

# Platform

**Product Name WA3003G4**

**Release 1.0**

**Guide Type**

Watermark

**Release 1.0**

**Doc. Code L3 JA01 2500 01 011 00**



Copyright © 2006 UTStarcom, Inc. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without prior, express and written permission from UTStarcom, Inc.

UTStarcom, Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of UTStarcom, Inc. to provide notification of such revision or changes.

UTStarcom, Inc. provides this documentation without warranty of any kind, implied or expressed, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. UTStarcom may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

**UNITED STATES GOVERNMENT LEGENDS:**

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

**United States Government Legend:** All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in UTStarcom's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

UTStarcom, the UTStarcom logo, PAS, mSwitch, Airstar, WACOS, Netman, Total Control, and CommWorks are registered trademarks of UTStarcom, Inc. and its subsidiaries. The UTStarcom name, AN-2000, and the CommWorks logo are trademarks of UTStarcom, Inc. and its subsidiaries.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Any rights not expressly granted herein are firmly reserved.



<b>1</b>	<b>Overview</b> .....	<b>3</b>
	Introduction.....	3
<b>2</b>	<b>WA3003G4 Installation</b> .....	<b>5</b>
<b>3</b>	<b>Configuration</b> .....	<b>9</b>
	3.1 Setup.....	9
	3.2 Establish the Connection.....	9
	3.3 Device Info .....	10
	3.3.1 Summary.....	10
	3.3.2 Device Info -- WAN.....	12
	3.3.3 Statistics.....	12
	3.3.3.1. Device Info Statistics -- LAN .....	13
	3.3.3.2 Device Info Statistics -- WAN.....	14
	3.3.3.3 Device Info Statistics -- ATM .....	15
	3.3.3.4 Device Info Statistics -- ADSL.....	16
	3.3.3.5 Device Info Statistics -- VDSL .....	17
	3.3.4 Device Info Route.....	18
	3.3.5 Device Info ARP .....	19
	<i>Figure 3.3.5 Device Info ARP</i> .....	19
	3.3.6 Device Info DHCP .....	20
	3.4 Advanced Setup .....	20
	3.4.1 Advanced Setup -- WAN .....	21
	Figure 3.4.1 Advanced Setup – Wide Area Network (WAN) Setup.....	21
	Figure 3.4.1.1 Advanced Setup – ATM PVC Configuration .....	22
	3.4.2 Advanced Setup – LAN.....	34
	3.4.3 Advanced Setup – NAT.....	35
	3.4.3.1 Advanced Setup – NAT—Virtual Servers .....	35
	1. Advanced Setup – NAT— Port Triggering Setup .....	37
	2. Advanced Setup – NAT— DMZ Host.....	39
	3. Advanced Setup – NAT— ALG.....	39
	3.4.4 Advanced Setup – Security.....	40

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**IMPORTANT NOTE:**

**FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

# 1

## Overview

This chapter provides an overview of the **UTStarcom WA3003G4 VDSL 2 Modem** and describes its Features and System Requirements.

This chapter contains the following topics:

- Introduction
- Features
- System Requirements

---

## Introduction

Congratulations on becoming the owner of the **WA3003G4**. Your LAN (local area network) will now be able to access the Internet using your high-speed VDSL connection. This User Guide will show you how to install and set up your **WA3003G4**.

### Features

- Internal VDSL modem for high speed internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- 802.11b/g WLAN supported
- Network configuration through DHCP
- Configuration program you access via an HTML browser

### System Requirements

In order to use your **WA3003G4** router, you must have the following:

- VDSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card or 802.11b/g WLAN card/adaptor
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later





# 2

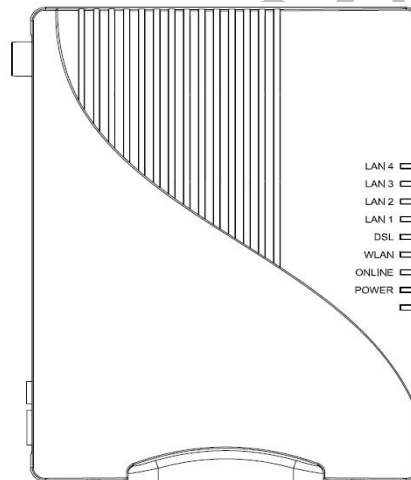
## WA3003G4 Installation

In addition to this document, your **WA3003G4** should arrive with the following:

- One **WA3003G4**
- One power adapter and power cord
- One cross-over/straight Ethernet cable
- One RJ-11 to RJ-11 telephone Cable
- One splitter or low-pass filter

### Front Panel

The front panel contains 7 LEDs indicating the status of **WA3003G4** showing as Figure 2.1:



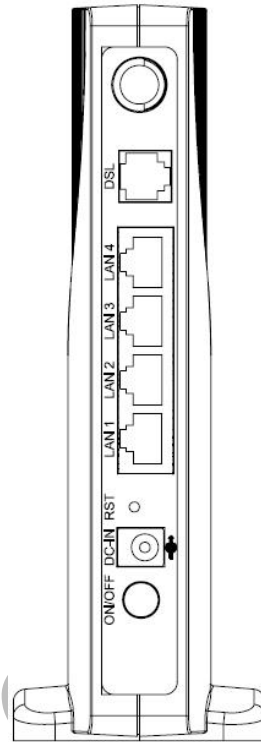
**Figure 2.1 WA3003G4 Front Panel.**

Label	Color	Function
Power	Green	On: Unit is powered on Off: Unit is powered off
ONLINE	Red	On: Major alarm occurs. Off: Unit is functioning well.
WLAN	Green	On: Wireless LAN is active Off: No wireless card or wireless LAN isn't active Flashes during data transfer
DSL	Green	Flashes during the training mode. On: VDSL link is established and active
LAN1-4	Green	On: LAN link established and active Off: No LAN link Flashes during data transfer

**Table 2.1 Illustration of WA3003G4 Front Panel**

## Rear Panel

The rear panel contains the ports for **WA3003G4** data and power connections showing as Figure 2.2

**Figure 2.2 WA3003G4 Back Panel.**

Label	Function
<i>Antenna</i>	For WiFi functionality.
<i>DSL</i>	RJ-11 connector: Connects the device to a telephone jack or splitter using the supplied cable
<i>LAN1-4</i>	RJ-45 connector: Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided
<i>RST</i>	Reset the configuration to factory default
<i>DC-IN</i>	Connects to the supplied power converter cable
<i>On/Off</i>	Switches the device on and off

**Table 2.2 Illustration of WA3003G4 Back Panel**

## Connecting the Hardware

**WARNING**

**Before you begin, turn the power off for all devices.** These include your computer(s), your LAN hub/switch (if applicable), and the WA3003G4.

Figure 2.3 illustrates the hardware connections.

The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

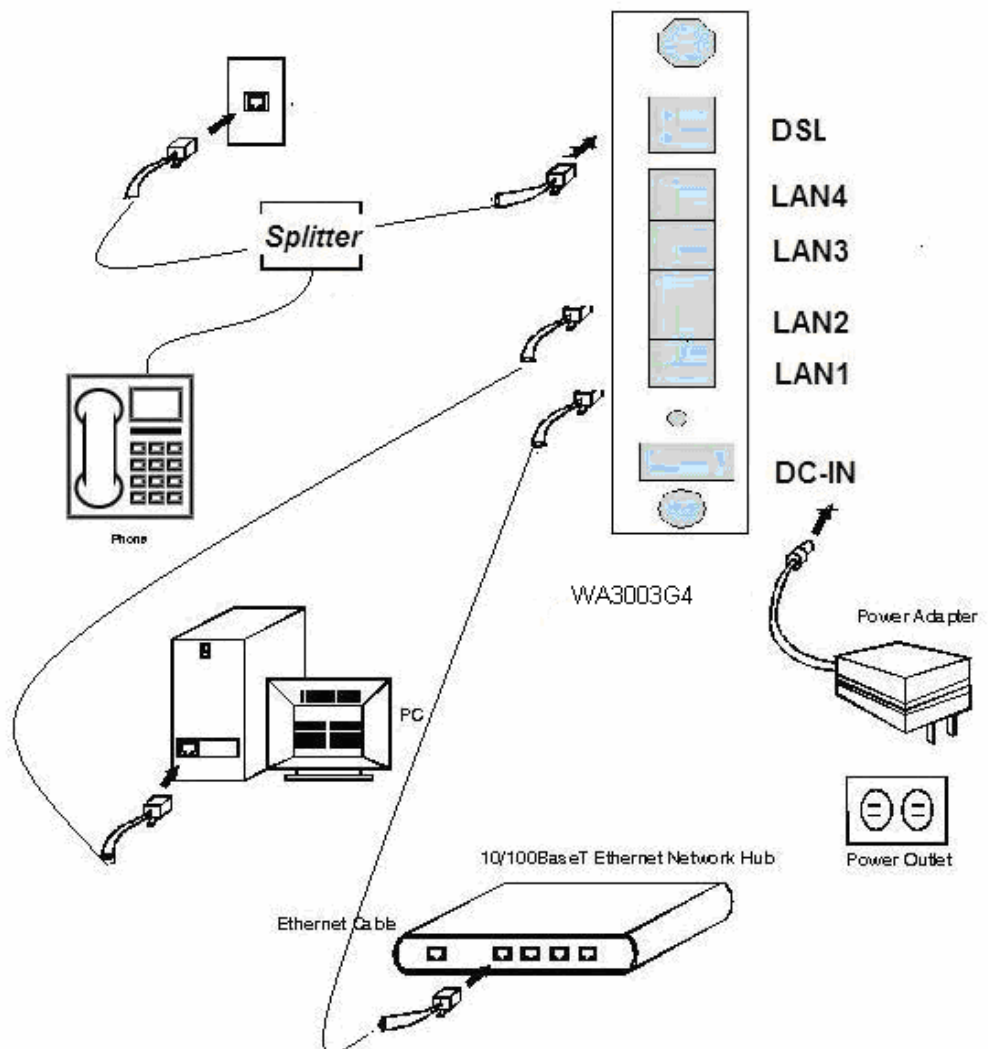
**WA3003G4**

Figure 2.3. Overview of Hardware Connections

**Step 1. Connect the VDSL cable and optional telephone.**

Connect one end of the provided phone cable to the port labeled VDSL on the rear panel of the device. Connect the other end to your wall phone jack.

You can attach a telephone line to the device. This is helpful when the VDSL line uses the only convenient wall phone jack. If desired, connect the telephone cable to the port labeled PHONE.

**WARNING**

*Although you use the same type of cable, The VDSL and PHONE ports are **not** interchangeable. Do not route the VDSL connection through the PHONE port.*

**Step 2. Connect the Ethernet cable.**

If you are connecting a LAN to **WA3003G4**, attach one end of a provided Ethernet cable to a regular hub port and the other to the Ethernet port on **WA3003G4**.

**Step 3. Attach the power connector.**

Connect the AC power adapter to the DC-IN connector on the back of **WA3003G4** and plug in the adapter to a wall outlet or power strip.

**Step 4. Turn on the WA3003G4 and power up your systems.**

Press the Power switch on the back panel of the device to the ON position.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

**Step 5. Configure the WA3003G4 through the WEB interface**

The detail step3 would be described in Chapter3. It would help you configure the **WA3003G4** to meet your need.

**Step 6. Save the configurations and Reboot.**

To make the settings you made on **WA3003G4** take effect.

# 3

## Configuration

### 3.1 Setup

- Step 1: Connect **WA3003G4** and PC with an Ethernet cable.
- Step 2: Power on the **WA3003G4**.
- Step 3: The default IP of the **WA3003G4** is *192.168.1.1*.

### 3.2 Establish the Connection

Enter the IP address (default is *192.168.1.1*) of **WA3003G4** from the Web Browser. A Dialogue Box will be popped up to request the user to login. (Figure 3.2.1)



**Figure 3.2.1. Authentication**

Please enter the management username/password into the fields then click on the OK button (default username/password is *admin/admin*).

If the authentication passes, the home page “*Device Info*” will be displayed on the browser. (Figure 3.2.2)

Device Info

Board ID:	96358M
Software Version:	3.10L.01_V02.A2p8022g.d20e
Bootloader (CFE) Version:	1.0.37-10.1
Firmware Version:	WA3003G4-0021.01
Hardware Version:	WA3003G4 1.0
Model Name:	WA3003G4
VDSL Software Version:	09.03.06, 2007-02-26
Wireless Driver Version:	4.100.27.0.cpe2.1

This information reflects the current status of your DSL connection.

B0 Traffic Type:	
B0 Line Rate - Upstream (Kbps):	
B0 Line Rate - Downstream (Kbps):	
B1 Traffic Type:	
B1 Line Rate - Upstream (Kbps):	
B1 Line Rate - Downstream (Kbps):	
LAN IP Address:	172.24.131.64
Default Gateway:	
Primary DNS Server:	172.24.131.64
Secondary DNS Server:	172.24.131.64

Figure 3.2.2. WA3003G4 Device Info

### 3.3 Device Info

The system administrator can configure **WA3003G4** remotely or locally via a Web Browser. Network configuration must be planned and decided before starting the configuration procedure.

Under “**Device Info**” selection, based on different information characteristics, they are grouped into following categories:

**Summary**

**WAN**

**Statistics**

**Route**

**ARP**

**DHCP**

#### 3.3.1 Summary

Click on “**Summary**” in the left frame, Figure 3.3.1 **WA3003G4 Device Info – Summary** shows up as following.

- Device Info
- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- Advanced Setup
- Wireless
- Diagnostics
- Management

Device Info

Board ID:	96358M
Software Version:	3.10L_01_V02.A2pB022g.d20e
Bootloader (CFE) Version:	1.0.37-10.1
Firmware Version:	WA3003G4-0021.01
Hardware Version:	WA3003G4 1.0
Model Name:	WA3003G4
VDSL Software Version:	09.03.06, 2007-02-26
Wireless Driver Version:	4.100.27.0.cpe2.1

This information reflects the current status of your DSL connection.

B0 Traffic Type:	
B0 Line Rate - Upstream (Kbps):	
B0 Line Rate - Downstream (Kbps):	
B1 Traffic Type:	
B1 Line Rate - Upstream (Kbps):	
B1 Line Rate - Downstream (Kbps):	
LAN IP Address:	172.24.131.64
Default Gateway:	
Primary DNS Server:	172.24.131.64
Secondary DNS Server:	172.24.131.64

**Figure 3.3.1. WA3003G4 Device Info – Summary**

Figure 3.3.1 reflects two different category information of WA3003G4 as following:

Device Info

Board ID, Software Version, Bootloader (CFE) Version, Firmware Version, Hardware Version, Model Name, VDSL Software Version and Wireless Driver Version.

Status of DSL connection

B0 Traffic Type: B0 Line Rate, Upstream and Downstream.

B1 Traffic Type: B0 Line Rate, Upstream and Downstream.

LAN IP address, Default Gateway, Primary and Secondary DNS

### 3.3.2 Device Info -- WAN

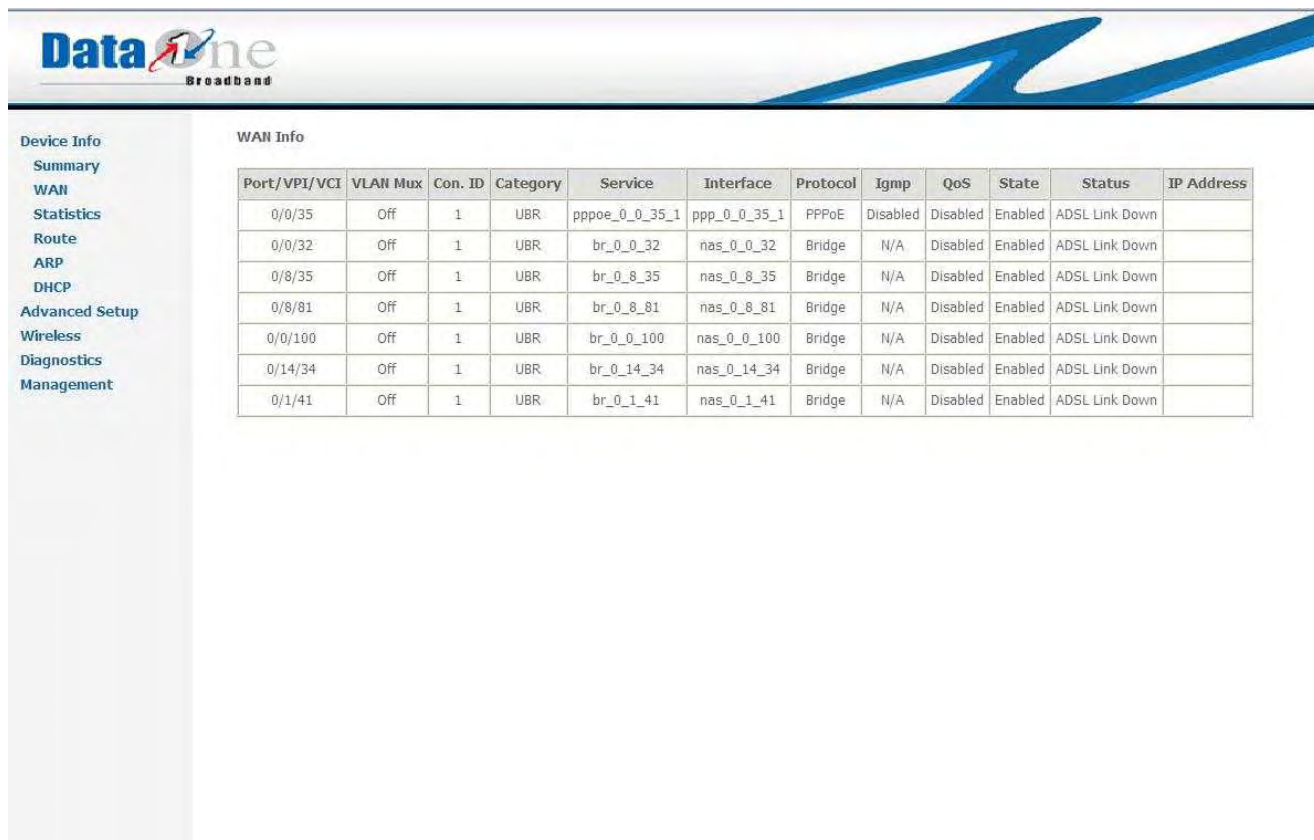


Figure 3.3.2. Device Info – WAN

Figure 3.3.2 displays the WAN status of **WA3003G4**

### 3.3.3 Statistics

Selecting **Statistics** will display following statistics information of **WA3003G4**

**LAN**

**WAN**

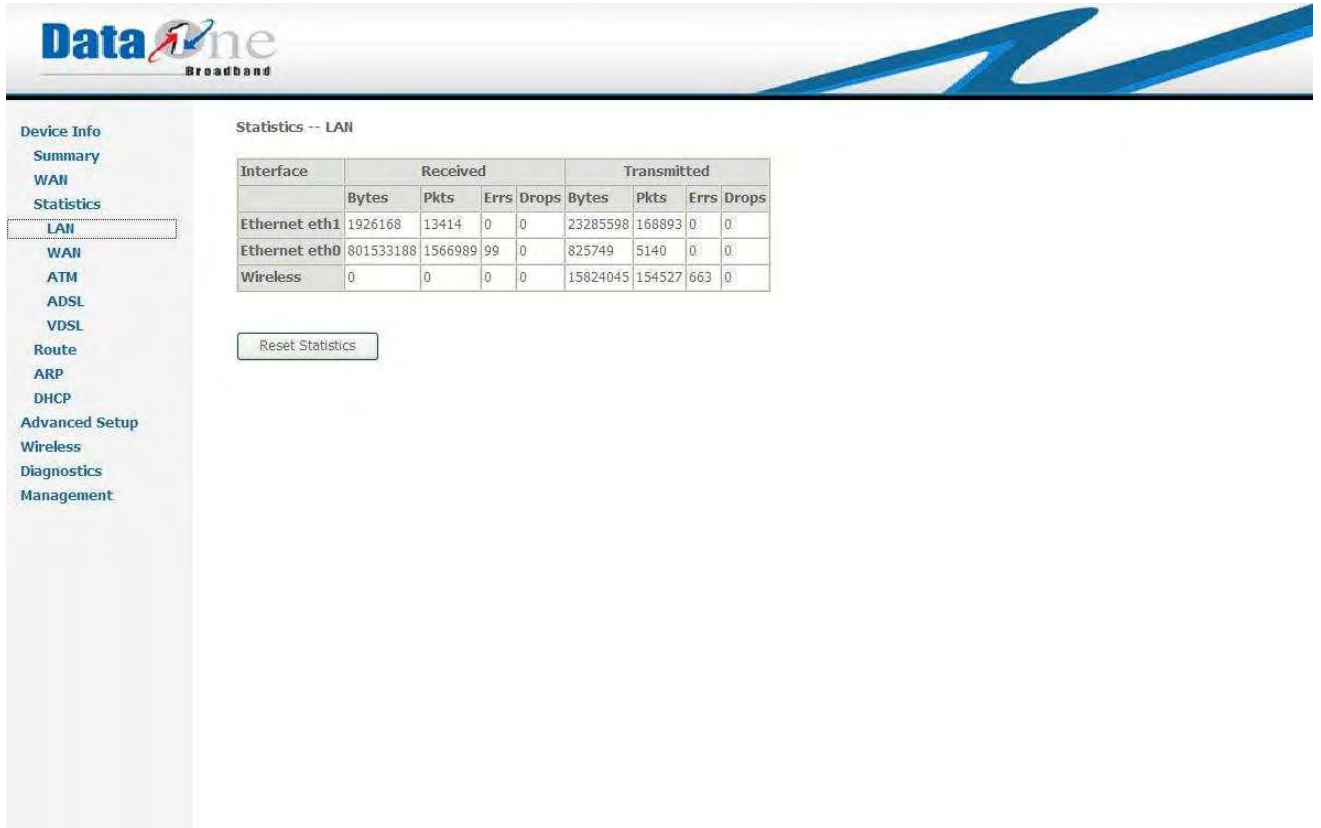
**ATM**

**ADSL**

**VDSL**



### 3.3.3.1. Device Info Statistics -- LAN




**Figure 3.3.3.1. Device Info Statistics – LAN**

Check to Enable/Disable IGMP Multicast and WAN Service.  
Click on "Next" to go to next step.

Water

3.3.3.2 Device Info Statistics -- WAN



Device Info

- Summary
- WAN
- Statistics
- LAN
- WAN
- ATM
- ADSL
- VDSL
- Route
- ARP
- DHCP
- Advanced Setup
- Wireless
- Diagnostics
- Management

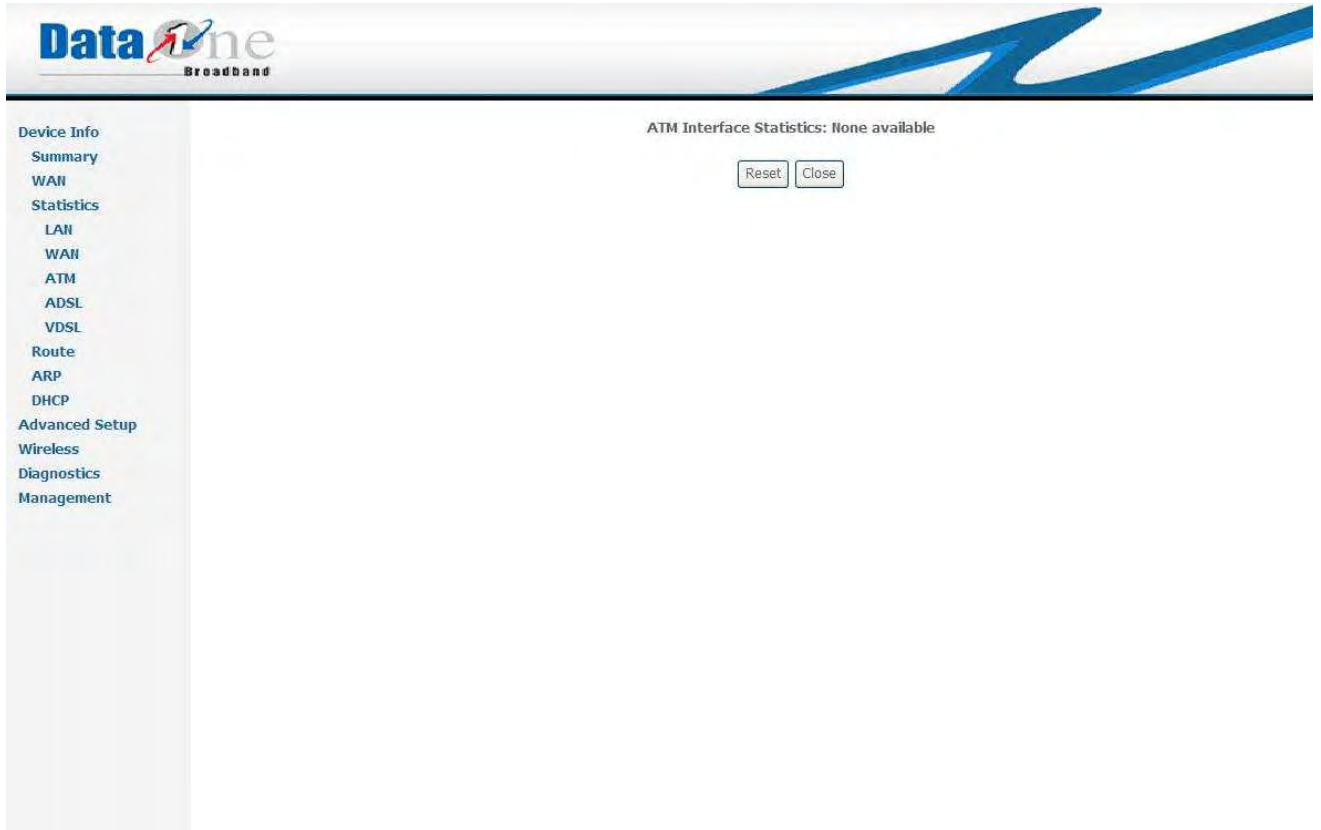
Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted				
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	
pppoe_0_0_35_1	0/0/35	PPPoE	ppp_0_0_35_1	0	0	0	0	0	0	0	0	0
br_0_0_32	0/0/32	Bridge	nas_0_0_32	0	0	0	0	942	13	0	527187	
br_0_8_35	0/8/35	Bridge	nas_0_8_35	0	0	0	0	872	12	0	527186	
br_0_8_81	0/8/81	Bridge	nas_0_8_81	0	0	0	0	732	10	0	527186	
br_0_0_100	0/0/100	Bridge	nas_0_0_100	0	0	0	0	592	8	0	527186	
br_0_14_34	0/14/34	Bridge	nas_0_14_34	0	0	0	0	452	6	0	527186	
br_0_1_41	0/1/41	Bridge	nas_0_1_41	0	0	0	0	312	4	0	527186	

3.3.3.2 Device Info Statistics -- WAN

Watermark

### 3.3.3.3 Device Info Statistics -- ATM



**Figure 3.3.3.3 Device Info Statistics -- ATM**

Enable the WiFi function here and configure the SSID for the WiFi interface.

### 3.3.3.4 Device Info Statistics -- ADSL

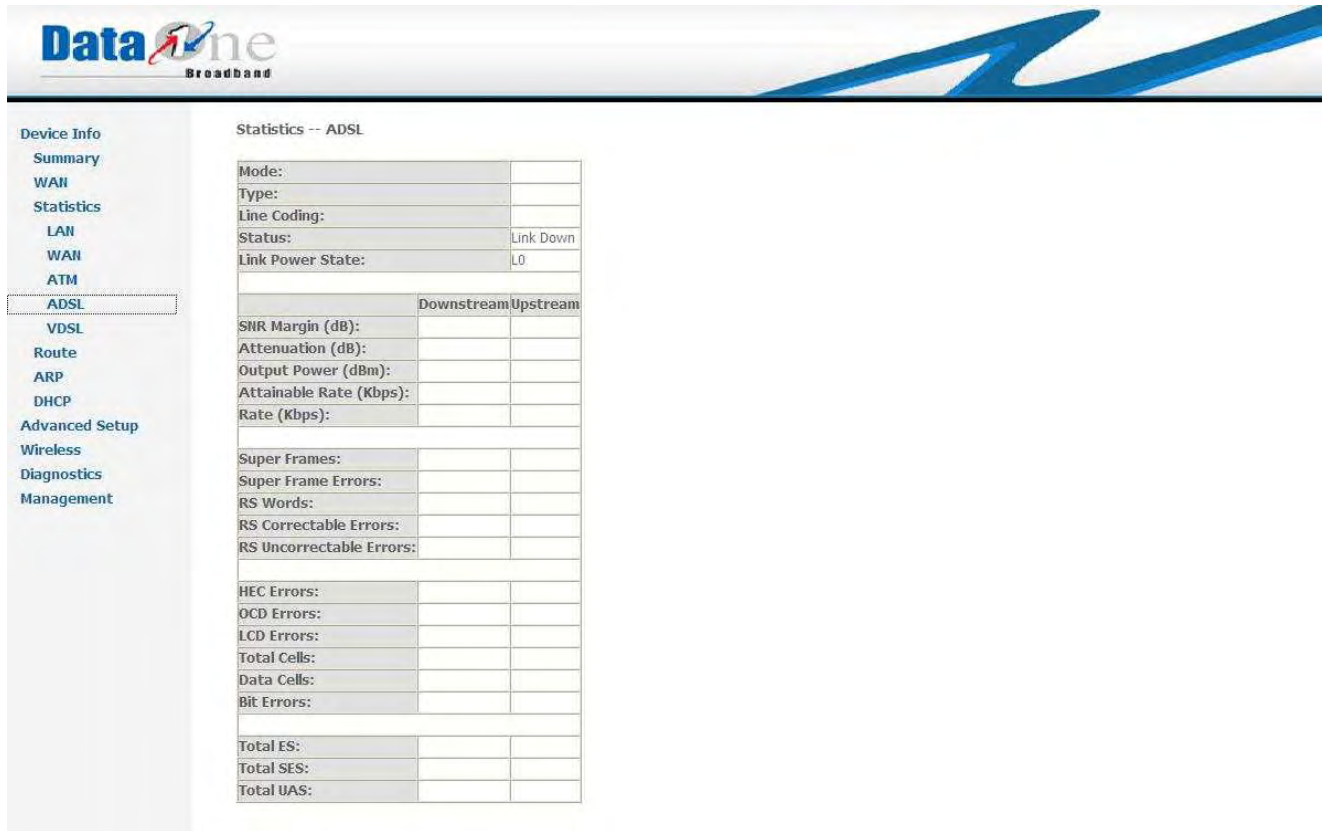


Figure 3.3.3.4 Device Info Statistics – ADSL

### 3.3.3.5 Device Info Statistics -- VDSL

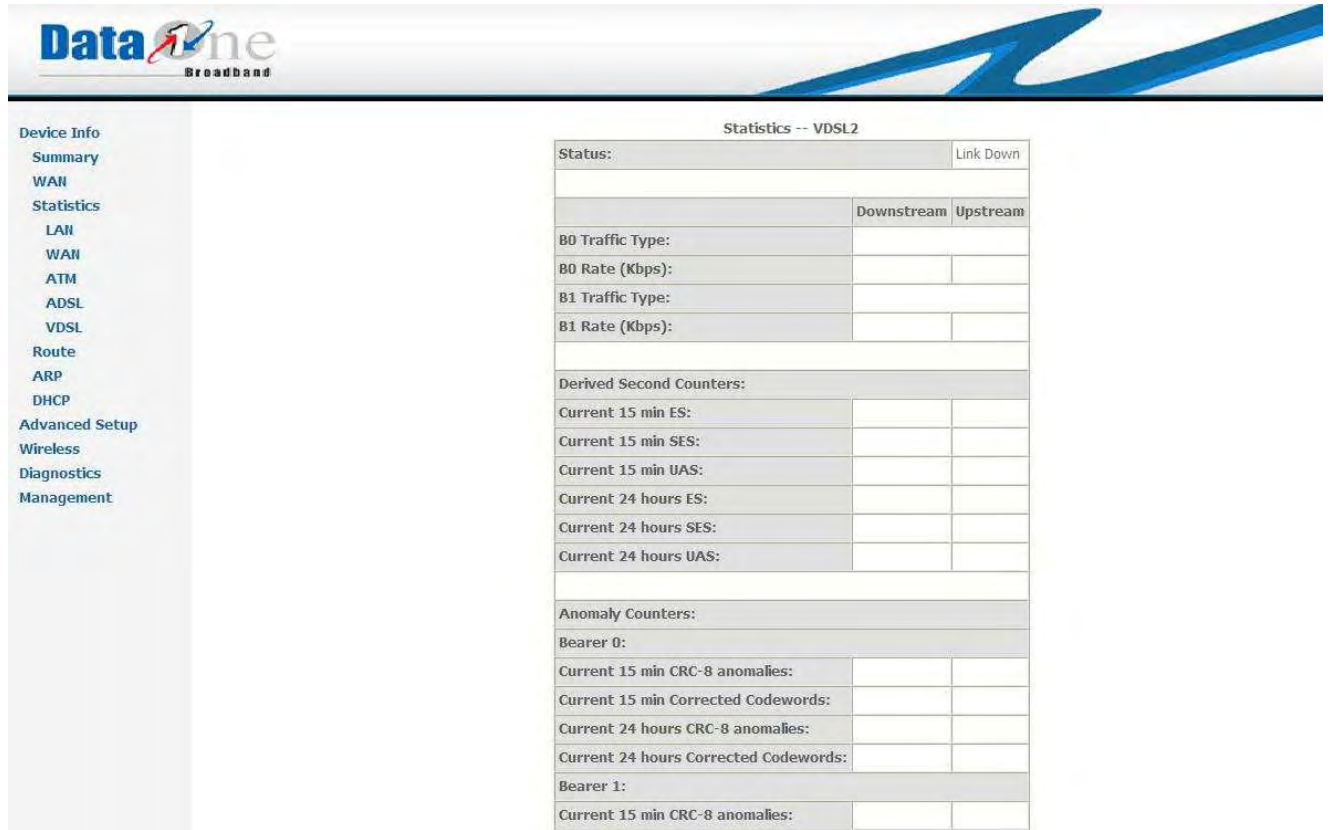


Figure 3.3.3.5 Device Info Statistics – VDSL

### 3.3.4 Device Info Route

**DataOne**  
Broadband

Device Info  
Summary  
WAN  
Statistics  
**Route**  
ARP  
DHCP  
Advanced Setup  
Wireless  
Diagnostics  
Management

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.24.131.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 3.3.4 Device Info Route

### 3.3.5 Device Info ARP



The screenshot shows the DataOne Broadband management interface. On the left is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP, DHCP, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- ARP" and contains a table with the following data:

IP address	Flags	HW Address	Device
172.24.131.88	Complete	00:18:F3:2F:4E:49	br0

Figure 3.3.5 Device Info ARP

Watermark

### 3.3.6 Device Info DHCP

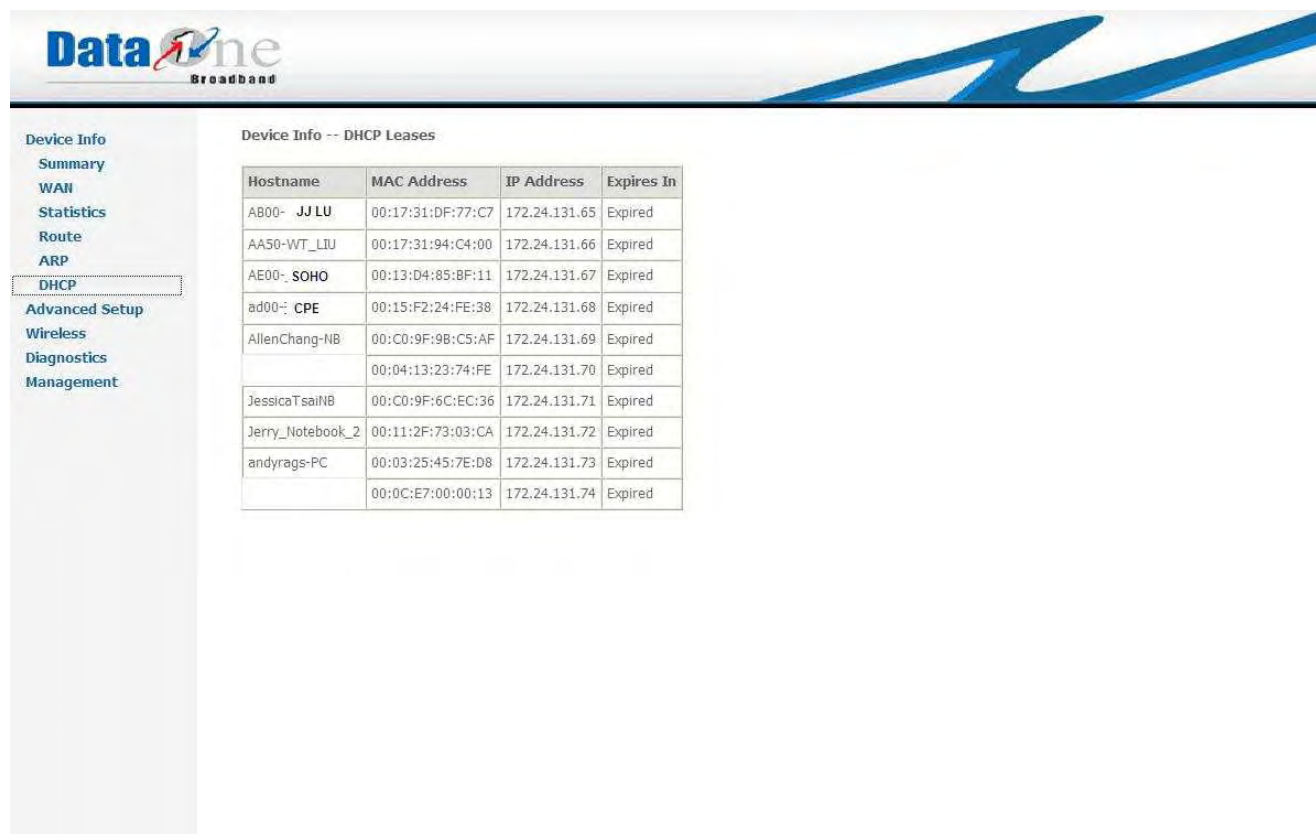


Figure 3.3.6 Device Info DHCP

## 3.4 Advanced Setup

Advanced Setup allows system administrator to configure the following topics:

*WAN*

*LAN*

*Security*

*Quality of Service*

*Routing*

*DNS*

*DSL*

*Print Server*

*Port Mapping*

*IPSec*

*Certificate*



### 3.4.1 Advanced Setup -- WAN

**DataOne Broadband**

Device Info  
Advanced Setup  
WAN  
LAN  
NAT  
Security  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPSec  
Certificate  
Wireless  
Diagnostics  
Management

#### Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Icmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/0/32	Off	1	UBR	br_0_0_32	nas_0_0_32	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/8/35	Off	1	UBR	br_0_8_35	nas_0_8_35	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/8/81	Off	1	UBR	br_0_8_81	nas_0_8_81	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/0/100	Off	1	UBR	br_0_0_100	nas_0_0_100	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/14/34	Off	1	UBR	br_0_14_34	nas_0_14_34	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/1/41	Off	1	UBR	br_0_1_41	nas_0_1_41	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit

Add Remove Save/Reboot

**Figure 3.4.1 Advanced Setup – Wide Area Network (WAN) Setup**

This page shows the current existing WAN interfaces in the system. User can choose Add, Edit, or Remove to configure WAN interfaces.

#### 3.4.1.1 Advanced Setup – add WAN Interface

To add a WAN interface, click “Add”, Figure 3.4.1.1 shows up as below:

**DataOne**  
Broadband

**Device Info**  
Advanced Setup  
WAN  
LAN  
NAT  
Virtual Servers  
Port Triggering  
DMZ Host  
ALG  
Security  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPsec  
Certificate  
Wireless  
Diagnostics  
Management

**ATM PVC Configuration**  
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

PORT: [0-3]   
VPI: [0-255]   
VCI: [32-65535]

VLAN Mux - Enable Multiple Protocols Over a Single PVC

Service Category: UBR Without PCR

**Enable Quality Of Service**  
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

**Figure 3.4.1.1 Advanced Setup – ATM PVC Configuration**

Give proper PORT, VPI/VCI values; for detail information, please consult with your ISP. provider. Enable the QoS function for this PVC here. Use “**Advanced Setup/Quality of Service**” to assign priorities for the application.

To configure VLAN, please check “**VLAN Mux – Enable Multiple Protocols Over a Single PVC**”, and Figure 3.4.1.1.a will show up as following:

The screenshot displays the 'DataOne Broadband' configuration interface. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, IPSec, Certificate, Wireless), Diagnostics, and Management. The main content area is titled 'ATM PVC Configuration' and includes the following fields and options:

- Instruction: 'This screen allows you to configure an ATM PVC Identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.'
- PORT: [0-3]
- VPI: [0-255]
- VCI: [32-65535]
- VLAN Mux - Enable Multiple Protocols Over a Single PVC
- 802.1Q VLAN ID: [0-4095]
- Service Category: UBR Without PCR (dropdown menu)
- Enable Quality Of Service
- Help text: 'Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.'
- Buttons: Back, Next

Figure 3.4.1.1.a Advanced Setup –**VLAN Configuration**

Input proper VLAN ID and click on “**Next**” to go to next step. Three different connection types show as below.

### 3.4.1.1.1 PPP over Ethernet Connection

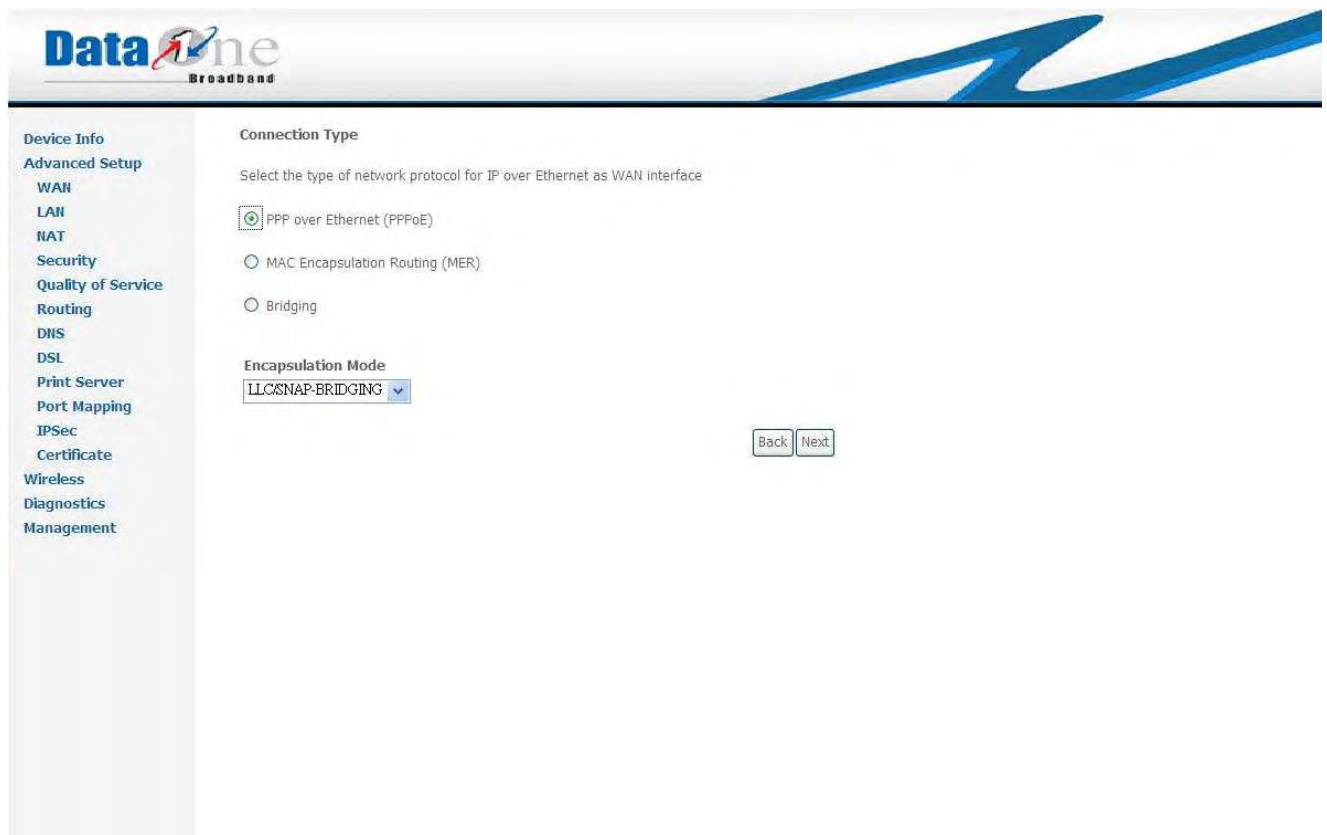


Figure 3.4.1.1.1.a Advanced Setup – **PPPoE Connection Type**

To establish a PPPoE connection, select “**PPP over Ethernet (PPPoE)**” and “**Encapsulation Mode**” click “**Next**” for next step.

**DataOne Broadband**

**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
 Security  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPsec  
 Certificate  
 Wireless  
 Diagnostics  
 Management

**PPP Username and Password**

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:   
 PPP Password:   
 PPPoE Service Name:   
 Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IP Address

Retry PPP password on authentication error

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

Figure 3.4.1.1.1.b Advanced Setup – **PPP Username and Password**

Give “PPP Username”, “PPP Password”, “PPPoE Service Name” and select “Authentication Method” (AUTO/PAP/CHAP). Please consult with your ISP provider for detail information.

The “Dial on Demand” function, if checked, will tear down the PPP link automatically if there is no outgoing packet for the programmed period of time, WA3003-G4 will display a box for input “Inactivity Timeout” as showing in Figure 3.4.1.1.d

The “PPP IP extension” function, if checked, will assign the IP address from the ISP provider to the internal PC via DHCP. In this mode, the internal PC will be assigned with a public IP from PPP, and WA3003-G4 will act as a bridge between the PC and PPPoE server. Click “Next” for next step; *Enable IGMP Multicast, and WAN Service.*

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:   
PPP Password:   
PPPoE Service Name:   
Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

PPP IP extension

Use Static IP Address

Retry PPP password on authentication error

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

Figure 3.4.1.1.1.c Advanced Setup – **PPP Username and Password Inactivity Timeout**

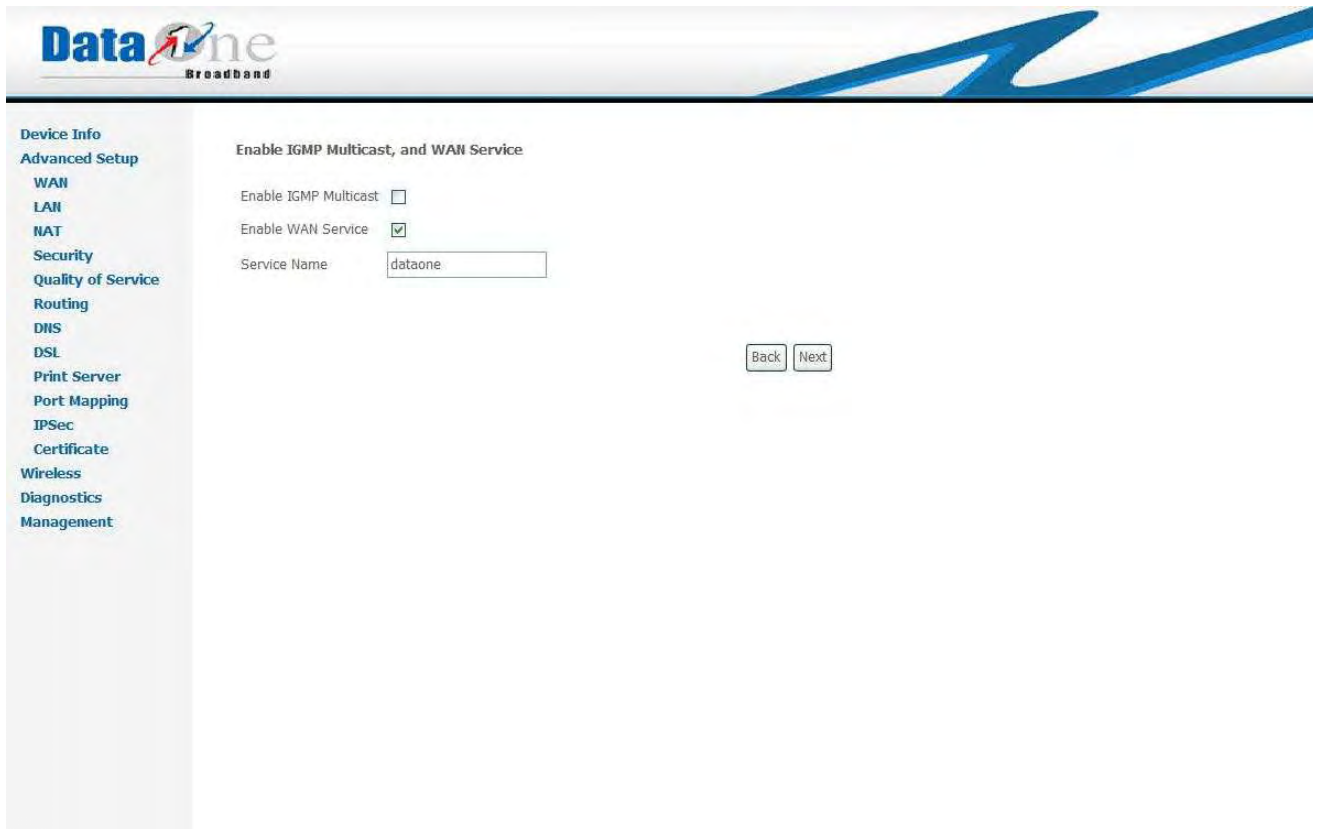


Figure 3.4.1.1.1.d Advanced Setup – **Enable IGMP Multicast, and WAN Service.**

Check “Enable/Disable IGMP Multicast” and “WAN Service”.  
Click on “Next” to go to next step.



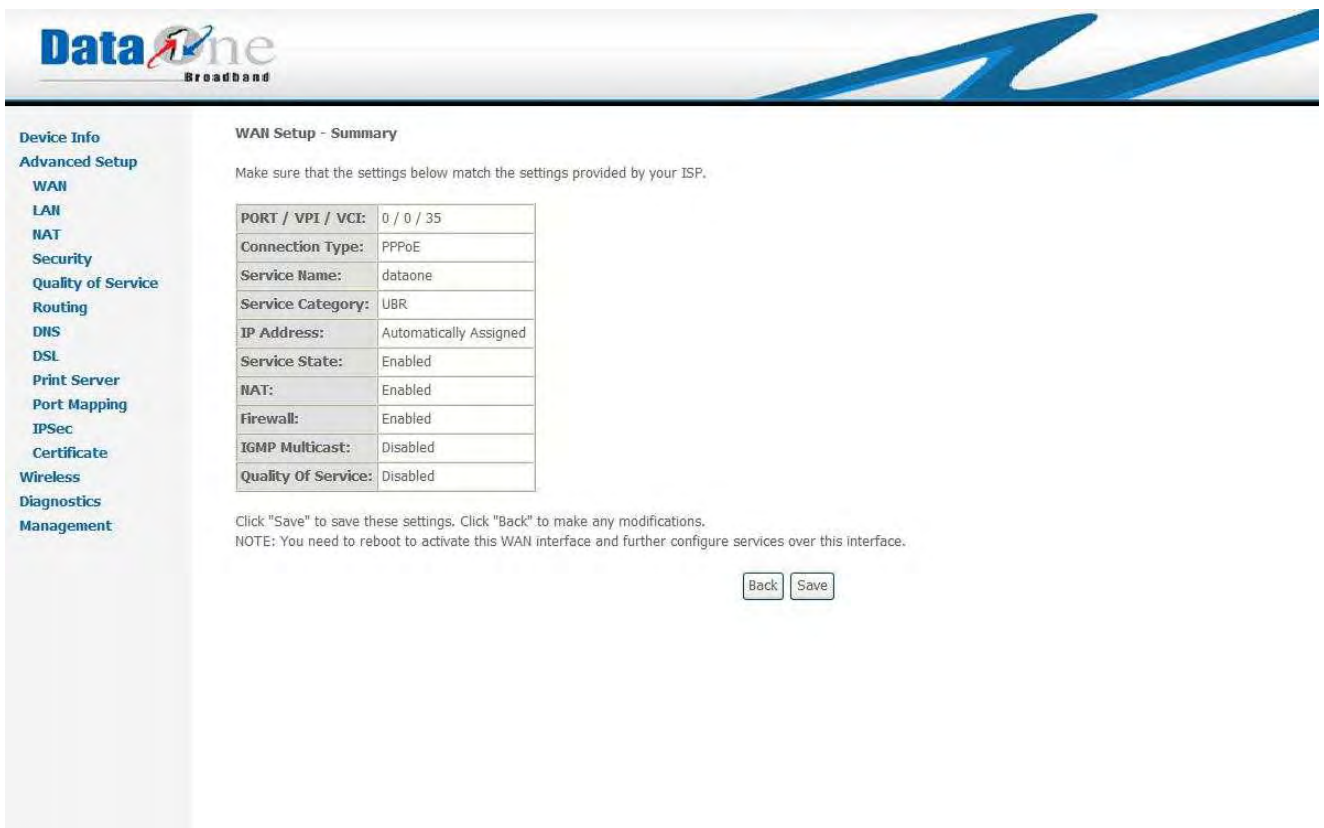


Figure 3.4.1.1.1.e Advanced Setup – WAN Setup – Summary

Figure 3.4.1.1.1.e gives a summary of previous steps (PPPoE). Make sure that the configurations match the settings provided by your ISP provider, and then click on “**Save**” button to complete the configuration procedure displays all the settings in previous steps. Click “**Back**” if you need to revise previous settings

#### 3.4.1.1.2 MAC Encapsulation Routing (MER) Connection



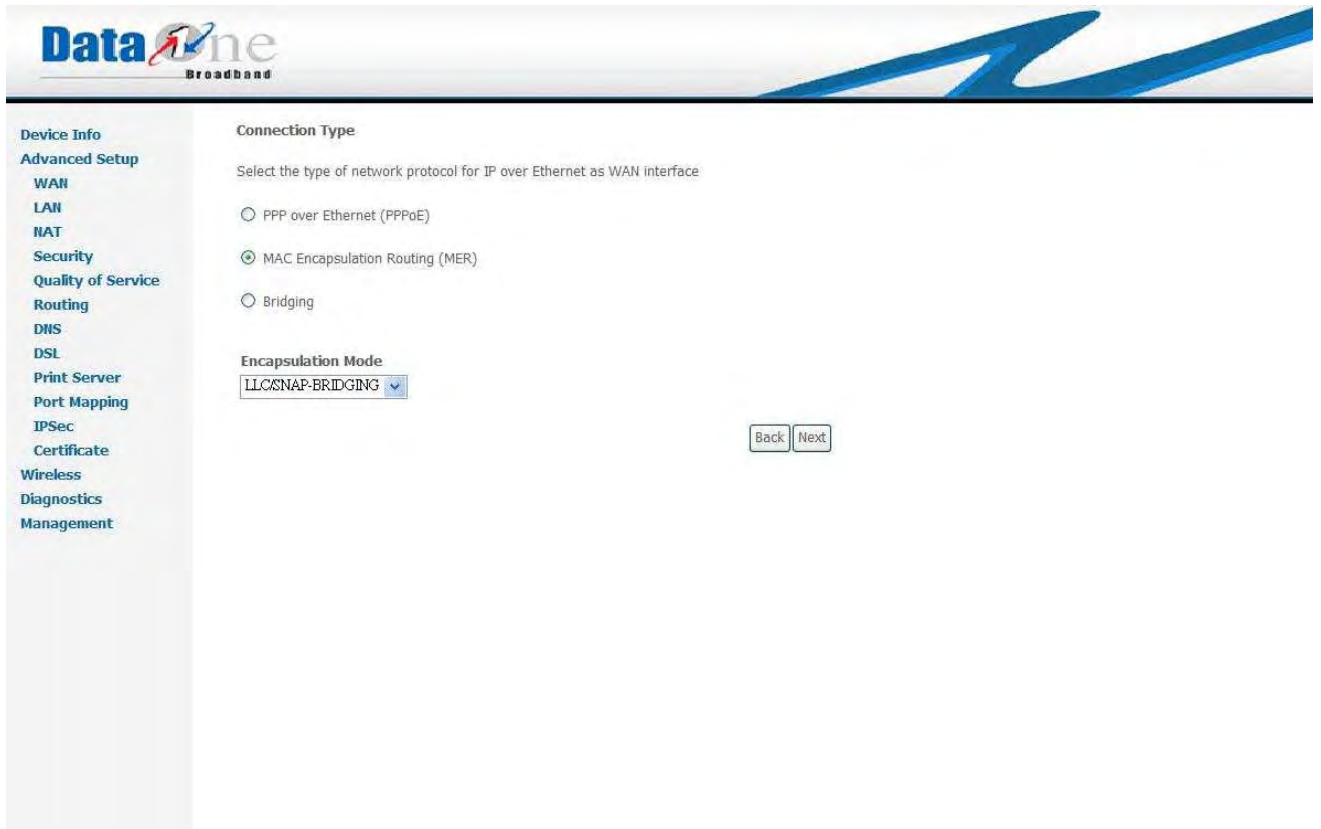


Figure 3.4.1.1.2.a Advanced Setup –*MER Connection Type*

Select "MAC Encapsulation Routing (MER)", and the "Encapsulation Mode". Please consult with your ISP provider for detail information. Click on "Next" to go to next step.

**DataOne**  
Broadband

**Device Info**

**Advanced Setup**

- WAN**
- LAN
- NAT
- Security
- Quality of Service
- Routing
- DNS
- DSL
- Print Server
- Port Mapping
- IPSec
- Certificate
- Wireless
- Diagnostics
- Management

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

Obtain an IP address automatically  
 Use the following IP address:  
 WAN IP Address:   
 WAN Subnet Mask:

Obtain default gateway automatically  
 Use the following default gateway:  
 Use IP Address:   
 Use WAN Interface:

Obtain DNS server addresses automatically  
 Use the following DNS server addresses:  
 Primary DNS server:   
 Secondary DNS server:

Back Next

Figure 3.4.1.1.2.b Advanced Setup –**Connection Type MER WAN IP Settings**

WAN IP/Subnet Mask, Default Gateway, and DNS Server can either be obtained automatically or set manually. The WAN IP can be either fixed (assigned by your ISP provider) or dynamic (via DHCP Client). Enter the "Vendor ID" if DHCP Client is selected and your ISP requests for it. Click on "Next" for next step.

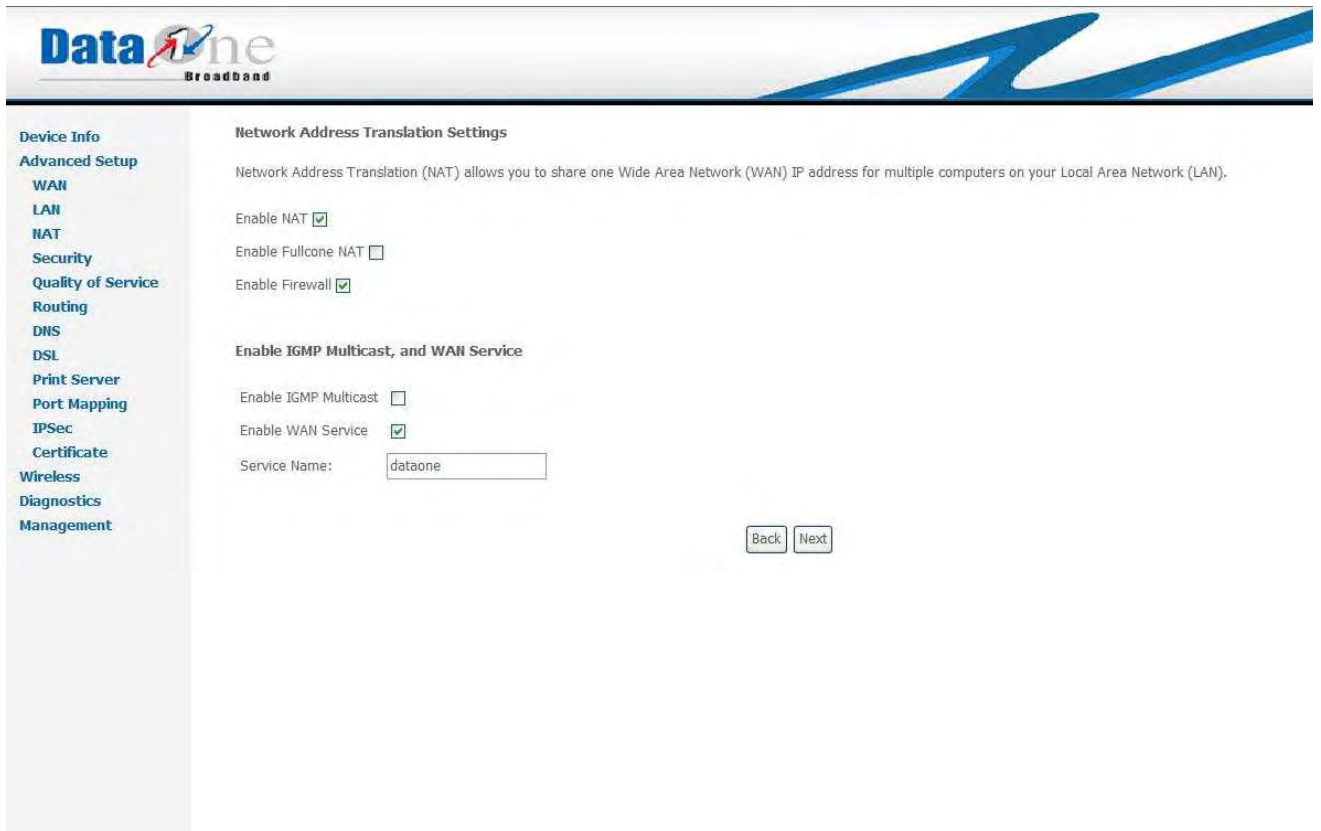


Figure 3.4.1.1.2.c Advanced Setup –MER- NAT, Firewall, IGMP Multicast and WAN service

Check to Enable/Disable **NAT**, **Fullcone NAT** and **Firewall** functions.  
Use "**Advanced Setup – Security**" to assign filter rules.  
Check to Enable/Disable IGMP Multicast and WAN Service.  
Click on "Next" to go to next step.

**DataOne**  
Broadband

**Device Info**  
**Advanced Setup**  
WAN  
LAN  
NAT  
Security  
IP Filtering  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPSec  
Certificate  
Wireless  
Diagnostics  
Management

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	MER
Service Name:	dataone
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.  
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

Figure 3.4.1.1.2.d Advanced Setup WAN Setup – Summary

Figure 3.4.1.1.2.d gives a summary of previous steps (MER). Make sure that the configurations match the settings provided by your ISP provider, and then click on “**Save**” button to complete the configuration procedure displays all the settings in previous steps. Click “**Back**” if you need to revise previous settings

### 3.4.1.1.3 Bridging Connection

Select “**Bridging**”, and the “**Encapsulation Mode**”. Please contact you ISP for the information. Click on “**Next**” to go to next step.

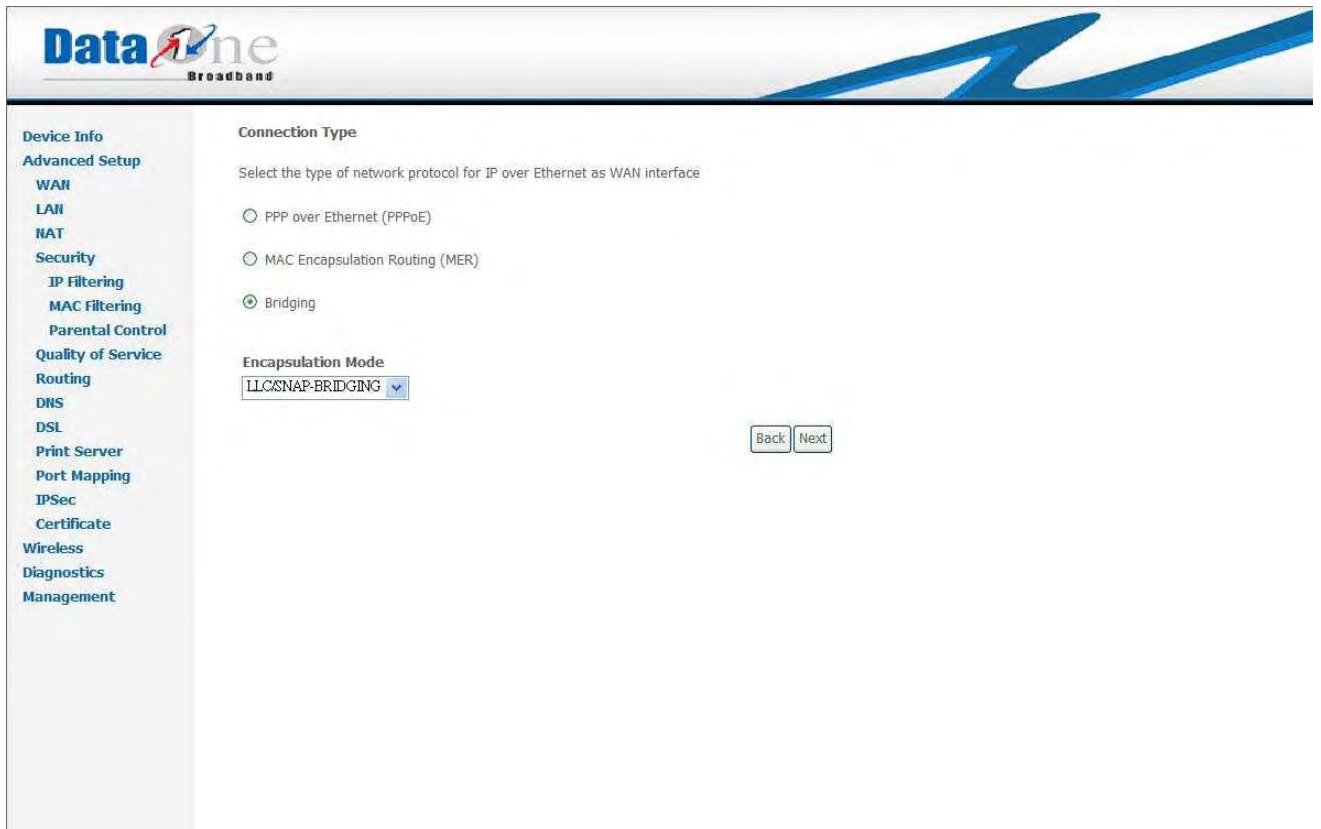


Figure 3.4.1.1.3.a Advanced Setup –**Bridging Type**

To disable WAN service, unselect “Enable Bridge Service” check box, click “Next” for next step

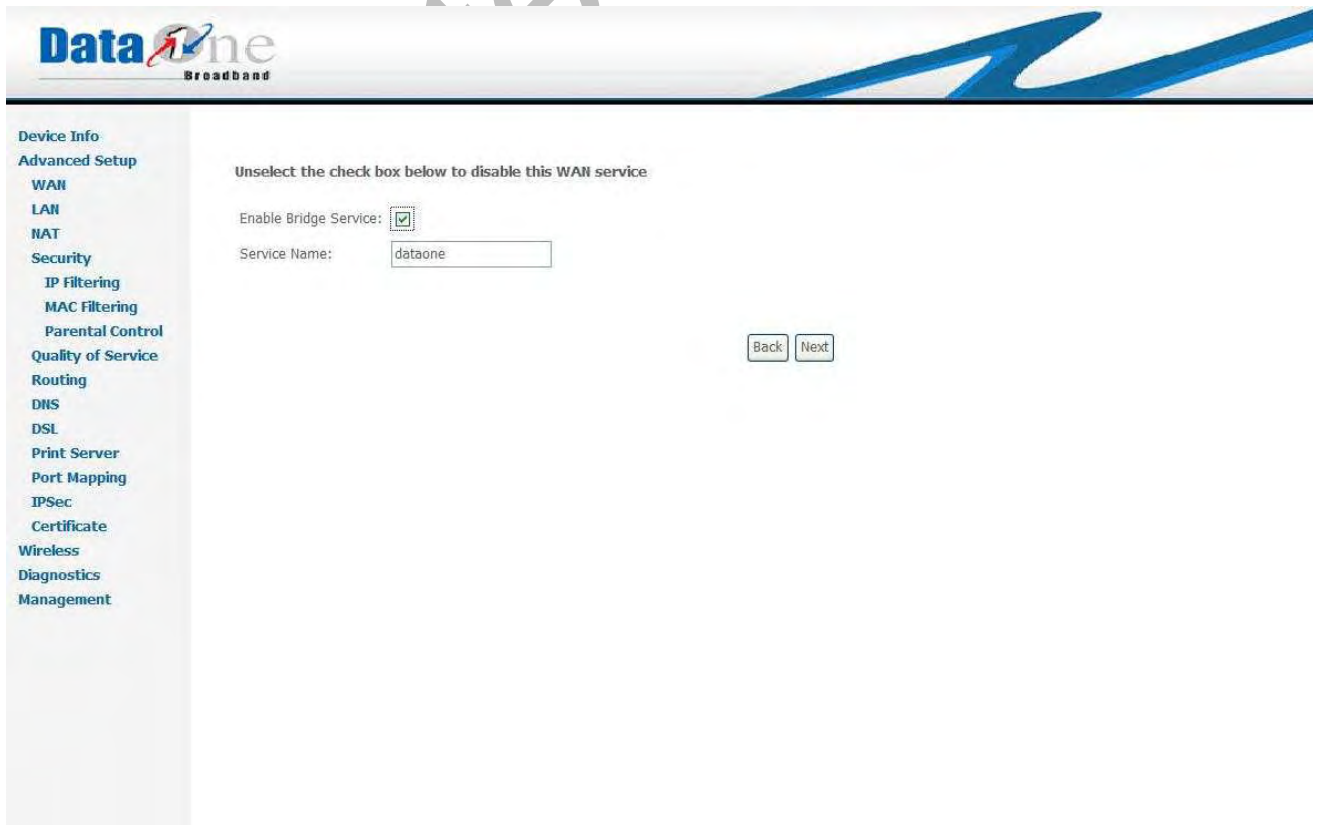


Figure 3.4.1.1.3.b Advanced Setup –**Bridging Type** – WAN Service

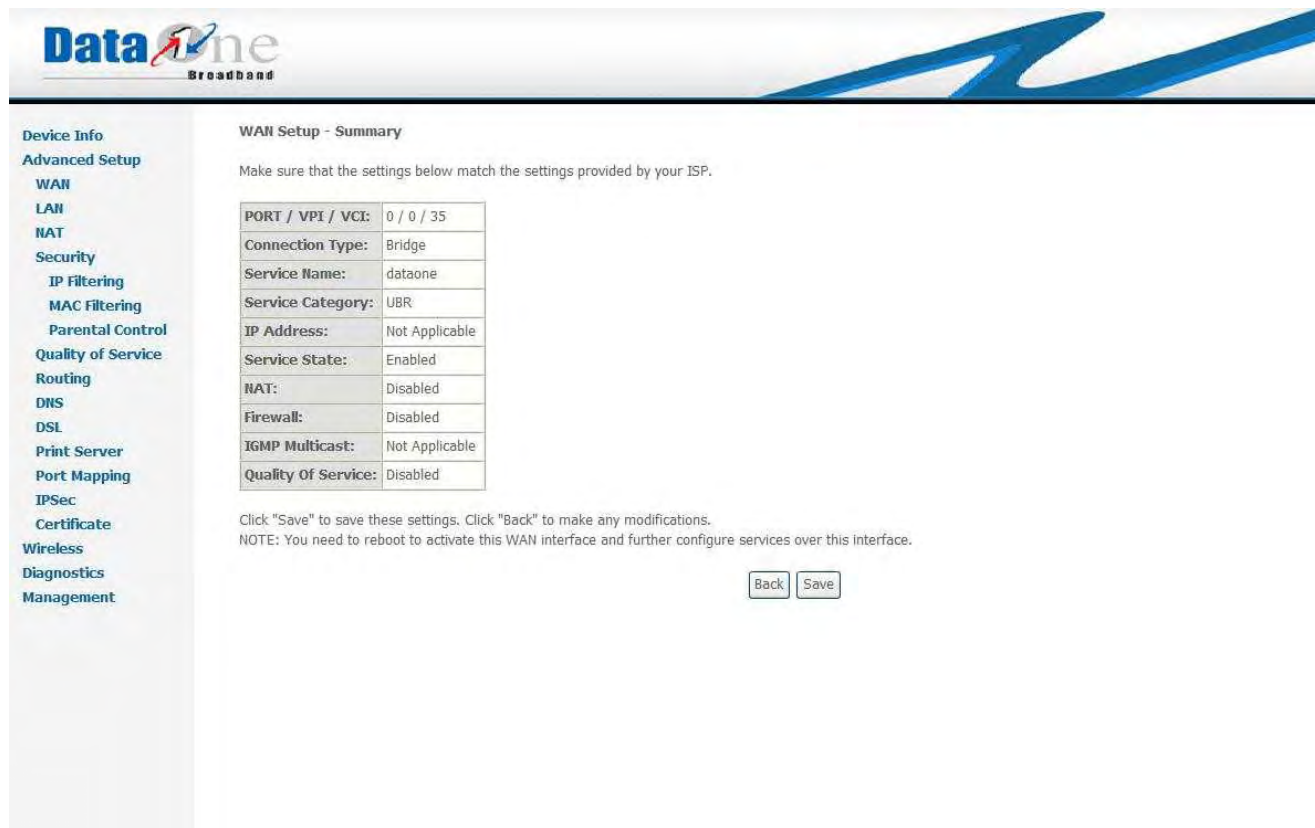


Figure 3.4.1.1.3.c Advanced Setup WAN Setup – Summary

Figure 3.4.1.1.3.c gives a summary of previous steps (Bridging). Make sure that the configurations match the settings provided by your ISP provider, and then click on “**Save**” button to complete the configuration procedure displays all the settings in previous steps. Click “**Back**” if you need to revise previous settings

## 3.4.2 Advanced Setup – LAN

**DataOne Broadband**

**Local Area Network (LAN) Setup**

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:

Subnet Mask:

Enable UPnP

Enable IGMP Snooping

Standard Mode

Blocking Mode

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

Figure 3.4.2 Advanced Setup – LAN

Give IP (LAN IP) and Subnet Mask to the device.

Select to Disable/Enable DHCP Server and configure related settings for that mode.

If necessary, check the “Secondary IP” to configure the secondary IP address and Subnet Mask for LAN. This IP address is used for management only.

Note that Network Address Translation function (NAT) is default enabled and is not showing on the page to prevent it from being disabled.

Click on “Next” to go to next step.

### 3.4.3 Advanced Setup – NAT

#### 3.4.3.1 Advanced Setup – NAT—Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.



Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

ALG

Security

Quality of Service

Routing

DNS

DSL

Print Server

Port Mapping

IPSec

Certificate

Wireless

Diagnostics

Management

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	-------------	--------

Figure 3.4.3.1.a Advanced Setup – NAT

Click **"Add"** for next step

Watermark



**DataOne**  
Broadband

Device Info  
Advanced Setup  
WAN  
LAN  
NAT  
Virtual Servers  
Port Triggering  
DMZ Host  
ALG  
Security  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPSec  
Certificate  
Wireless  
Diagnostics  
Management

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

Remaining number of entries that can be configured:32

Server Name:  
 Select a Service:   
 Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Figure 3.4.3.1 b Advanced Setup – NAT – Virtual Servers

Select the service name, and enter the server IP address and click "**Save/Apply**" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

Remaining number of entries that can be configured: 32

### 1. Advanced Setup – NAT— Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

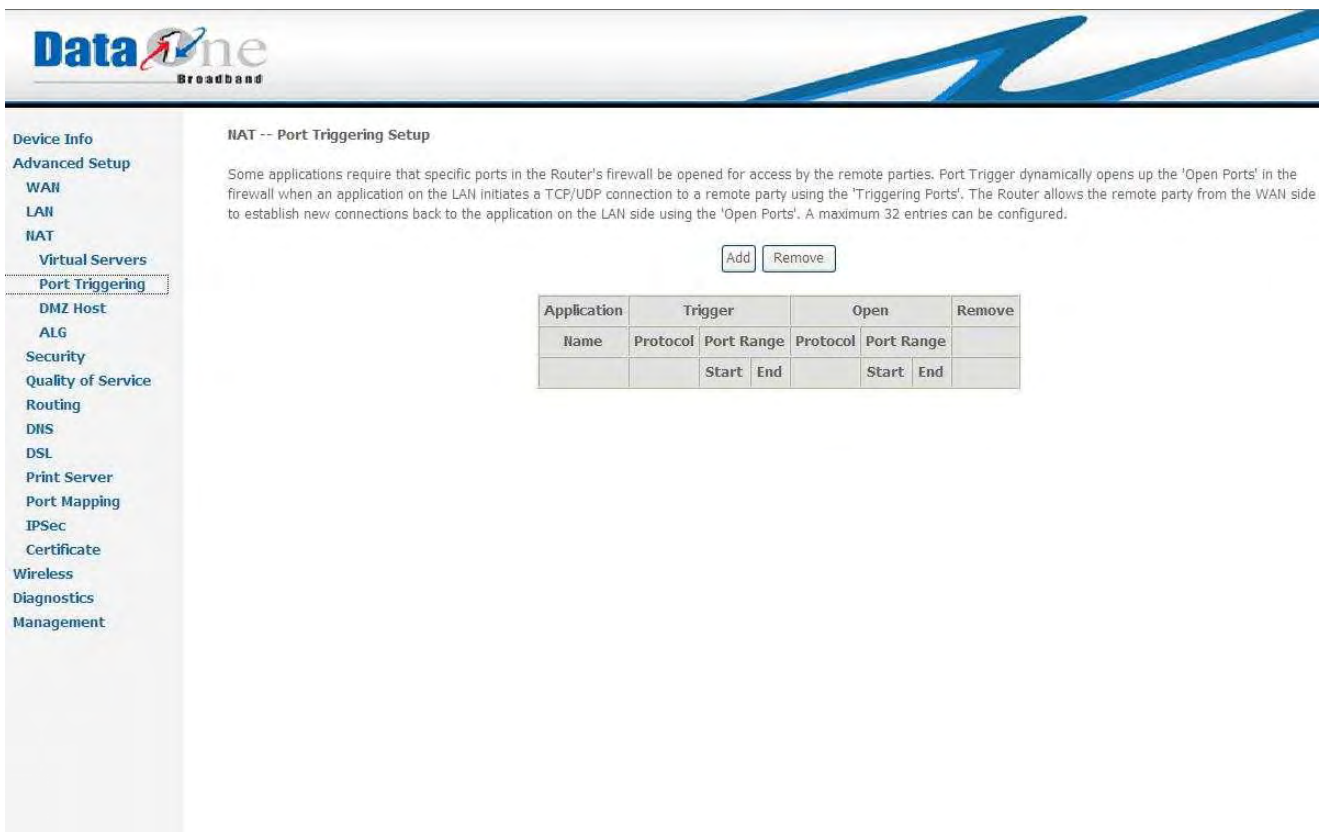


Figure 3.4.3.2.a Advanced Setup – NAT – Port Triggering Setup

Click **"Add"** for next step

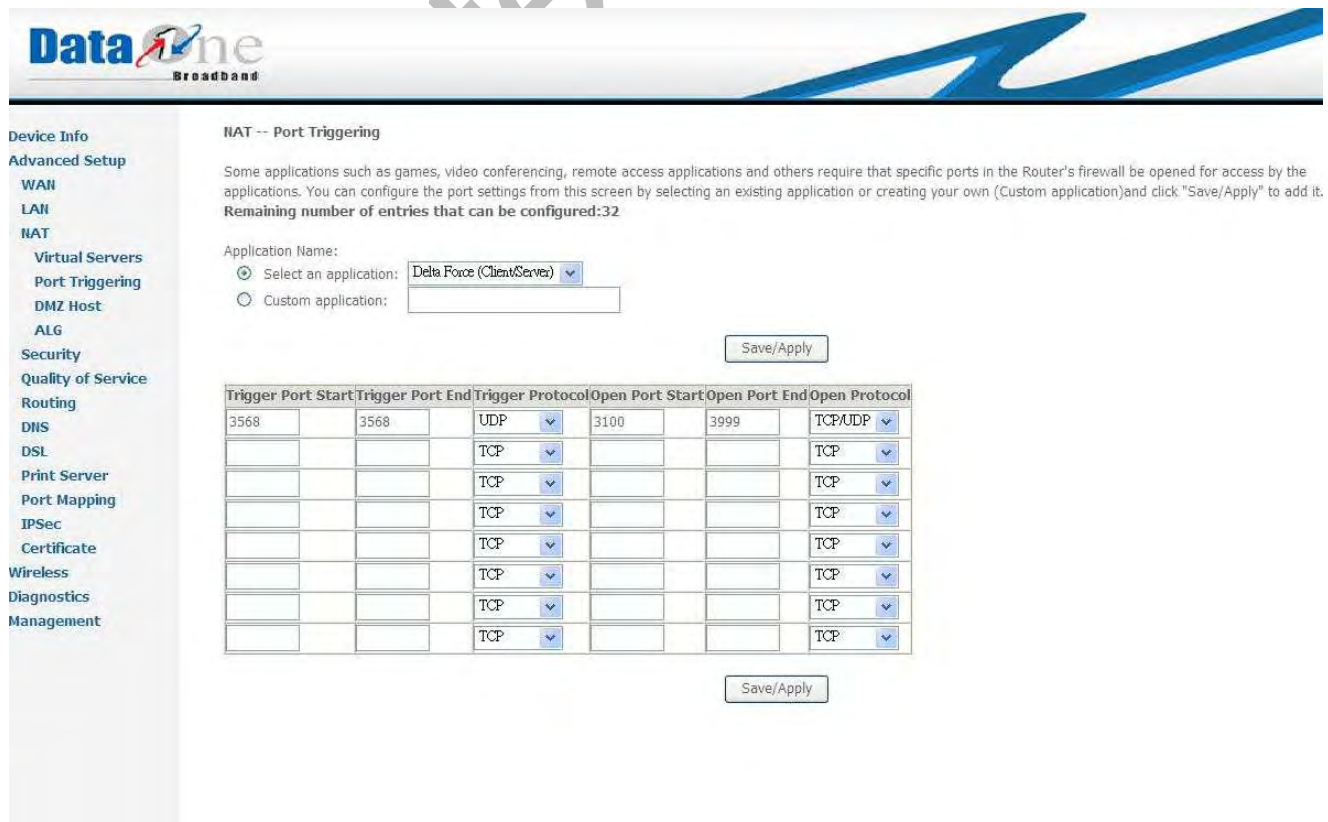


Figure 3.4.3.2.b Advanced Setup – NAT – Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "**Save/Apply**" to add it.

Remaining number of entries that can be configured: 32

## 2. Advanced Setup – NAT— DMZ Host

**WA3003-G4** will forward IP packets from the WAN which do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

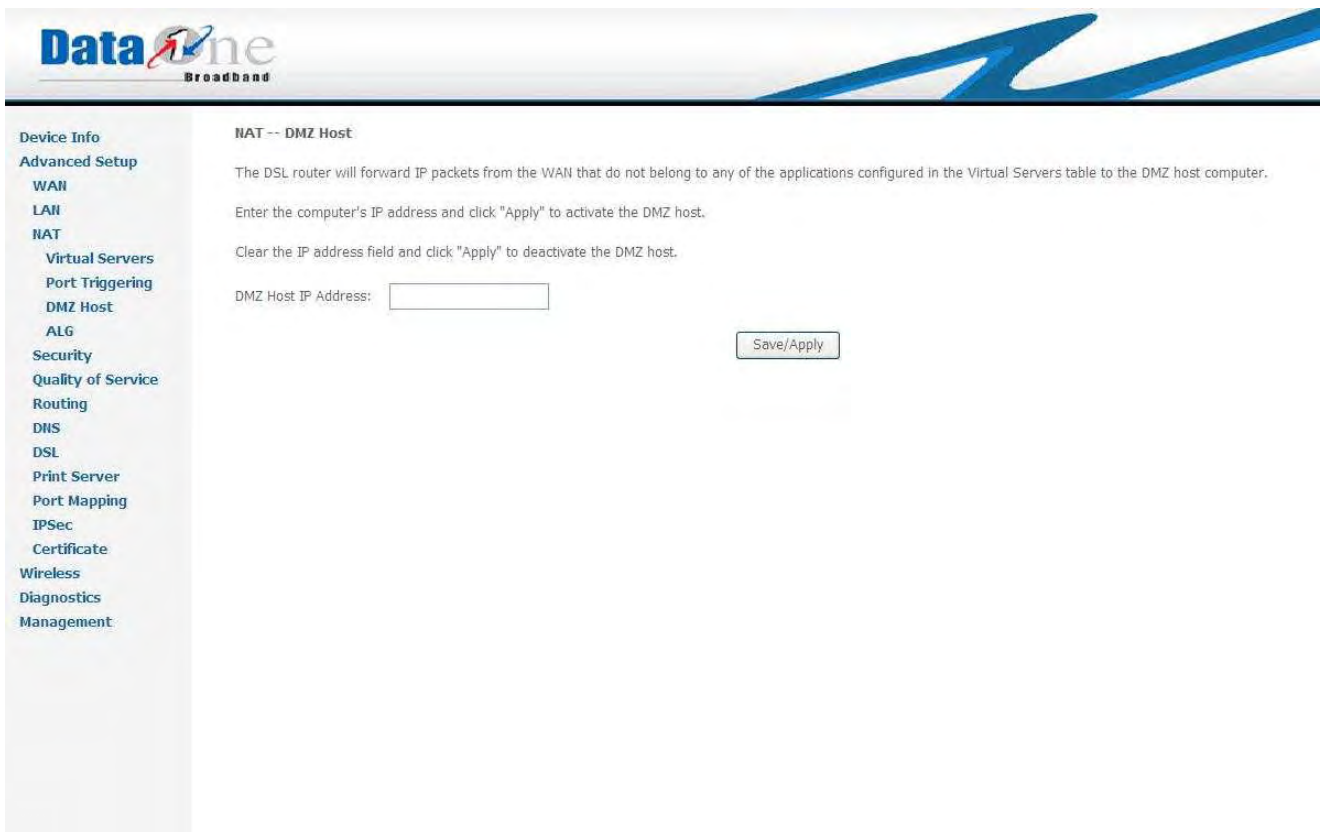


Figure 3.4.3.3 Advanced Setup – NAT— DMZ Host

## 3. Advanced Setup – NAT— ALG

**WA3003-G4** provides SIP Enable application, check SIP Enable selection and click "**Save/Apply**" for this setting if necessary.

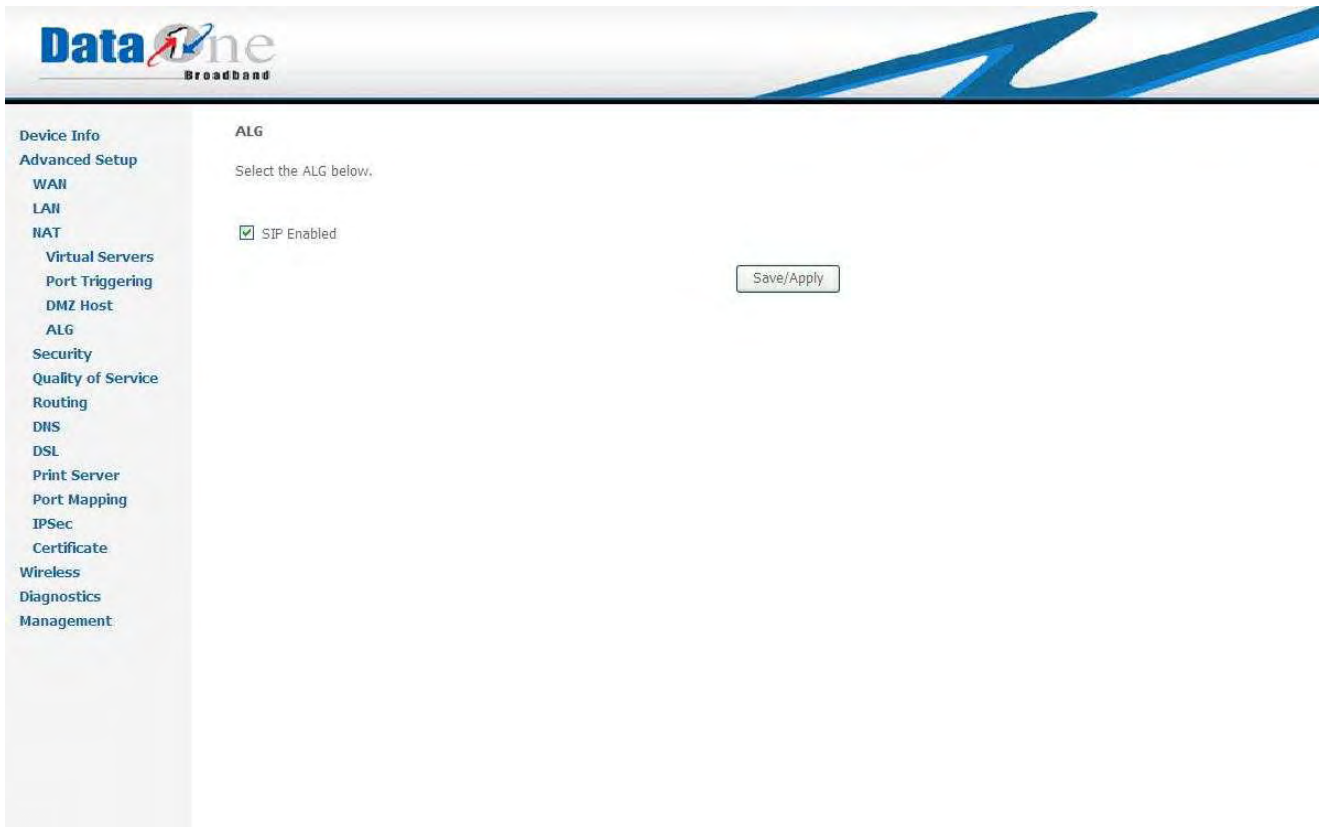


Figure 3.4.3.4 Advanced Setup – NAT— ALG

## 3.4.4 Advanced Setup – Security

### 3.4.4.1 Advanced Setup – Security – IP Filter

#### 3.4.4.1.1 Advanced Setup – Security – IP Filter -- Outgoing

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Click “**Add**” for next step:

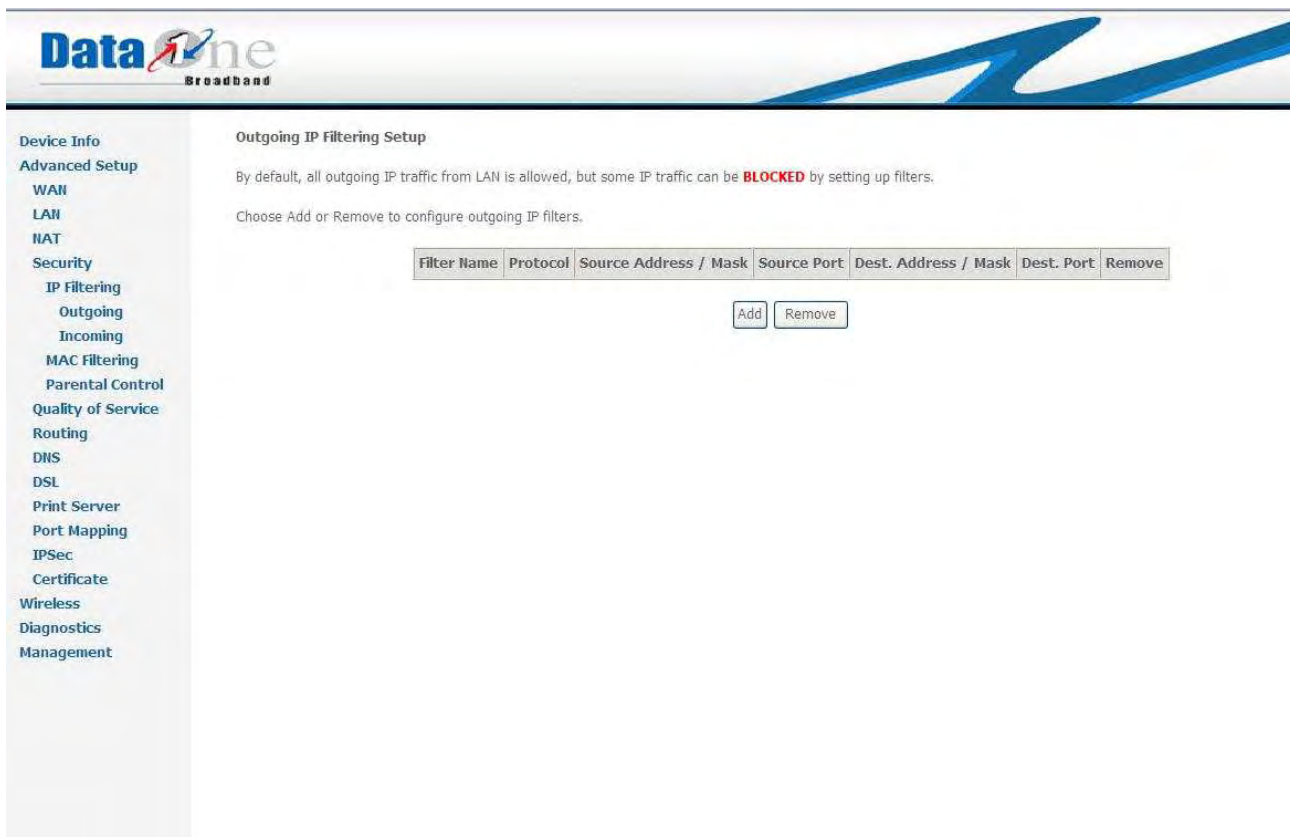


Figure 3.4.4.1.1.a Advanced Setup – Security – IP Filter -- Outgoing

**WA3003G4** allows the users to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

#### Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Save/Apply

### 3.4.4.1.1.b Advanced Setup – Security – IP Filter—Add Outgoing Rules

### 3.4.4.1.2 Advanced Setup – Security – IP Filter – Incoming

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters



**DataOne**  
Broadband

Device Info  
Advanced Setup  
WAN  
LAN  
NAT  
Security  
IP Filtering  
Outgoing  
**Incoming**  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPSec  
Certificate  
Wireless  
Diagnostics  
Management

### Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

Figure 3.4.4.1.2.a Advanced Setup – Security –IP Filter – Incoming

**WA3003G4** allows the users to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. When there are multiple WAN interfaces configured, users can choose which interface(s) will apply the rule.

**DataOne**  
Broadband

Device Info  
Advanced Setup  
WAN  
LAN  
NAT  
Security  
IP Filtering  
Outgoing  
Incoming  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPsec  
Certificate  
Wireless  
Diagnostics  
Management

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

- Select All
- pppoe\_0\_0\_35\_1/ppp\_0\_0\_35\_1
- dataone/ppp\_0\_0\_35\_2
- dataone/ppp\_0\_0\_35\_4
- dataone/ppp\_0\_0\_35\_6

Save/Apply

Figure 3.4.4.1.2.b Advanced Setup – Security –IP Filter – Add Incoming Rules

### 3.4.4.2 Advanced Setup – Security – MAC Filter

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. “**FORWARDED**” means that all MAC layer frames will be **FORWARDED** for those matching with any of the specified rules in Figure 3.4.4.2.a MAC Filter Rules. “**BLOCKED**” means that all MAC layer frames will be **BLOCKED** for those matching with any of the specified rules in Figure 3.4.4.2.a Advanced Setup – Security – MAC Filter Rules



- Device Info
- Advanced Setup
  - WAN
  - LAN
  - NAT
- Security
  - IP Filtering
  - MAC Filtering
  - Parental Control
- Quality of Service
- Routing
  - DNS
  - DSL
- Print Server
- Port Mapping
- IPSec
- Certificate
- Wireless
- Diagnostics
- Management

**MAC Filtering Setup**

MAC Filtering Global Policy: **FORWARDED**

Change Policy

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the follo table.

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	PPPoE	00:19:15:a6:b4:56	00:19:15:a6:b4:58	LAN<=>WAN	<input type="checkbox"/>

Add Remove

Figure 3.4.4.2.a Advanced Setup – Security – MAC Filter

Click **“Add”** to add a MAC Filter Rule as shows in Figure 3.4.4.2.b Advanced Setup – Security – Add MAC Filter

**DataOne**  
Broadband

Device Info  
Advanced Setup  
WAN  
LAN  
NAT  
Security  
IP Filtering  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
IPsec  
Certificate  
Wireless  
Diagnostics  
Management

### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- Select All
- dataone/nas\_0\_0\_35.2
- br\_0\_0\_32/nas\_0\_0\_32
- br\_0\_8\_35/nas\_0\_8\_35
- br\_0\_8\_81/nas\_0\_8\_81
- br\_0\_0\_100/nas\_0\_0\_100
- br\_0\_14\_34/nas\_0\_14\_34

Figure 3.4.4.2.b Advanced Setup – Security – Add MAC Filter

To clean all MAC Filter Rules, click **“Change Policy”** in Figure 3.4.4.2.a Advanced Setup – Security – MAC Filter.

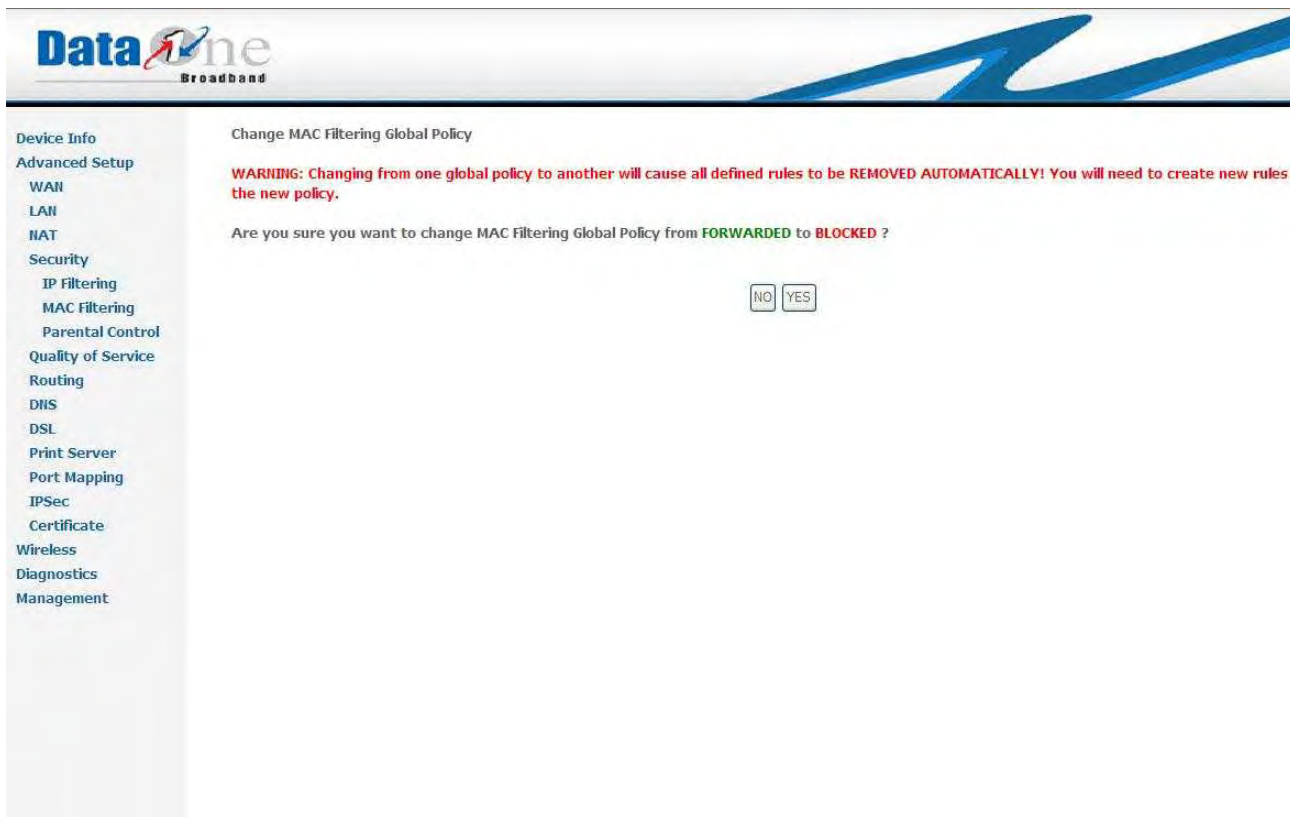


Figure 3.4.4.2.c Advanced Setup – Security – Clean MAC Filter Rules

### 3.4.4.3 Advanced Setup – Security – Parental Control

WA3003G4 provides Parental Control utility to limit internet usage as showing below:

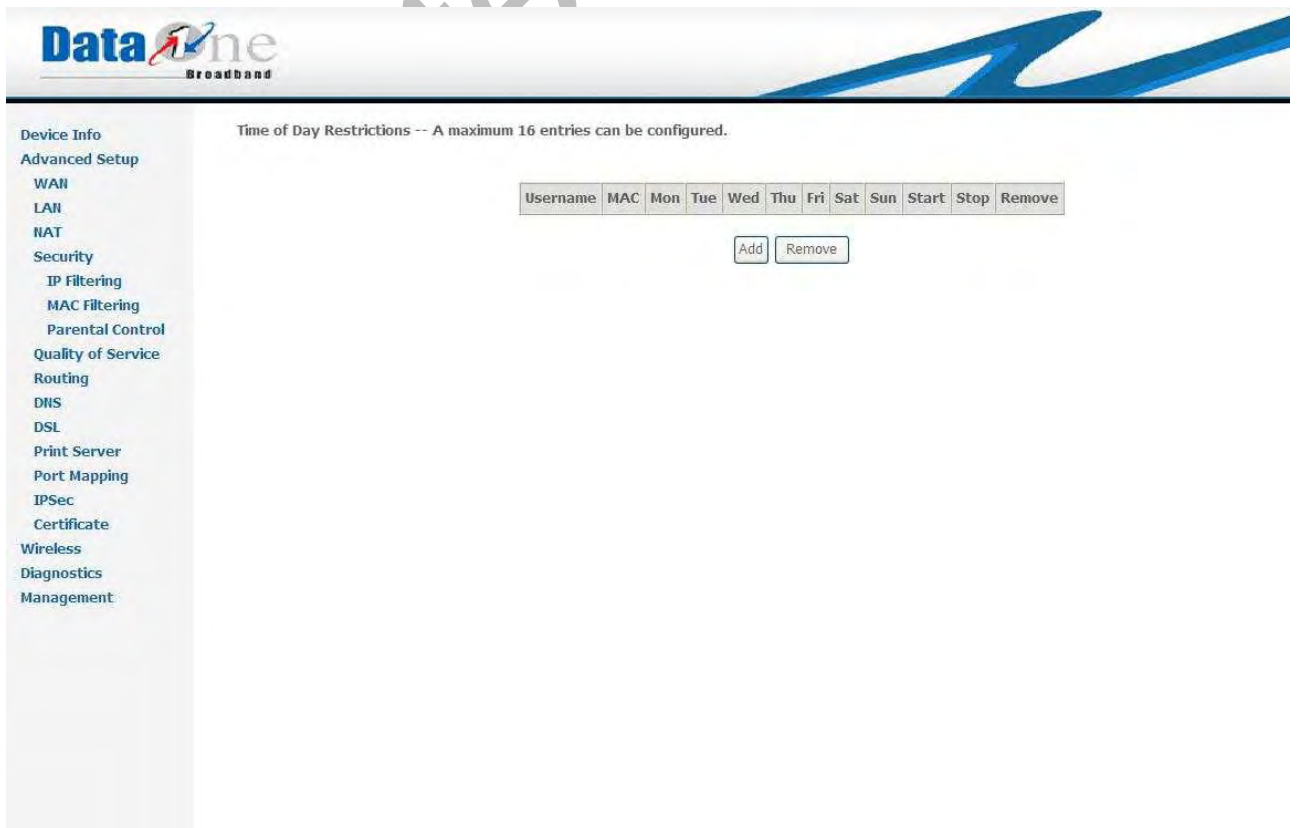


Figure 3.4.4.3.a Advanced Setup – Security – Parental Control

Click “**Add**” to set restriction rules as following:

**DataOne Broadband**

**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
**Security**  
 IP Filtering  
 MAC Filtering  
 Parental Control  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPSec  
 Certificate  
 Wireless  
 Diagnostics  
 Management

**Time of Day Restriction**

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 3.4.4.3.b Advanced Setup – Security – Parental Control – Add Restrictions

### 3.4.5 Advanced Setup – Quality of Service

### 3.4.6 Advanced Setup – Routing

WA3003G4 provides three different routing types as below:

#### 3.4.6.1 Advanced Setup – Routing – Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

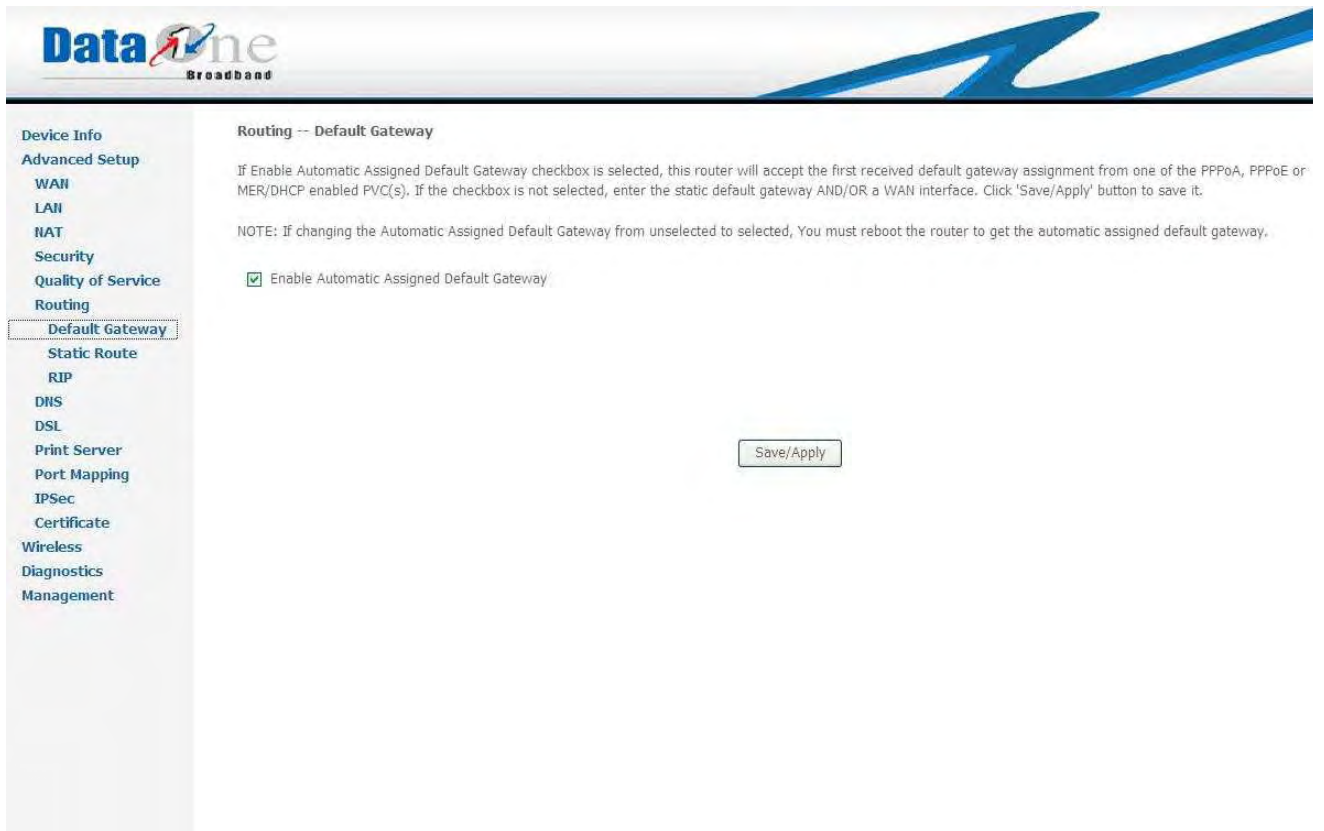


Figure 3.4.6.1 Advanced Setup – Routing – Default Gateway

### 3.4.6.2 Advanced Setup – Routing – Static Route

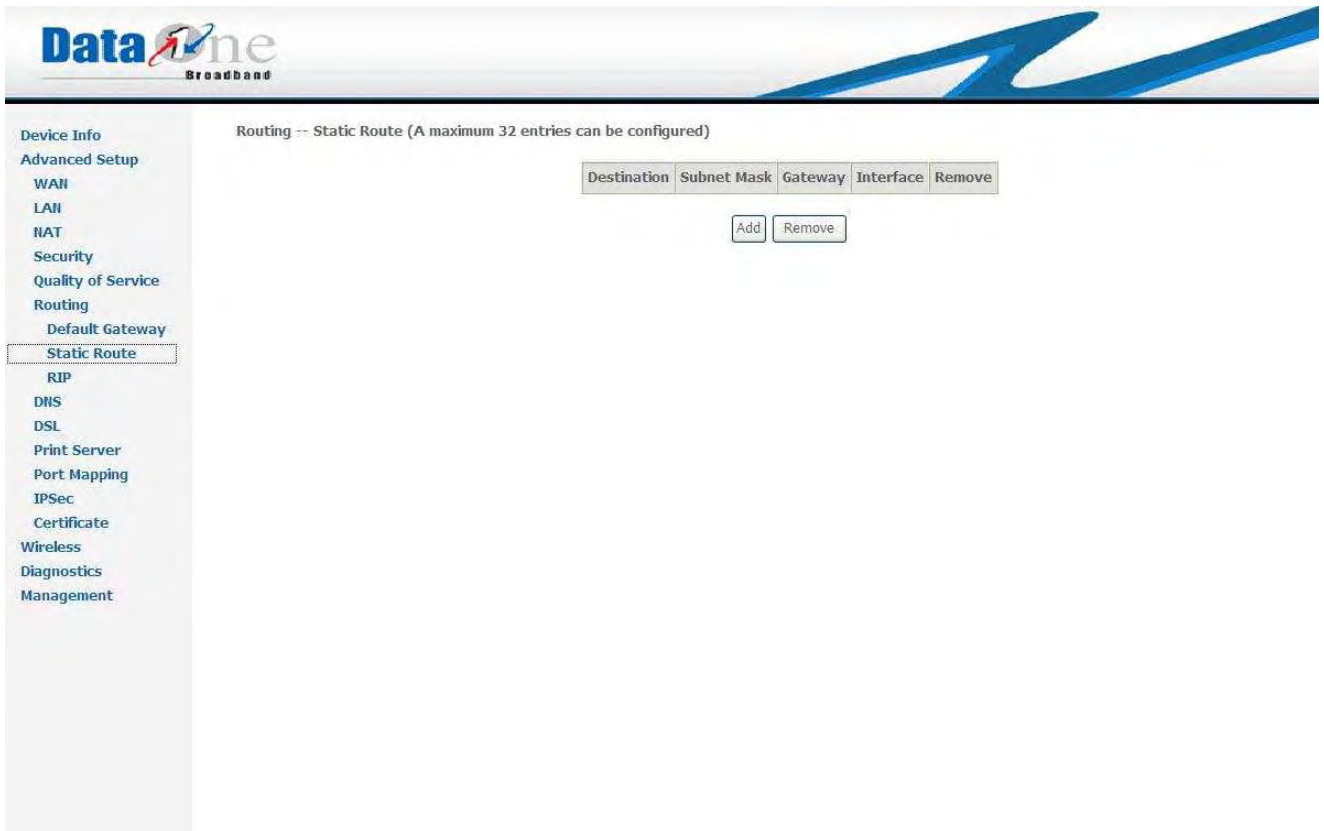


Figure 3.4.6.2.a Advanced Setup – Routing –Static Route

Click on **"Add"** to create a new Static Route. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **"Save/Apply"** to add the entry to the routing table as showing in Figure 3.4.6.2.b Advanced Setup – Routing –Static Route



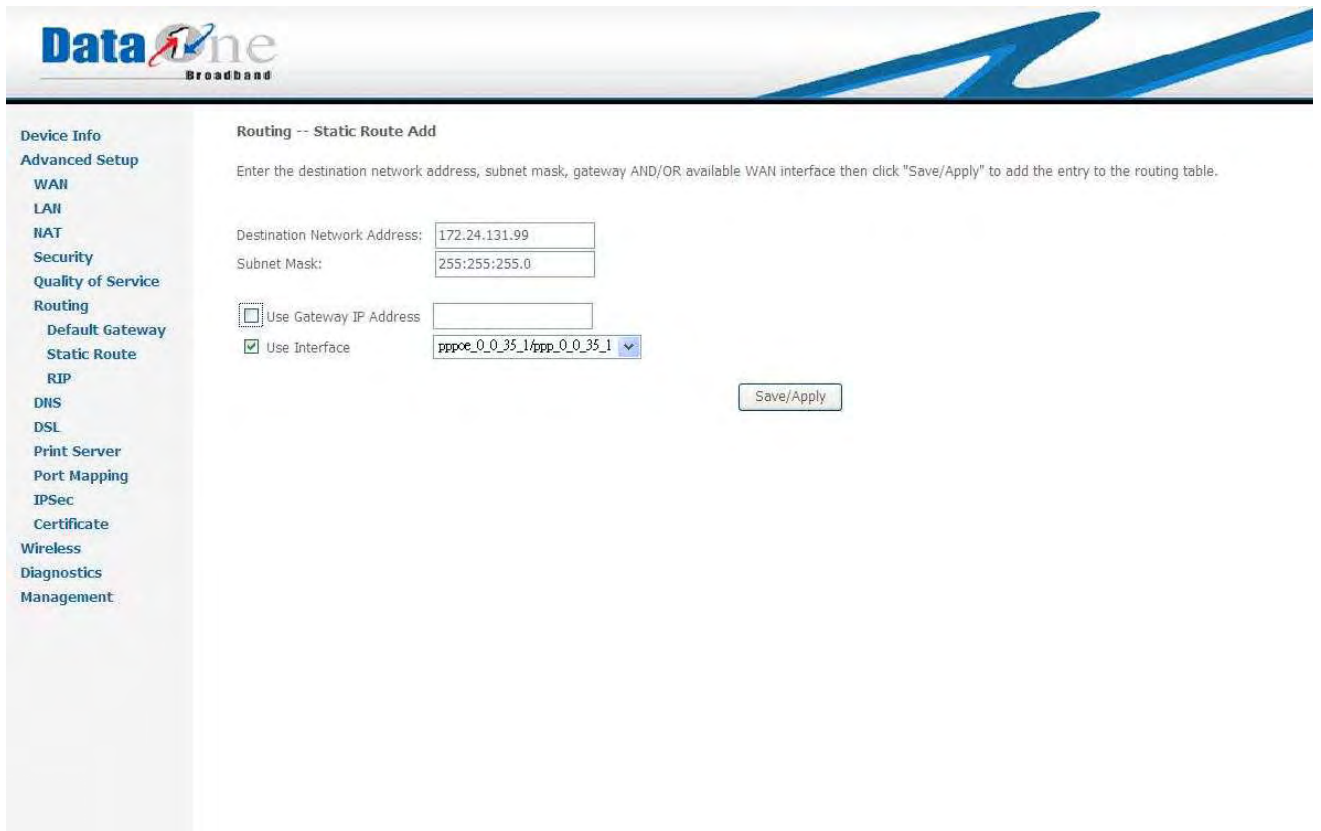


Figure 3.4.6.2.a Advanced Setup – Routing –Static Route

### 3.4.6.3 Advanced Setup – Routing – RIP

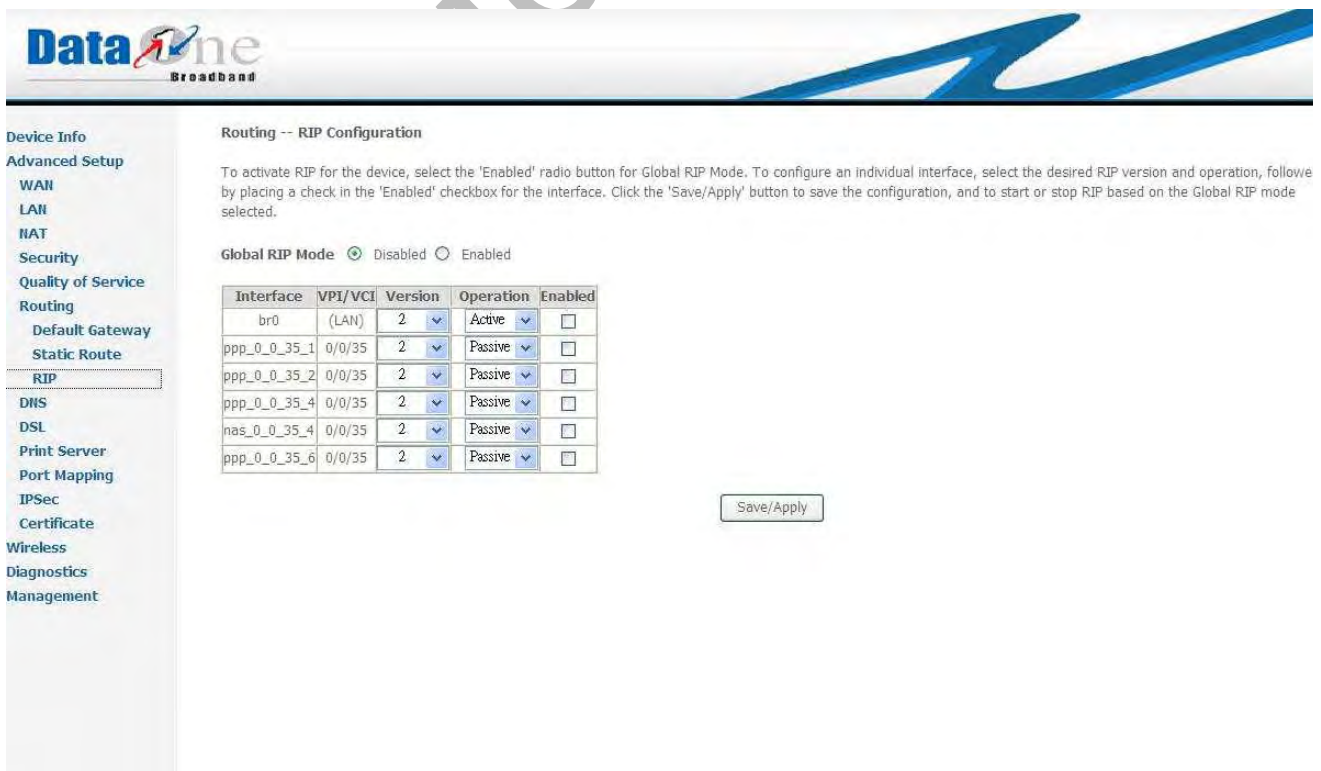


Figure 3.4.6.3 Advanced Setup – Routing –RIP

To activate RIP for the device, select the '**Enabled**' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the '**Enabled**' checkbox for the interface. Click the '**Save/Apply**' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

### 3.4.7 Advanced Setup – DNS

#### 3.4.7.1 Advanced Setup – DNS – DNS Server

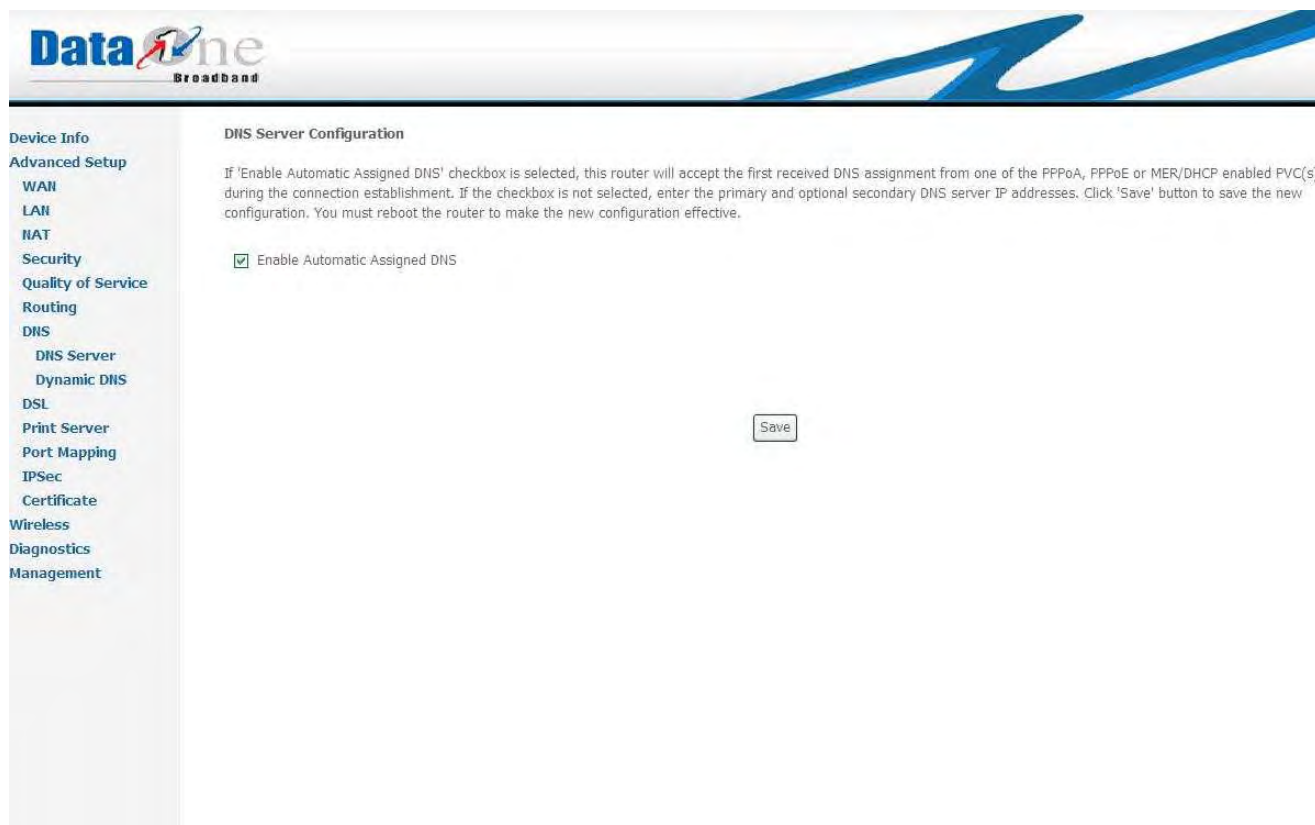


Figure 3.4.7.1 Advanced Setup –DNS – DNS Server

If '**Enable Automatic Assigned DNS**' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click '**Save**' button to save the new configuration. You must reboot the router to make the new configuration effective.

#### 3.4.7.2 Advanced Setup – DNS – Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.



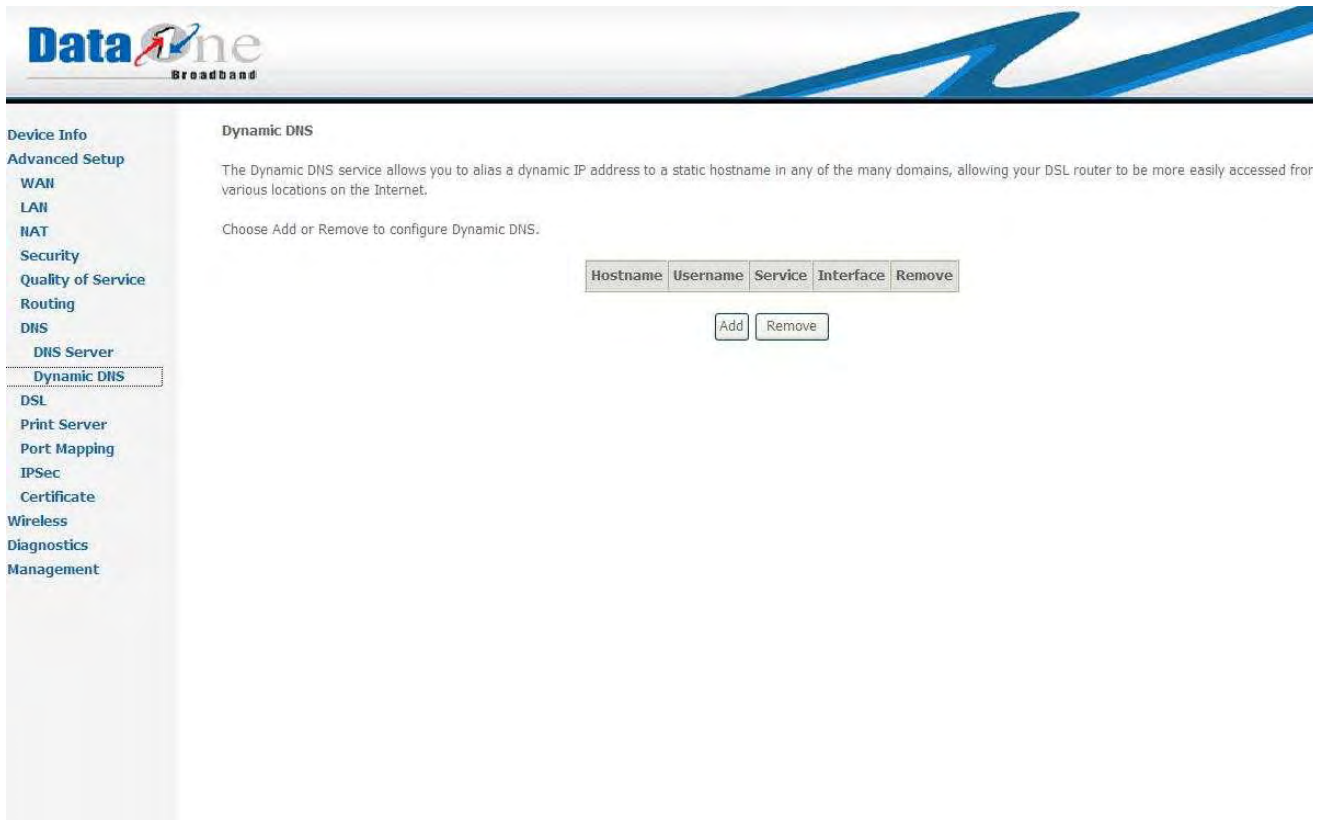


Figure 3.4.7.2.a Advanced Setup –DNS –Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

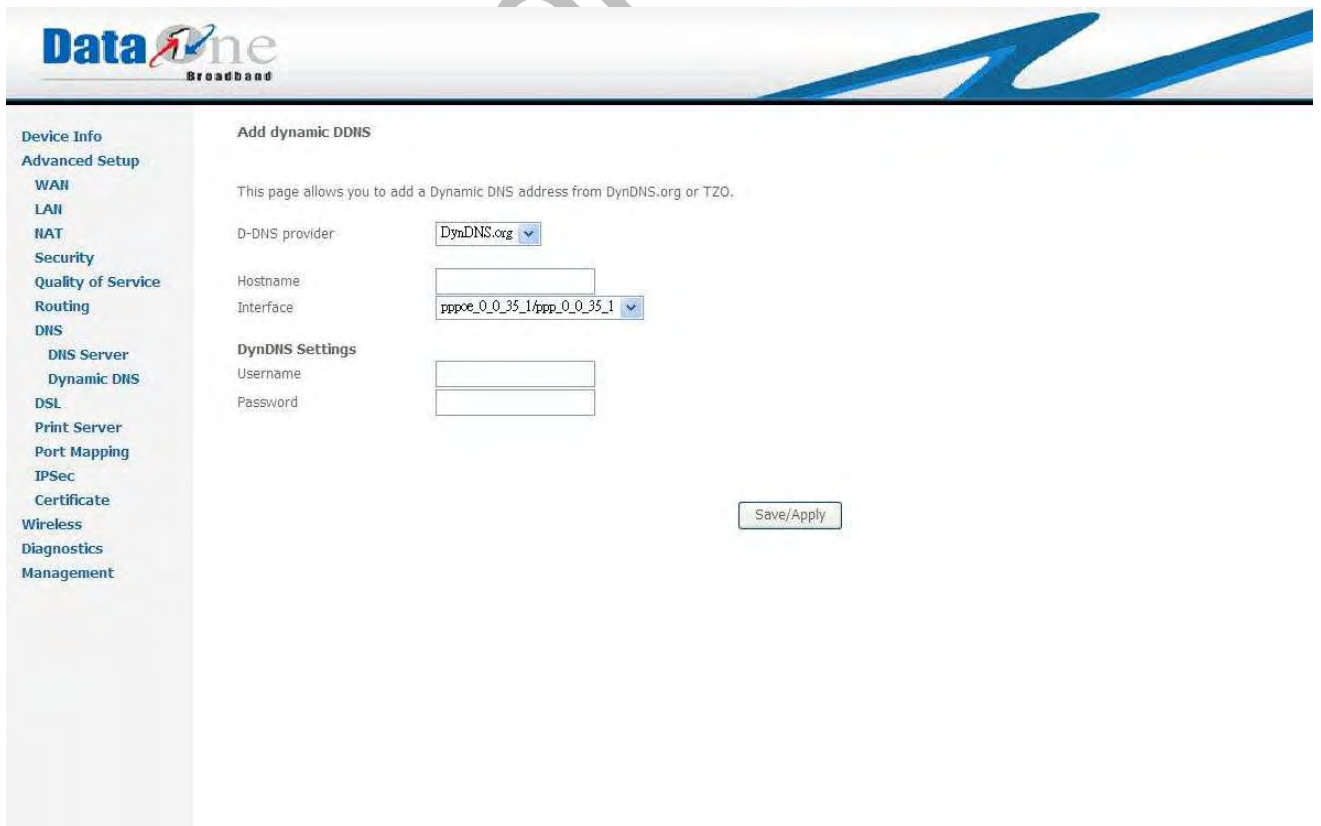


Figure 3.4.7.2.b Advanced Setup –DNS –Dynamic DNS

### 3.4.8 Advanced Setup – DSL

Under DLS settings, a lot of DSL modulations can be set including: G.DMT, G.lite, T1.413 ADSL2, Annex L, M and ADSL2+; also the phone line pair and capability showing as Figure 3.4.8.1 Advanced Setup – DSL Settings.

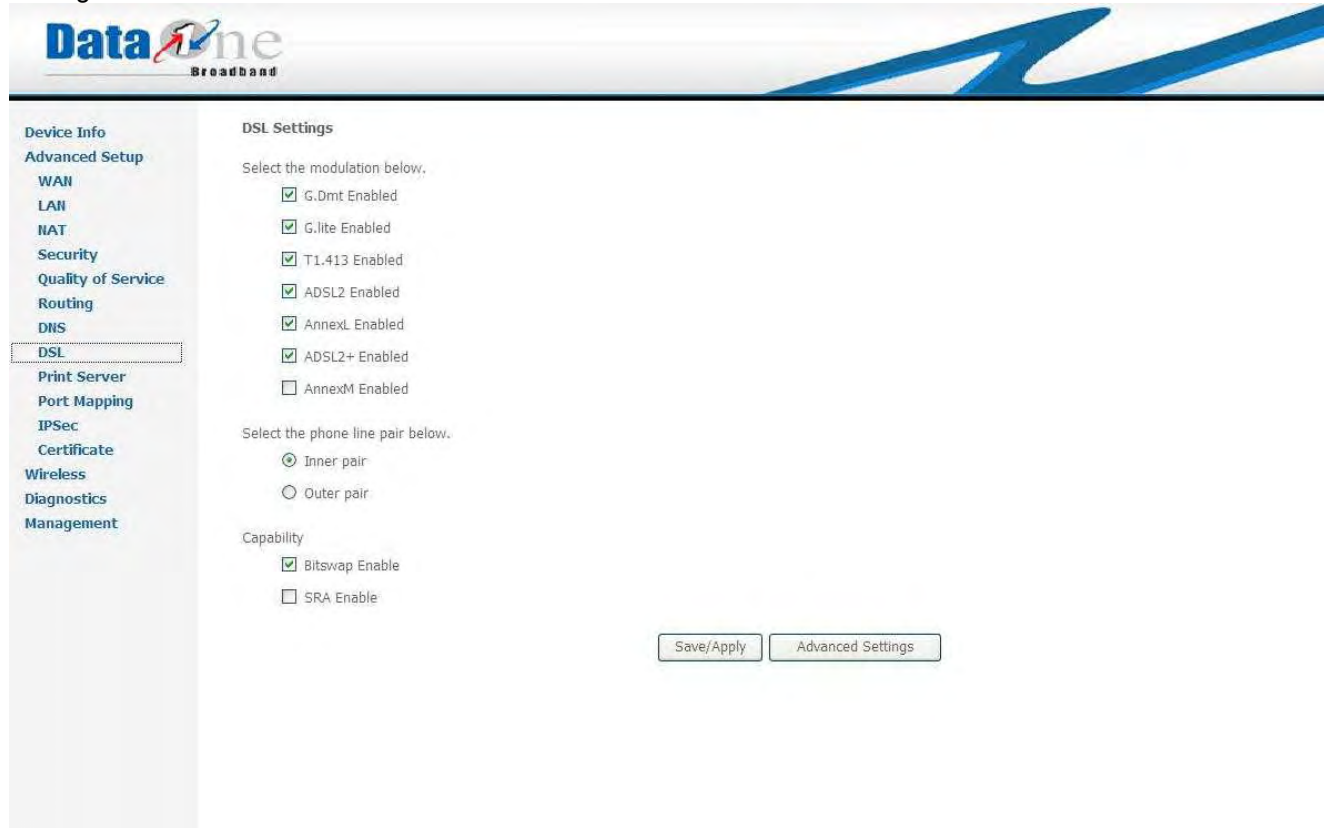


Figure 3.4.8.1 Advanced Setup – DSL Settings

Click "**Advanced Settings**", Figure 3.4.8.2 Advanced Setup – DSL Advanced Settings showing as below

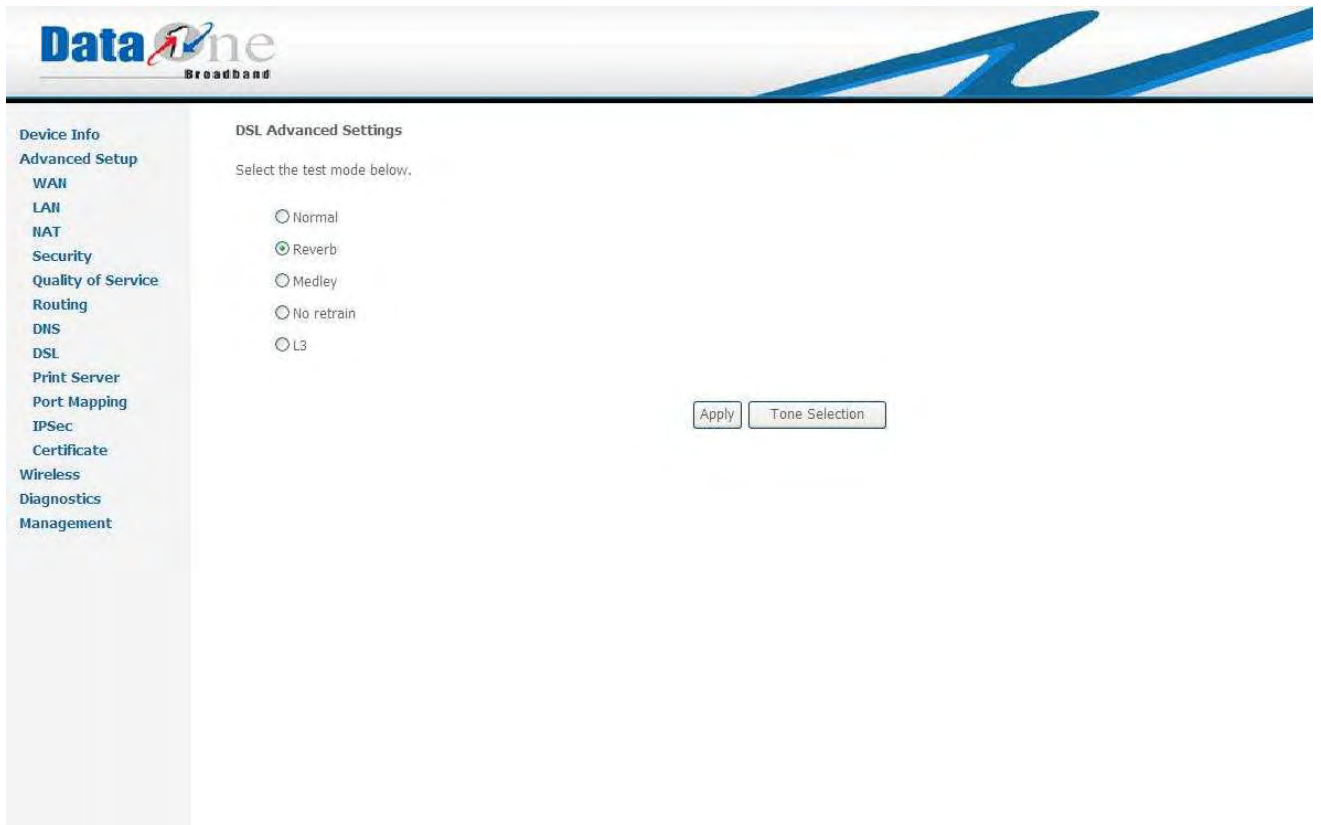


Figure 3.4.8.2 Advanced Setup – DSL Advanced Settings

A capable of test modes including: Normal, Reverb, Medley, No retrain and L3 are available for choice. Click “**Tone Selection**”, Figure 3.4.8.3 Advanced Setup – DSL -- ADSL Tone Settings shows as below: Before any changes of these settings, please make sure you do understand the actual meaning of each setting; otherwise, please leave as it. For detail information, please consult with your ISP provider.

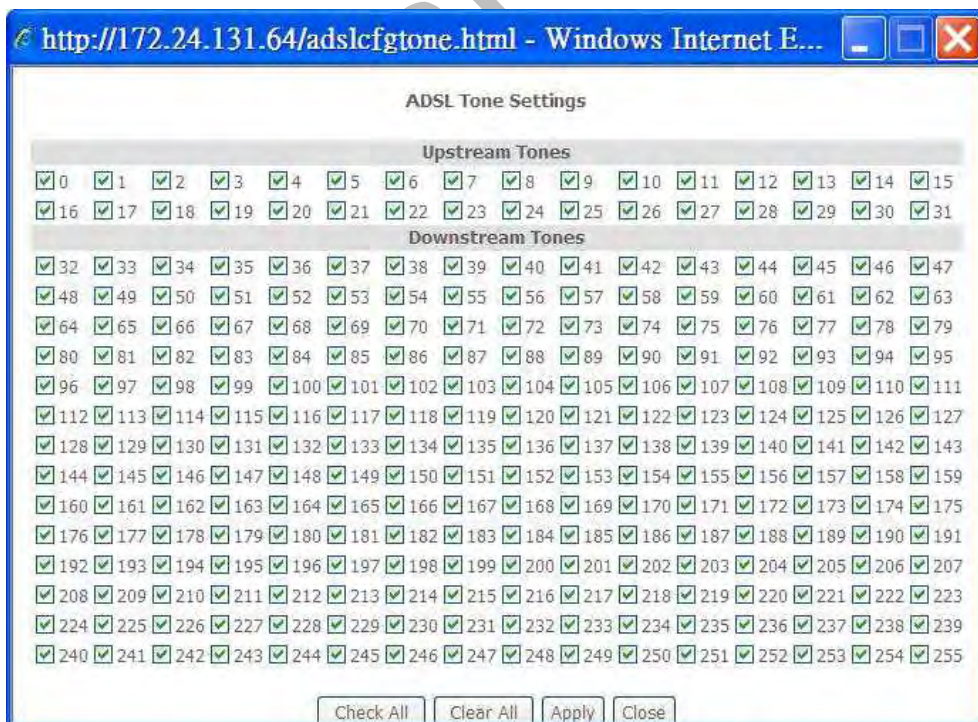


Figure 3.4.8.3 Advanced Setup – DSL -- ADSL Tone Settings

### 3.4.9 Advanced Setup – Print Server

You are able to set up the print server through this page, enable “**Enable on-board print server**” checkbox, and input “**Printer name**” and “**Make and model**”; click “**Save/Apply**” as showing on Figure 3.4.9 Advanced Setup – Print Server.

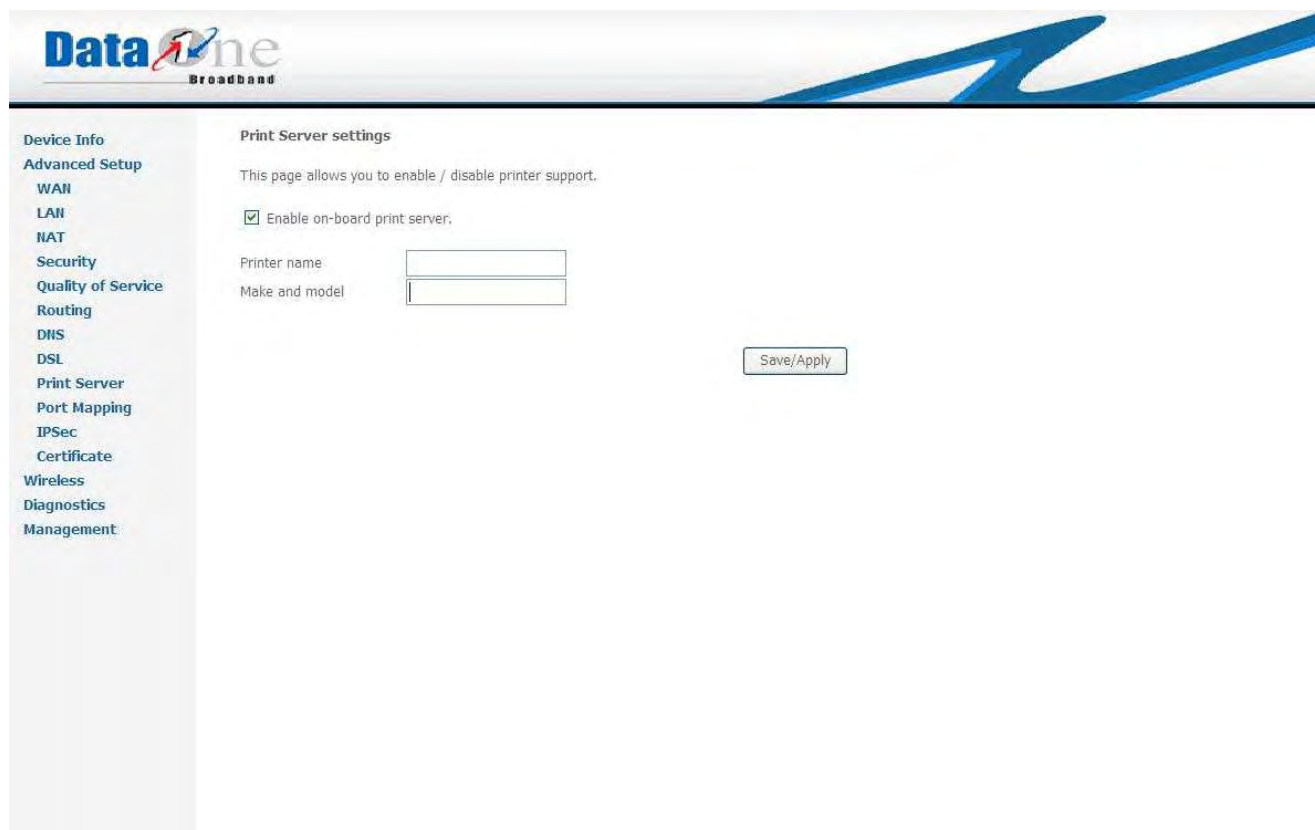


Figure 3.4.9 Advanced Setup – Print Server

### 3.4.10 Advanced Setup – Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove checkbox will remove the grouping and add the ungrouped interfaces back to the Default group. Only the default group has IP interface.

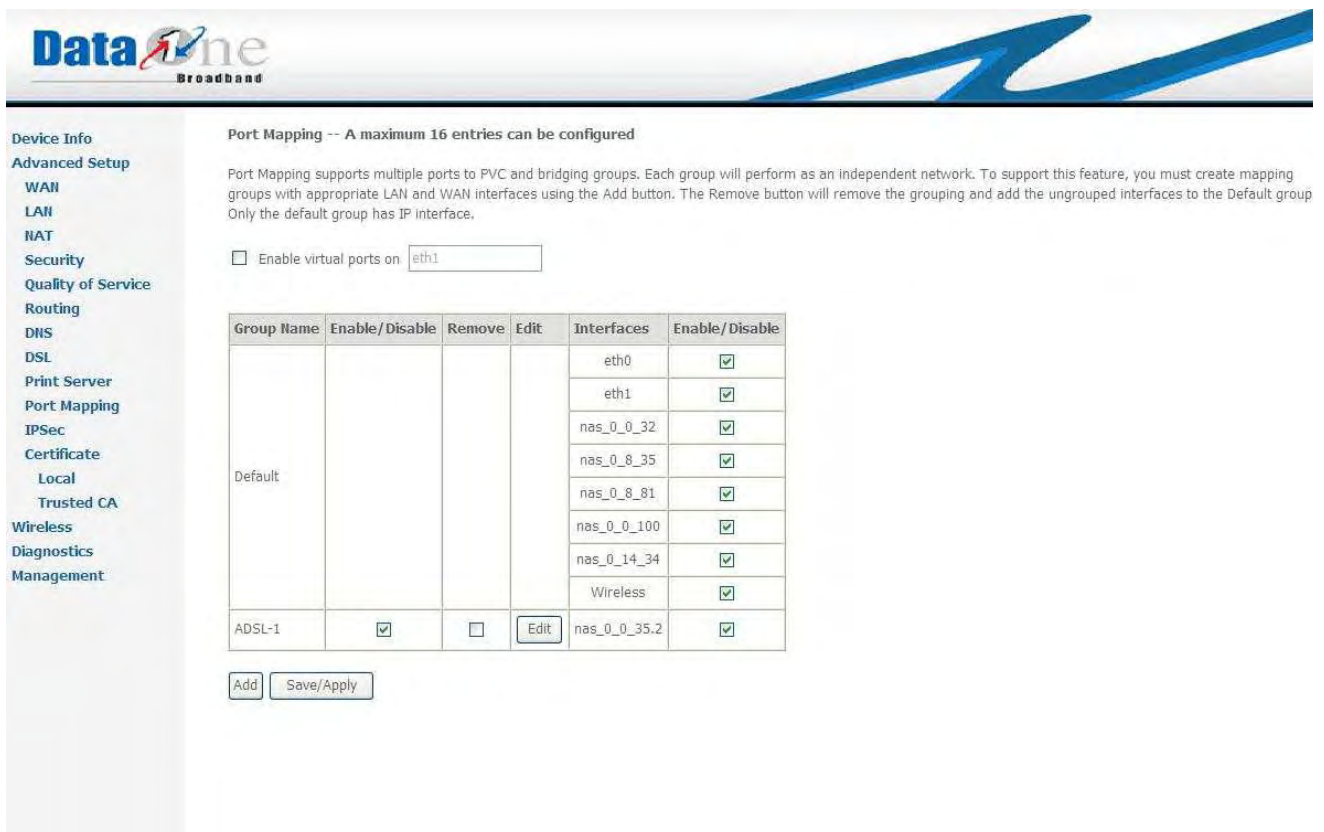


Figure 3.4.10.a Advanced Setup – Port Mapping

### Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately

Note that the selected interfaces will be removed from their existing groups and added to the new group.

**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address. Figure 3.4.10.b Advanced Setup – Port Mapping Configuration.



**DataOne Broadband**

**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
 Security  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPsec  
 Certificate  
 Local  
 Trusted CA  
 Wireless  
 Diagnostics  
 Management

**Port Mapping Configuration**

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.  
**Note that these clients may obtain public IP addresses**
3. Click Save/Apply button to make the changes effective immediately

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

**IMPORTANT** If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces:

Available Interfaces:

```
eth0
eth1
vnet_0_0_100
vnet_0_0_101
vnet_0_0_102
vnet_0_0_103
vnet_0_0_104
vnet_0_0_105
vnet_0_0_106
vnet_0_0_107
vnet_0_0_108
vnet_0_0_109
vnet_0_0_110
vnet_0_0_111
vnet_0_0_112
vnet_0_0_113
vnet_0_0_114
vnet_0_0_115
vnet_0_0_116
vnet_0_0_117
vnet_0_0_118
vnet_0_0_119
vnet_0_0_120
vnet_0_0_121
vnet_0_0_122
vnet_0_0_123
vnet_0_0_124
vnet_0_0_125
vnet_0_0_126
vnet_0_0_127
vnet_0_0_128
vnet_0_0_129
vnet_0_0_130
vnet_0_0_131
vnet_0_0_132
vnet_0_0_133
vnet_0_0_134
vnet_0_0_135
vnet_0_0_136
vnet_0_0_137
vnet_0_0_138
vnet_0_0_139
vnet_0_0_140
vnet_0_0_141
vnet_0_0_142
vnet_0_0_143
vnet_0_0_144
vnet_0_0_145
vnet_0_0_146
vnet_0_0_147
vnet_0_0_148
vnet_0_0_149
vnet_0_0_150
vnet_0_0_151
vnet_0_0_152
vnet_0_0_153
vnet_0_0_154
vnet_0_0_155
vnet_0_0_156
vnet_0_0_157
vnet_0_0_158
vnet_0_0_159
vnet_0_0_160
vnet_0_0_161
vnet_0_0_162
vnet_0_0_163
vnet_0_0_164
vnet_0_0_165
vnet_0_0_166
vnet_0_0_167
vnet_0_0_168
vnet_0_0_169
vnet_0_0_170
vnet_0_0_171
vnet_0_0_172
vnet_0_0_173
vnet_0_0_174
vnet_0_0_175
vnet_0_0_176
vnet_0_0_177
vnet_0_0_178
vnet_0_0_179
vnet_0_0_180
vnet_0_0_181
vnet_0_0_182
vnet_0_0_183
vnet_0_0_184
vnet_0_0_185
vnet_0_0_186
vnet_0_0_187
vnet_0_0_188
vnet_0_0_189
vnet_0_0_190
vnet_0_0_191
vnet_0_0_192
vnet_0_0_193
vnet_0_0_194
vnet_0_0_195
vnet_0_0_196
vnet_0_0_197
vnet_0_0_198
vnet_0_0_199
vnet_0_0_200
vnet_0_0_201
vnet_0_0_202
vnet_0_0_203
vnet_0_0_204
vnet_0_0_205
vnet_0_0_206
vnet_0_0_207
vnet_0_0_208
vnet_0_0_209
vnet_0_0_210
vnet_0_0_211
vnet_0_0_212
vnet_0_0_213
vnet_0_0_214
vnet_0_0_215
vnet_0_0_216
vnet_0_0_217
vnet_0_0_218
vnet_0_0_219
vnet_0_0_220
vnet_0_0_221
vnet_0_0_222
vnet_0_0_223
vnet_0_0_224
vnet_0_0_225
vnet_0_0_226
vnet_0_0_227
vnet_0_0_228
vnet_0_0_229
vnet_0_0_230
vnet_0_0_231
vnet_0_0_232
vnet_0_0_233
vnet_0_0_234
vnet_0_0_235
vnet_0_0_236
vnet_0_0_237
vnet_0_0_238
vnet_0_0_239
vnet_0_0_240
vnet_0_0_241
vnet_0_0_242
vnet_0_0_243
vnet_0_0_244
vnet_0_0_245
vnet_0_0_246
vnet_0_0_247
vnet_0_0_248
vnet_0_0_249
vnet_0_0_250
vnet_0_0_251
vnet_0_0_252
vnet_0_0_253
vnet_0_0_254
vnet_0_0_255
vnet_0_0_256
vnet_0_0_257
vnet_0_0_258
vnet_0_0_259
vnet_0_0_260
vnet_0_0_261
vnet_0_0_262
vnet_0_0_263
vnet_0_0_264
vnet_0_0_265
vnet_0_0_266
vnet_0_0_267
vnet_0_0_268
vnet_0_0_269
vnet_0_0_270
vnet_0_0_271
vnet_0_0_272
vnet_0_0_273
vnet_0_0_274
vnet_0_0_275
vnet_0_0_276
vnet_0_0_277
vnet_0_0_278
vnet_0_0_279
vnet_0_0_280
vnet_0_0_281
vnet_0_0_282
vnet_0_0_283
vnet_0_0_284
vnet_0_0_285
vnet_0_0_286
vnet_0_0_287
vnet_0_0_288
vnet_0_0_289
vnet_0_0_290
vnet_0_0_291
vnet_0_0_292
vnet_0_0_293
vnet_0_0_294
vnet_0_0_295
vnet_0_0_296
vnet_0_0_297
vnet_0_0_298
vnet_0_0_299
vnet_0_0_300
vnet_0_0_301
vnet_0_0_302
vnet_0_0_303
vnet_0_0_304
vnet_0_0_305
vnet_0_0_306
vnet_0_0_307
vnet_0_0_308
vnet_0_0_309
vnet_0_0_310
vnet_0_0_311
vnet_0_0_312
vnet_0_0_313
vnet_0_0_314
vnet_0_0_315
vnet_0_0_316
vnet_0_0_317
vnet_0_0_318
vnet_0_0_319
vnet_0_0_320
vnet_0_0_321
vnet_0_0_322
vnet_0_0_323
vnet_0_0_324
vnet_0_0_325
vnet_0_0_326
vnet_0_0_327
vnet_0_0_328
vnet_0_0_329
vnet_0_0_330
vnet_0_0_331
vnet_0_0_332
vnet_0_0_333
vnet_0_0_334
vnet_0_0_335
vnet_0_0_336
vnet_0_0_337
vnet_0_0_338
vnet_0_0_339
vnet_0_0_340
vnet_0_0_341
vnet_0_0_342
vnet_0_0_343
vnet_0_0_344
vnet_0_0_345
vnet_0_0_346
vnet_0_0_347
vnet_0_0_348
vnet_0_0_349
vnet_0_0_350
vnet_0_0_351
vnet_0_0_352
vnet_0_0_353
vnet_0_0_354
vnet_0_0_355
vnet_0_0_356
vnet_0_0_357
vnet_0_0_358
vnet_0_0_359
vnet_0_0_360
vnet_0_0_361
vnet_0_0_362
vnet_0_0_363
vnet_0_0_364
vnet_0_0_365
vnet_0_0_366
vnet_0_0_367
vnet_0_0_368
vnet_0_0_369
vnet_0_0_370
vnet_0_0_371
vnet_0_0_372
vnet_0_0_373
vnet_0_0_374
vnet_0_0_375
vnet_0_0_376
vnet_0_0_377
vnet_0_0_378
vnet_0_0_379
vnet_0_0_380
vnet_0_0_381
vnet_0_0_382
vnet_0_0_383
vnet_0_0_384
vnet_0_0_385
vnet_0_0_386
vnet_0_0_387
vnet_0_0_388
vnet_0_0_389
vnet_0_0_390
vnet_0_0_391
vnet_0_0_392
vnet_0_0_393
vnet_0_0_394
vnet_0_0_395
vnet_0_0_396
vnet_0_0_397
vnet_0_0_398
vnet_0_0_399
vnet_0_0_400
vnet_0_0_401
vnet_0_0_402
vnet_0_0_403
vnet_0_0_404
vnet_0_0_405
vnet_0_0_406
vnet_0_0_407
vnet_0_0_408
vnet_0_0_409
vnet_0_0_410
vnet_0_0_411
vnet_0_0_412
vnet_0_0_413
vnet_0_0_414
vnet_0_0_415
vnet_0_0_416
vnet_0_0_417
vnet_0_0_418
vnet_0_0_419
vnet_0_0_420
vnet_0_0_421
vnet_0_0_422
vnet_0_0_423
vnet_0_0_424
vnet_0_0_425
vnet_0_0_426
vnet_0_0_427
vnet_0_0_428
vnet_0_0_429
vnet_0_0_430
vnet_0_0_431
vnet_0_0_432
vnet_0_0_433
vnet_0_0_434
vnet_0_0_435
vnet_0_0_436
vnet_0_0_437
vnet_0_0_438
vnet_0_0_439
vnet_0_0_440
vnet_0_0_441
vnet_0_0_442
vnet_0_0_443
vnet_0_0_444
vnet_0_0_445
vnet_0_0_446
vnet_0_0_447
vnet_0_0_448
vnet_0_0_449
vnet_0_0_450
vnet_0_0_451
vnet_0_0_452
vnet_0_0_453
vnet_0_0_454
vnet_0_0_455
vnet_0_0_456
vnet_0_0_457
vnet_0_0_458
vnet_0_0_459
vnet_0_0_460
vnet_0_0_461
vnet_0_0_462
vnet_0_0_463
vnet_0_0_464
vnet_0_0_465
vnet_0_0_466
vnet_0_0_467
vnet_0_0_468
vnet_0_0_469
vnet_0_0_470
vnet_0_0_471
vnet_0_0_472
vnet_0_0_473
vnet_0_0_474
vnet_0_0_475
vnet_0_0_476
vnet_0_0_477
vnet_0_0_478
vnet_0_0_479
vnet_0_0_480
vnet_0_0_481
vnet_0_0_482
vnet_0_0_483
vnet_0_0_484
vnet_0_0_485
vnet_0_0_486
vnet_0_0_487
vnet_0_0_488
vnet_0_0_489
vnet_0_0_490
vnet_0_0_491
vnet_0_0_492
vnet_0_0_493
vnet_0_0_494
vnet_0_0_495
vnet_0_0_496
vnet_0_0_497
vnet_0_0_498
vnet_0_0_499
vnet_0_0_500
vnet_0_0_501
vnet_0_0_502
vnet_0_0_503
vnet_0_0_504
vnet_0_0_505
vnet_0_0_506
vnet_0_0_507
vnet_0_0_508
vnet_0_0_509
vnet_0_0_510
vnet_0_0_511
vnet_0_0_512
vnet_0_0_513
vnet_0_0_514
vnet_0_0_515
vnet_0_0_516
vnet_0_0_517
vnet_0_0_518
vnet_0_0_519
vnet_0_0_520
vnet_0_0_521
vnet_0_0_522
vnet_0_0_523
vnet_0_0_524
vnet_0_0_525
vnet_0_0_526
vnet_0_0_527
vnet_0_0_528
vnet_0_0_529
vnet_0_0_530
vnet_0_0_531
vnet_0_0_532
vnet_0_0_533
vnet_0_0_534
vnet_0_0_535
vnet_0_0_536
vnet_0_0_537
vnet_0_0_538
vnet_0_0_539
vnet_0_0_540
vnet_0_0_541
vnet_0_0_542
vnet_0_0_543
vnet_0_0_544
vnet_0_0_545
vnet_0_0_546
vnet_0_0_547
vnet_0_0_548
vnet_0_0_549
vnet_0_0_550
vnet_0_0_551
vnet_0_0_552
vnet_0_0_553
vnet_0_0_554
vnet_0_0_555
vnet_0_0_556
vnet_0_0_557
vnet_0_0_558
vnet_0_0_559
vnet_0_0_560
vnet_0_0_561
vnet_0_0_562
vnet_0_0_563
vnet_0_0_564
vnet_0_0_565
vnet_0_0_566
vnet_0_0_567
vnet_0_0_568
vnet_0_0_569
vnet_0_0_570
vnet_0_0_571
vnet_0_0_572
vnet_0_0_573
vnet_0_0_574
vnet_0_0_575
vnet_0_0_576
vnet_0_0_577
vnet_0_0_578
vnet_0_0_579
vnet_0_0_580
vnet_0_0_581
vnet_0_0_582
vnet_0_0_583
vnet_0_0_584
vnet_0_0_585
vnet_0_0_586
vnet_0_0_587
vnet_0_0_588
vnet_0_0_589
vnet_0_0_590
vnet_0_0_591
vnet_0_0_592
vnet_0_0_593
vnet_0_0_594
vnet_0_0_595
vnet_0_0_596
vnet_0_0_597
vnet_0_0_598
vnet_0_0_599
vnet_0_0_600
vnet_0_0_601
vnet_0_0_602
vnet_0_0_603
vnet_0_0_604
vnet_0_0_605
vnet_0_0_606
vnet_0_0_607
vnet_0_0_608
vnet_0_0_609
vnet_0_0_610
vnet_0_0_611
vnet_0_0_612
vnet_0_0_613
vnet_0_0_614
vnet_0_0_615
vnet_0_0_616
vnet_0_0_617
vnet_0_0_618
vnet_0_0_619
vnet_0_0_620
vnet_0_0_621
vnet_0_0_622
vnet_0_0_623
vnet_0_0_624
vnet_0_0_625
vnet_0_0_626
vnet_0_0_627
vnet_0_0_628
vnet_0_0_629
vnet_0_0_630
vnet_0_0_631
vnet_0_0_632
vnet_0_0_633
vnet_0_0_634
vnet_0_0_635
vnet_0_0_636
vnet_0_0_637
vnet_0_0_638
vnet_0_0_639
vnet_0_0_640
vnet_0_0_641
vnet_0_0_642
vnet_0_0_643
vnet_0_0_644
vnet_0_0_645
vnet_0_0_646
vnet_0_0_647
vnet_0_0_648
vnet_0_0_649
vnet_0_0_650
vnet_0_0_651
vnet_0_0_652
vnet_0_0_653
vnet_0_0_654
vnet_0_0_655
vnet_0_0_656
vnet_0_0_657
vnet_0_0_658
vnet_0_0_659
vnet_0_0_660
vnet_0_0_661
vnet_0_0_662
vnet_0_0_663
vnet_0_0_664
vnet_0_0_665
vnet_0_0_666
vnet_0_0_667
vnet_0_0_668
vnet_0_0_669
vnet_0_0_670
vnet_0_0_671
vnet_0_0_672
vnet_0_0_673
vnet_0_0_674
vnet_0_0_675
vnet_0_0_676
vnet_0_0_677
vnet_0_0_678
vnet_0_0_679
vnet_0_0_680
vnet_0_0_681
vnet_0_0_682
vnet_0_0_683
vnet_0_0_684
vnet_0_0_685
vnet_0_0_686
vnet_0_0_687
vnet_0_0_688
vnet_0_0_689
vnet_0_0_690
vnet_0_0_691
vnet_0_0_692
vnet_0_0_693
vnet_0_0_694
vnet_0_0_695
vnet_0_0_696
vnet_0_0_697
vnet_0_0_698
vnet_0_0_699
vnet_0_0_700
vnet_0_0_701
vnet_0_0_702
vnet_0_0_703
vnet_0_0_704
vnet_0_0_705
vnet_0_0_706
vnet_0_0_707
vnet_0_0_708
vnet_0_0_709
vnet_0_0_710
vnet_0_0_711
vnet_0_0_712
vnet_0_0_713
vnet_0_0_714
vnet_0_0_715
vnet_0_0_716
vnet_0_0_717
vnet_0_0_718
vnet_0_0_719
vnet_0_0_720
vnet_0_0_721
vnet_0_0_722
vnet_0_0_723
vnet_0_0_724
vnet_0_0_725
vnet_0_0_726
vnet_0_0_727
vnet_0_0_728
vnet_0_0_729
vnet_0_0_730
vnet_0_0_731
vnet_0_0_732
vnet_0_0_733
vnet_0_0_734
vnet_0_0_735
vnet_0_0_736
vnet_0_0_737
vnet_0_0_738
vnet_0_0_739
vnet_0_0_740
vnet_0_0_741
vnet_0_0_742
vnet_0_0_743
vnet_0_0_744
vnet_0_0_745
vnet_0_0_746
vnet_0_0_747
vnet_0_0_748
vnet_0_0_749
vnet_0_0_750
vnet_0_0_751
vnet_0_0_752
vnet_0_0_753
vnet_0_0_754
vnet_0_0_755
vnet_0_0_756
vnet_0_0_757
vnet_0_0_758
vnet_0_0_759
vnet_0_0_760
vnet_0_0_761
vnet_0_0_762
vnet_0_0_763
vnet_0_0_764
vnet_0_0_765
vnet_0_0_766
vnet_0_0_767
vnet_0_0_768
vnet_0_0_769
vnet_0_0_770
vnet_0_0_771
vnet_0_0_772
vnet_0_0_773
vnet_0_0_774
vnet_0_0_775
vnet_0_0_776
vnet_0_0_777
vnet_0_0_778
vnet_0_0_779
vnet_0_0_780
vnet_0_0_781
vnet_0_0_782
vnet_0_0_783
vnet_0_0_784
vnet_0_0_785
vnet_0_0_786
vnet_0_0_787
vnet_0_0_788
vnet_0_0_789
vnet_0_0_790
vnet_0_0_791
vnet_0_0_792
vnet_0_0_793
vnet_0_0_794
vnet_0_0_795
vnet_0_0_796
vnet_0_0_797
vnet_0_0_798
vnet_0_0_799
vnet_0_0_800
vnet_0_0_801
vnet_0_0_802
vnet_0_0_803
vnet_0_0_804
vnet_0_0_805
vnet_0_0_806
vnet_0_0_807
vnet_0_0_808
vnet_0_0_809
vnet_0_0_810
vnet_0_0_811
vnet_0_0_812
vnet_0_0_813
vnet_0_0_814
vnet_0_0_815
vnet_0_0_816
vnet_0_0_817
vnet_0_0_818
vnet_0_0_819
vnet_0_0_820
vnet_0_0_821
vnet_0_0_822
vnet_0_0_823
vnet_0_0_824
vnet_0_0_825
vnet_0_0_826
vnet_0_0_827
vnet_0_0_828
vnet_0_0_829
vnet_0_0_830
vnet_0_0_831
vnet_0_0_832
vnet_0_0_833
vnet_0_0_834
vnet_0_0_835
vnet_0_0_836
vnet_0_0_837
vnet_0_0_838
vnet_0_0_839
vnet_0_0_840
vnet_0_0_841
vnet_0_0_842
vnet_0_0_843
vnet_0_0_844
vnet_0_0_845
vnet_0_0_846
vnet_0_0_847
vnet_0_0_848
vnet_0_0_849
vnet_0_0_850
vnet_0_0_851
vnet_0_0_852
vnet_0_0_853
vnet_0_0_854
vnet_0_0_855
vnet_0_0_856
vnet_0_0_857
vnet_0_0_858
vnet_0_0_859
vnet_0_0_860
vnet_0_0_861
vnet_0_0_862
vnet_0_0_863
vnet_0_0_864
vnet_0_0_865
vnet_0_0_866
vnet_0_0_867
vnet_0_0_868
vnet_0_0_869
vnet_0_0_870
vnet_0_0_871
vnet_0_0_872
vnet_0_0_873
vnet_0_0_874
vnet_0_0_875
vnet_0_0_876
vnet_0_0_877
vnet_0_0_878
vnet_0_0_879
vnet_0_0_880
vnet_0_0_881
vnet_0_0_882
vnet_0_0_883
vnet_0_0_884
vnet_0_0_885
vnet_0_0_886
vnet_0_0_887
vnet_0_0_888
vnet_0_0_889
vnet_0_0_890
vnet_0_0_891
vnet_0_0_892
vnet_0_0_893
vnet_0_0_894
vnet_0_0_895
vnet_0_0_896
vnet_0_0_897
vnet_0_0_898
vnet_0_0_899
vnet_0_0_900
vnet_0_0_901
vnet_0_0_902
vnet_0_0_903
vnet_0_0_904
vnet_0_0_905
vnet_0_0_906
vnet_0_0_907
vnet_0_0_908
vnet_0_0_909
vnet_0_0_910
vnet_0_0_911
vnet_0_0_912
vnet_0_0_913
vnet_0_0_914
vnet_0_0_915
vnet_0_0_916
vnet_0_0_917
vnet_0_0_918
vnet_0_0_919
vnet_0_0_920
vnet_0_0_921
vnet_0_0_922
vnet_0_0_923
vnet_0_0_924
vnet_0_0_925
vnet_0_0_926
vnet_0_0_927
vnet_0_0_928
vnet_0_0_929
vnet_0_0_930
vnet_0_0_931
vnet_0_0_932
vnet_0_0_933
vnet_0_0_934
vnet_0_0_935
vnet_0_0_936
vnet_0_0_937
vnet_0_0_938
vnet_0_0_939
vnet_0_0_940
vnet_0_0_941
vnet_0_0_942
vnet_0_0_943
vnet_0_0_944
vnet_0_0_945
vnet_0_0_946
vnet_0_0_947
vnet_0_0_948
vnet_0_0_949
vnet_0_0_950
vnet_0_0_951
vnet_0_0_952
vnet_0_0_953
vnet_0_0_954
vnet_0_0_955
vnet_0_0_956
vnet_0_0_957
vnet_0_0_958
vnet_0_0_959
vnet_0_0_960
vnet_0_0_961
vnet_0_0_962
vnet_0_0_963
vnet_0_0_964
vnet_0_0_965
vnet_0_0_966
vnet_0_0_967
vnet_0_0_968
vnet_0_0_969
vnet_0_0_970
vnet_0_0_971
vnet_0_0_972
vnet_0_0_973
vnet_0_0_974
vnet_0_0_975
vnet_0_0_976
vnet_0_0_977
vnet_0_0_978
vnet_0_0_979
vnet_0_0_980
vnet_0_0_981
vnet_0_0_982
vnet_0_0_983
vnet_0_0_984
vnet_0_0_985
vnet_0_0_986
vnet_0_0_987
vnet_0_0_988
vnet_0_0_989
vnet_0_0_990
vnet_0_0_991
vnet_0_0_992
vnet_0_0_993
vnet_0_0_994
vnet_0_0_995
vnet_0_0_996
vnet_0_0_997
vnet_0_0_998
vnet_0_0_999
vnet_0_0_1000
```

Automatically Add Clients With the following DHCP Vendor IDs:

Figure 3.4.10.b Advanced Setup – Port Mapping Configuration.

3.4.11 Advanced Setup – IPsec

You are able to set up IPsec Tunnel through this page, fill up appropriate input and click “**Save/Apply**”

**DataOne Broadband**

**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
 Security  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPsec  
 Certificate  
 Local  
 Trusted CA  
 Wireless  
 Diagnostics  
 Management

**IPsec Settings**

IPsec Connection Name:

Remote IPsec Gateway Address:

Tunnel access from local IP addresses:

IP Address for VPN:

IP Subnetmask:

Tunnel access from remote IP addresses:

IP Address for VPN:

IP Subnetmask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Hide Advanced Settings:

Advanced IKE Settings:

Phase 1:

Mode:

Encryption Algorithm:

Integrity Algorithm:

Select Diffie-Hellman Group for Key Exchange:

Key Life Time:  Seconds

Phase 2:

Encryption Algorithm:

Integrity Algorithm:

Select Diffie-Hellman Group for Key Exchange:

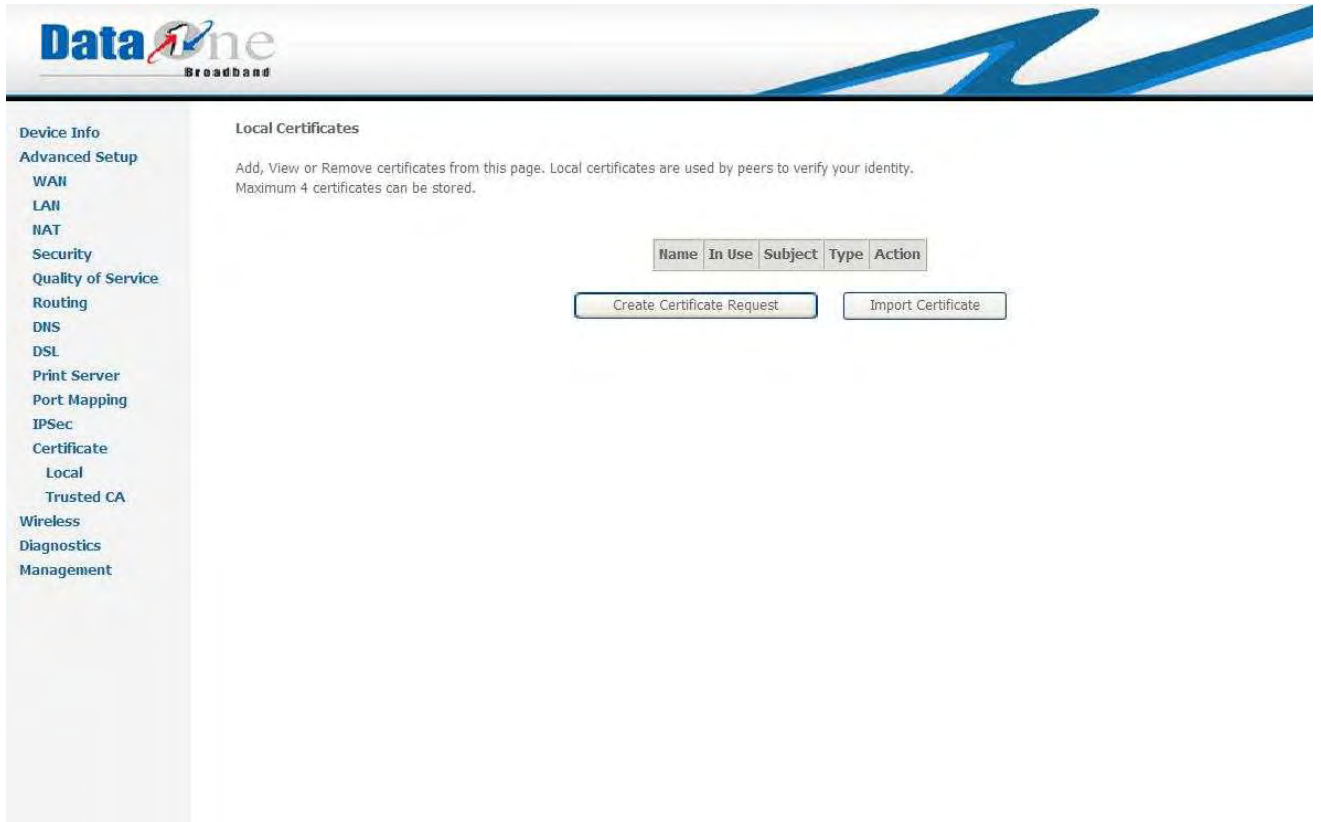
Key Life Time:  Seconds

Figure 3.4.11 Advanced Setup – IPsec

### 3.4.12 Advanced Setup – Certificate


#### 3.4.12.1 Advanced Setup – Certificate – Local Certificates

Add, View or Remove certificates through this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.



.Figure 3.4.12.1.a Advanced Setup – Certificate – Local Certificates

Click "**Create Certificate Request**" button on Figure 3.4.12.1.a Advanced Setup – Certificate – Local Certificates and Figure 3.4.12.1.b Advanced Setup – Certificate – Local Certificates shows up as below.



**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
 Security  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPsec  
 Certificate  
 Local  
 Trusted CA  
 Wireless  
 Diagnostics  
 Management


### Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:   
 Common Name:   
 Organization Name:   
 State/Province Name:   
 Country/Region Name:

#### 3.4.12.1.b Advanced Setup – Certificate – Create new certificate request

Enter appropriate data and click **“Apply”** button, Figure 3.4.12.1.c Advanced Setup – Certificate – Local Certificates – Certificate signing request shows up as following:



**Device Info**  
**Advanced Setup**  
 WAN  
 LAN  
 NAT  
 Security  
 Quality of Service  
 Routing  
 DNS  
 DSL  
 Print Server  
 Port Mapping  
 IPsec  
 Certificate  
 Local  
 Trusted CA  
 Wireless  
 Diagnostics  
 Management

### Certificate signing request

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	USA
Type	request
Subject	CN=USA/O=USA/ST=USA/C=US
Signing Request	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBdjCB4AIBADA3M0vnmCgYDVQQDEwNVU0ExDDAKBgNVBAoTA1VTQTEEMMAoGA1UE CMNDVWVNEM0swCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEEAAOBjOAwwYkCgYEA 0L5b0XjNPF3w4b0/jCigmIiG18eGdQvpm0ymLduUQzADymk6vpNoSB4ZDKqUITo8 6roRI tvmz8UaBW810c0UMTgR0ExOkzTyzonRr45N61PB3GWkx9pQFLSwBnKWoX1 11u6TKRqRwUQRBSb5B3v1KSERdzD3kqC7ByuWAVDAECAwEAAaAAMA0GCSqGSIb3 DQEBBAUAA4GBAFjyWS1oafcFDMIZGE1Fw4CduhD0yJry1R278iq340BDdPGpeMwJ T8vyyS7kxz0EBCF4aSRocLUhMY9ryOYgBkFRfz6eg9K05QVGBv15CbCndQ8gda41g PnYSx2a+qq tu1S6T1ws6+1vW8ws6m310sYMi7FbSsEV4WLWQRFgD+10j -----END CERTIFICATE REQUEST----- </pre>



Figure 3.4.12.1.c Advanced Setup – Certificate – Local Certificates – Certificate signing request shows

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device

Click “**Import Certificate**” button on Figure 3.4.12.1.a Advanced Setup – Certificate – Local Certificates and Figure 3.4.12.1.d Advanced Setup – Certificate – Local Certificates – Import certificate shows up

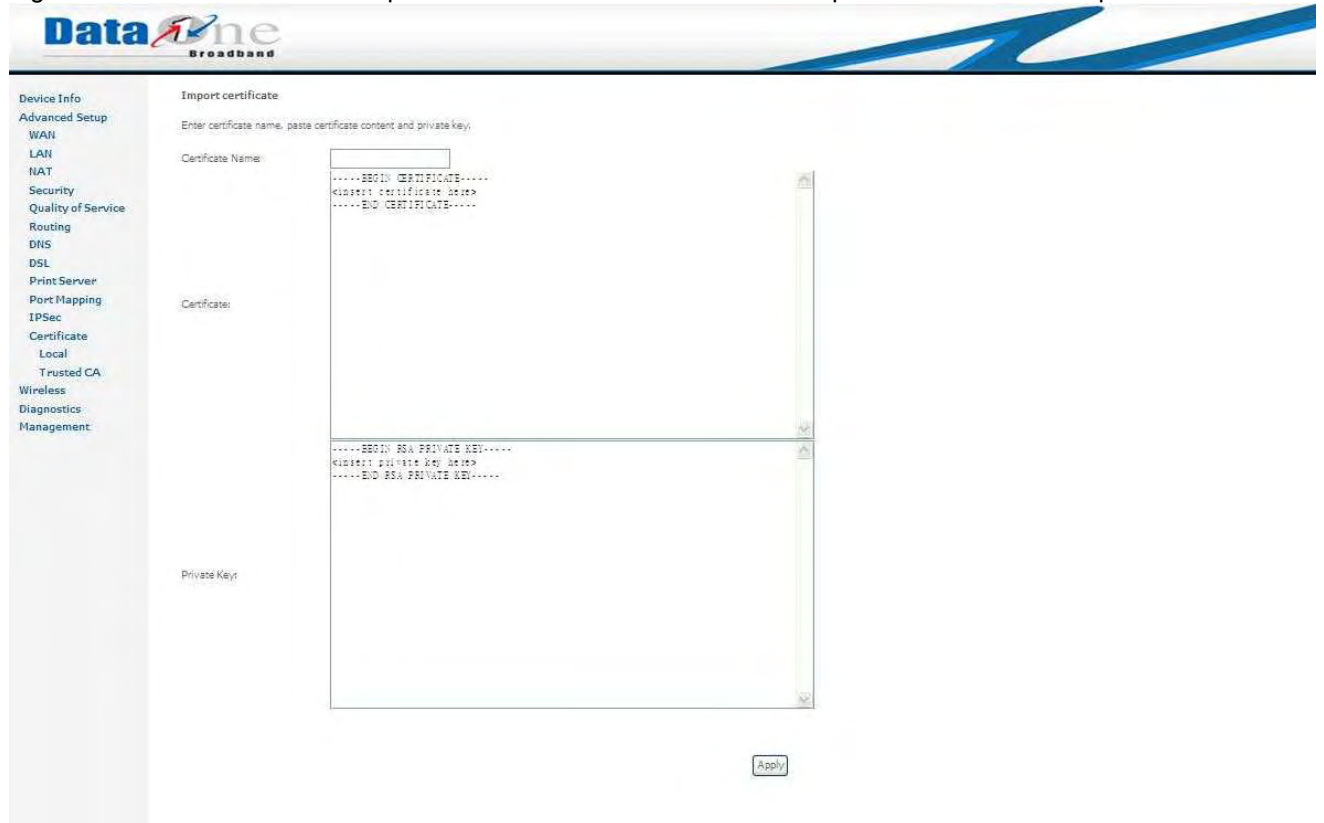


Figure 3.4.12.1.d Advanced Setup – Certificate – Local Certificates – Import certificate

### 3.4.12.2 Advanced Setup – Certificate – Trusted CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

- Device Info
- Advanced Setup
  - WAN
  - LAN
  - NAT
  - Security
  - Quality of Service
  - Routing
  - DNS
  - DSL
  - Print Server
  - Port Mapping
  - IPSec
  - Certificate
    - Local
    - Trusted CA
- Wireless
- Diagnostics
- Management

### Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
------	---------	------	--------

Import Certificate

### 3.4.12.2 .a Advanced Setup – Certificate – Trusted CA

Click "**Import Certificate**" button, 3.4.12.2.b Advanced Setup – Certificate – Trusted CA – Import CA Certificate shows up; click "**Apply**" when finish the input.

- Device Info
- Advanced Setup
  - WAN
  - LAN
  - NAT
  - Security
  - Quality of Service
  - Routing
  - DNS
  - DSL
  - Print Server
  - Port Mapping
  - IPSec
  - Certificate
    - Local
    - Trusted CA
- Wireless
- Diagnostics
- Management

### Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Certificate:

Apply

### 3.5 Wireless

Use the Wireless screen to configure WA3003-G4 for wireless access. Six parts are list as following:

- Basic
- Security
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info

#### 3.5.1 Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

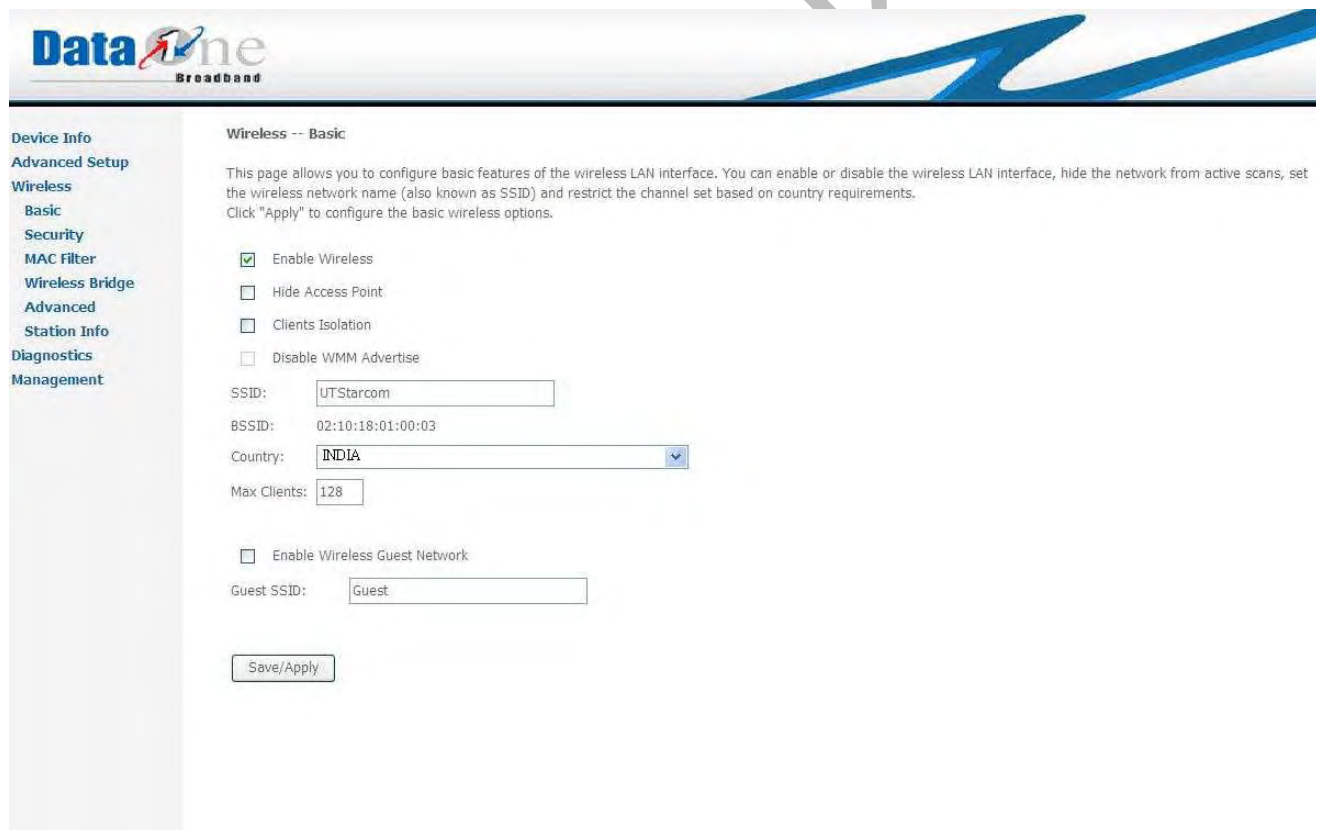


Figure 3.5.1 Wireless -- Basic

#### 3.5.2 Security

This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply" to configure the wireless security option

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply" to configure the wireless security options.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Save/Apply

Figure 3.5.2 Wireless -- Security

3.5.3 MAC Filter

This page allows users to Add/Remove hosts with the specified MAC addresses that are able or unable to access the wireless network. When users decide to use Allow, only the MAC addressed in the user defined list can access the wireless network. When users use Deny, only the user specified MAC addresses are unable to access to wireless network.

Note: The MAC addresses in the list would immediately take effect when Allow or Deny is checked.

- Device Info
- Advanced Setup
- Wireless
  - Basic
  - Security
  - MAC Filter**
  - Wireless Bridge
  - Advanced
  - Station Info
- Diagnostics
- Management

Wireless -- MAC Filter

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address Remove

Add Remove

3.5.4 Wireless Bridge

3.5.5 Advanced

3.5.6 Station Info

3.6 Diagnostics

3.7 Management

Watermark