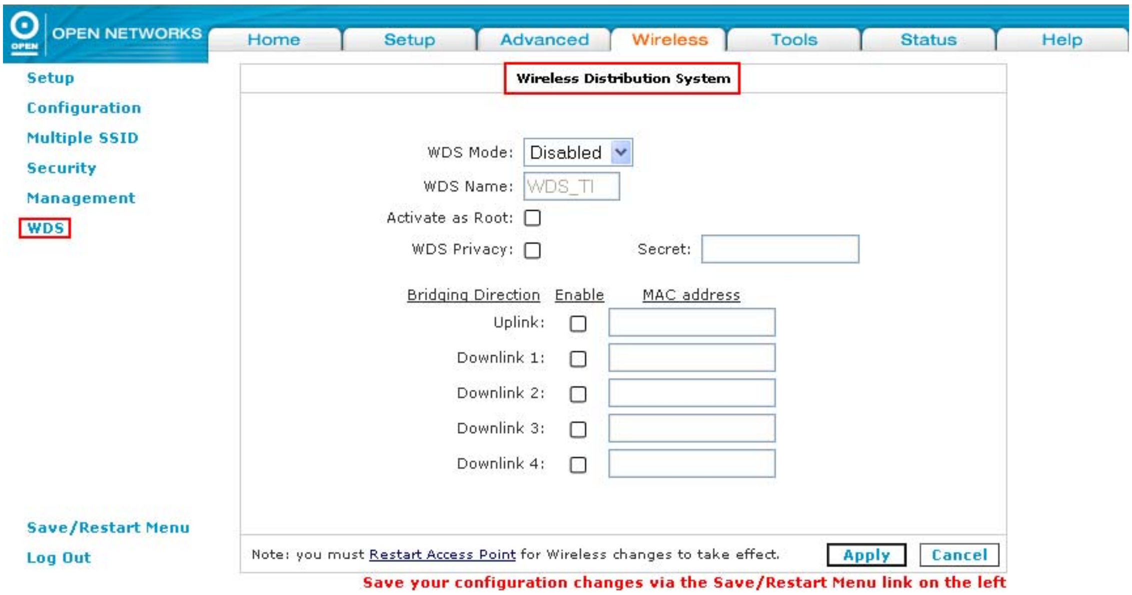
9.6 WDS

Wireless Distribution System (WDS) is a system that interconnects BSS (Basic Service Set) to build a premise wide network. BSS are communicating stations on a wireless LAN.

WDS network allows users of mobile equipment to roam and stay connected to the available network resources. You can configure your iConnect625W router AP as WDS mode using the WDS page.

To configure *WDS*, follow the steps below.

Step 1: From the ***Wireless*** tab, click the ***WDS*** link provided. The following page appears:



Wireless Distribution System

WDS Mode: Disabled

WDS Name: WDS_TI

Activate as Root: □

WDS Privacy: □ Secret:

Bridging Direction	Enable	MAC address
Uplink:	□	
Downlink 1:	□	
Downlink 2:	□	
Downlink 3:	□	
Downlink 4:	□	

Note: you must Restart Access Point for Wireless changes to take effect.

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the ***WDS Mode*** option from the drop-down list to enable WDS.

Step 3: The ***WDS Name*** is used to identify the WDS network. It is defaulted to WDS_TI.

Step 4: Check the ***Activate as Root*** checkbox for the WDS hierarchy to work.

Step 5: Check the ***WDS Privacy*** to use a secured connection between APs in the WDS network.

NOTE	**WDS Privacy is not supported in Crude mode.**

Step 6: Enter the secret privacy key in the ***Secret*** field.

Step 7: The ***Uplink*** checkbox enables the uplink to enter a MAC address to the upper device in the WDS hierarchy. It cannot be configured if *Root* is enabled.

Step 8: Check the ***Downlink 1 - 4*** checkboxes as required. Enter the MAC address of the lower device in the WDS hierarchy.

Step 9: Click the ***Apply*** button to apply the settings.

Step 10: To save your configuration, please refer to the section under ***Save / Restart Menu***.

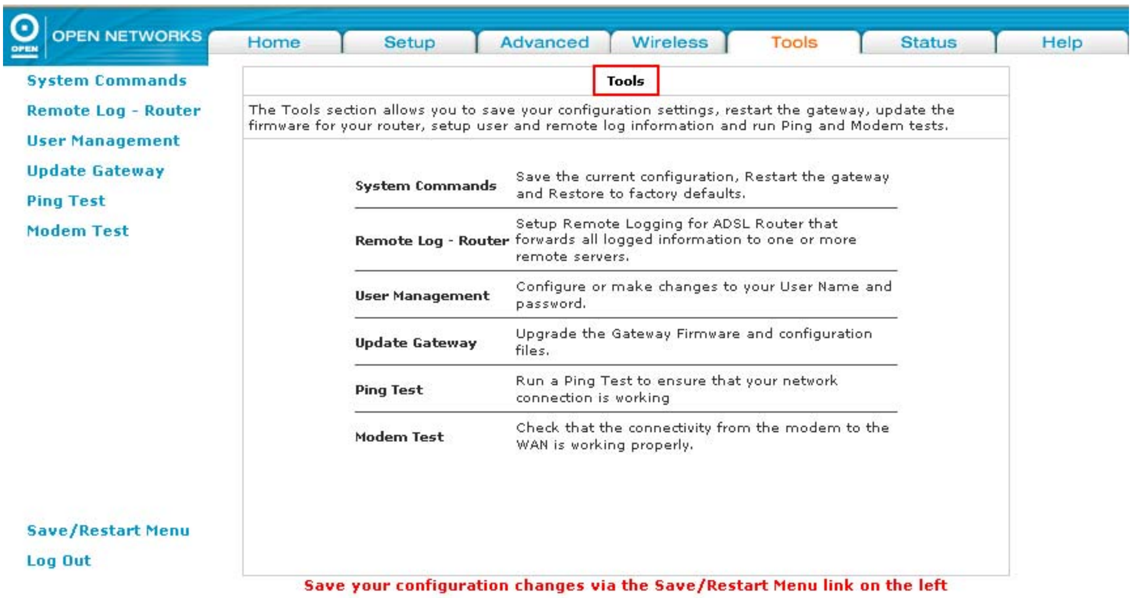
The following table lists the *WDS* screen fields and their definitions:

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td><b><i>WDS Mode</i></b></td><td colspan="2">The following <i>WDS modes</i> are available:
• <b><i>Bridge</i></b>: In <i>Bridge</i> mode, the AP BSS is enabled.
• <b><i>Repeater</i></b>: In <i>Repeater</i> mode, the AP BSS is disabled when connection to the upper layer AP is established.
• <b><i>Crude</i></b>: In <i>Crude</i> mode, the AP BSS service is always enabled, but the links between APs are configured statically and are not maintained.
• <b><i>Disabled (Default)</i></b>: WDS is inactive.
In both <i>Bridge</i> and <i>Repeater modes,</i> WDS uses management protocol to establish and maintain links between APs.</td></tr>
<tr><td><b><i>WDS Name</i></b></td><td colspan="2">This is the WDS name that identifies the WDS network. The field takes up to 8 characters. Two or more WDS networks may exist in the same area.</td></tr>
<tr><td><b><i>Activate as Root</i></b></td><td colspan="2">This field must be checked for the root device in the WDS hierarchy. Only one WDS root device may exist in the WDS network. This field is not applicable for Crude mode.</td></tr>
<tr><td><b><i>WDS Privacy</i></b></td><td colspan="2">Checking this field commands the WDS manager to use a secured connection between APs in the WDS network. Security settings must be the same in all APs in the WDS network.</td></tr>
<tr><td><b><i>Secret</i></b></td><td colspan="2">This is the 32-character alphanumeric privacy key.</td></tr>
<tr><td><b><i>Uplink</i></b></td><td colspan="2">This is the BSS ID of the upper device in the WDS hierarchy. This uplink cannot be configured if <i>Root</i> is enabled.</td></tr>
<tr><td rowspan="4"><b><i>Downlink</i></b></td><td><b><i>Downlink 1</i></b></td><td rowspan="4">These are the BSS IDs of the lower device in the WDS hierarchy connected to this AP. Up to four downlinks can be configured.</td></tr>
<tr><td><b><i>Downlink 2</i></b></td></tr>
<tr><td><b><i>Downlink 3</i></b></td></tr>
<tr><td><b><i>Downlink 4</i></b></td></tr>
</table>

10. Tools

The *Tools* main page provides access to the following features:

- Systems Commands
- Remote Log - Router
- User Management
- Update Gateway
- Ping Test
- Modem Test



Tools

The Tools section allows you to save your configuration settings, restart the gateway, update the firmware for your router, setup user and remote log information and run Ping and Modem tests.

System Commands	Save the current configuration, Restart the gateway and Restore to factory defaults.
Remote Log - Router	Setup Remote Logging for ADSL Router that forwards all logged information to one or more remote servers.
User Management	Configure or make changes to your User Name and password.
Update Gateway	Upgrade the Gateway Firmware and configuration files.
Ping Test	Run a Ping Test to ensure that your network connection is working
Modem Test	Check that the connectivity from the modem to the WAN is working properly.

Save your configuration changes via the Save/Restart Menu link on the left

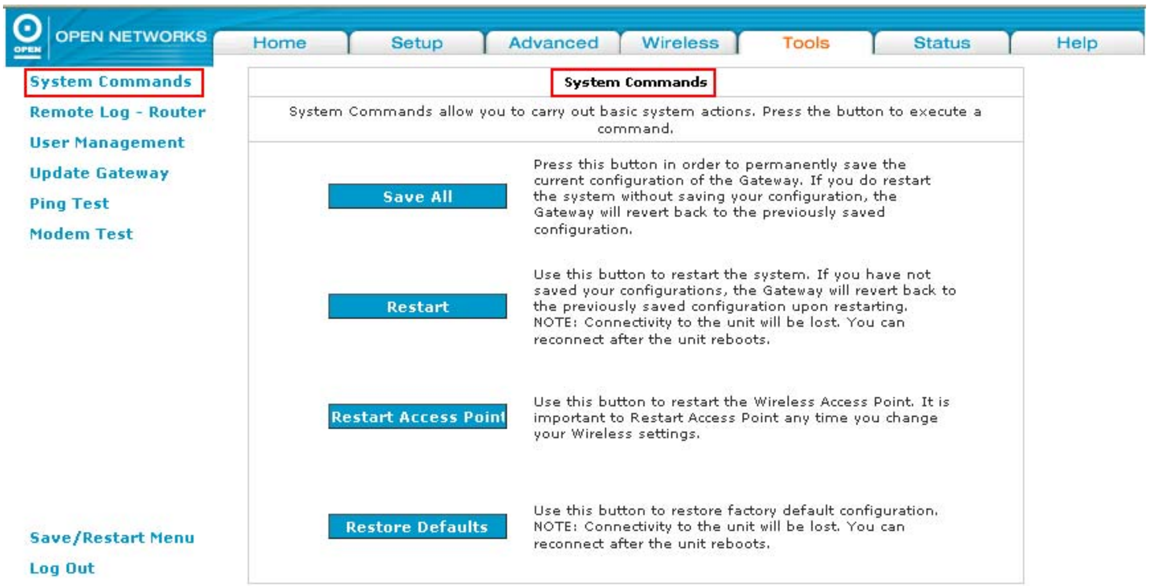
The following sections describe these features in detail.

10.1 System Commands

Systems Commands allows you to save all your new settings, restart the iConnect625W router, restart the Wireless Access Point and to restore default configurations.

To access *System Commands*, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***System Commands*** link provided. The following page appears:



System Commands

System Commands allow you to carry out basic system actions. Press the button to execute a command.

Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.

Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.

Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Step 2: Read the definitions in the table below for the purpose of each of the System Commands buttons: *Save All, Restart, Restart Access Point* and *Restore Defaults*.

The following table describes the *Systems Commands* screen fields and their definitions:

Field	Description
Save All	This command allows you to permanently save the current configuration of your iConnect625W router. If you restart the system without saving your configuration, the iConnect625W reverts to the previously saved configuration.
Restart	This command allows you to restart the system.
Restart Access Point	This command allows you to restart the wireless AP. It is important to restart the AP anytime you change your wireless settings.
Restore Defaults	Use this command to restore factory default configuration. NOTE *Connectivity to the unit will be lost. You can reconnect after the unit reboots.*

10.2 Remote Log

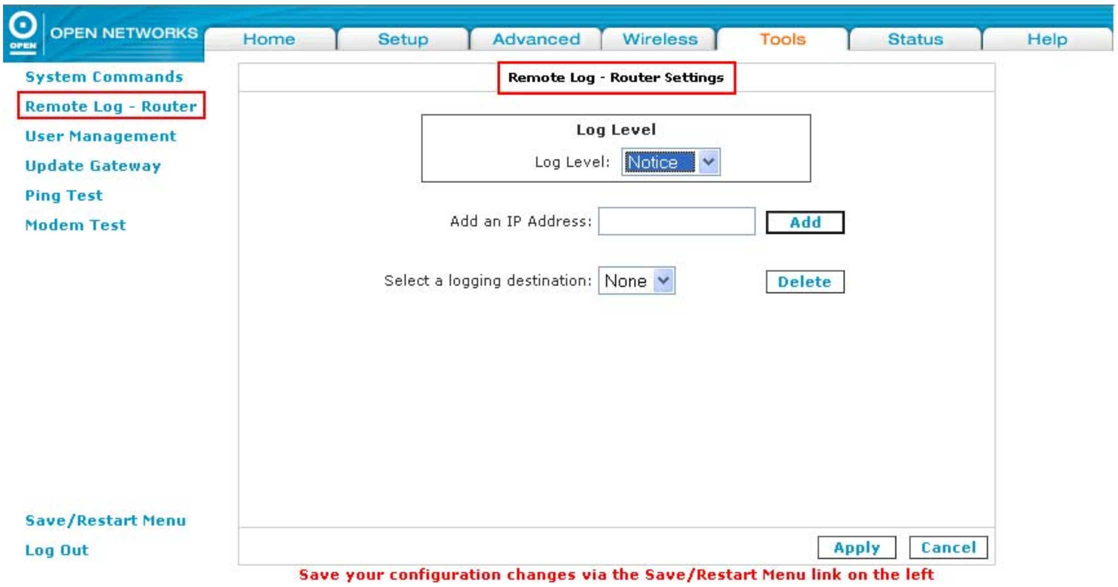
The Remote Log feature is used in conjunction with the PC tool (software provided with your iConnect625W router). You can select the Log Level, add an IP address and select a logging destination on the Remote Log page.

The Remote Log feature allows you to forward all logged information to one or more remote syslog servers. The type of information forwarded to the remote server depends on the Log Level selected. Each log message is assigned a severity level, which indicates how seriously the triggering event affects the iConnect625W functions.

When you configure logging, you must specify a severity level. Log Levels that are rated at that level or higher are sent to the syslog server and can be viewed using the syslog server application.

To configure the router settings using *Remote Log*, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***Remote Log - Router*** link provided. The following page appears:



Remote Log - Router Settings

Log Level

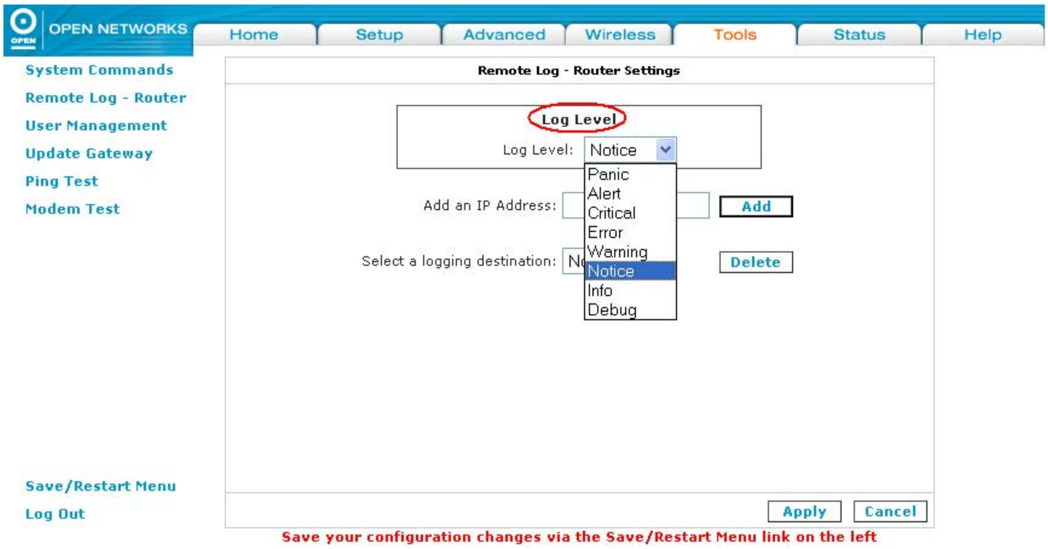
Log Level: Notice

Add an IP Address:

Select a logging destination: None

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the ***Log Level*** from the drop-down options, as shown below. For PPPoE and PPPoA connections, you can select ***Debug*** if you want to log the connection information. This is helpful when trying to debug connection problems.



Log Level: Notice

Add an IP Address:

Select a logging destination: N

Save your configuration changes via the Save/Restart Menu link on the left

NOTE	**When you select a log level, all log information within this severity level and levels above it (i.e. more severe levels) are sent to the remote station.**

Step 3: Enter the ***IP Address*** of the remote station, e.g. the syslog server that the log information is to be sent to.

Step 4: Click the ***Add*** button. This station will be added to the drop-down list of the ***Select A Logging Destination*** field.

Step 5: Select the ***Logging Destination.*** You can edit the logging destination listing using the ***Add*** or ***Delete*** buttons.

Step 6: Click the ***Apply*** button to apply the settings.

Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

The following table describes the *Remote Log - Router* screen fields and their definitions:

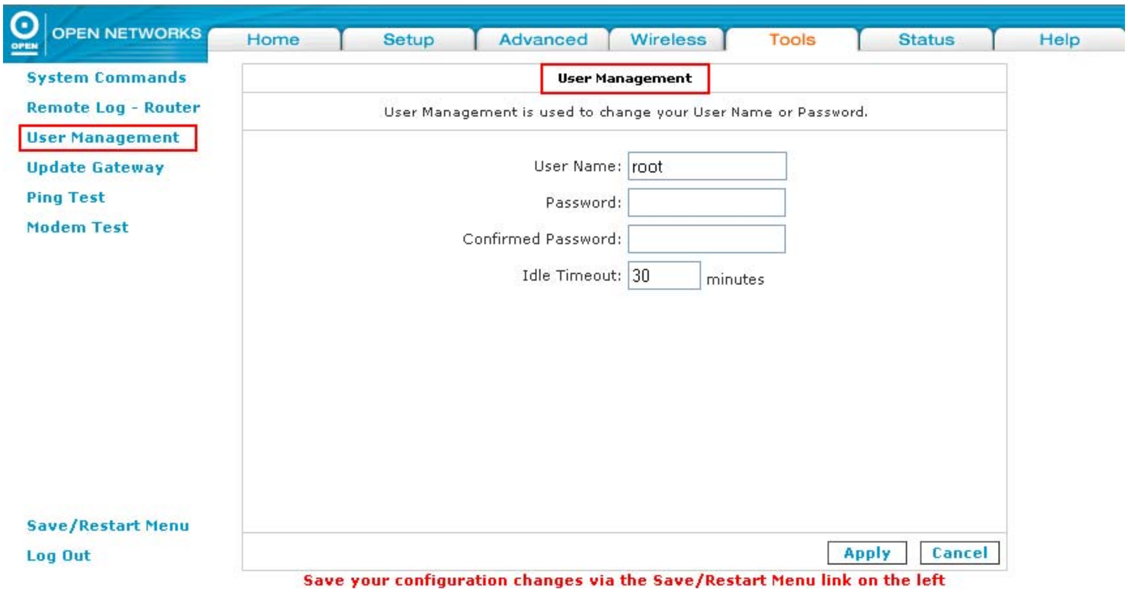
Field	Description	
Log Level	There are 8 log levels listed in order of severity. The default log level is *Notice.* NOTE *When you select a log level, all log information within this severity level and levels above it (i.e. more severe levels) are sent to the remote station.*	
	Panic	System panic or other condition that causes the iConnect625W router to stop functioning.
	Alert	Conditions that require immediate correction, such as a corrupted system database.
	Critical	Critical conditions, such as hard drive errors.
	Error	Error conditions that generally have less serious consequences than errors in the emergency, alert and critical levels.
	Warning	Conditions that require monitoring.
	Notice	Conditions that are errors but might require special handling.
	Info	Events or non-error conditions of interest.
	Debug	Software debugging message. Specify the level only when so directed by a technical support representative.
Add an IP Address	You should enter the IP address of the remote host to which you want the log information to be forwarded. You can add more IP addresses and any IP addresses added will appear in the drop-down list of the next field, *Select a Logging Destination*.	
Select a Logging Destination	You can select a destination IP address to delete. You can customize the destination using the ***Add*** or ***Delete*** button.	

10.3 User Management

The User Management feature allows you to change your login and password details and to define the idle timeout lapse time.

To access and make changes in the User Management page, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***User Management*** link provided. The following page appears:



User Management

User Management is used to change your User Name or Password.

User Name: root

Password:

Confirmed Password:

Idle Timeout: 30 minutes

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Your default user name is ***root.*** Enter a new user name in the ***User Name*** field, if required.

Step 3: Your default password is ***ØP3N*** (zero-P-three-N). Enter a new password in the ***Password*** field, if required.

NOTE	**If you have forgotten your password, you may press and hold the Reset button located at the back of your router for 10 seconds or more. The iConnect625W router will reset to its factory default configuration and all custom configurations will be lost.**

Step 4: Enter your new password again in the ***Confirmed Password*** field.

Step 5: The default ***Idle Timeout*** field is *30* minutes. You will have to log back into the iConnect625W router after your session has been inactive for 30 minutes. You can amend the timeout period in the field, if required.

Step 6: Click the ***Apply*** button to apply the settings.

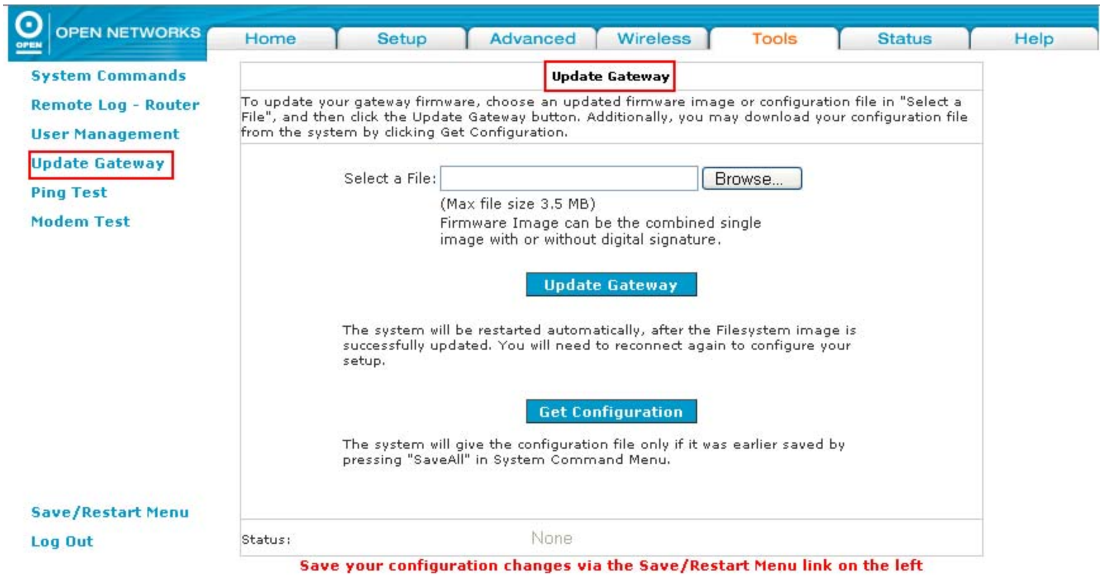
Step 7: To save your configuration, please refer to the section under ***Save / Restart Menu***.

10.4 Update Gateway

The Update Gateway page allows you to update the iConnect625W router's firmware and configuration files.

To upload and download configuration files and firmware for your iConnect625W router using *Update Gateway*, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***Update Gateway*** link provided. The following page appears:



Update Gateway

To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.

Select a File:

(Max file size 3.5 MB)
Firmware Image can be the combined single image with or without digital signature.

The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.

The system will give the configuration file only if it was earlier saved by pressing "SaveAll" in System Command Menu.

Status: None

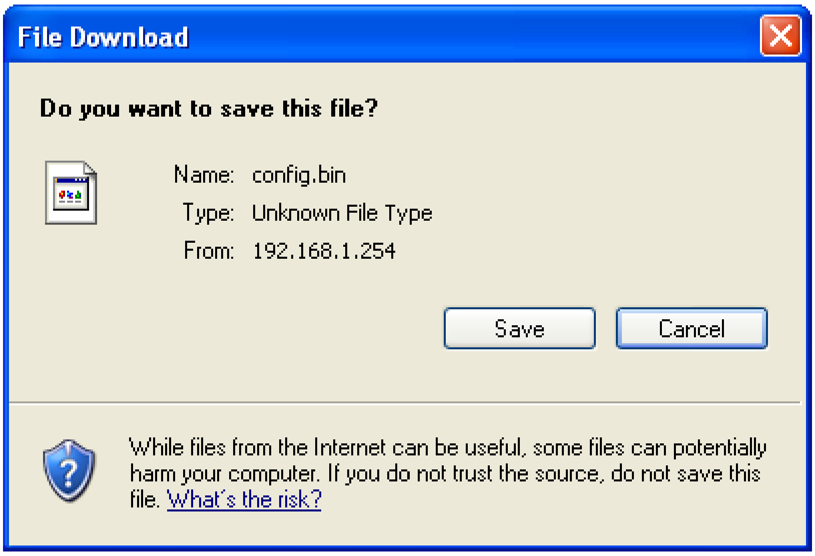
Save your configuration changes via the Save/Restart Menu link on the left

Step 2: **Upload Firmware:** click the ***Browse*** button and select the location of the firmware file to be uploaded, e.g. *'C:\Program Files\firmware v1.1'.*

NOTE	**The file size should not exceed 3.5MB as specified on the Update Gateway screen.**

Step 3: Click the ***Update Gateway*** button. The status of the uploading appears at the bottom of the page. When the upload is completed, the iConnect625W router reboots and you are prompted to log in again.

Step 4: **Get Configuration:** Click the ***Get Configuration*** button. The following dialogue box appears. Click the ***Save*** button to download the configuration file.



File Download

Do you want to save this file?

Name: config.bin

Type: Unknown File Type

From: 192.168.1.254

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

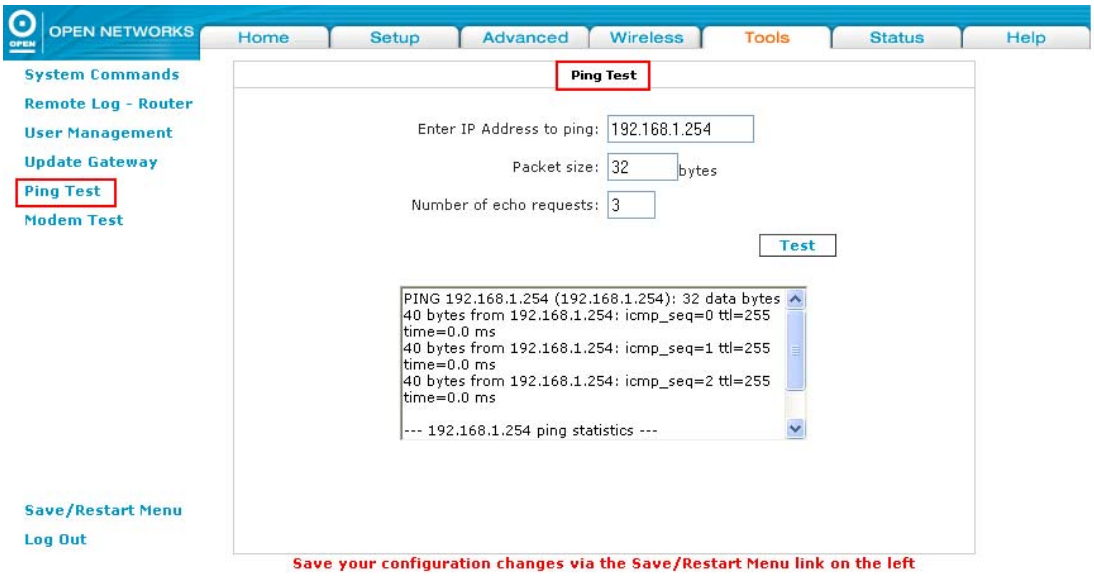
Step 5: **Upload Configuration:** Follow Step 1 above to select the configuration file to upload. Click the ***Update Gateway*** button to upload the configuration file. The status of the uploading appears at the bottom of the page. When the upload is completed, the iConnect625W router reboots and you are prompted to log in again.

10.5 Ping Test

Once the iConnect625W router has been configured, it is a good idea to make sure that you can ping the network. If you can ping an IP on the WAN side successfully, you should be able to surf the Internet.

To perform a *Ping Test*, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***Ping Test*** link provided. The following page appears:



Enter IP Address to ping: 192.168.1.254

Packet size: 32 bytes

Number of echo requests: 3

```
PING 192.168.1.254 (192.168.1.254): 32 data bytes
40 bytes from 192.168.1.254: icmp_seq=0 ttl=255
time=0.0 ms
40 bytes from 192.168.1.254: icmp_seq=1 ttl=255
time=0.0 ms
40 bytes from 192.168.1.254: icmp_seq=2 ttl=255
time=0.0 ms

--- 192.168.1.254 ping statistics ---
```

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Change or leave the default settings of the following fields:

- ***Enter the IP Address to Ping*** field where default setting is *192.168.1.254.* This is the WAN-side IP address that you want to ping;

- ***Packet Size*** field where the default settings is *32* bytes. You can define the packet size of the ping test;

- ***Number of Echo Requests*** field where the default settings is *3.* You can define how many times the IP address will be pinged.

Step 3: Click the ***Test*** button. The ping results are displayed in the box shown on the page. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the ping test failed, you should restart the iConnect625W router.

10.6 Modem Test

The Modem Test feature is used to check the connectivity to the WAN. There are four test types: F4 End, F4 Seg, F5 End, F5 Seg. Each of these types may take a few seconds to complete. In order for the test to work, at least one WAN connection must be configured and a valid DSL link is available. If the DSL link is not connected, the test will fail.

The OAM (operation, administration and maintenance) loopback cells (F4/F5) are used to verify the connection between the iConnect625W and the ATM network. For the iConnect625W, OAM loopback provides a valuable tool for diagnosing problems with the DSL line. The two main purposes of the F4/F5 cells are:

- Fault Management (detection and notification);
- Loopback testing and link integrity

The ATM OAM is divided into several levels:

- **F4: VP Level**
  - OAM information flows between network elements (NEs) used within virtual paths to report an unavailable path or virtual path (VP) that cannot be guaranteed. Segment flows are processed, as well as end-to-end flows that terminate in the management processor.

- **F5: VC Level**
  - OAM information flows between network elements (NEs) used within virtual connections to report degraded virtual channel (VC) performance such as late arriving cells, lost cells and cell insertion problems. Segment flows are processed, as well as end-to-end flows that terminate in the management processor.

Both F4 and F5 flows can be configured as one of the test types:

- **Segment**
  - This test verifies that ATM continuity exists between the virtual channel link segments from the iConnect625W router to the DSL provider network (typically this is a DSLAM at the DSL provider site). DSLAM stands for *Digital Subscriber Line Access Multiplexer.*

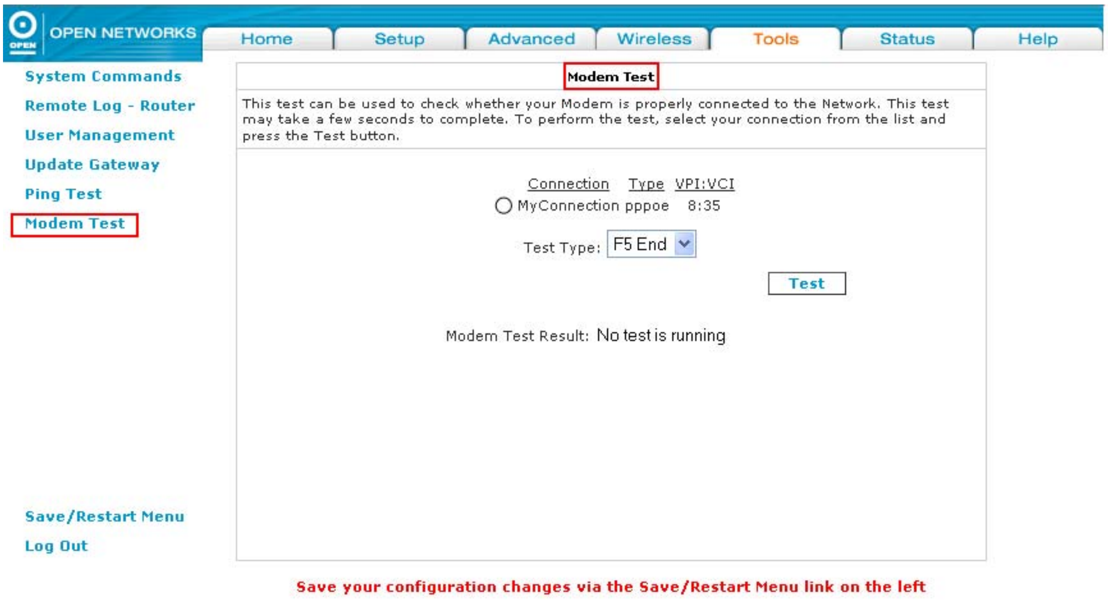
- **End-to-End**
  - This test verifies ATM continuity exists of the virtual channel link with the ATM endpoint, such as a remote broadband access router located at the DSL provider or ISP site.

Before you attempt any of these modem tests, ensure the following:

- Your DSL Provider / ISP supports them;
- You have a valid DSL link.

To perform a modem test, follow the steps below.

Step 1: From the ***Tools*** tab, click the ***Modem Test*** link provided. The following page appears:



Modem Test

This test can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button.

	Connection	Type	VPI:VCI
○	MyConnection	pppoe	8:35

Test Type: F5 End

Test

Modem Test Result: No test is running

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Select the ***Connection*** you want to test and the ***Test Type.***

NOTE	**You will not be able to perform a modem test without any WAN connections configured.**

Step 3: Click the ***Test*** button. The modem test results are displayed on the page.

The following table describes the *Modem Test Types* and their definitions:

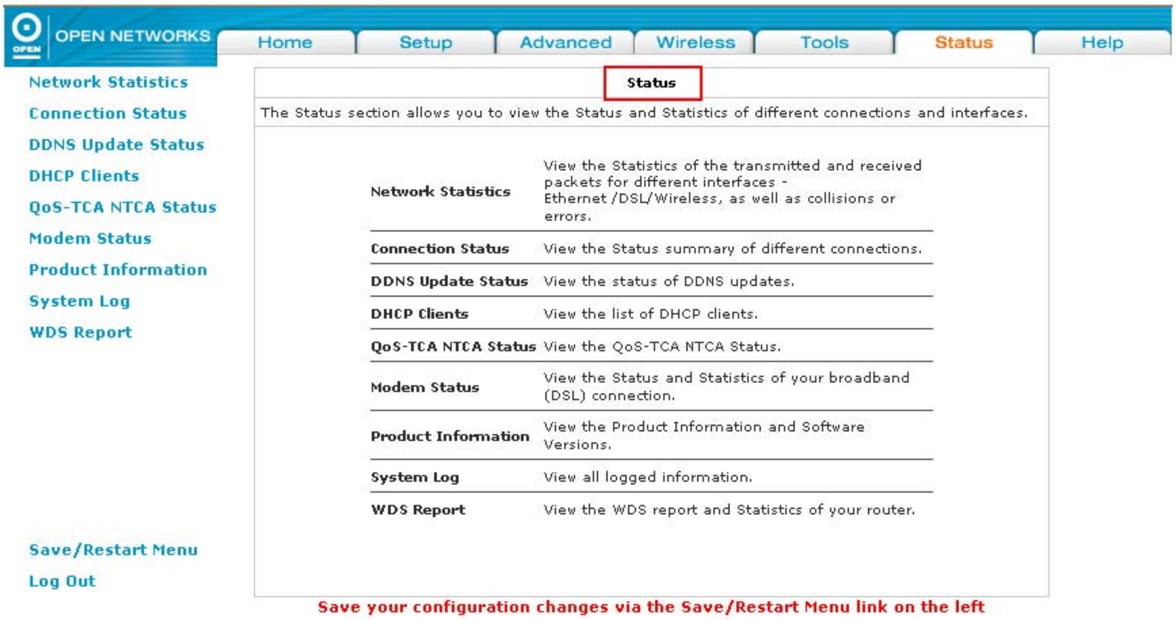
Field	Description	
Test Type	There are 4 Test Types available.	
	F5 End	Connectivity to the BRAS server can be verified by initiating an *F5 Seg* loopback via the DSLAM and to the authentication server. A DLSAM is a mechanism at the service provider's central location that links many customer DSL connections to a single-speed ATM line.
	F5 Seg	Lost and corrupted ATM cells can be quickly ruled out in the field by initiating a F5 Seg loopback (also known as ATM ping) to the DSLAM and have the DSLAM respond by looping back the OAM cells. By ruling out problems with the ATM Layer, the service provider can then focus on examining higher layer protocols and other configurations to isolate the problem.
	F4 Seg	*Segment* **-** the end of the connection segment.
	F4 End	*End-to-End* - the end of t a VC/VP connection where the ATM cells are terminated.

11. Status

The Status tab of the iConnect625W web interface allows you to view the status and statistics of different connections and interfaces. This page provides access to the following status pages:

- Network Statistics;
- Connection Status;
- DDNS Update Status;
- DHCP Clients;
- QOS-TCA NTCA Status;
- Modem Status;
- Production Information;
- System Log;
- WDS Report

Each of the features under the *Status Tab* is described in the following sections.



Status

The Status section allows you to view the Status and Statistics of different connections and interfaces.

Network Statistics	View the Statistics of the transmitted and received packets for different interfaces - Ethernet /DSL/Wireless, as well as collisions or errors.
Connection Status	View the Status summary of different connections.
DDNS Update Status	View the status of DDNS updates.
DHCP Clients	View the list of DHCP clients.
QoS-TCA NTCA Status	View the QoS-TCA NTCA Status.
Modem Status	View the Status and Statistics of your broadband (DSL) connection.
Product Information	View the Product Information and Software Versions.
System Log	View all logged information.
WDS Report	View the WDS report and Statistics of your router.

Save your configuration changes via the Save/Restart Menu link on the left

11.1 Network Statistics

The *Network Statistics* page shows you details of transmitted and received packets for your Ethernet and DSL connections, along with any collisions or errors.

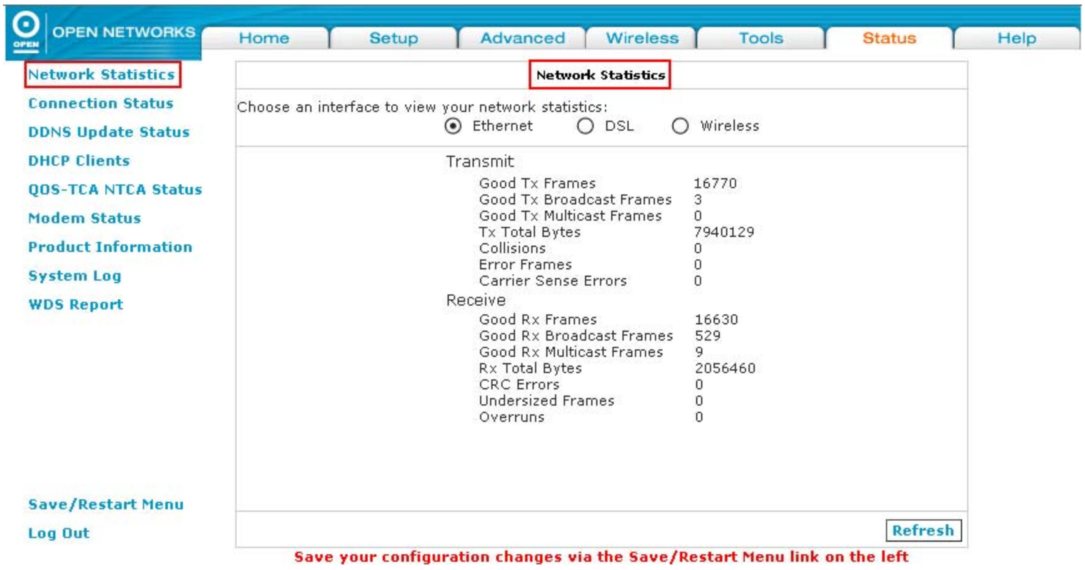
From the Ethernet Network Statistics screen, you can view the network statistics of the following interfaces by clicking the appropriate radio button at the top of the screen:

- Ethernet;
- DSL;
- Wireless.

To access and view the *Network Statistics* screen and interfaces, follow the steps in the four sections below.

11.1.1 Ethernet Statistics

Step 1: Click the ***Status*** tab and the ***Network Statistics*** link. The following page appears:



Network Statistics

Choose an interface to view your network statistics:
● Ethernet ○ DSL ○ Wireless

```
Transmit
     Good Tx Frames              16770
     Good Tx Broadcast Frames    3
     Good Tx Multicast Frames    0
     Tx Total Bytes              7940129
     Collisions                  0
     Error Frames                0
     Carrier Sense Errors        0
Receive
     Good Rx Frames              16630
     Good Rx Broadcast Frames    529
     Good Rx Multicast Frames    9
     Rx Total Bytes              2056460
     CRC Errors                  0
     Undersized Frames           0
     Overruns                    0
```

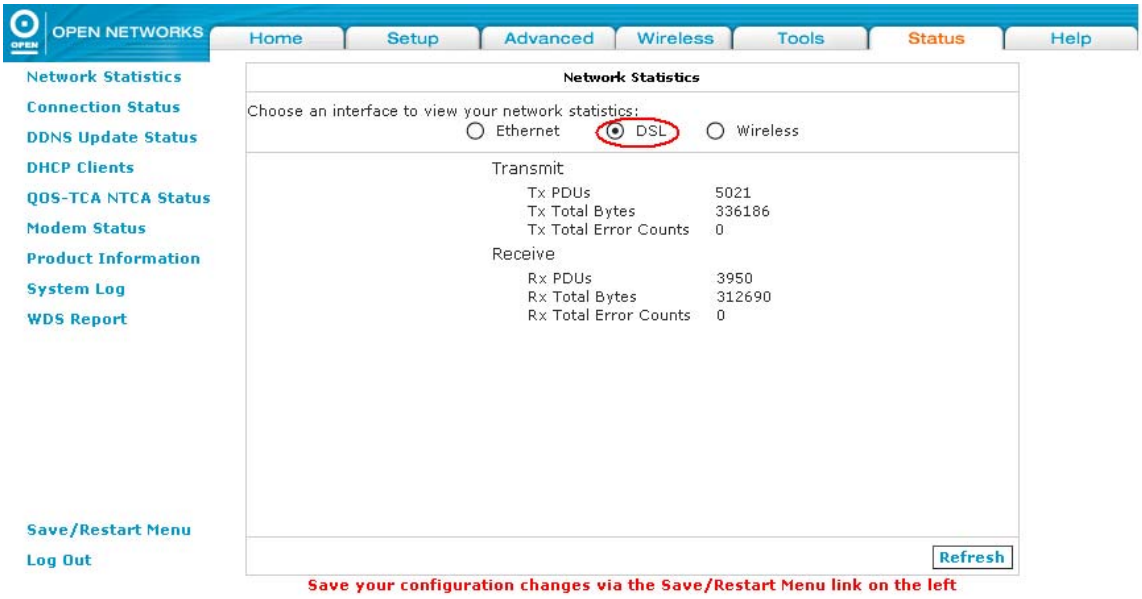
Save your configuration changes via the Save/Restart Menu link on the left

Step 2: The default setting for the *Network Statistics* interface is ***Ethernet***.

Step 3: Click the ***Refresh*** button to update the screen details of the network statistics.

11.1.2 DSL Statistics

Step 1: From the ***Network Statistics*** page, highlight the ***DSL*** interface radio button to view the DSL network statistics. The following page appears:



Network Statistics

Choose an interface to view your network statistics:
○ Ethernet ● DSL ○ Wireless

Transmit

Tx PDUs	5021
Tx Total Bytes	336186
Tx Total Error Counts	0

Receive

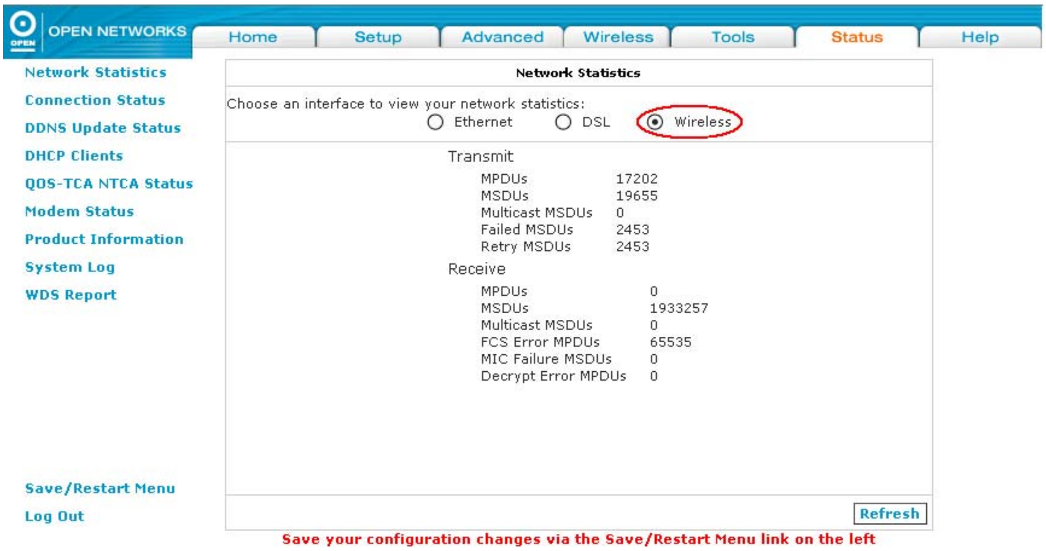
Rx PDUs	3950
Rx Total Bytes	312690
Rx Total Error Counts	0

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Click the ***Refresh*** button to update the screen details the DSL network statistics.

11.1.3 Wireless Statistics

Step 1: From the ***Network Statistics*** page, highlight the ***Wireless*** radio button to view the Wireless network statistics. The following page appears:



Network Statistics

Choose an interface to view your network statistics:
○ Ethernet ○ DSL ● Wireless

```
Transmit
    MPDUs              17202
    MSDUs              19655
    Multicast MSDUs    0
    Failed MSDUs       2453
    Retry MSDUs        2453
Receive
    MPDUs                   0
    MSDUs                   1933257
    Multicast MSDUs         0
    FCS Error MPDUs         65535
    MIC Failure MSDUs       0
    Decrypt Error MPDUs     0
```

Save your configuration changes via the Save/Restart Menu link on the left

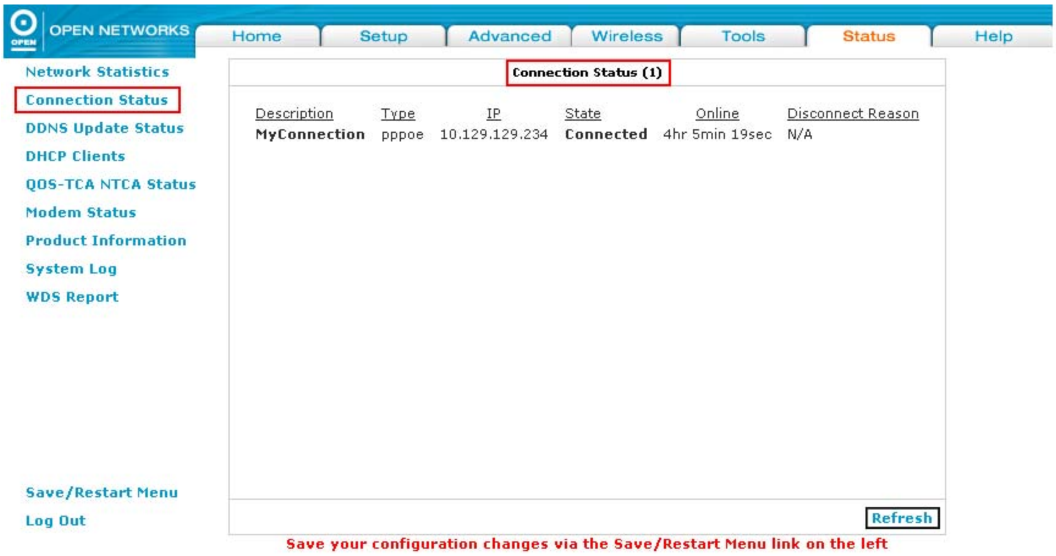
Step 2: Click the ***Refresh*** button to update the screen details for the Wireless network statistics.

11.2 Connection Status

The *Connection Status* screen displays a status summary of the ADSL connection.

To view the *Connection Status*, follow the steps below.

Step 1: Click the ***Status*** tab and the ***Connection Status*** link. The following page appears:



Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
MyConnection	pppoe	10.129.129.234	Connected	4hr 5min 19sec	N/A

Save your configuration changes via the Save/Restart Menu link on the left

The following table describes the *Modem Test Types* and their definitions:

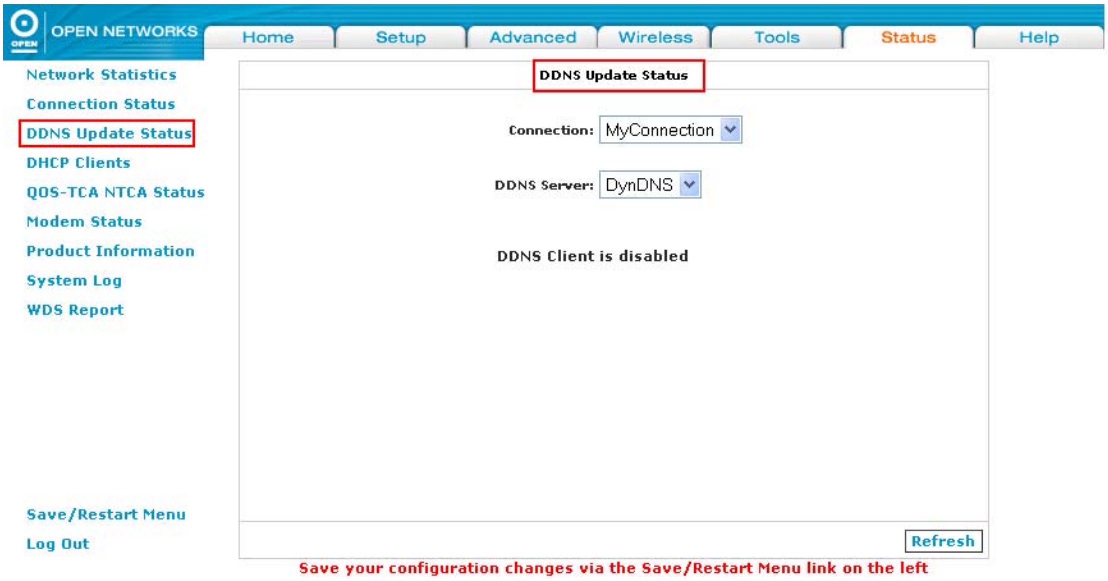
Field	Description
Description	This is the name of the connected ADSL profile.
Type	This is the authentication type of the ADSL connection. E.g.: *PPPoE, PPPoA, Static.*
IP	The WAN IP Address is displayed here when the connection is established.
State	The ADSL connection status is displayed here. This is the connection between your iConnect625W and the DSLAM at your ISP. In normal operation, this must be connected.
Online	This is the duration of the Internet connection time for the connection *Type* specified.
Disconnect Reason	If the connection is not active, the reason for disconnection is displayed here.

11.3 DDNS Update Status

DDNS stands for Dynamic Domain Name System. It provides you with a view of your WAN connection and the DDNS update status of your iConnect625W.

To view the DDNS update status of your iConnect625W router, follow the steps below.

Step 1: Click the ***Status*** tab and the ***DDNS Update Status*** link. The following page appears:



DDNS Update Status

Connection: MyConnection

DDNS Server: DynDNS

DDNS Client is disabled

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: As shown on the screen above, the DDNS is disabled by default for your iConnect625W router. To enable DDNS, refer to the section on *Dynamic DNS Client*. When the DDNS client is enabled, the DDNS client updates every time the iConnect625W router gets a new IP address.

Step 3: Select the ***DDNS server*** from a list of DDNS service providers. The status and error description (if any) will be displayed.

The following table describes the *DDNS Status* fields and their definitions:

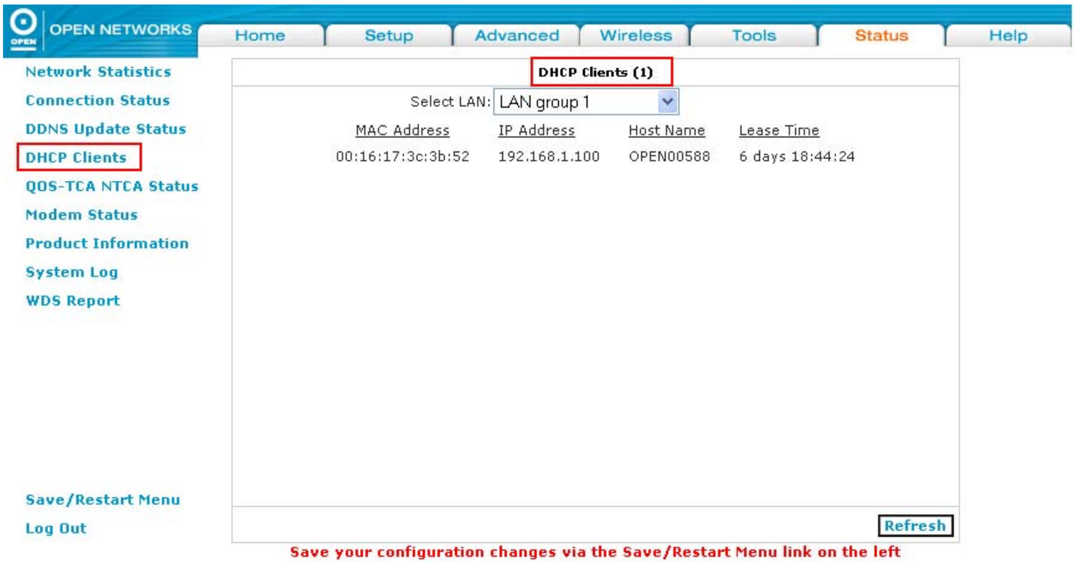
Field	Description	
Connection	This field defaults to your iConnect625W's WAN connection over which your router can be accessed.	
DDNS Server	This is where you select the server from different DDNS service providers. Only *DynDNS* and *TZO* are supported.	
Status	The status could be one of the following:	
	Updated	The IP address of the client has been changed and an update has been sent to the DDNS server.
	No Change	The IP address of the client has not changed.
	Error	There is an error with the DDNS update.
Error Description	If the DDNS update status is *Error*, this field gives a description of the error.	

11.4 DHCP Clients

If you have enabled the DHCP server, you can view a list of the DHCP clients on your LAN from the *DHCP Clients* page.

To view *DHCP Clients*, follow the steps below.

Step 1: Click the ***Status*** tab and the ***DHCP Clients*** link. The following page appears:



DHCP Clients (1)

Select LAN: LAN group 1

MAC Address	IP Address	Host Name	Lease Time
00:16:17:3c:3b:52	192.168.1.100	OPEN00588	6 days 18:44:24

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: From the ***Select LAN*** drop-down list, select the LAN group whose DHCP details you wish to view.

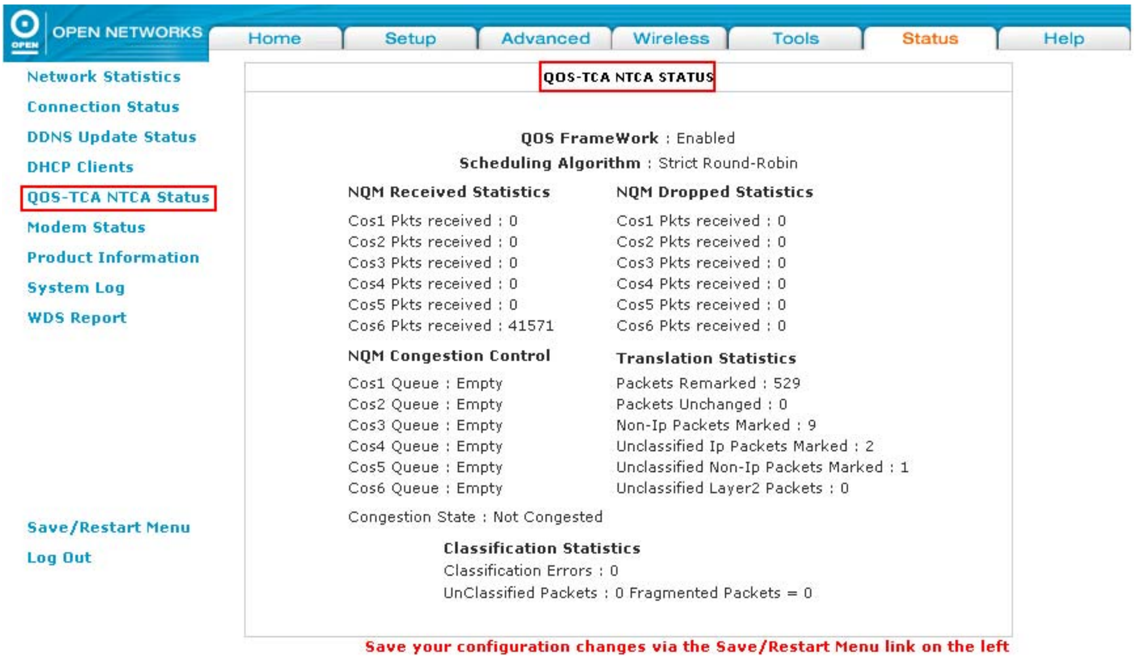
Step 3: Click the ***Refresh*** button to update the screen details. The following information of the DHCP LAN clients is displayed:

- MAC Address
- IP Address
- Host Name
- Lease Time

11.5 QoS-TCA NTCA Status

To view *QoS-TCA NTCA Status*, follow the steps below.

Step 1: Click the ***Status*** tab and the ***QoS-TCA NTCA Status*** link. The following page appears:



QOS-TCA NTCA STATUS

QOS FrameWork : Enabled
Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics	NQM Dropped Statistics
Cos1 Pkts received : 0	Cos1 Pkts received : 0
Cos2 Pkts received : 0	Cos2 Pkts received : 0
Cos3 Pkts received : 0	Cos3 Pkts received : 0
Cos4 Pkts received : 0	Cos4 Pkts received : 0
Cos5 Pkts received : 0	Cos5 Pkts received : 0
Cos6 Pkts received : 41571	Cos6 Pkts received : 0

NQM Congestion Control	Translation Statistics
Cos1 Queue : Empty	Packets Remarked : 529
Cos2 Queue : Empty	Packets Unchanged : 0
Cos3 Queue : Empty	Non-Ip Packets Marked : 9
Cos4 Queue : Empty	Unclassified Ip Packets Marked : 2
Cos5 Queue : Empty	Unclassified Non-Ip Packets Marked : 1
Cos6 Queue : Empty	Unclassified Layer2 Packets : 0

Congestion State : Not Congested

Classification Statistics
Classification Errors : 0
UnClassified Packets : 0 Fragmented Packets = 0

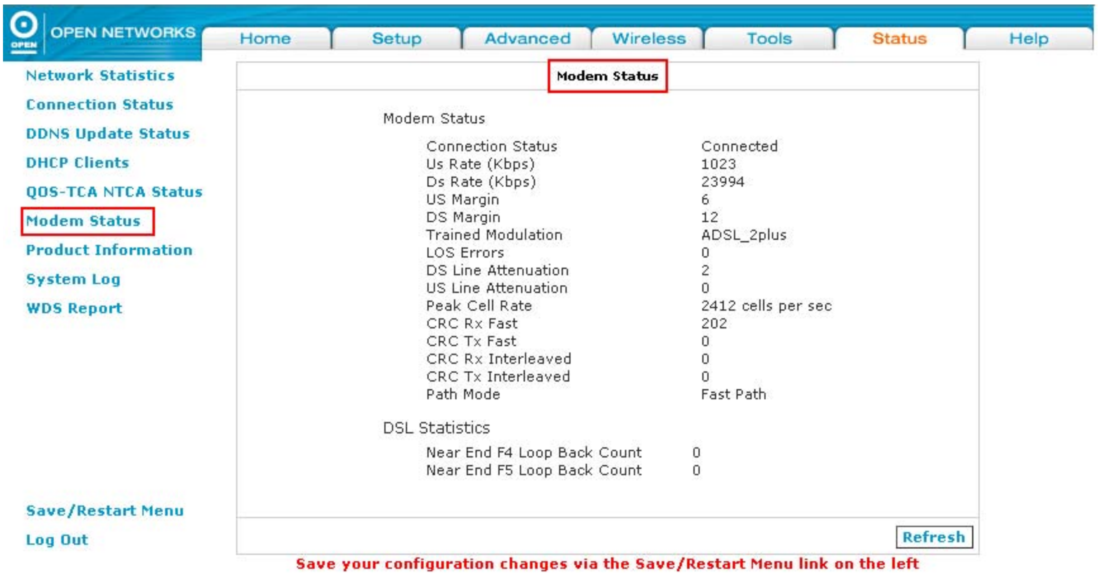
Save your configuration changes via the Save/Restart Menu link on the left

11.6 Modem Status

The Modem Status page provides the status and statistics of your broadband (DSL) connection.

To view Modem Status, follow the steps below.

Step 1: Click the ***Status*** tab and the ***Modem Status*** link. The following page appears:



Modem Status

Modem Status

Connection Status	Connected
Us Rate (Kbps)	1023
Ds Rate (Kbps)	23994
US Margin	6
DS Margin	12
Trained Modulation	ADSL_2plus
LOS Errors	0
DS Line Attenuation	2
US Line Attenuation	0
Peak Cell Rate	2412 cells per sec
CRC Rx Fast	202
CRC Tx Fast	0
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path

DSL Statistics

Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

Save your configuration changes via the Save/Restart Menu link on the left

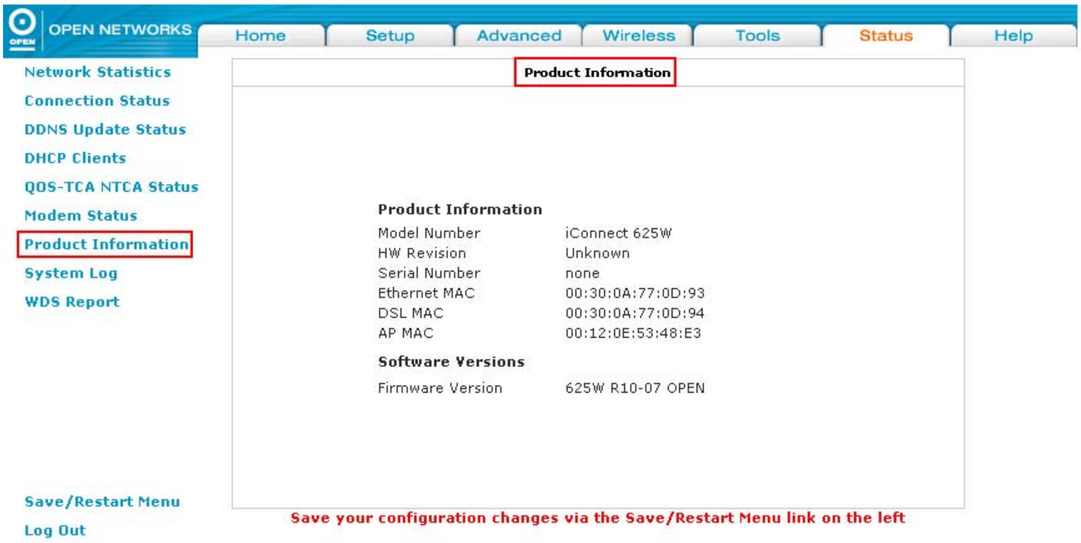
Step 2: Click the ***Refresh*** button to update the screen details.

11.6 Product Information

You can verify product information such as the model, driver, hardware and software versions in the *Product Information* area of the web interface.

To view the *Product Information* page, follow the step below.

Step 1: Click the ***Status*** tab and the ***Product Information*** link. The following page appears:



Product Information

Product Information

Model Number	iConnect 625W
HW Revision	Unknown
Serial Number	none
Ethernet MAC	00:30:0A:77:0D:93
DSL MAC	00:30:0A:77:0D:94
AP MAC	00:12:0E:53:48:E3

Software Versions

Firmware Version	625W R10-07 OPEN

Save your configuration changes via the Save/Restart Menu link on the left

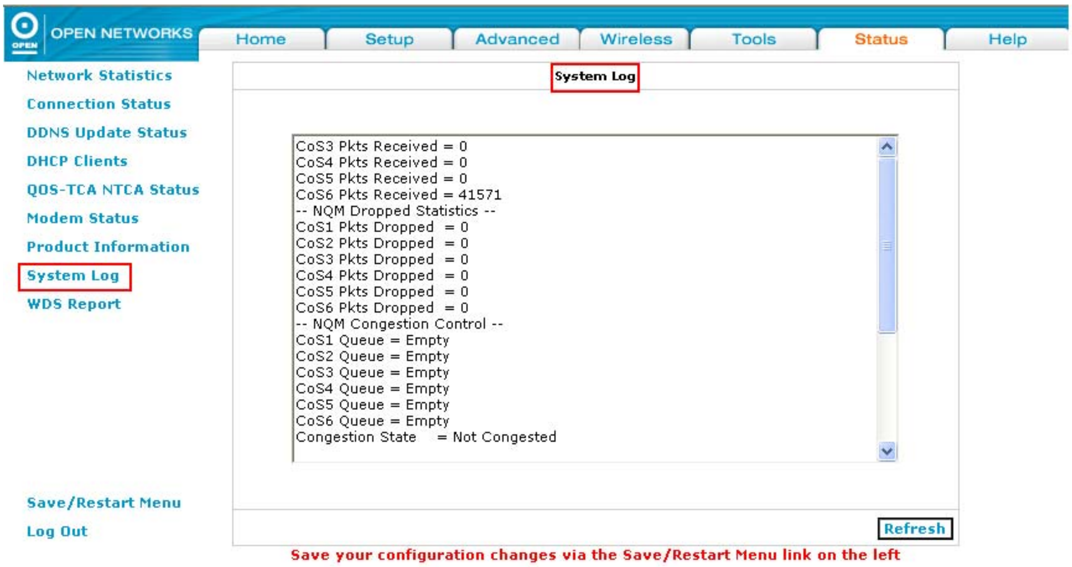
11.7 System Log

You can view all logged information in the *System Log* area of the web interface. This page allows you to view all logged information.

Depending on the severity level, the logged information generates log reports to a remote host (if remote logging is enabled). Up to 32 logs can be displayed on this page.

To view the *System Log* page, follow the steps below.

Step 1: Click the ***Status*** tab and the ***System Log*** link. The following page appears:



```
CoS3 Pkts Received = 0
CoS4 Pkts Received = 0
CoS5 Pkts Received = 0
CoS6 Pkts Received = 41571
-- NQM Dropped Statistics --
CoS1 Pkts Dropped  = 0
CoS2 Pkts Dropped  = 0
CoS3 Pkts Dropped  = 0
CoS4 Pkts Dropped  = 0
CoS5 Pkts Dropped  = 0
CoS6 Pkts Dropped  = 0
-- NQM Congestion Control --
CoS1 Queue = Empty
CoS2 Queue = Empty
CoS3 Queue = Empty
CoS4 Queue = Empty
CoS5 Queue = Empty
CoS6 Queue = Empty
Congestion State    = Not Congested
```

Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Click the ***Refresh*** button to update the screen details.

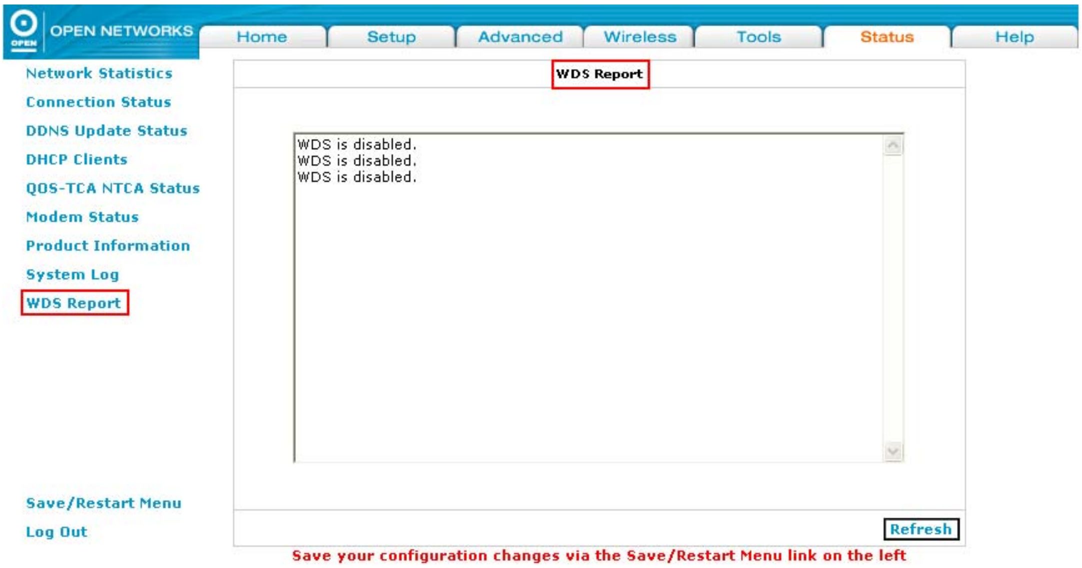
11.9 WDS Report

The WDS report allows you to view the following WDS-related wireless activities of your iConnect625W router:

- WDS configuration and states;
- WDS management statistics;
- WDS database

To view the *WDS Report* page, follow the steps below.

Step 1: Click the ***Status*** tab and the ***WDS Report*** link. The following page appears:



```
WDS is disabled.
WDS is disabled.
WDS is disabled.
```

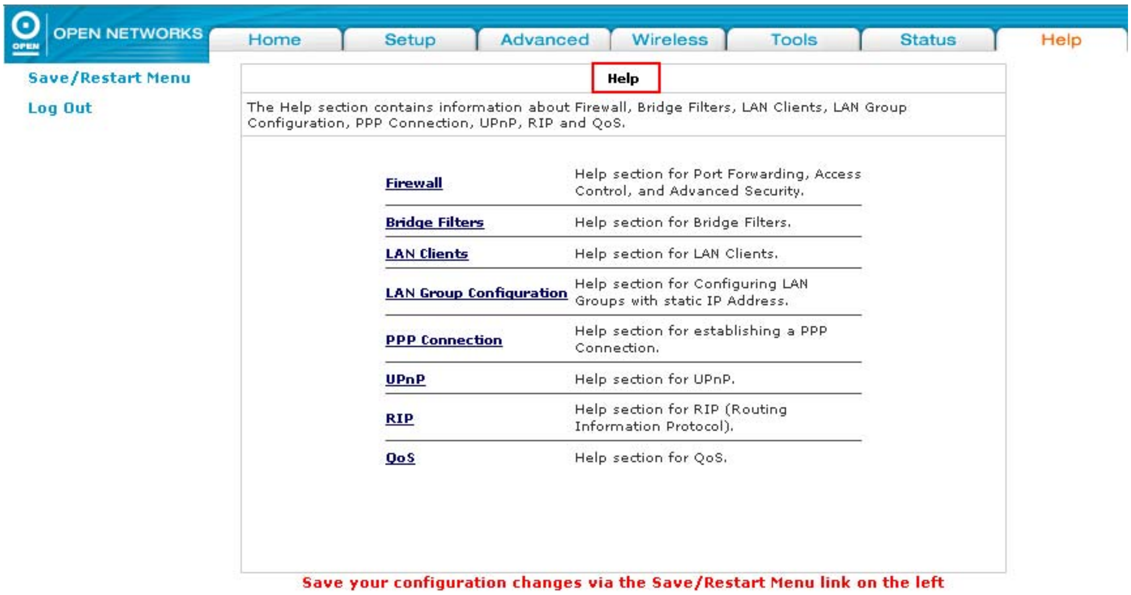
Save your configuration changes via the Save/Restart Menu link on the left

Step 2: Click the ***Refresh*** button to update the screen details.

12. Help

The Help tab allows you to access the various *Help* sections for the following:

- Firewall
- Bridge Filters
- LAN Clients
- LAN Group Configuration
- PPP Connnection
- UPnP
- RIP
- QoS



Help

The Help section contains information about Firewall, Bridge Filters, LAN Clients, LAN Group Configuration, PPP Connection, UPnP, RIP and QoS.

Firewall	Help section for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
LAN Group Configuration	Help section for Configuring LAN Groups with static IP Address.
PPP Connection	Help section for establishing a PPP Connection.
UPnP	Help section for UPnP.
RIP	Help section for RIP (Routing Information Protocol).
QoS	Help section for QoS.

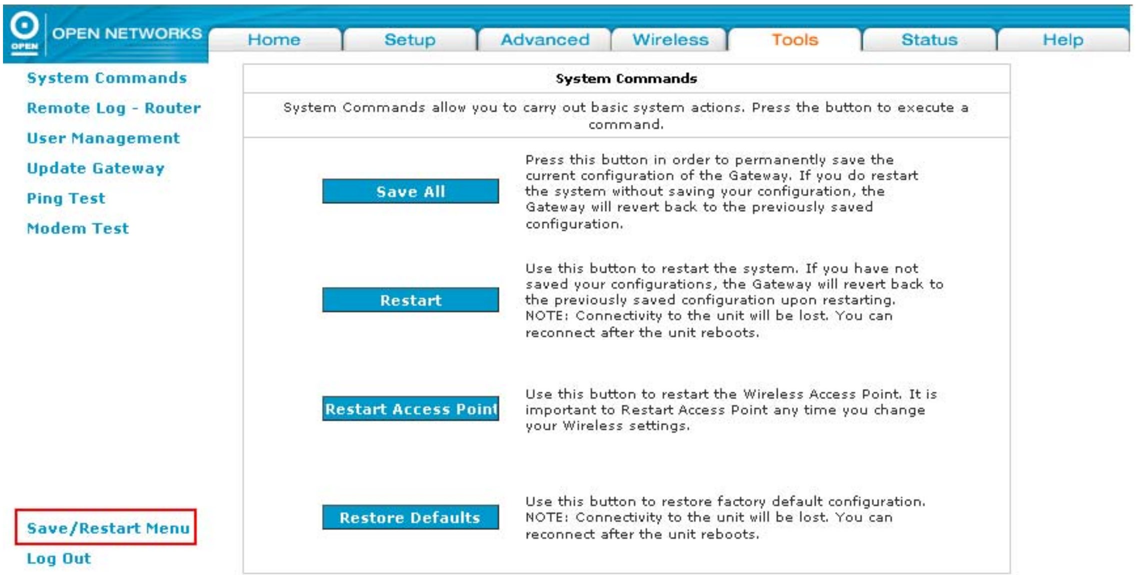
Save your configuration changes via the Save/Restart Menu link on the left

13. Save / Restart Menu

The Save / Restart Menu link on the left menu is the same page as that of Systems Commands. It allows you to save all your new settings, restart the iConnect625W router, restart the Wireless Access Point and to restore default configurations.

To access *Save/Restart Menu*, follow the steps below.

Step 1: From the left menu, click the ***Save/Restart Menu*** link provided. The following page appears:



System Commands

System Commands allow you to carry out basic system actions. Press the button to execute a command.

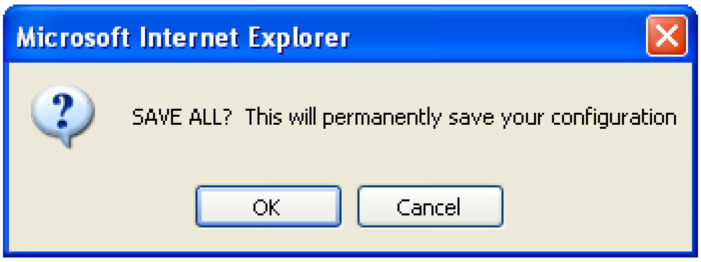
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.

Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Use this button to restart the Wireless Access Point. It is important to Restart Access Point any time you change your Wireless settings.

Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

Step 2: Click the ***Save All*** button to save the configurations made. A message dialogue box appears. Click the ***OK*** button to save your configurations permanently.



SAVE ALL? This will permanently save your configuration

Step 3: Click the ***Restart*** button if you wish to restart the router.

Step 4: Read the definitions in the table below for the purpose of each of the System Commands buttons: *Save All, Restart, Restart Access Point* and *Restore Defaults*.

The following table describes the *Save/Restart Menu* screen fields and their definitions:

Field	Description
Save All	This command allows you to permanently save the current configuration of your iConnect625W router. If you restart the system without saving your configuration, the iConnect625W reverts to the previously saved configuration.
Restart	This command allows you to restart the system. If you have not saved your configurations
Restart Access Point	This command allows you to restart the wireless AP. It is important to restart the AP anytime you change your wireless settings.
Restore Defaults	Use this command to restore factory default configuration. NOTE *Connectivity to the unit will be lost. You can reconnect after the unit reboots.*

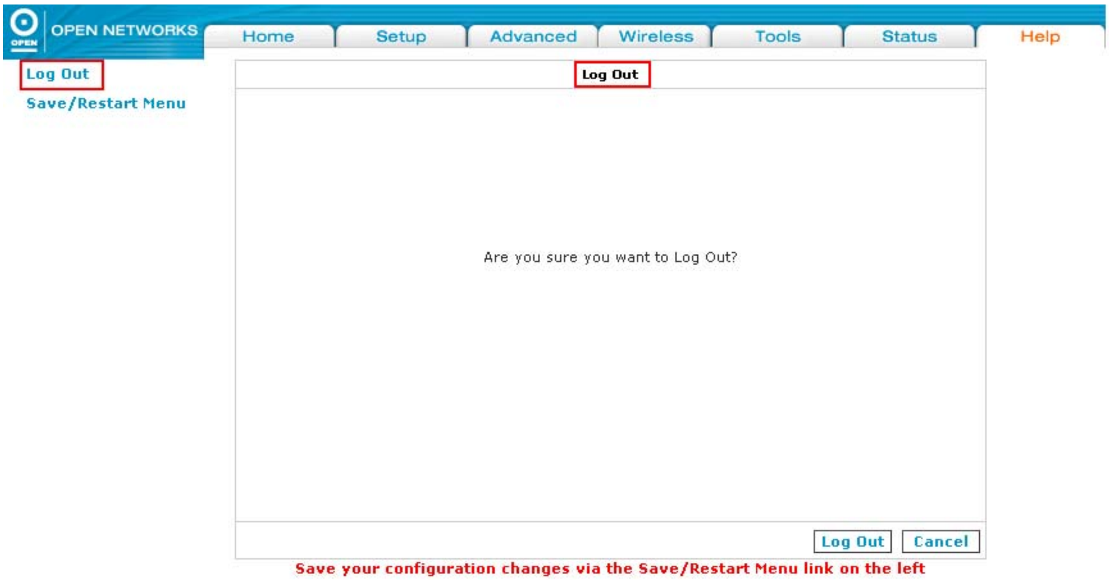
14. Log Out

After you have completed configuring your iConnect625W router, you may log out of the router.

To *Log Out*, follow the steps below.

Step 1: Before you log out of the router, ensure that you have saved any changes made.

Step 2: Click the ***Log Out*** link on the left menu. The following page appears with the message prompt: *Are you sure you want to Log Out?*



Are you sure you want to Log Out?

Save your configuration changes via the Save/Restart Menu link on the left

Step 3: Click the ***Log Out*** button to exit, or click the ***Cancel*** button to return to the main menu.

15. Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting your service provider.

15.1 Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adaptor and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password by referring to Section 3. If this fails, you can restore your router to its factory settings by holding the ***Reset*** button on the back of your router for more than 6 seconds.

15.2 Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

15.3 Problems with the LAN Interface

Problem	Corrective Action
Cannot ping any computers on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a computer connected. If it is off, check the cables between your router and the computer. Make sure you have uninstalled any software firewall for troubleshooting.

16. Glossary Table

Term	Definition
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
AP	Access Point
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BRAS	Broadband Routing Authentication Service
BSS	Basic Service Set
CDVT	Cell Relay Variation Tolerance
CHAP	Challenge Handshake Authentication Protocol
CoS	Class of Service
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Control Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Service Code Protocol
DSLAM	Digital Subscriber Line Access Multiplexer
DTIM	Delivery Traffic Identification Map
EAP	Extensible Authentication Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
MAC	Media Access Control
MBS	Maximum Burst Size
MBPS	Megabits per second
MTU	Maximum Transmission Unit
NAT	Network Address Translation
PAP	Password Authentication Protocol
PCR	Peak Cell Rate
PPP	Point-To-Point Protocol
PPPoA	Point-To-Point Protocol over ATM
PPPoE	Point-To-Point Protocol over Ethernet
PPTP	Point-To-Point Tunnelling Protocol
PRIOWRR	Priority Weighted Round Robin
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RFC	Request for Comments
RIP	Routing Information Protocol
SCR	Sustained Cell Rate
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPI	Stateful Packet Installation
SR IE	Supported Rate Information Element
SSID	Service Set Identification
TCP/IP	Transfer Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Services

Term	Definition
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VAD	Voice Activity Detection
VC	Virtual Circuit
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VP	Virtual Path
VPI	Virtual Path Identifier
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wireless Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access