Platform

Product Name WA3003G4
Release 1.0
Guide Type

Release 1.0

Doc. Code L3 JA01 2500 01 011 00

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/adapter
- 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:

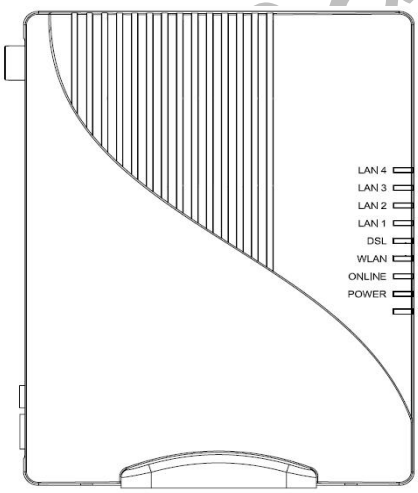


Figure 2.1 WA3003G4 Front Panel.

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

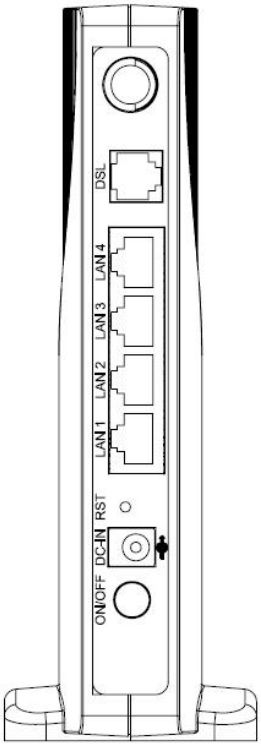


Figure 2.2 WA3003G4 Back Panel.

Label	Function
Antenna	For WiFi functionality.
DSL	RJ-11 connector: Connects the device to a telephone jack or splitter using the supplied cable
LAN1-4	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
RST	Reset the configuration to factory default
DC-IN	Connects to the supplied power converter cable
On/Off	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

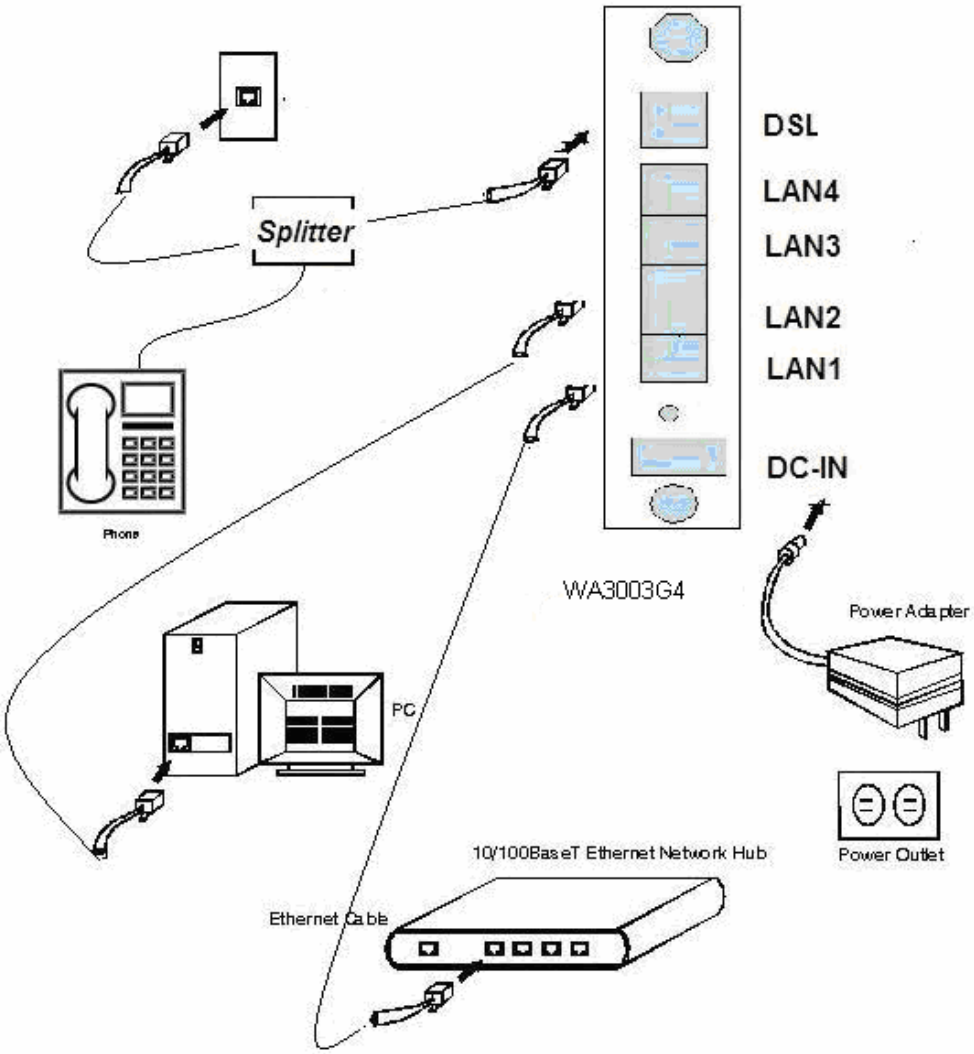


Figure 2.3. Overview of Hardware Connections

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)

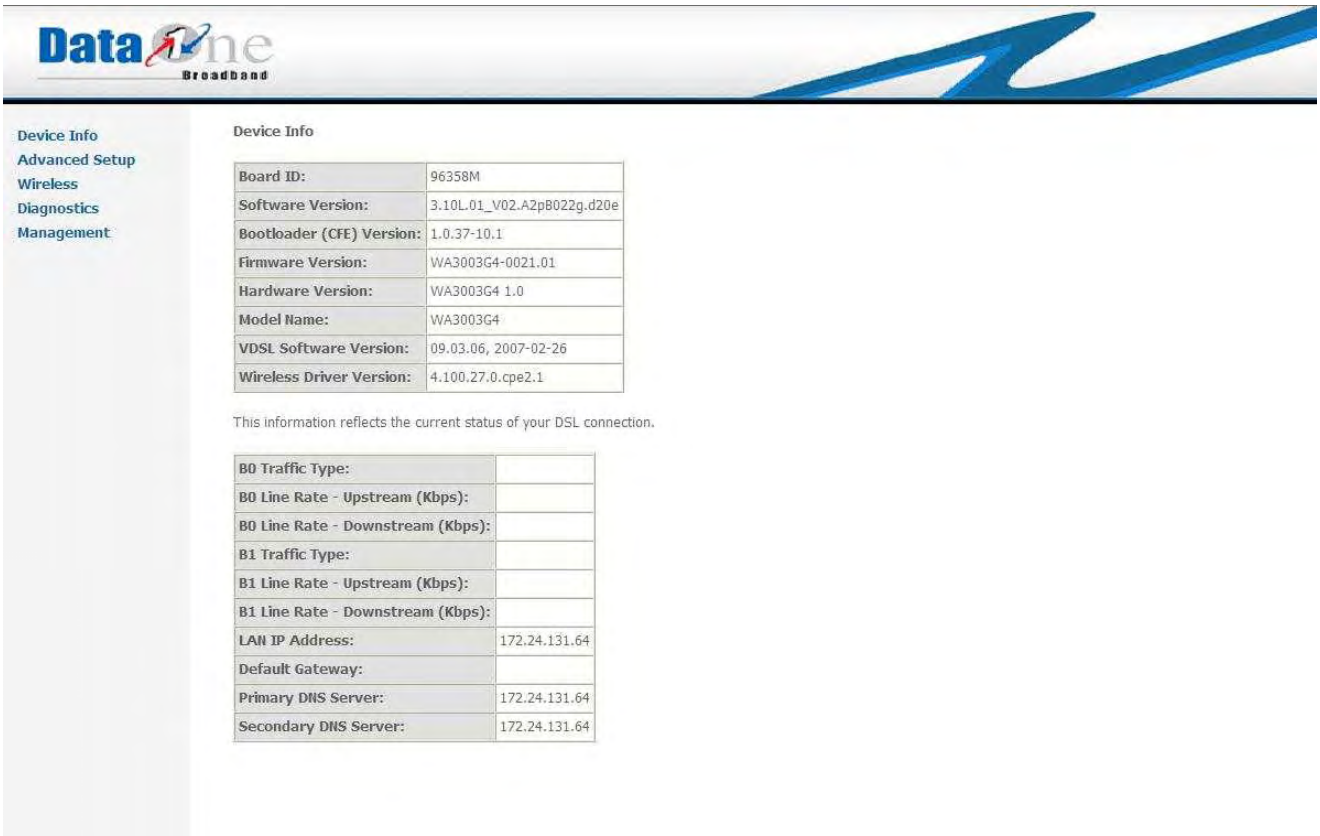


Figure 3.2.2. WA3003G4 Device Info

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.

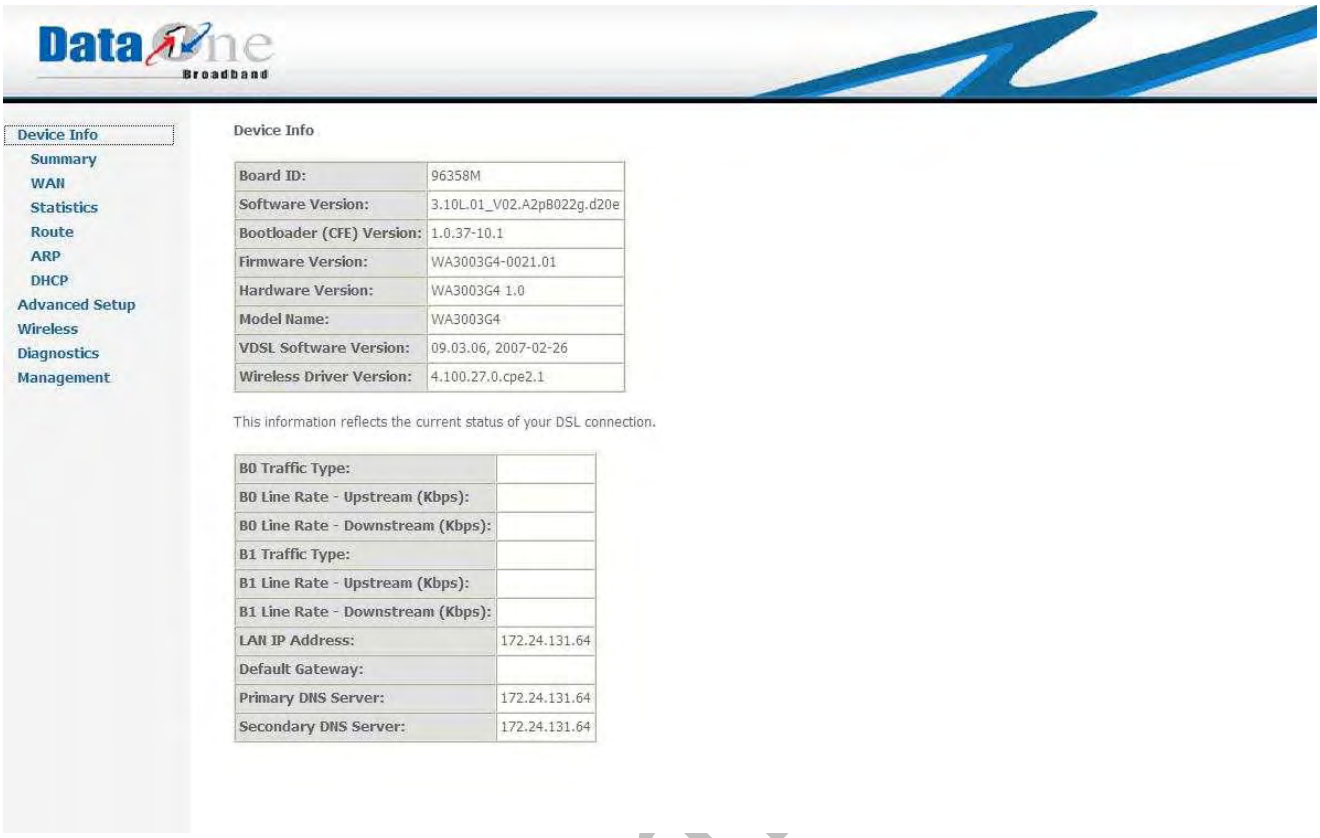


Figure 3.3.1. WA3003G4 Device Info – Summary

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

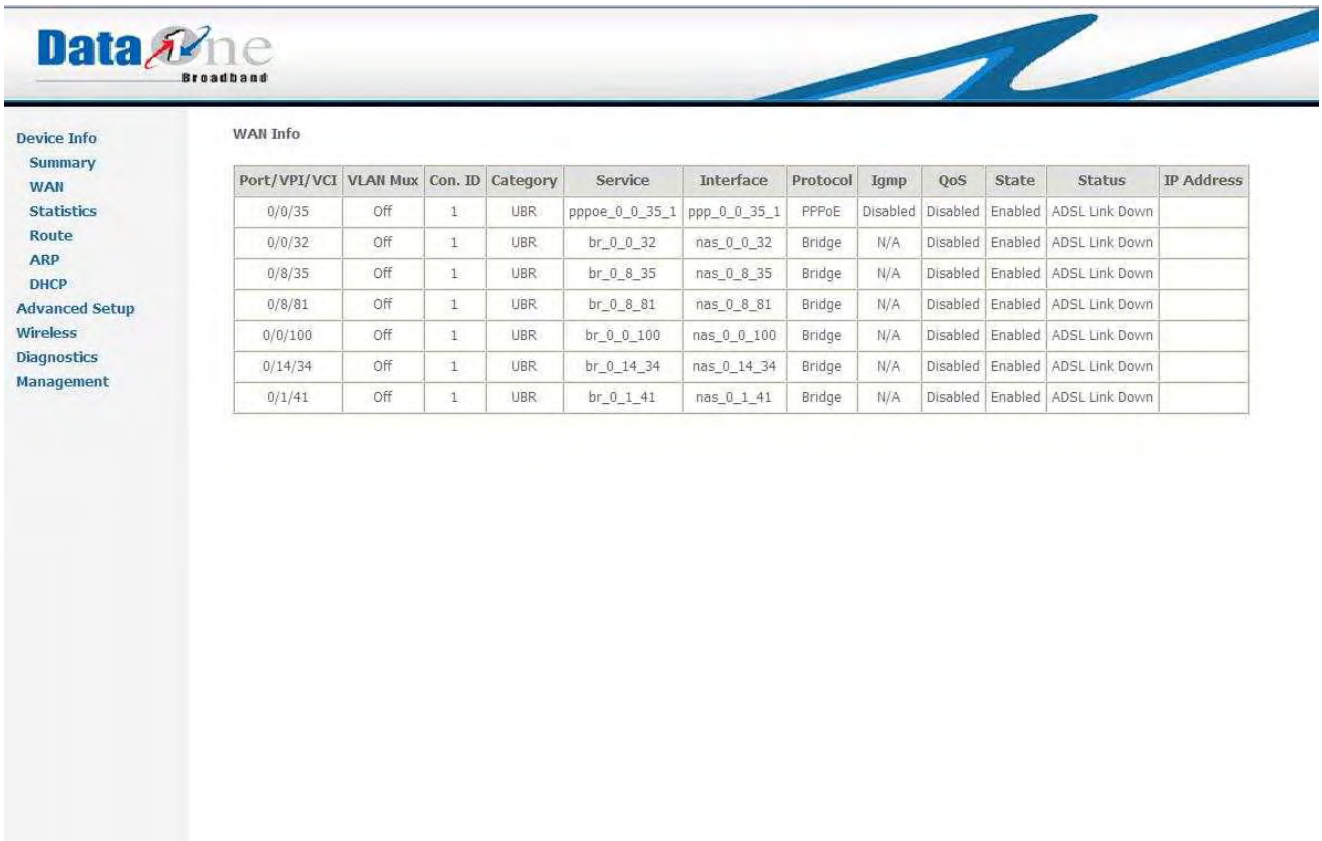
Device Info

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



Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
0/0/35	Off	1	UBR	pppoe_0_0_35_1	ppp_0_0_35_1	PPPoE	Disabled	Disabled	Enabled	ADSL Link Down	
0/0/32	Off	1	UBR	br_0_0_32	nas_0_0_32	Bridge	N/A	Disabled	Enabled	ADSL Link Down	
0/8/35	Off	1	UBR	br_0_8_35	nas_0_8_35	Bridge	N/A	Disabled	Enabled	ADSL Link Down	
0/8/81	Off	1	UBR	br_0_8_81	nas_0_8_81	Bridge	N/A	Disabled	Enabled	ADSL Link Down	
0/0/100	Off	1	UBR	br_0_0_100	nas_0_0_100	Bridge	N/A	Disabled	Enabled	ADSL Link Down	
0/14/34	Off	1	UBR	br_0_14_34	nas_0_14_34	Bridge	N/A	Disabled	Enabled	ADSL Link Down	
0/1/41	Off	1	UBR	br_0_1_41	nas_0_1_41	Bridge	N/A	Disabled	Enabled	ADSL Link Down	

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

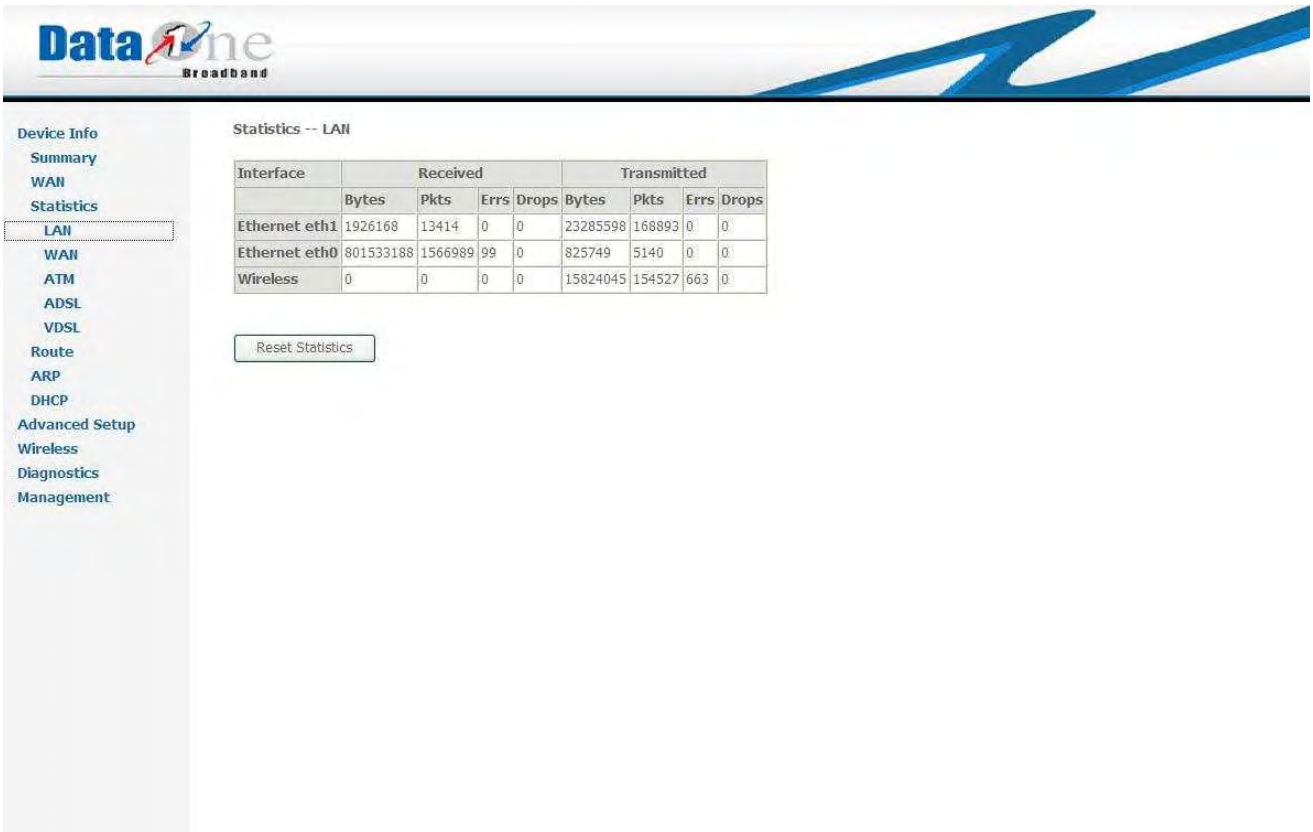
WAN

ATM

ADSL

VDSL

3.3.3.1. Device Info Statistics -- LAN

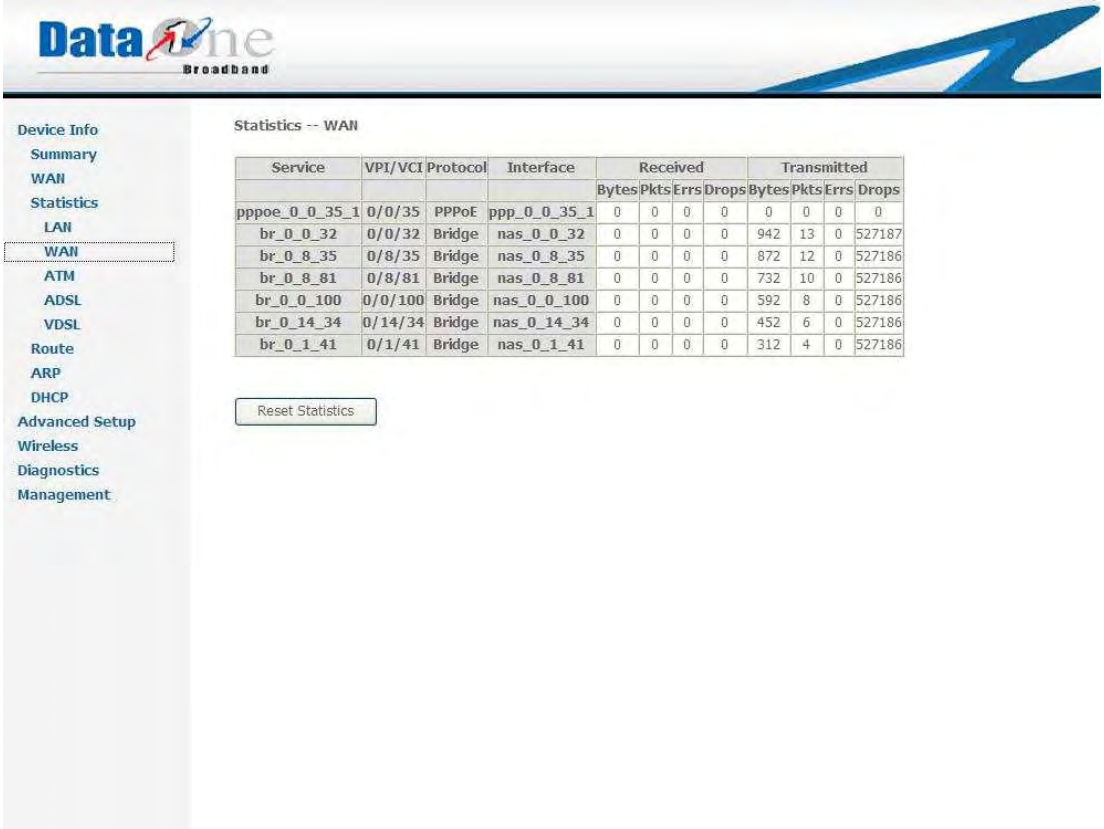


Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth1	1926168	13414	0	0	23285598	168893	0	0
Ethernet eth0	801533188	1566989	99	0	825749	5140	0	0
Wireless	0	0	0	0	15824045	154527	663	0

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.

3.3.3.2 Device Info 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
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

3.3.3.3 Device Info Statistics -- ATM

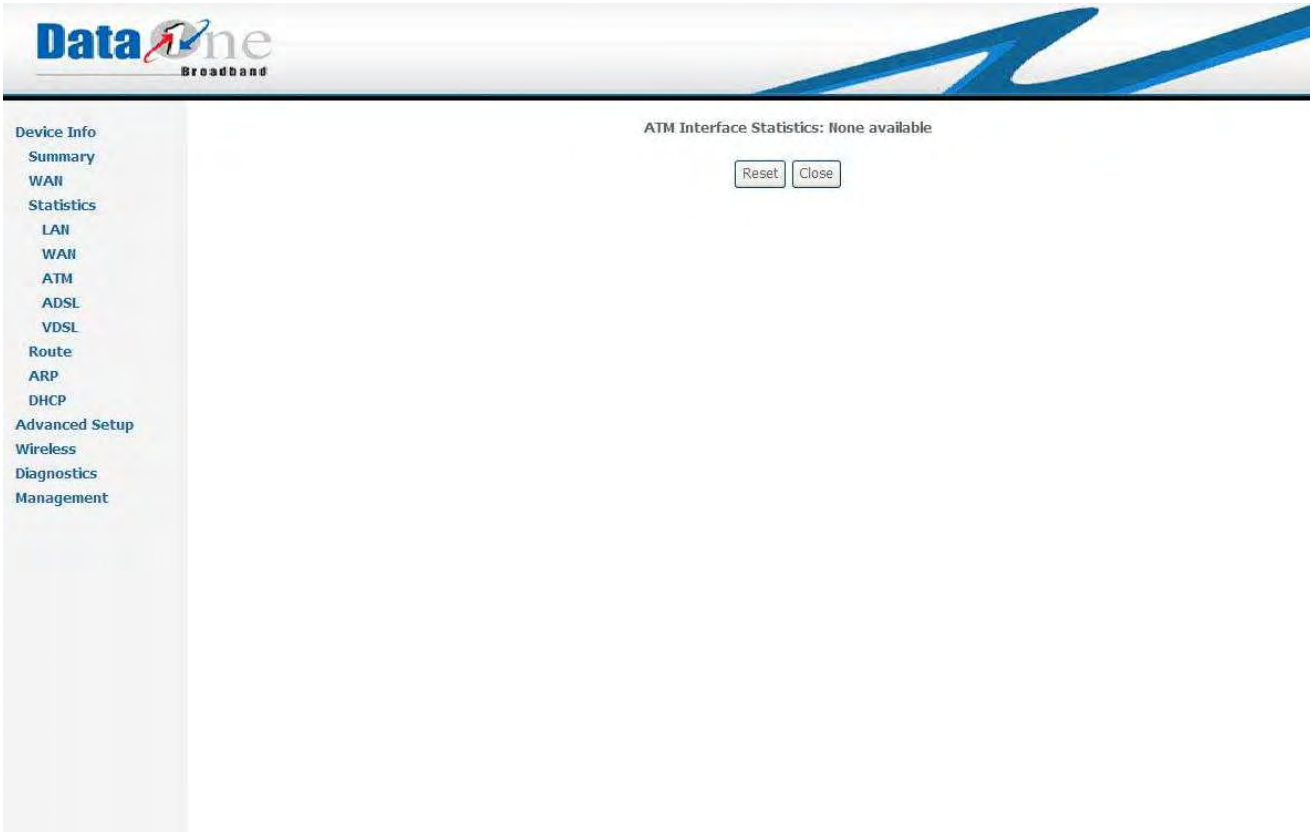


Figure 3.3.3.3 Device Info Statistics -- ATM

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

3.3.3.4 Device Info Statistics -- ADSL

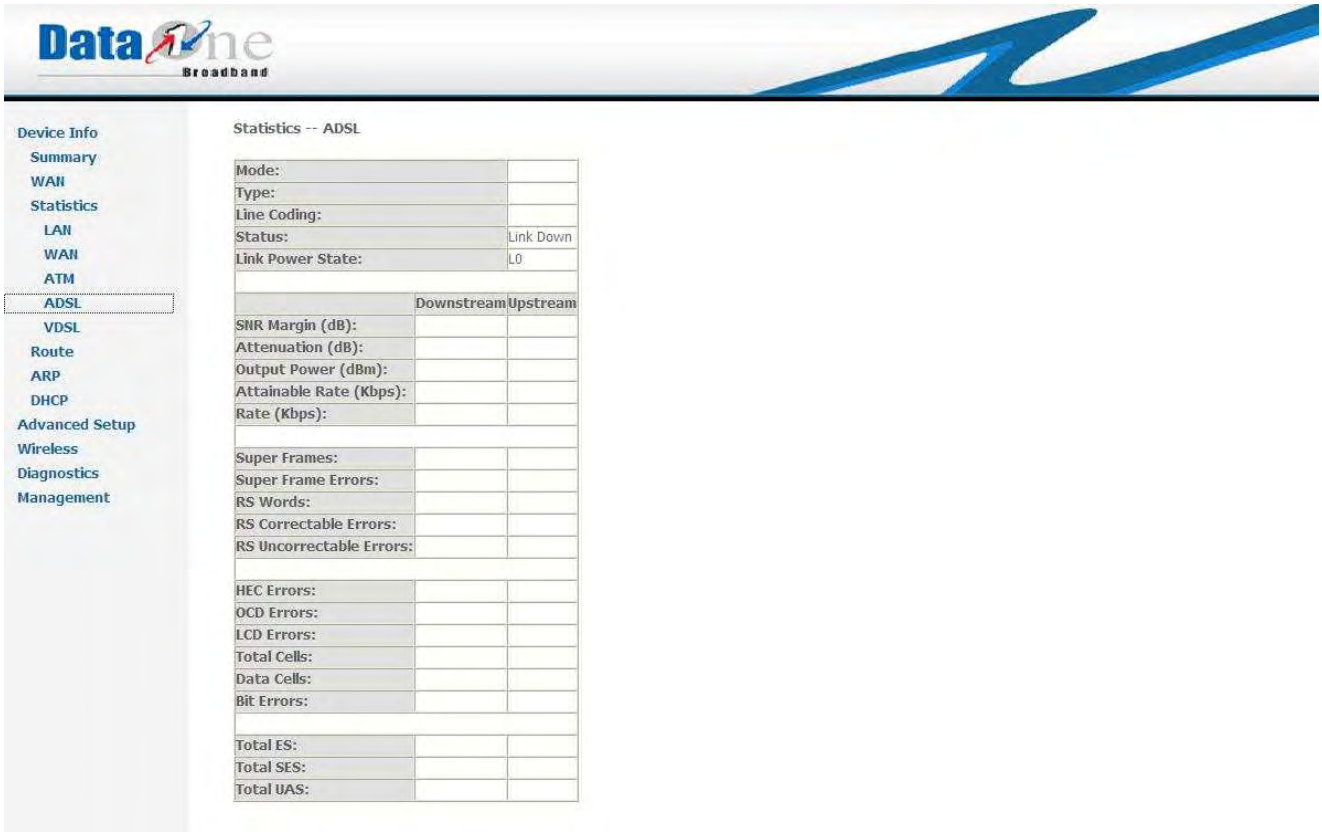


Figure 3.3.3.4 Device Info Statistics – ADSL

3.3.3.5 Device Info Statistics -- VDSL

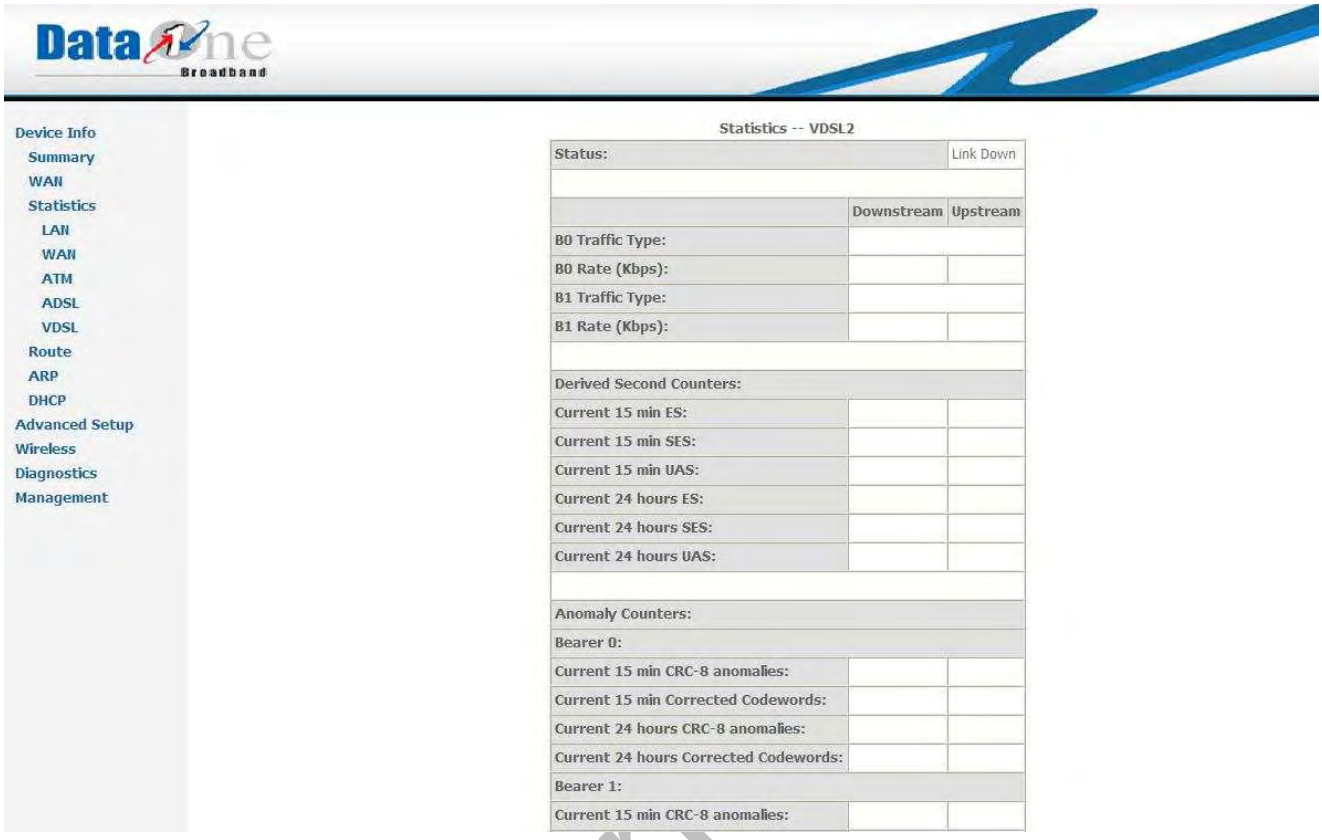


Figure 3.3.3.5 Device Info Statistics – VDSL

3.3.4 Device Info Route

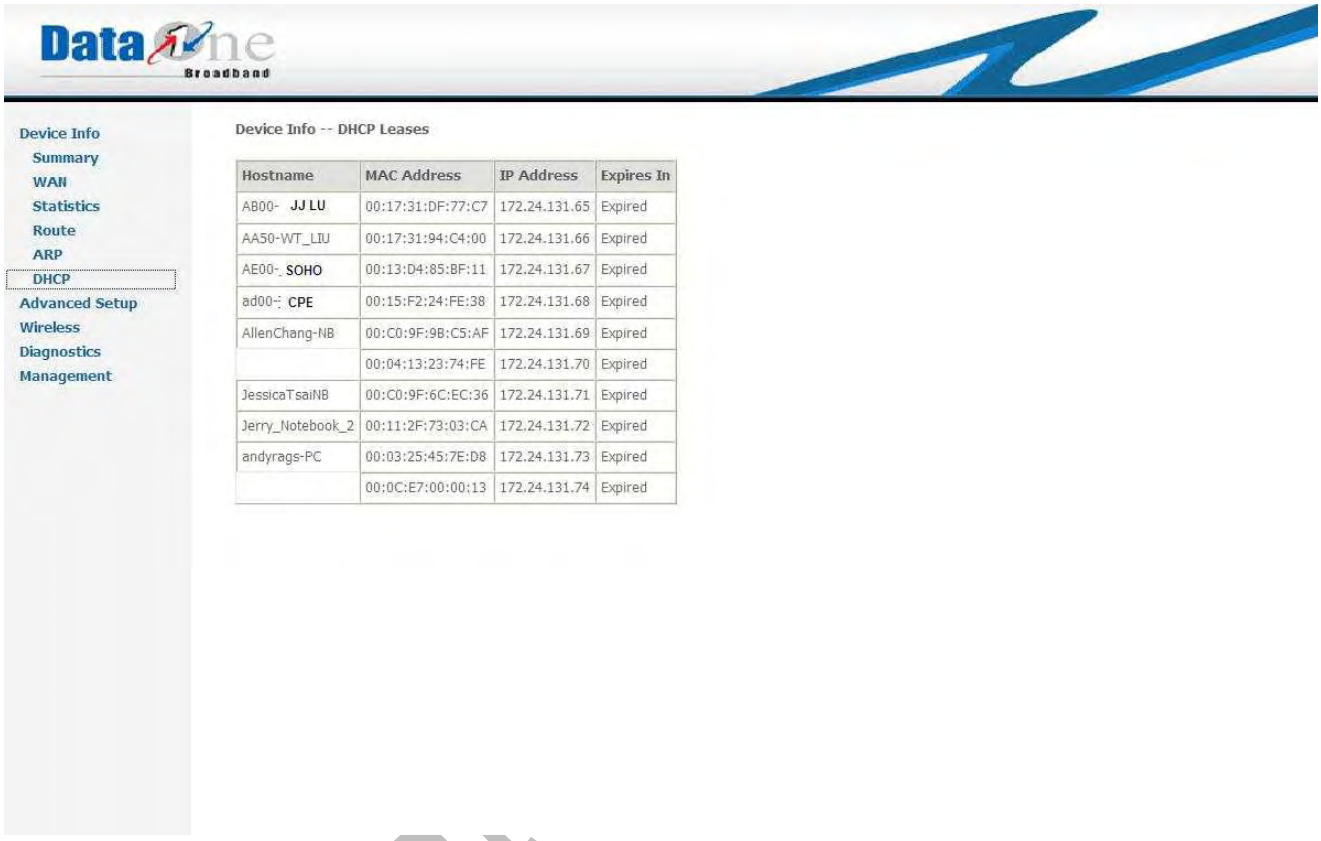
Figure 3.3.4 Device Info Route

3.3.5 Device Info ARP

Figure **3.3.5 Device Info ARP**

.

3.3.6 Device Info DHCP



Hostname	MAC Address	IP Address	Expires In
AB00- JJ LU	00:17:31:DF:77:C7	172.24.131.65	Expired
AA50-WT_LIU	00:17:31:94:C4:00	172.24.131.66	Expired
AE00-. SOHO	00:13:D4:85:BF:11	172.24.131.67	Expired
ad00-: CPE	00:15:F2:24:FE:38	172.24.131.68	Expired
AllenChang-NB	00:C0:9F:9B:C5:AF	172.24.131.69	Expired
	00:04:13:23:74:FE	172.24.131.70	Expired
JessicaTsaiNB	00:C0:9F:6C:EC:36	172.24.131.71	Expired
Jerry_Notebook_2	00:11:2F:73:03:CA	172.24.131.72	Expired
andyrags-PC	00:03:25:45:7E:D8	172.24.131.73	Expired
	00:0C:E7:00:00:13	172.24.131.74	Expired

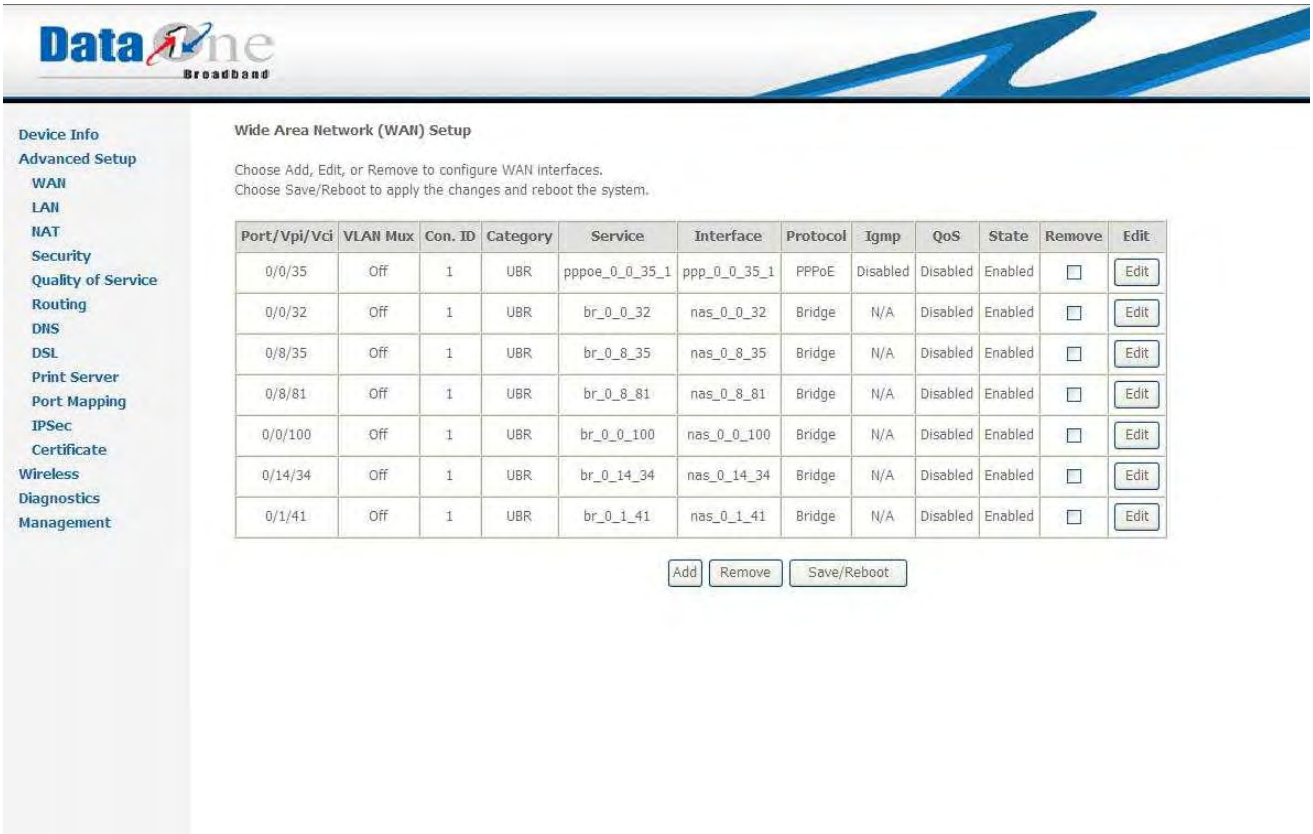
Figure 3.3.6 Device Info DHCP

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



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

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:

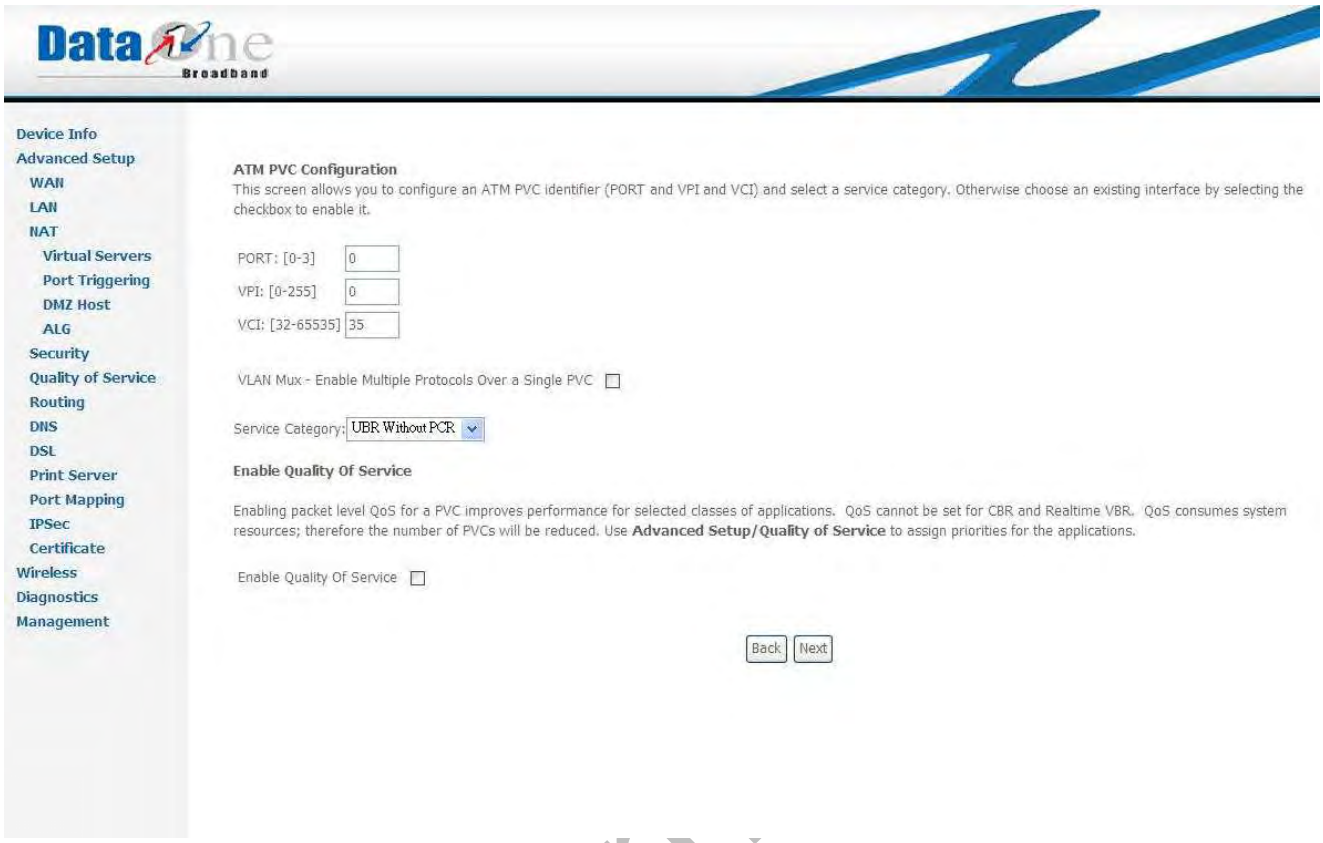


Figure 3.4.1.1 Advanced Setup – ATM PVC Configuration

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:

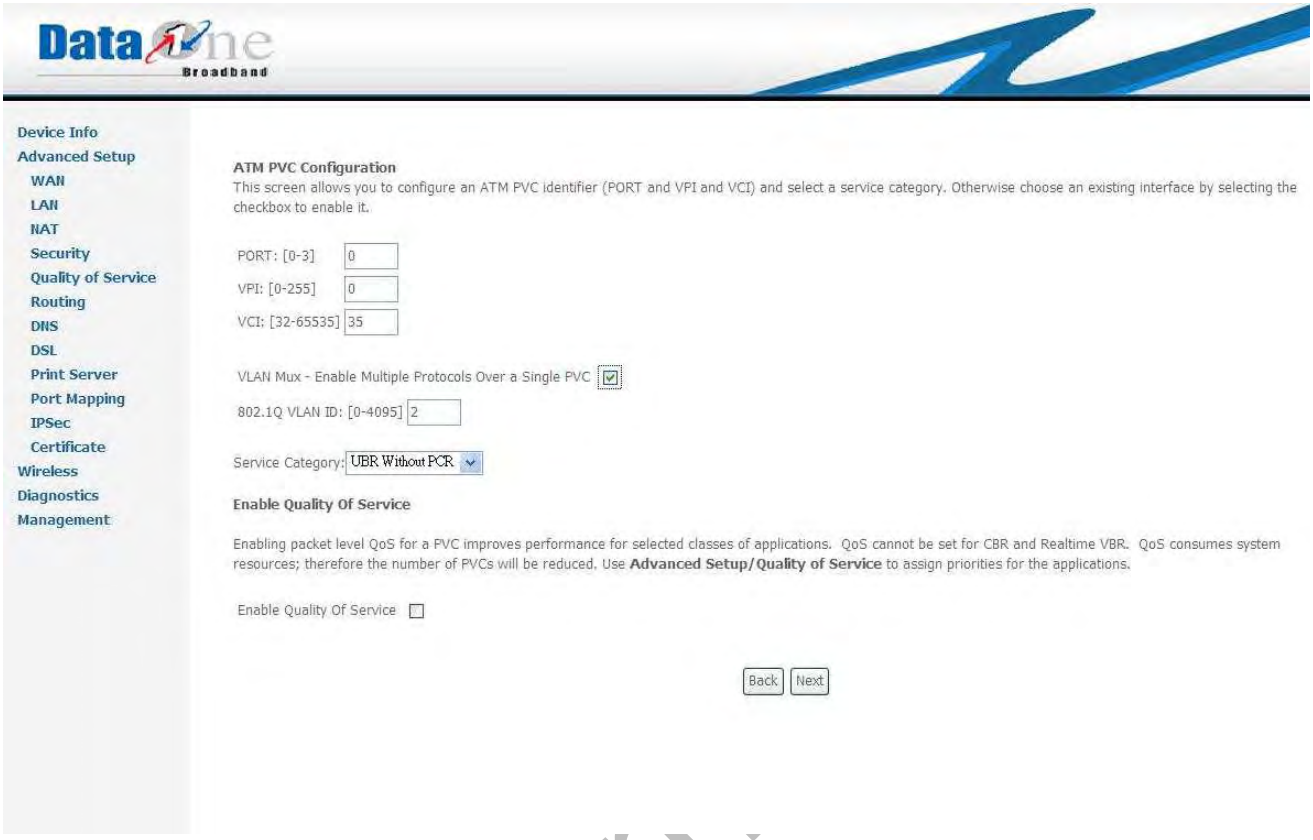


Figure 3.4.1.1.a Advanced Setup –***VLAN Configuration***

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

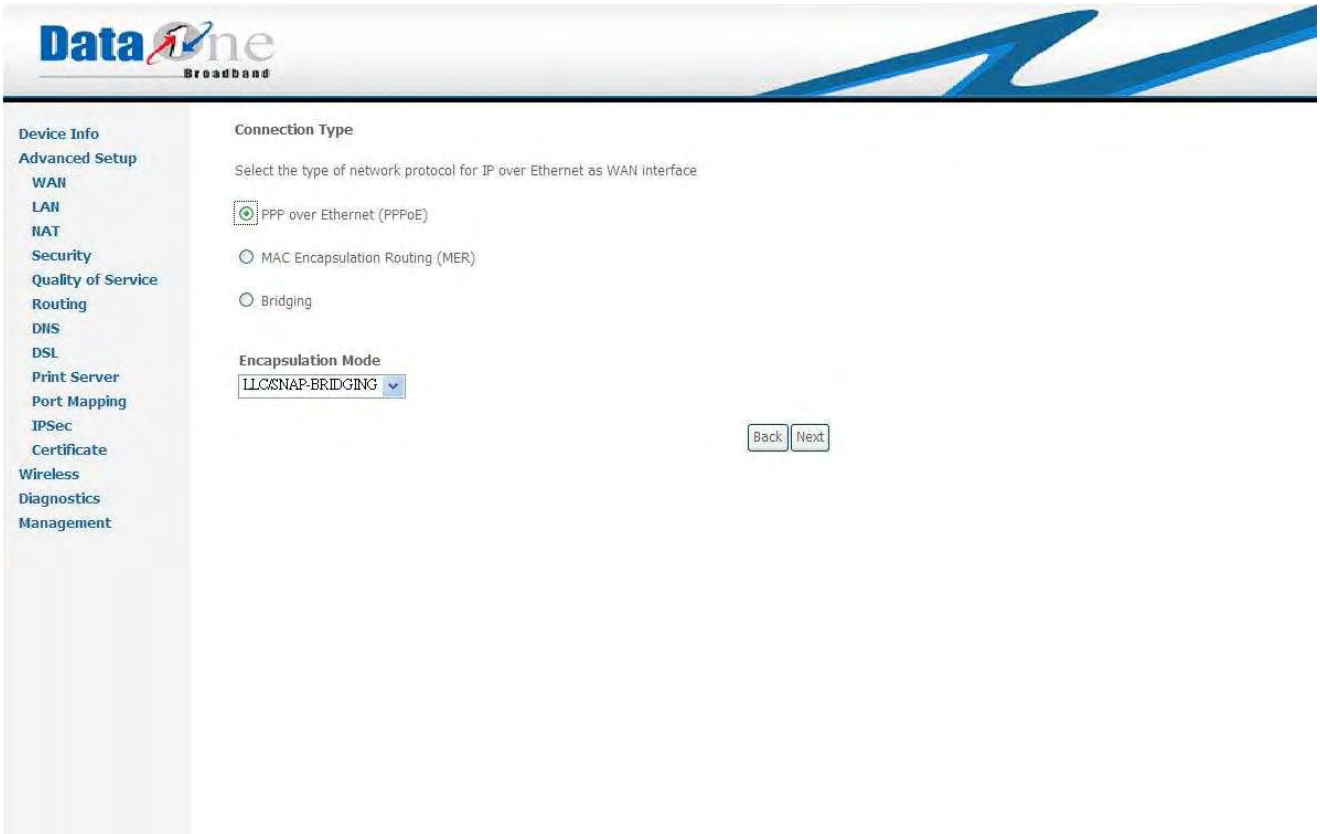


Figure 3.4.1.1.1.a Advanced Setup – ***PPPoE Connection Type***

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

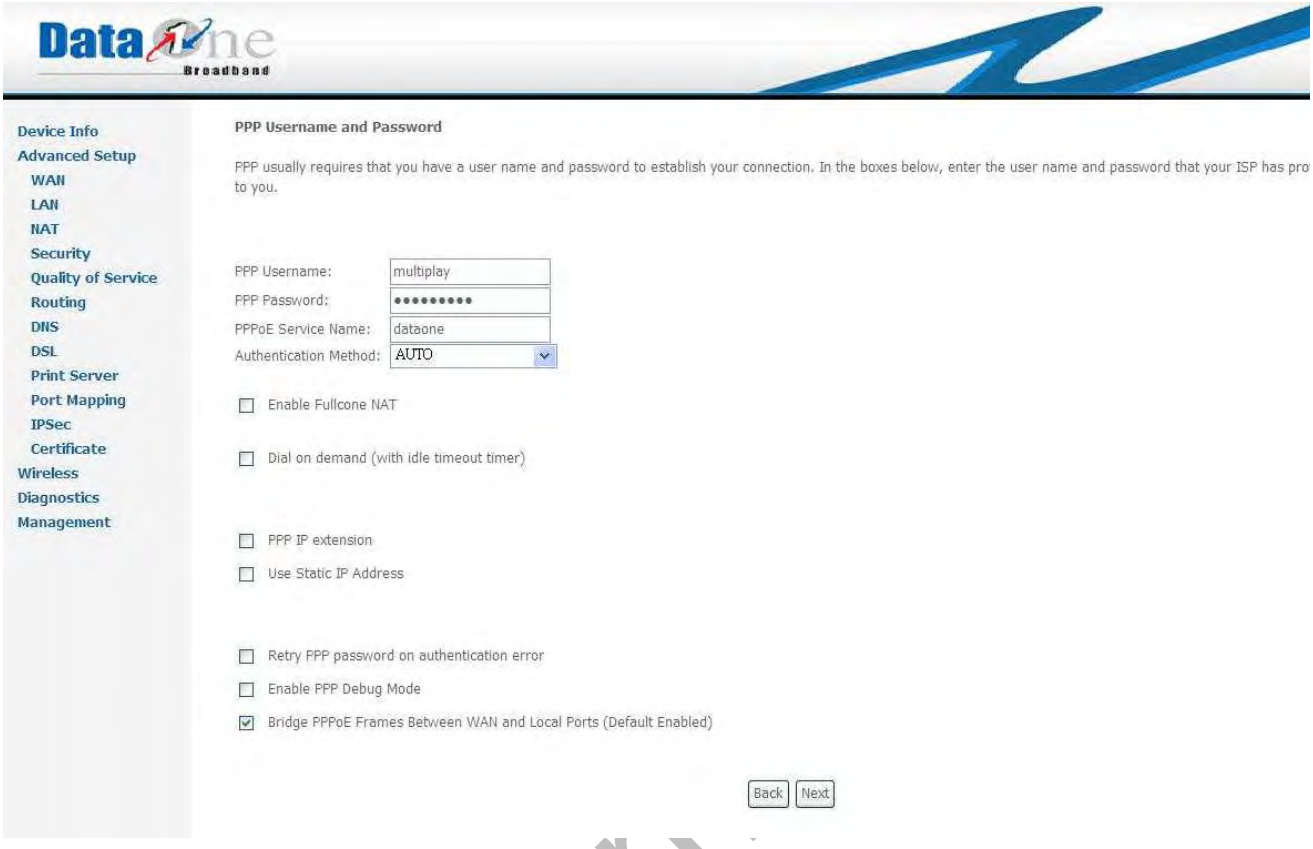


Figure 3.4.1.1.1.b Advanced Setup – ***PPP Username and Password***

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.*

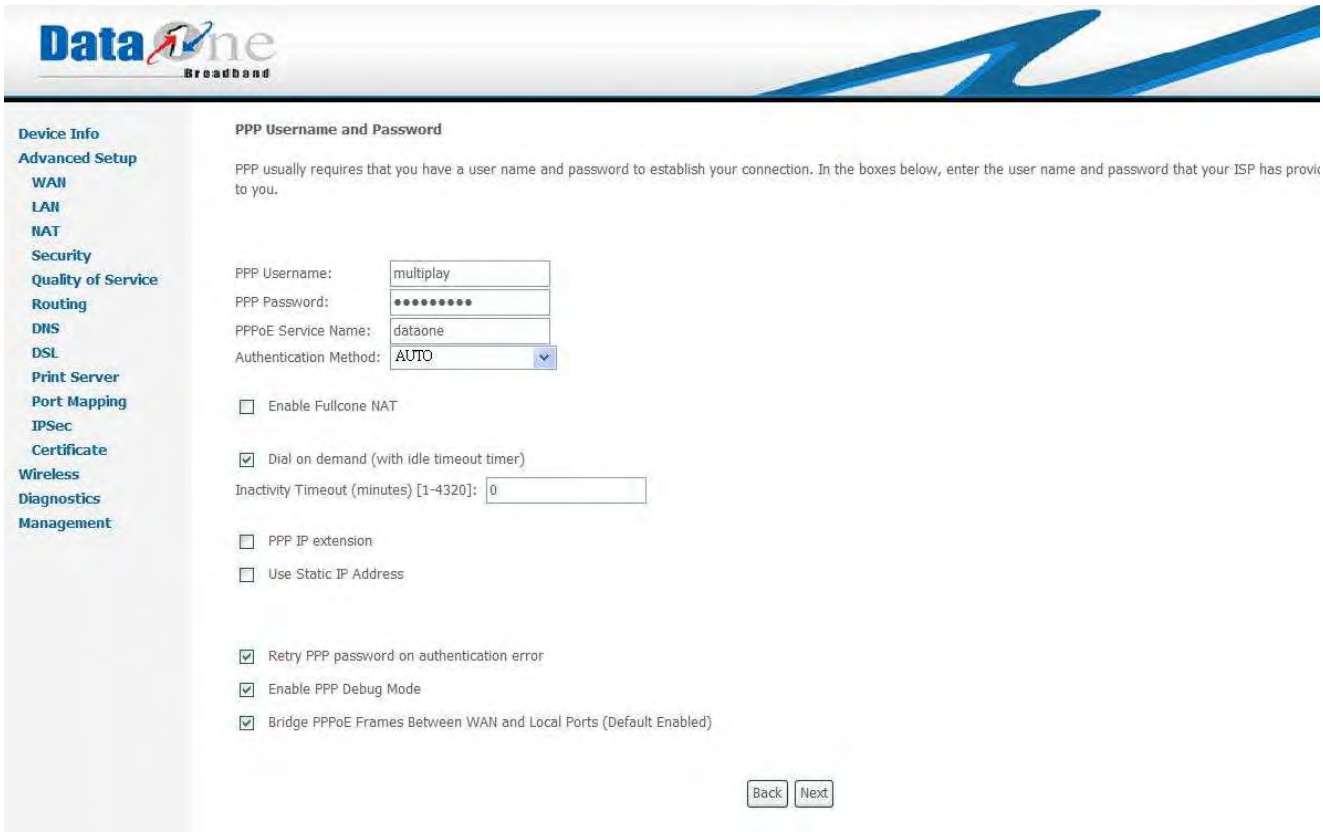


Figure 3.4.1.1.1.c Advanced Setup – ***PPP Username and Password Inactivity Timeout***

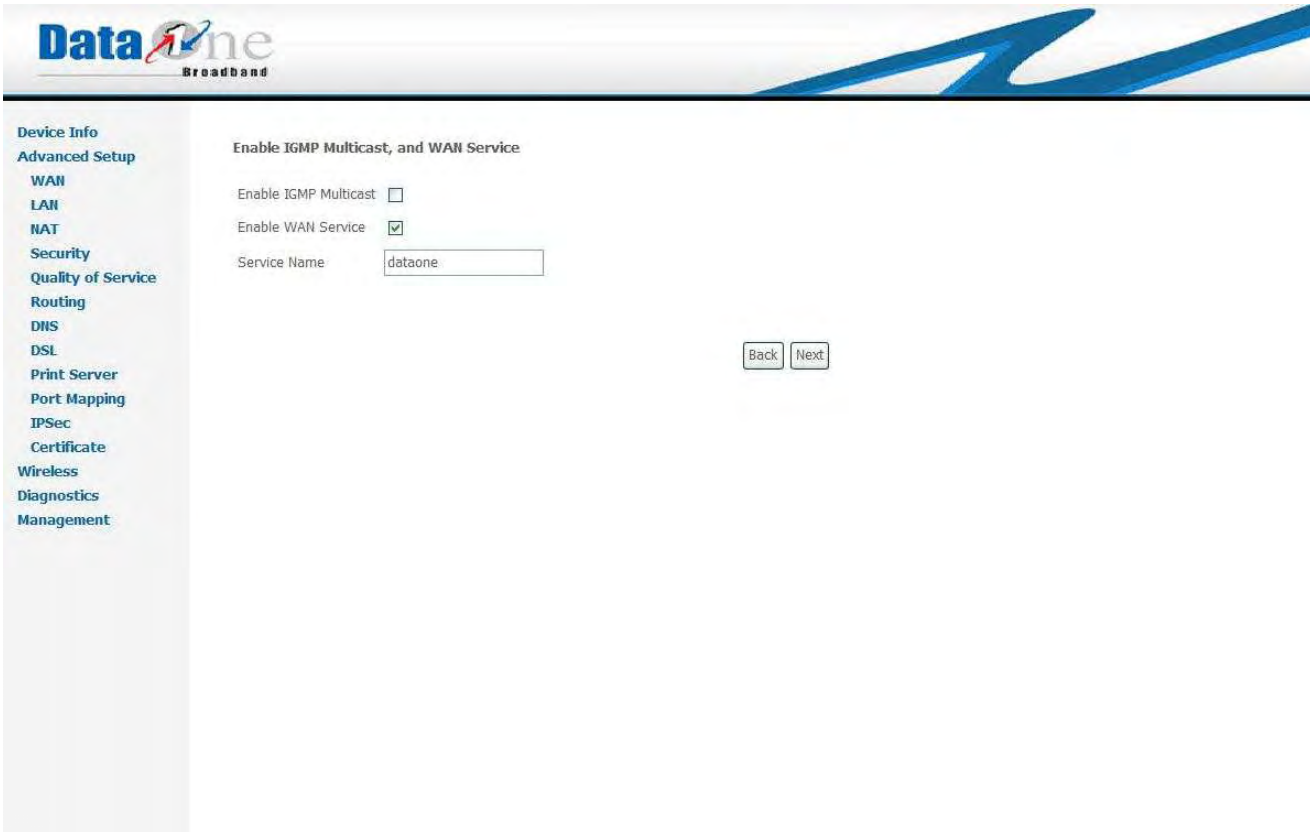


Figure 3.4.1.1.1.d Advanced Setup – ***Enable IGMP Multicast, and WAN Service.***

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

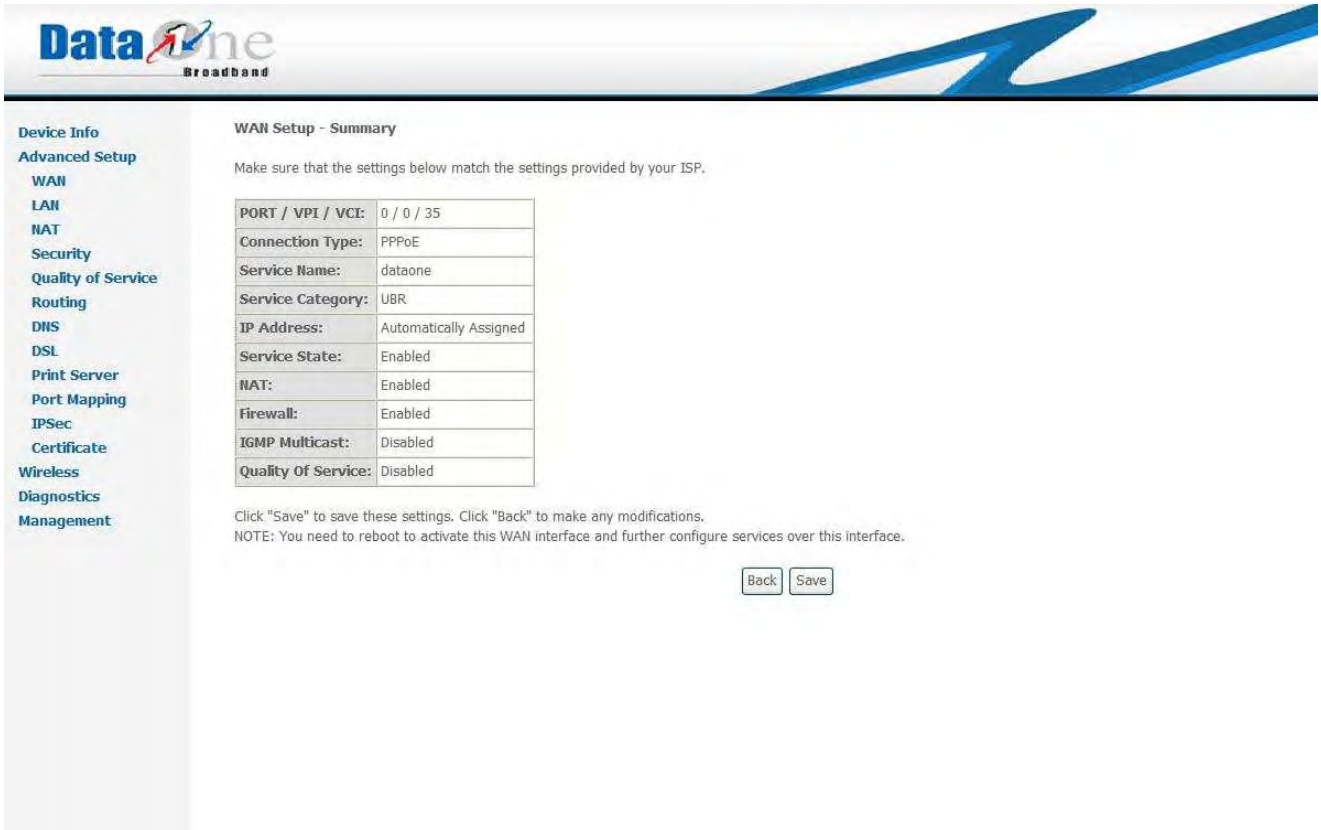


Figure 3.4.1.1.1.e Advanced Setup – WAN Setup – Summary

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

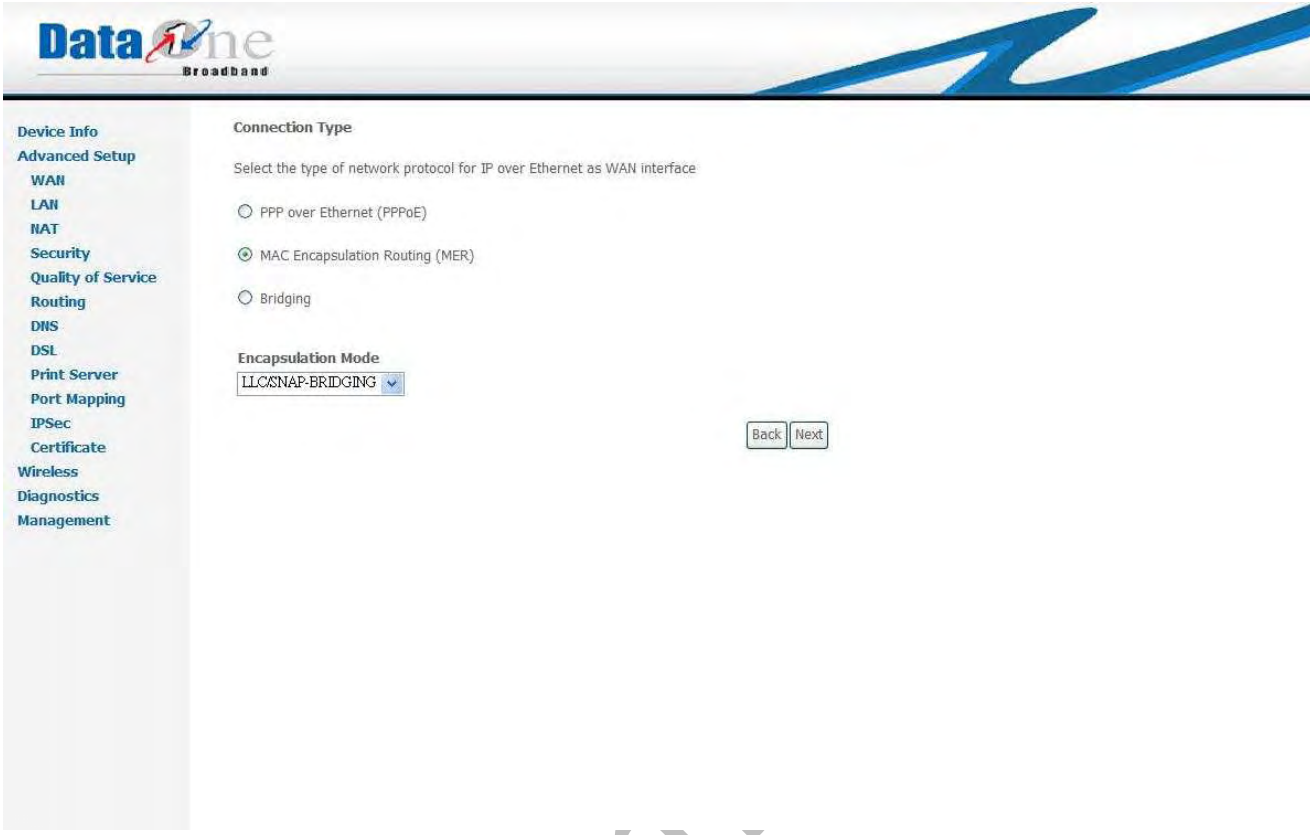


Figure 3.4.1.1.2.a Advanced Setup –***MER Connection Type***

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.
.

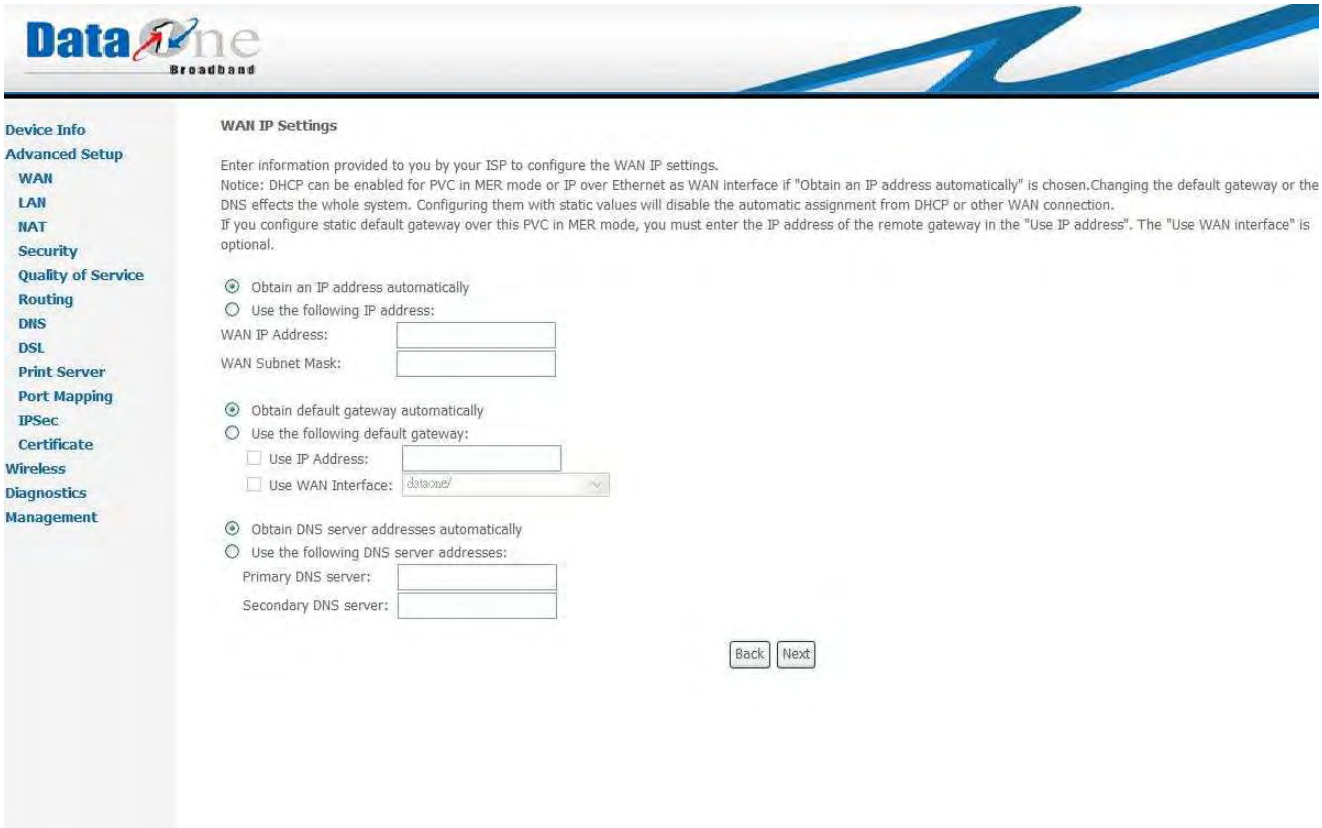


Figure 3.4.1.1.2.b Advanced Setup –***Connection Type MER WAN IP Settings***

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.

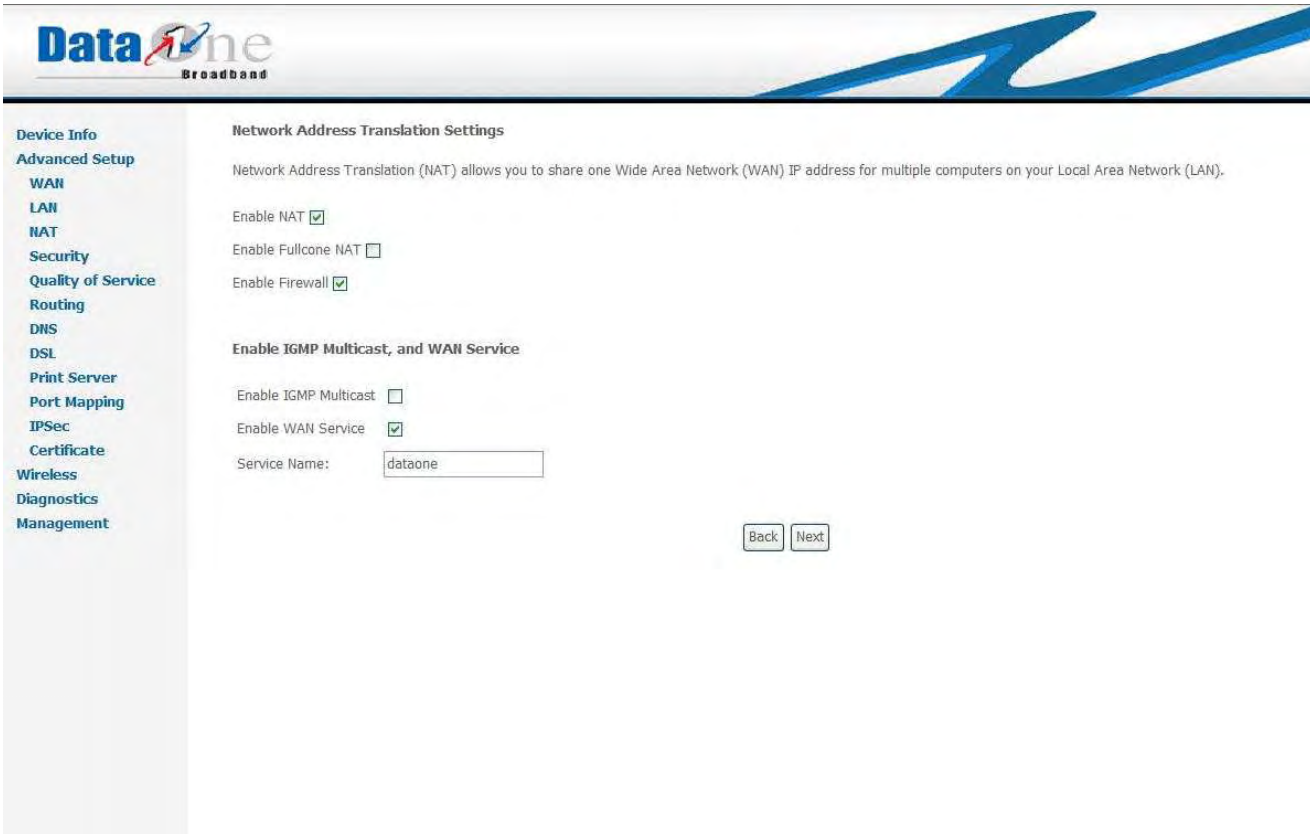


Figure 3.4.1.1.2.c Advanced Setup –MER- NAT, Firewall, IGMP Multicast and WAN service

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.

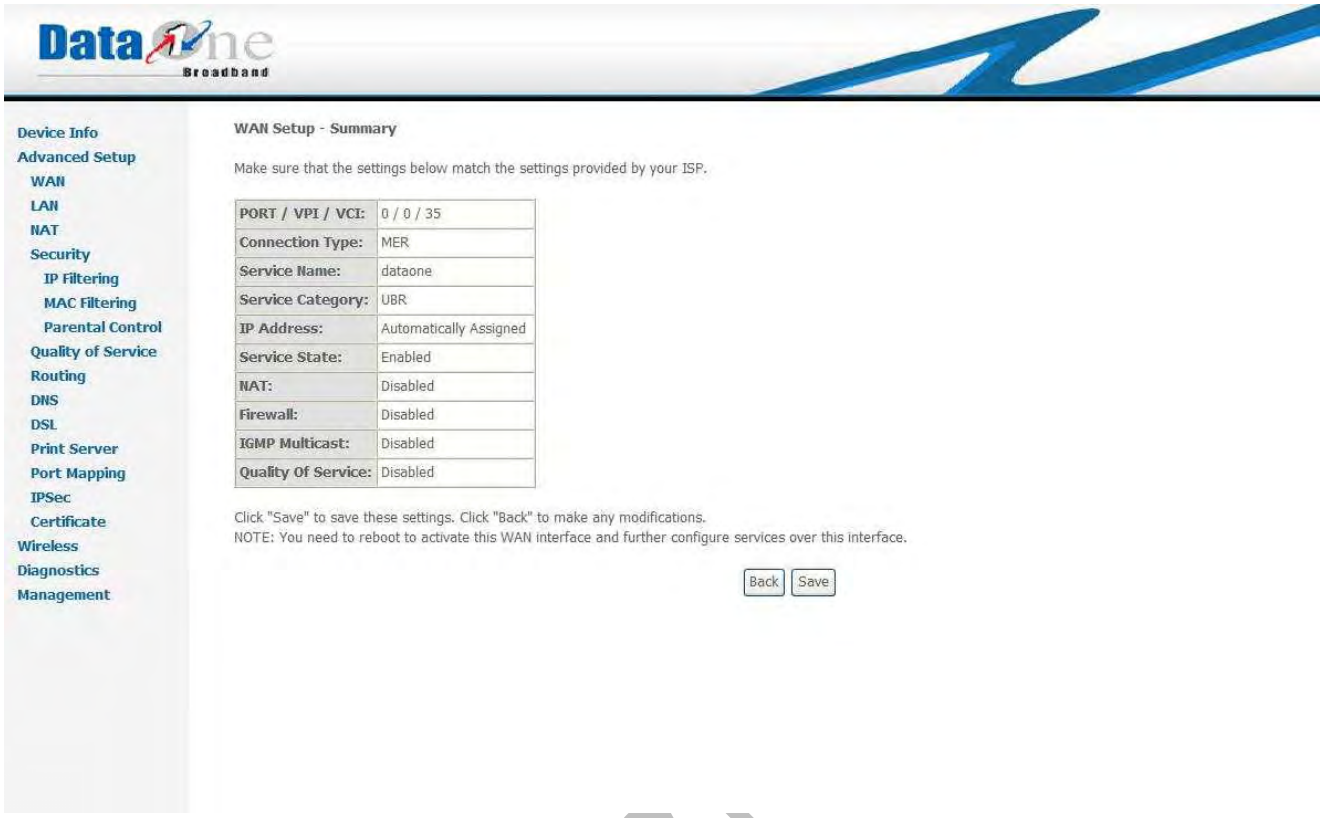


Figure 3.4.1.1.2.d Advanced Setup WAN Setup – Summary

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.

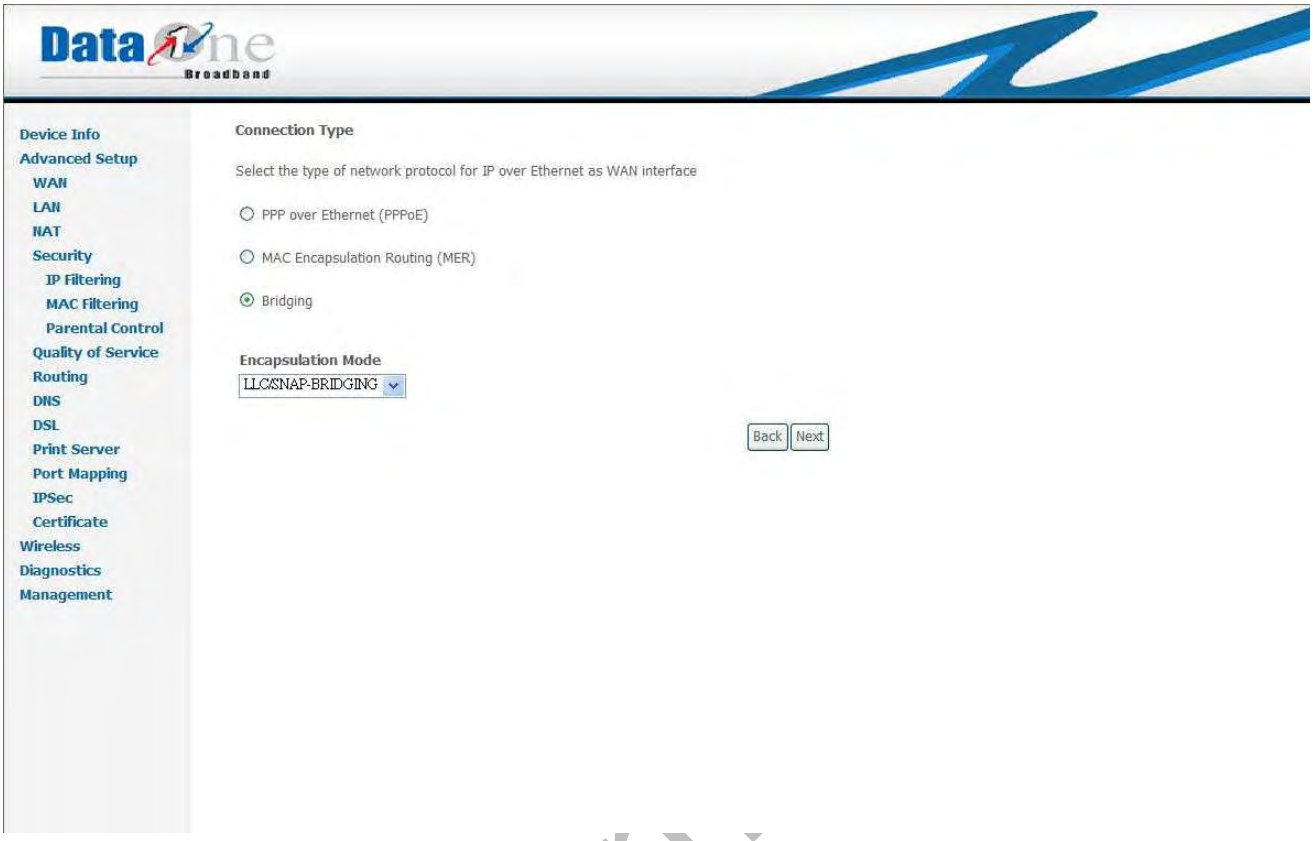


Figure 3.4.1.1.3.a Advanced Setup –***Bridging Type***

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

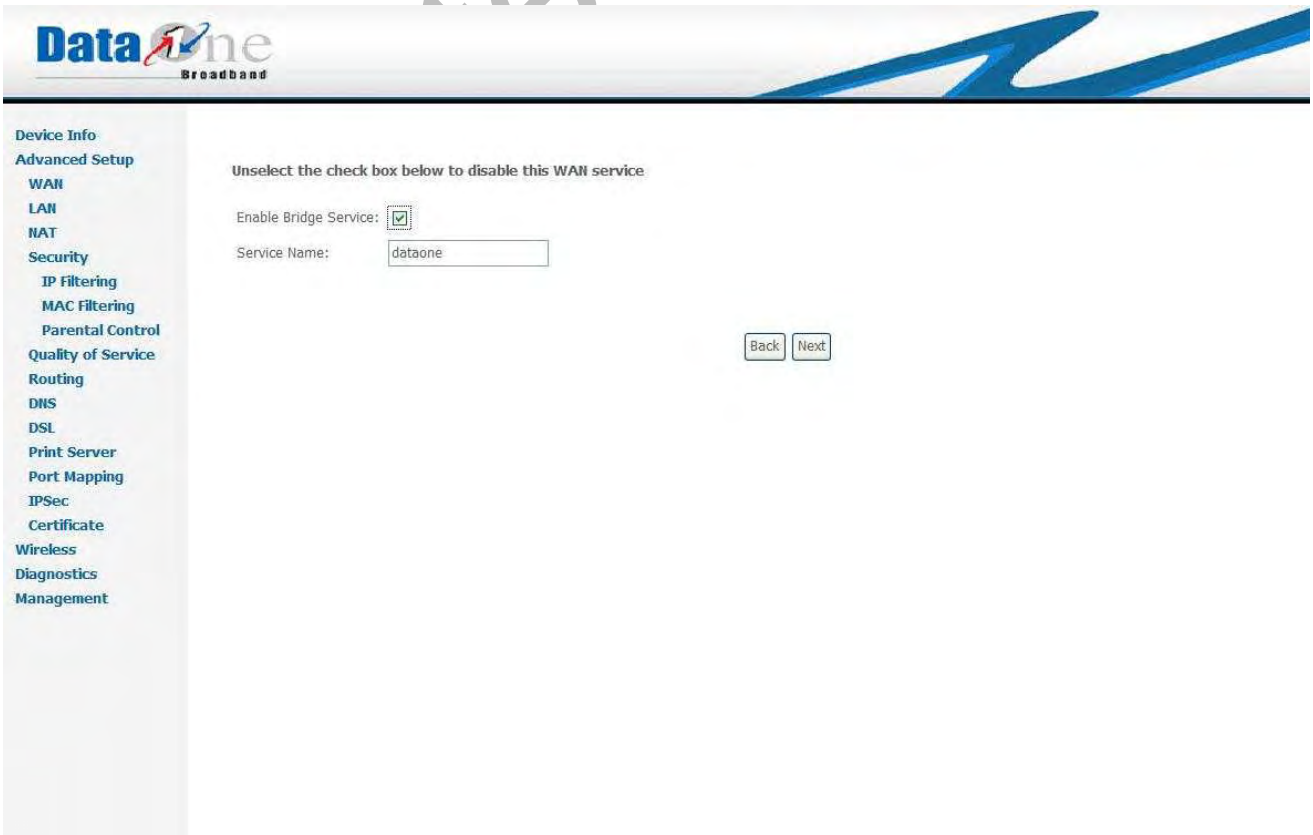


Figure 3.4.1.1.3.b Advanced Setup –***Bridging Type – WAN Service***

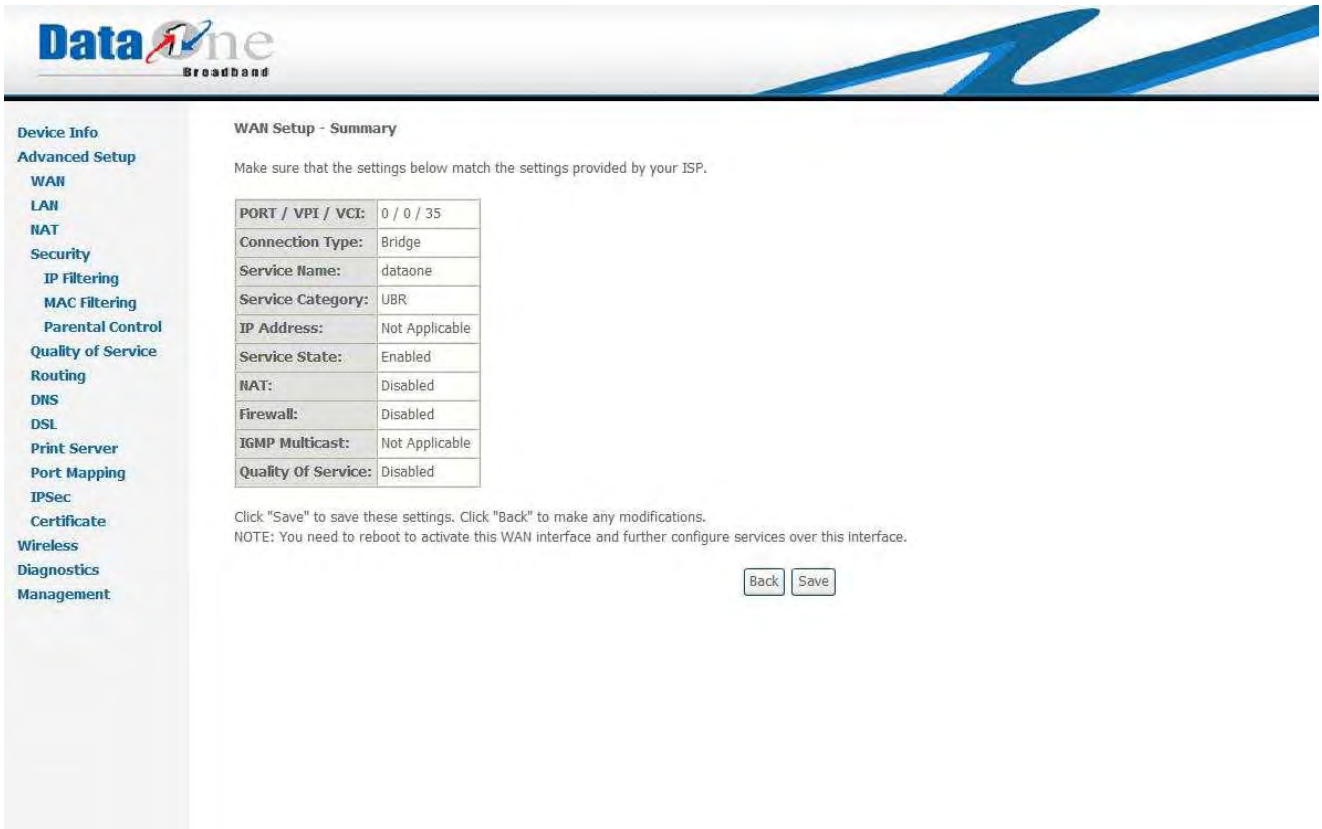


Figure 3.4.1.1.3.cAdvanced Setup WAN Setup – Summary

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

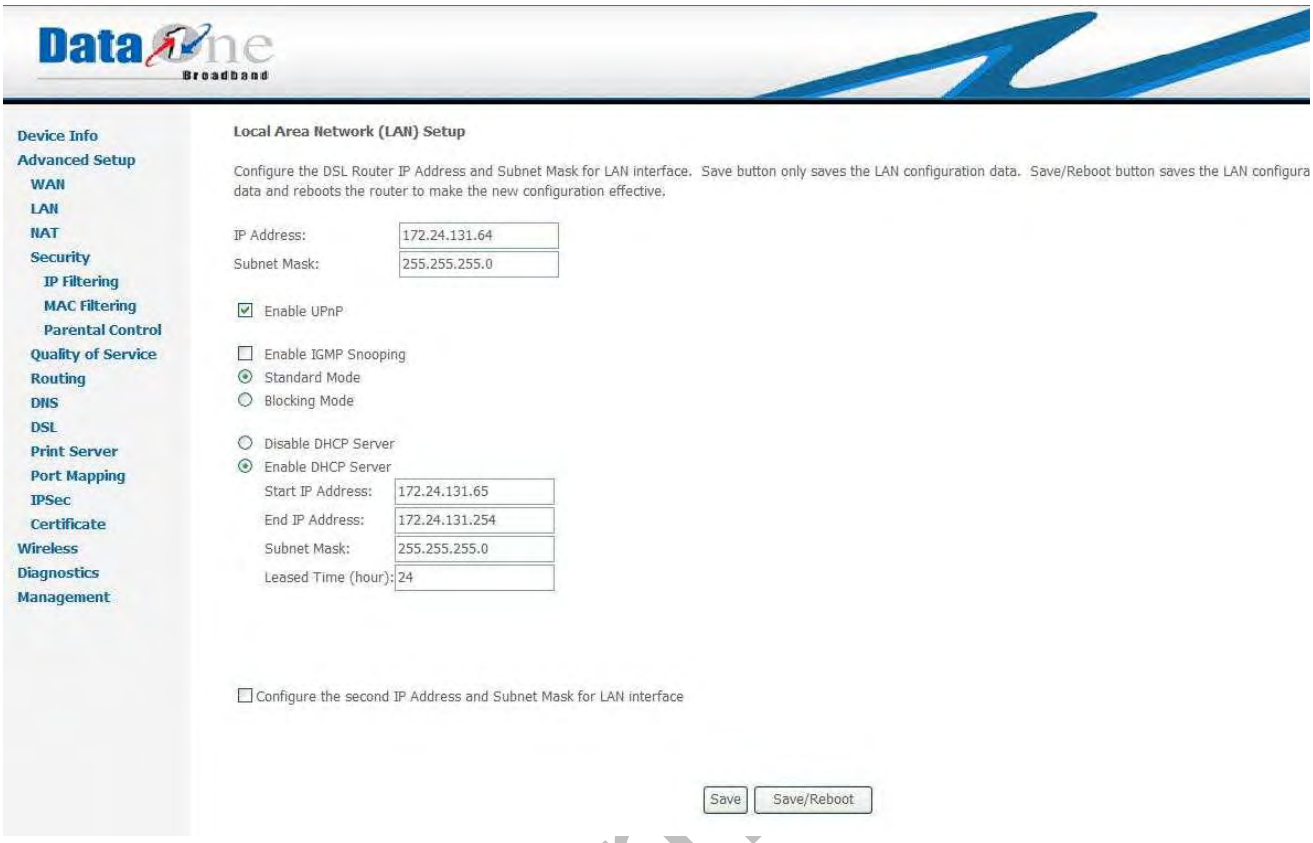


Figure 3.4.2 Advanced Setup – LAN

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.

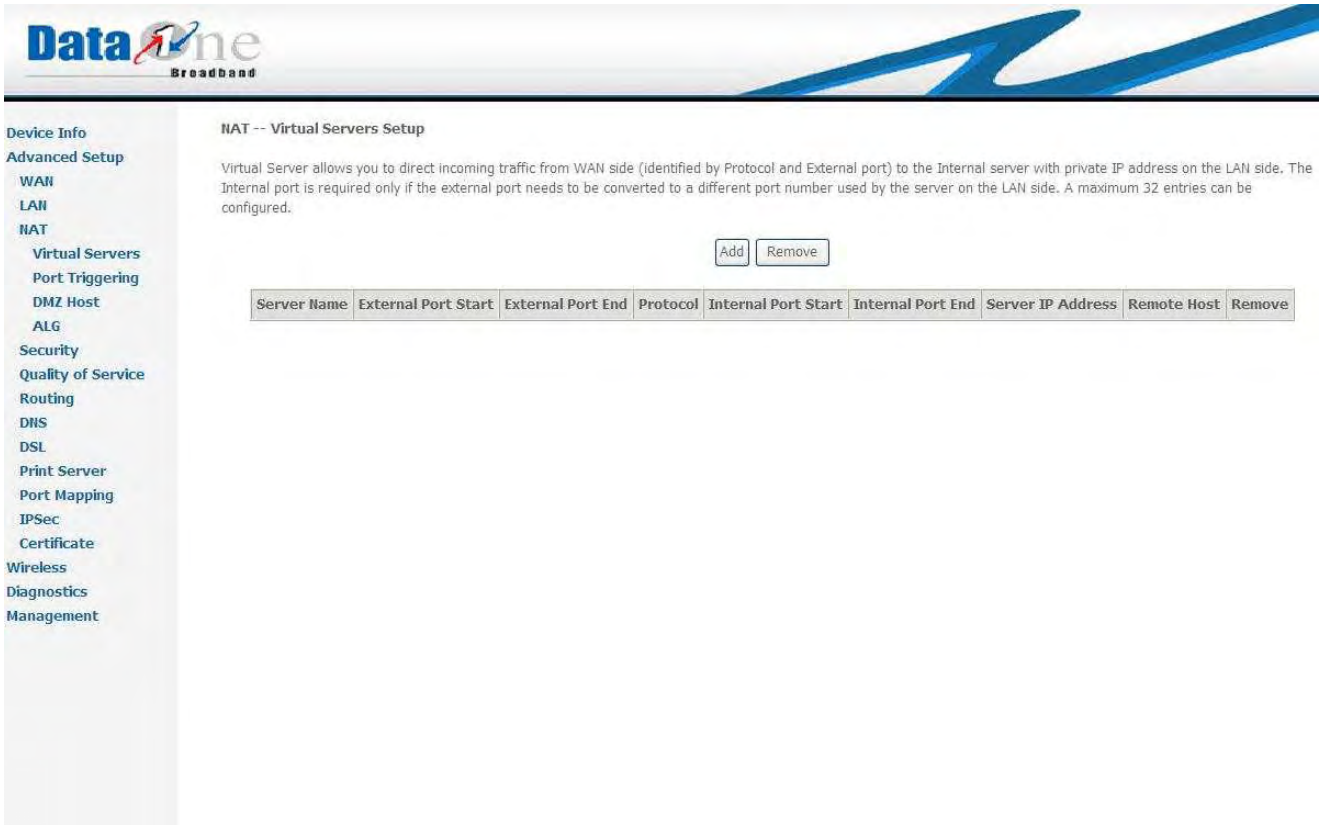


Figure 3.4.3.1.a Advanced Setup – NAT

Click "***Add***" for next step

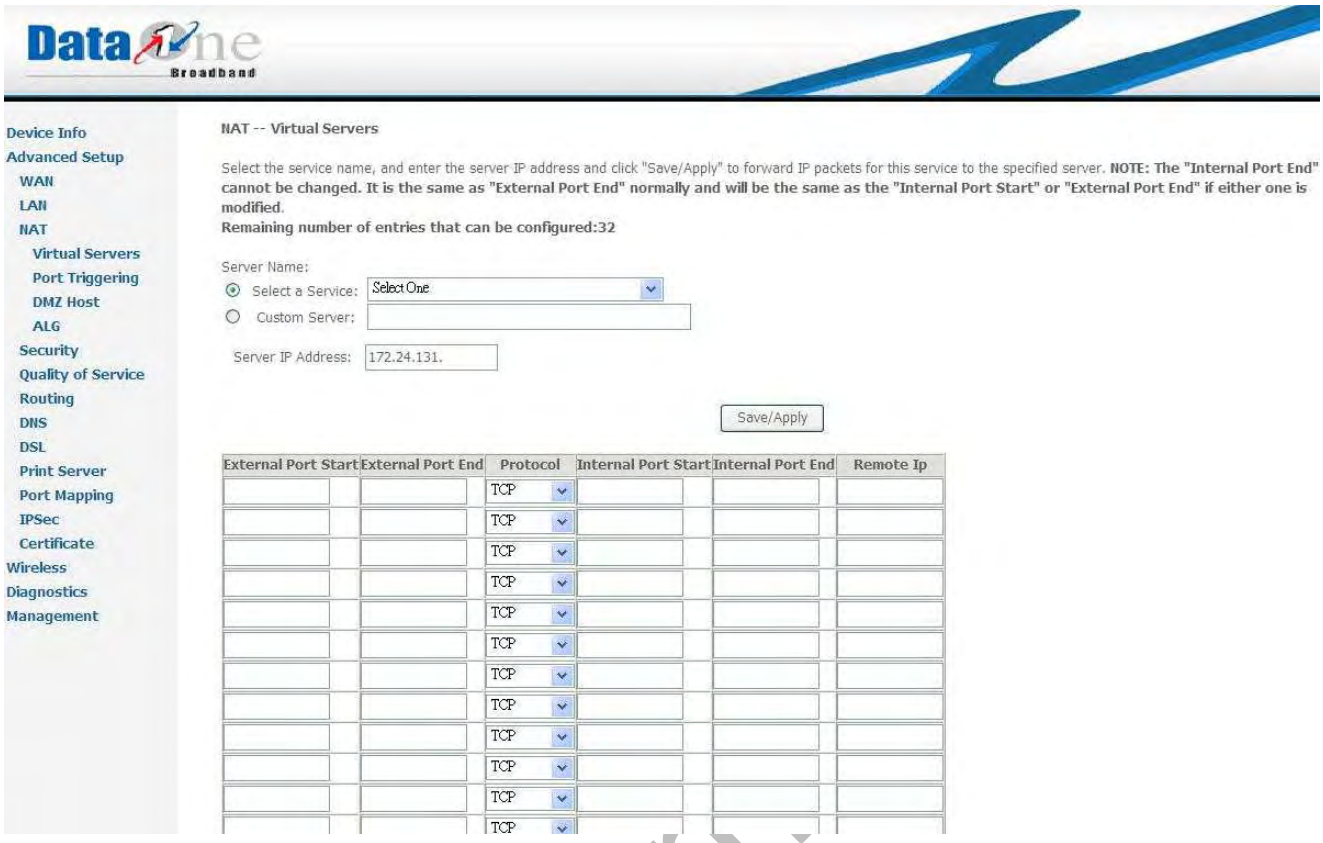


Figure 3.4.3.1 b Advanced Setup – NAT – Virtual Servers

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.

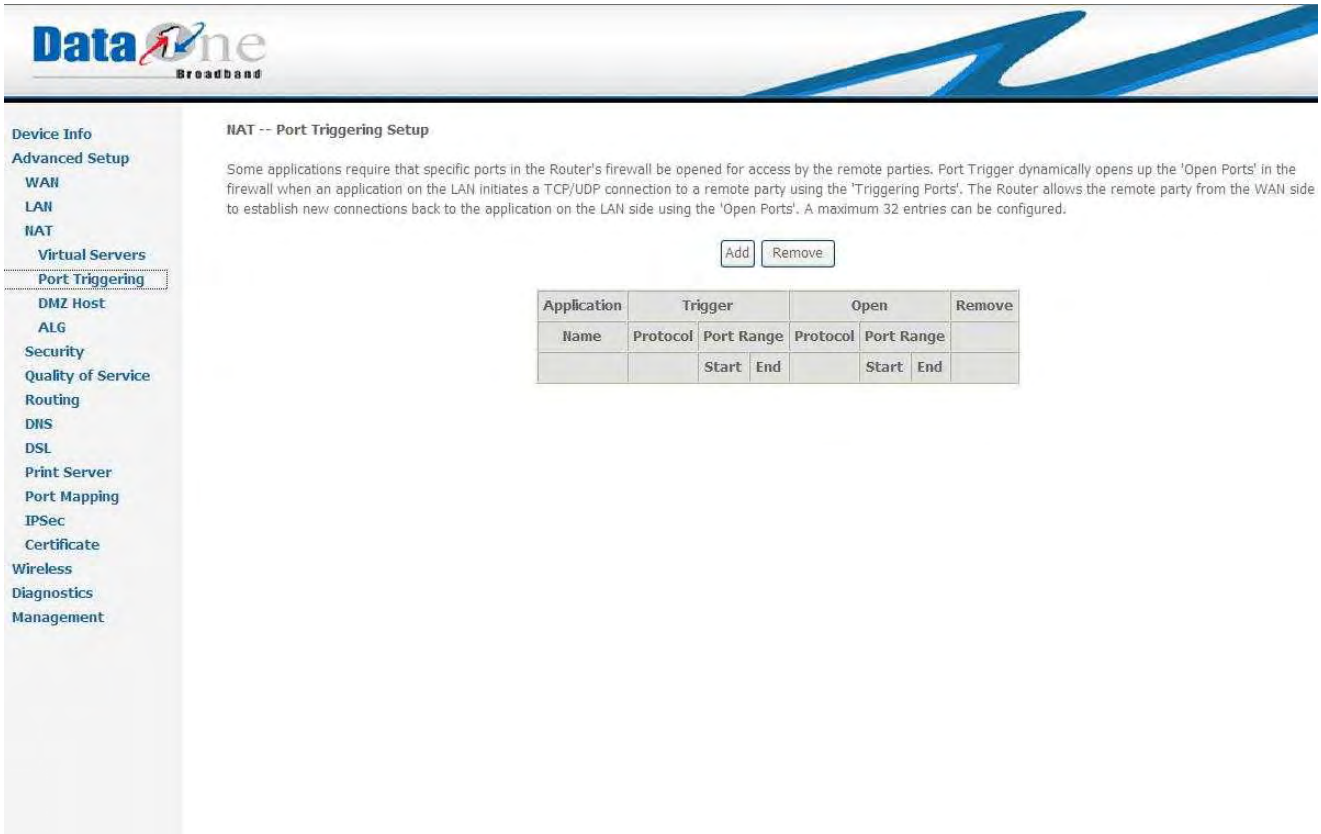


Figure 3.4.3.2.a Advanced Setup – NAT – Port Triggering Setup

Click "***Add***" for next step

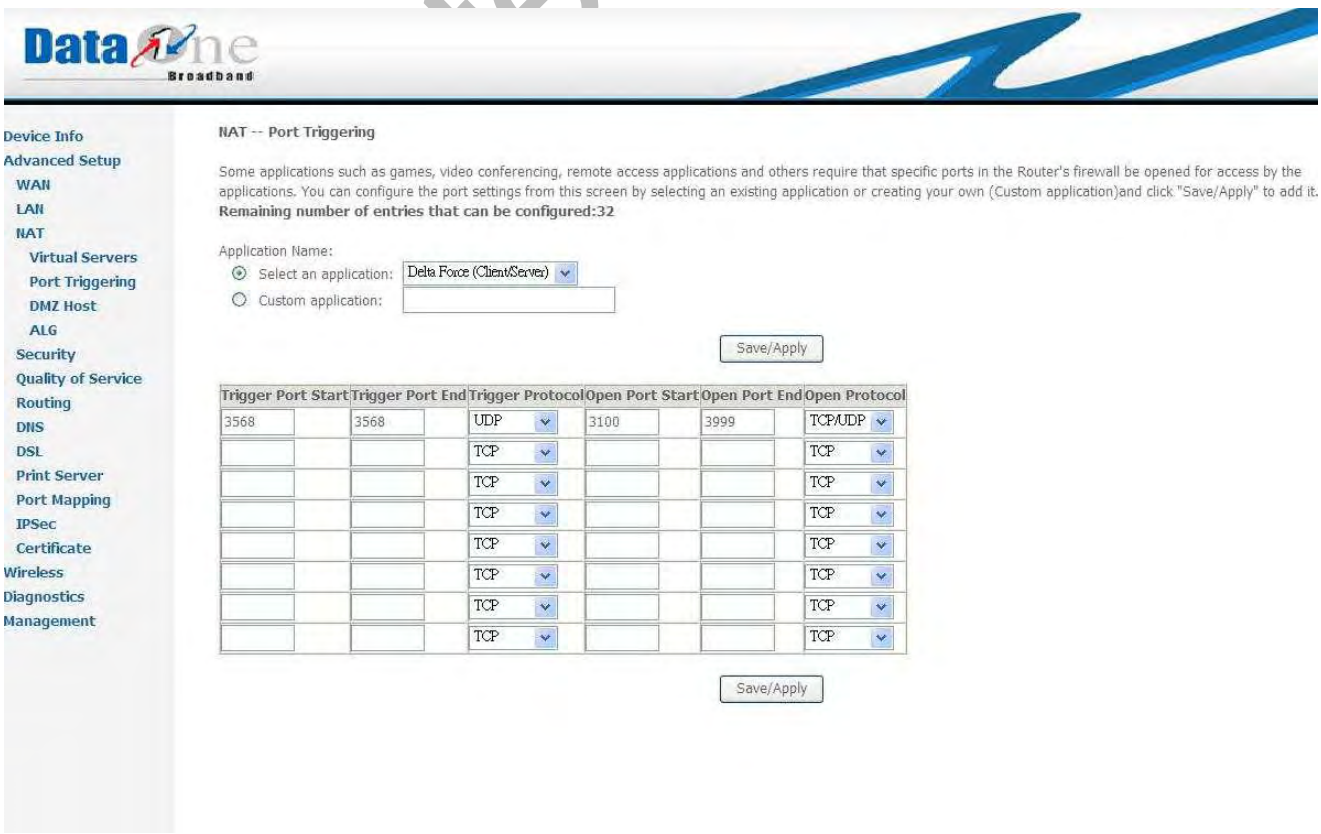


Figure 3.4.3.2.b Advanced Setup – NAT – Port Triggering

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.

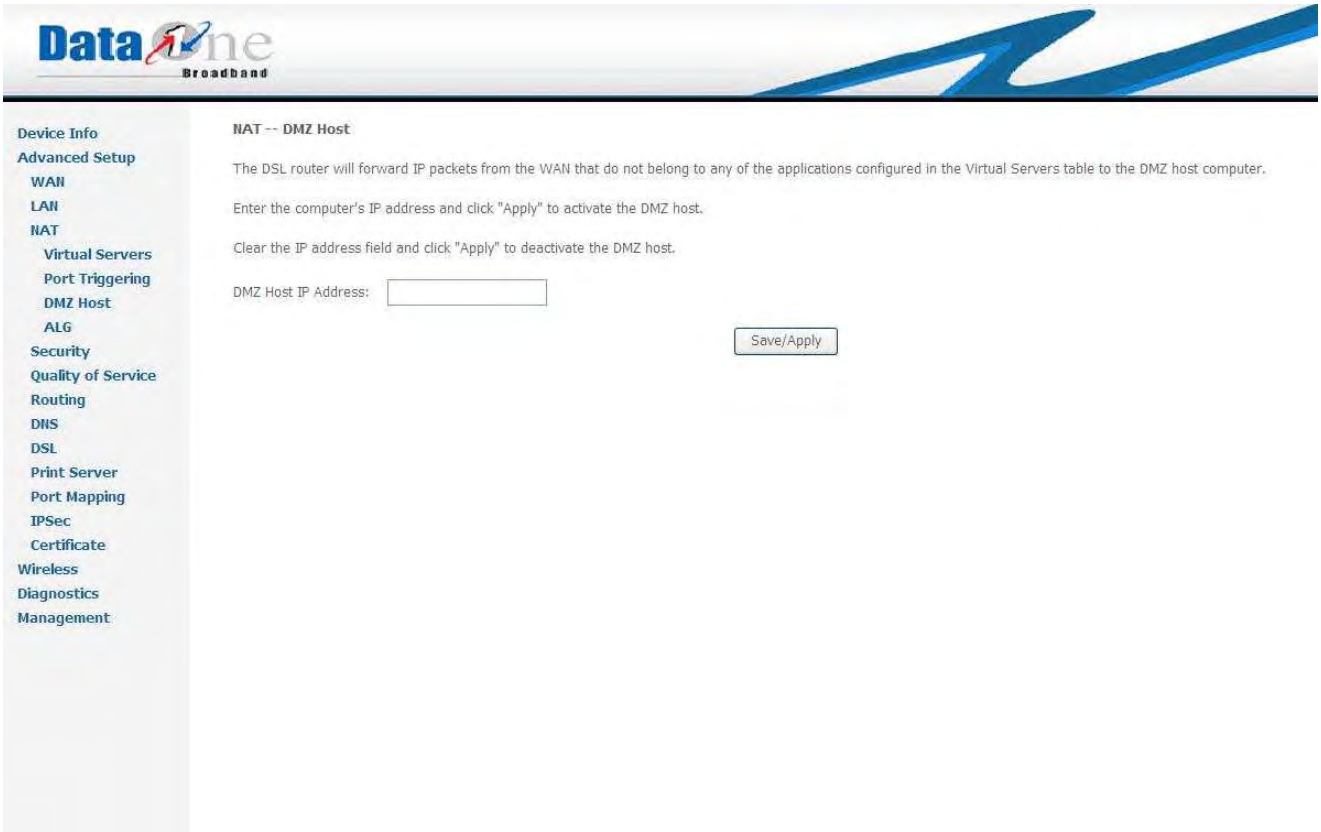


Figure 3.4.3.3 Advanced Setup – NAT— DMZ Host

3. Advanced Setup – NAT— ALG

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

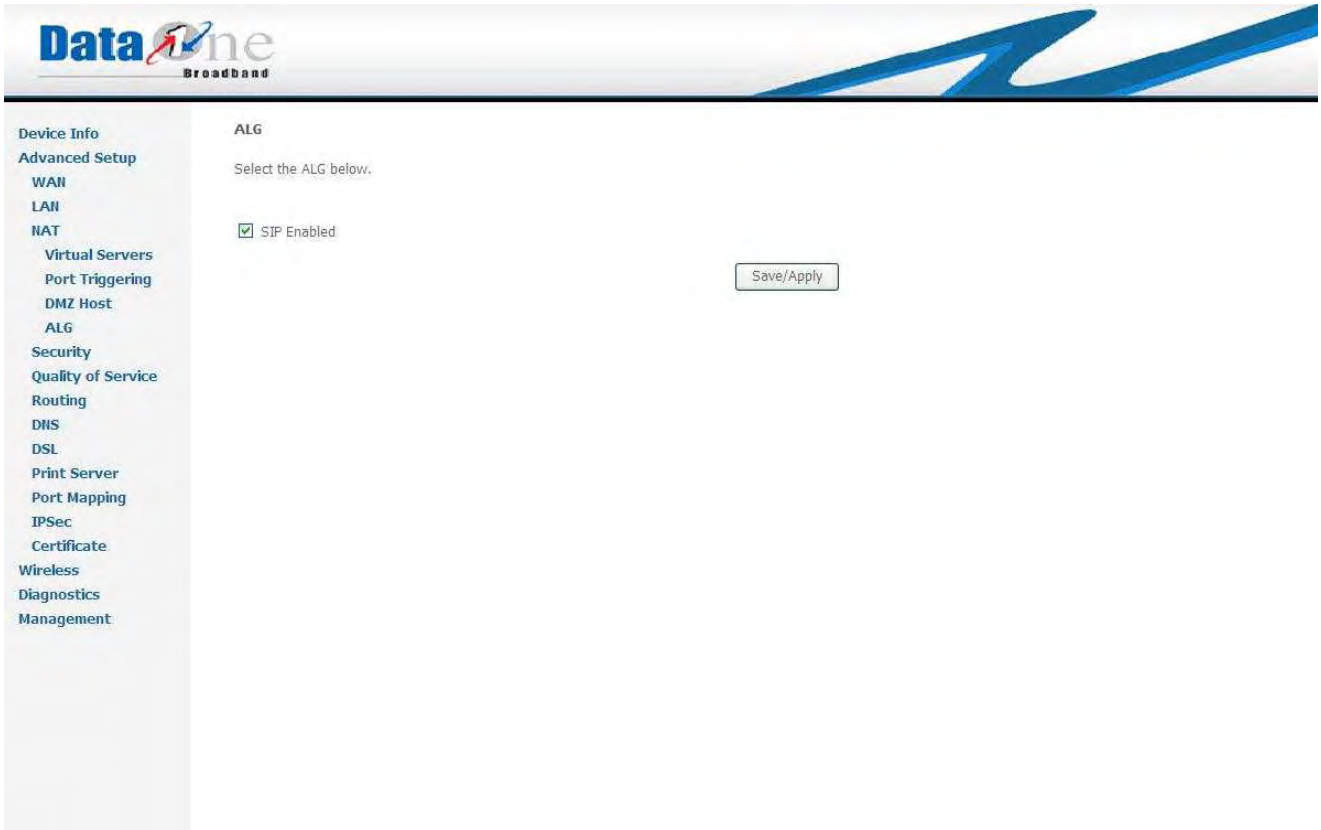


Figure 3.4.3.4 Advanced Setup – NAT— ALG

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:

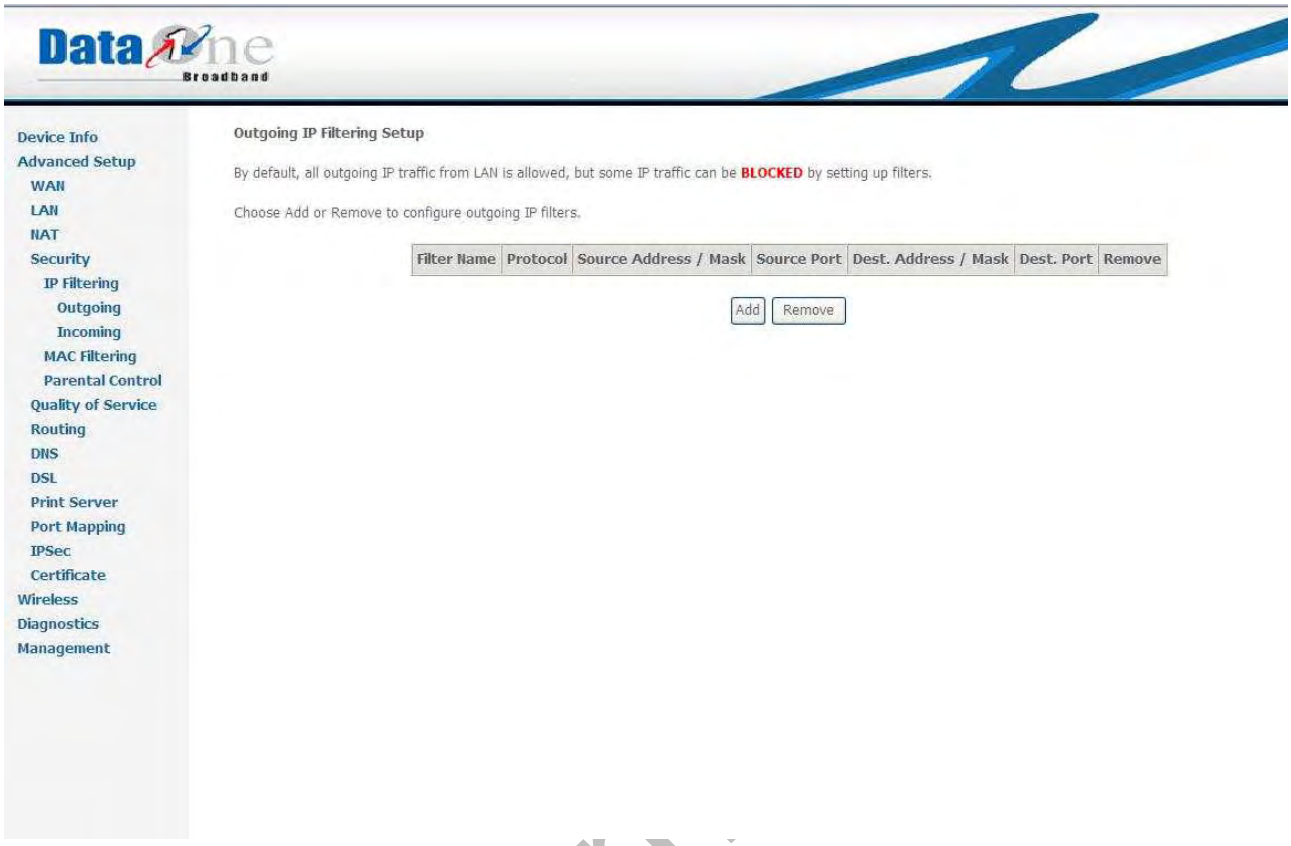
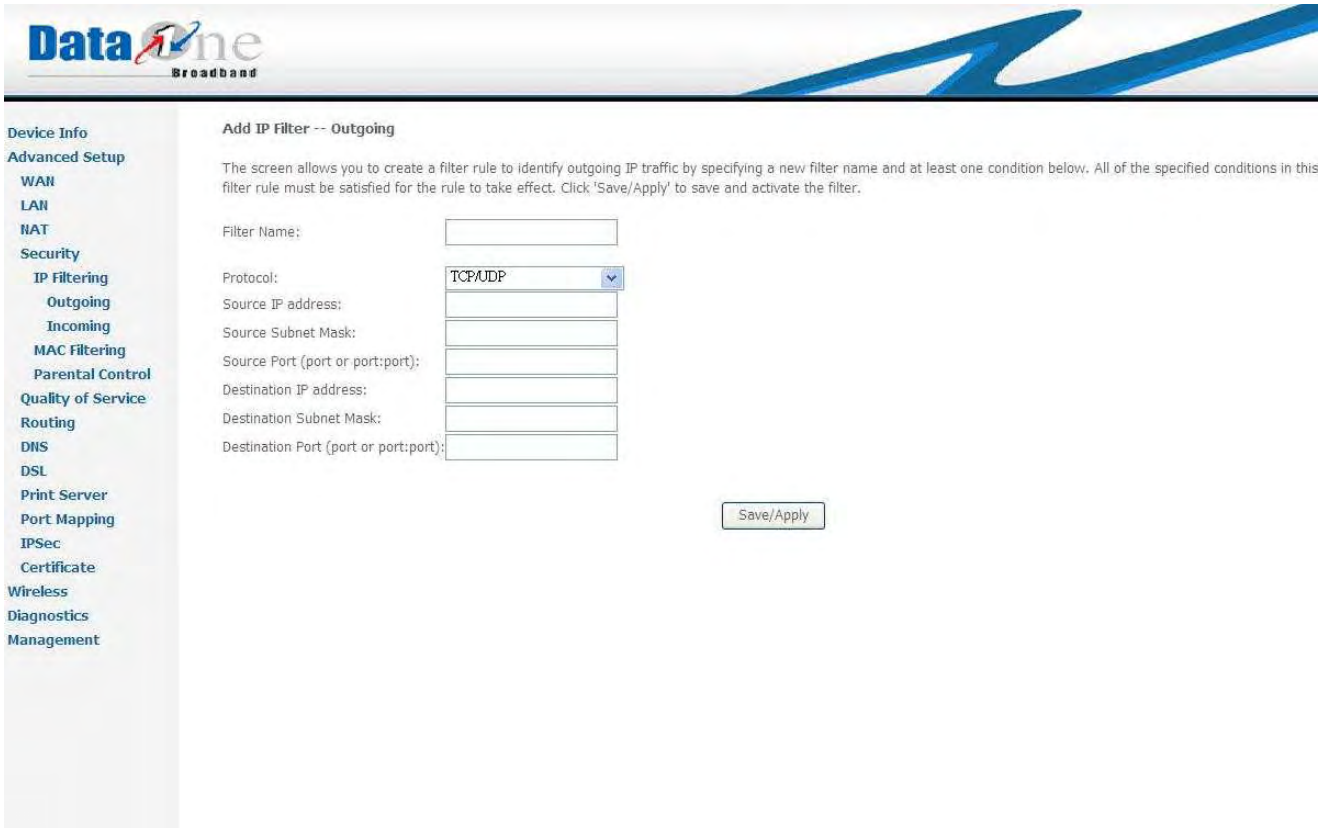


Figure **3.4.4.1.1.a Advanced Setup – Security – IP Filter -- Outgoing**

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.



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

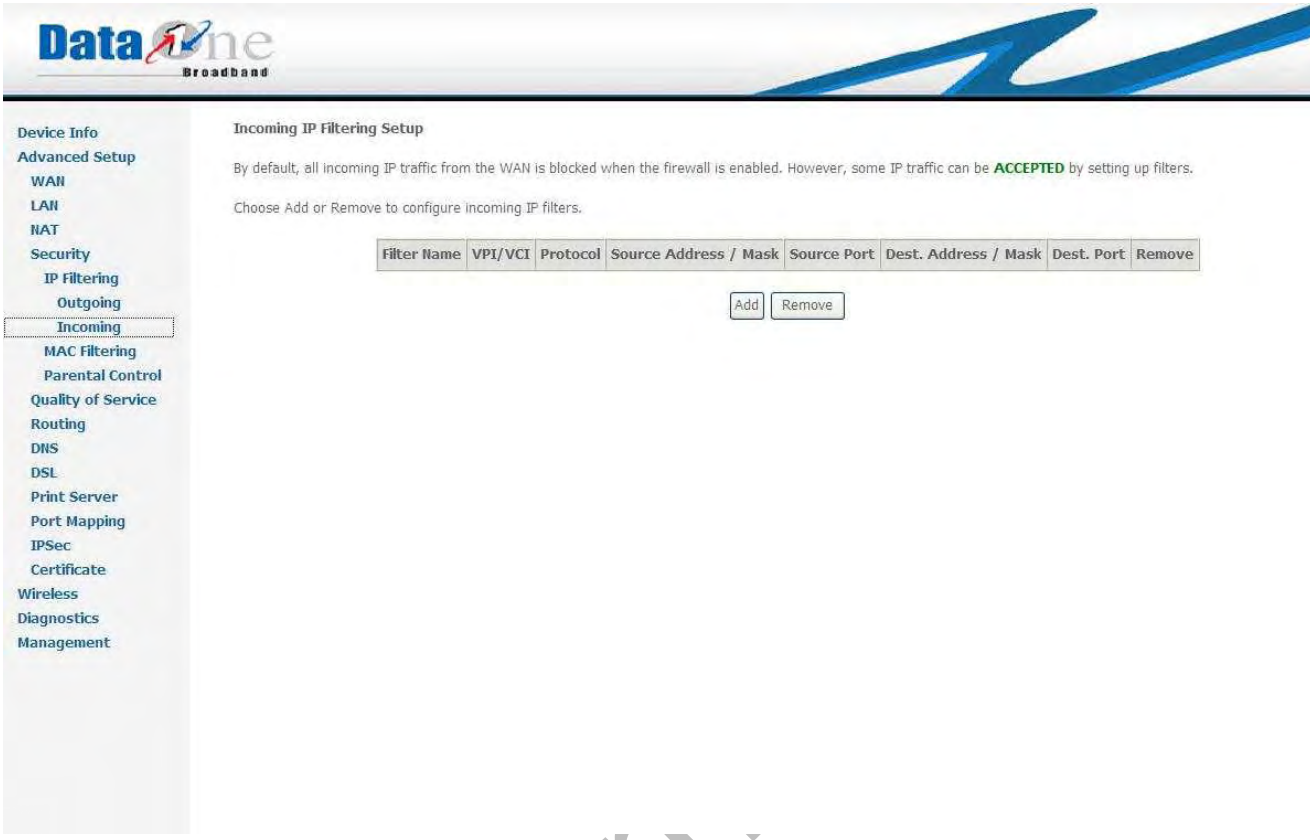


Figure **3.4.4.1.2.a Advanced Setup – Security –IP Filter – Incoming**

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.

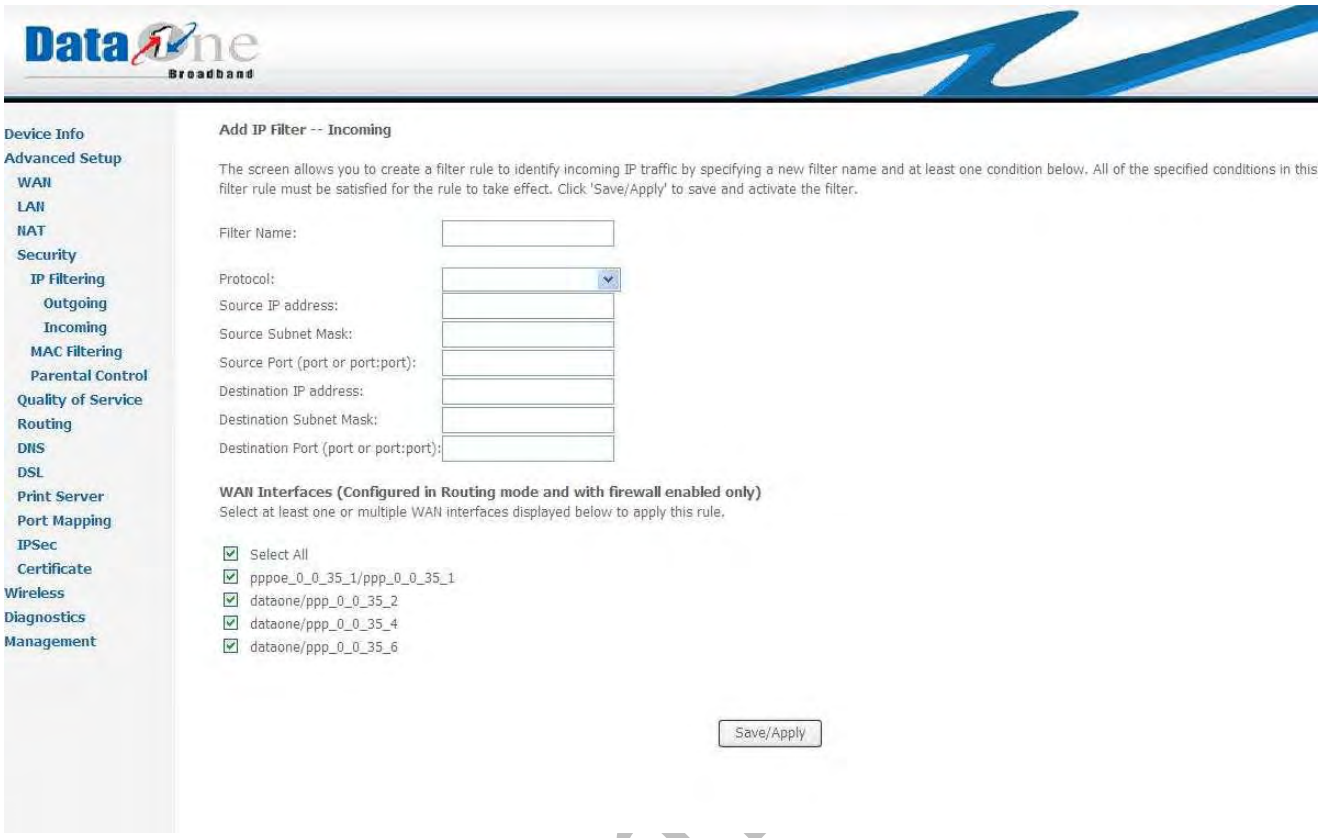


Figure **3.4.4.1.2.b Advanced Setup – Security –IP Filter – Add Incoming Rules**

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

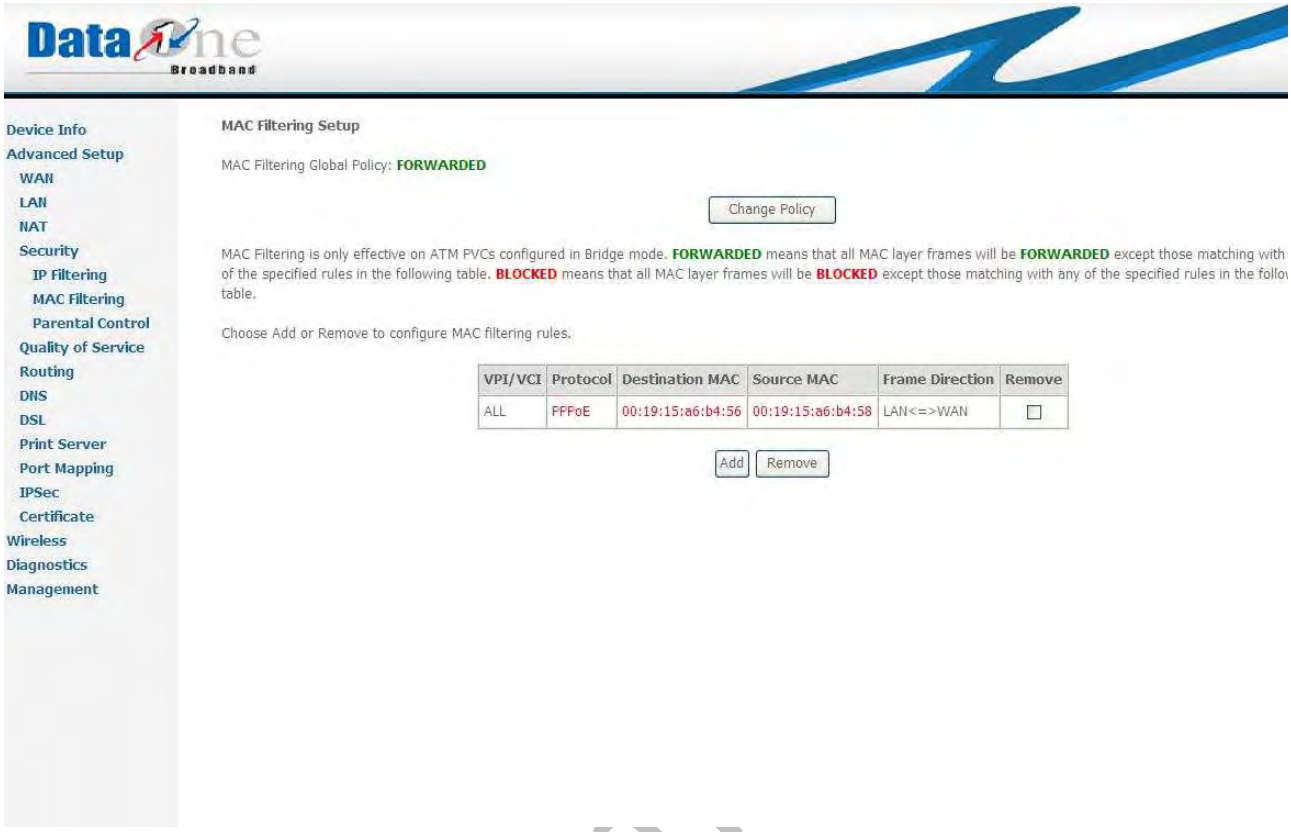


Figure 3.4.4.2.a Advanced Setup – Security – MAC Filter

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

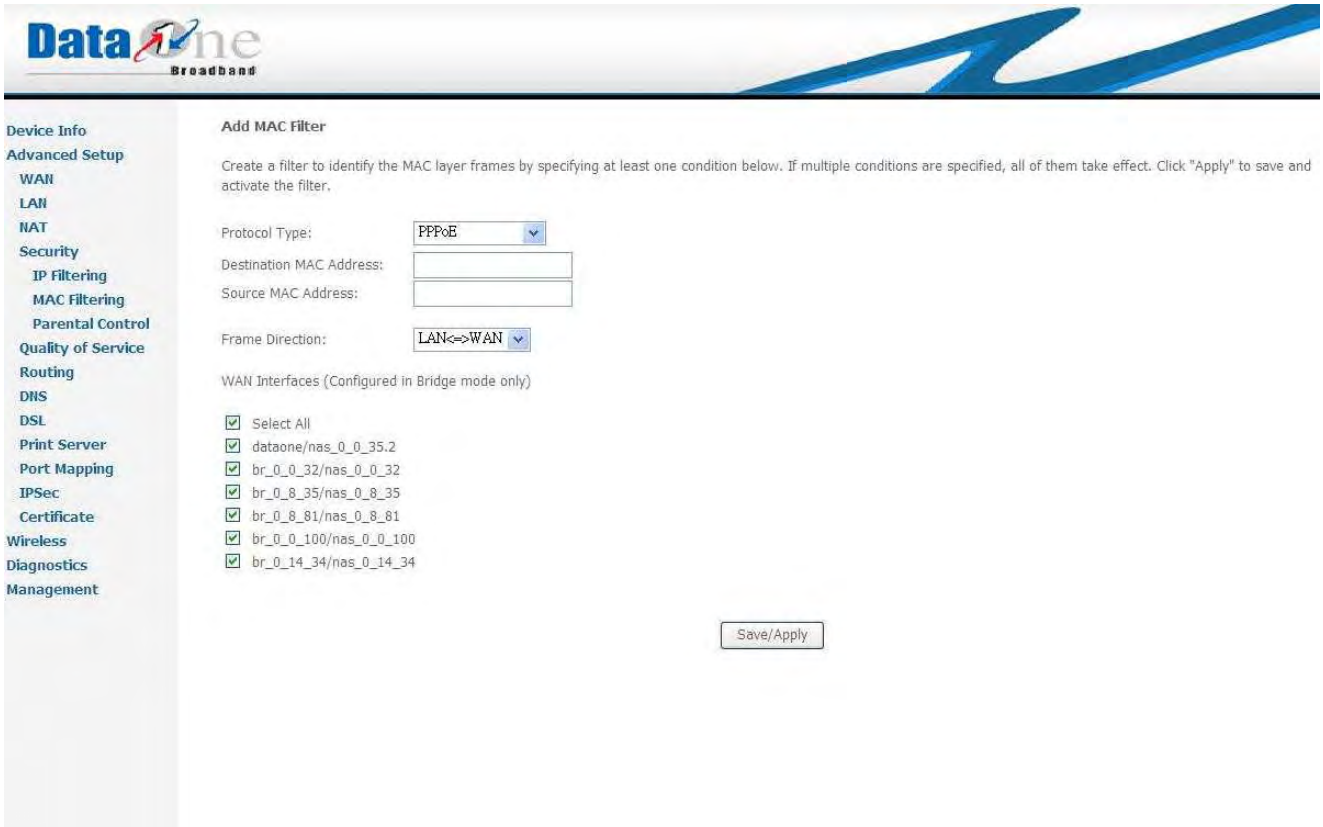


Figure 3.4.4.2.b Advanced Setup – Security – Add MAC Filter

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

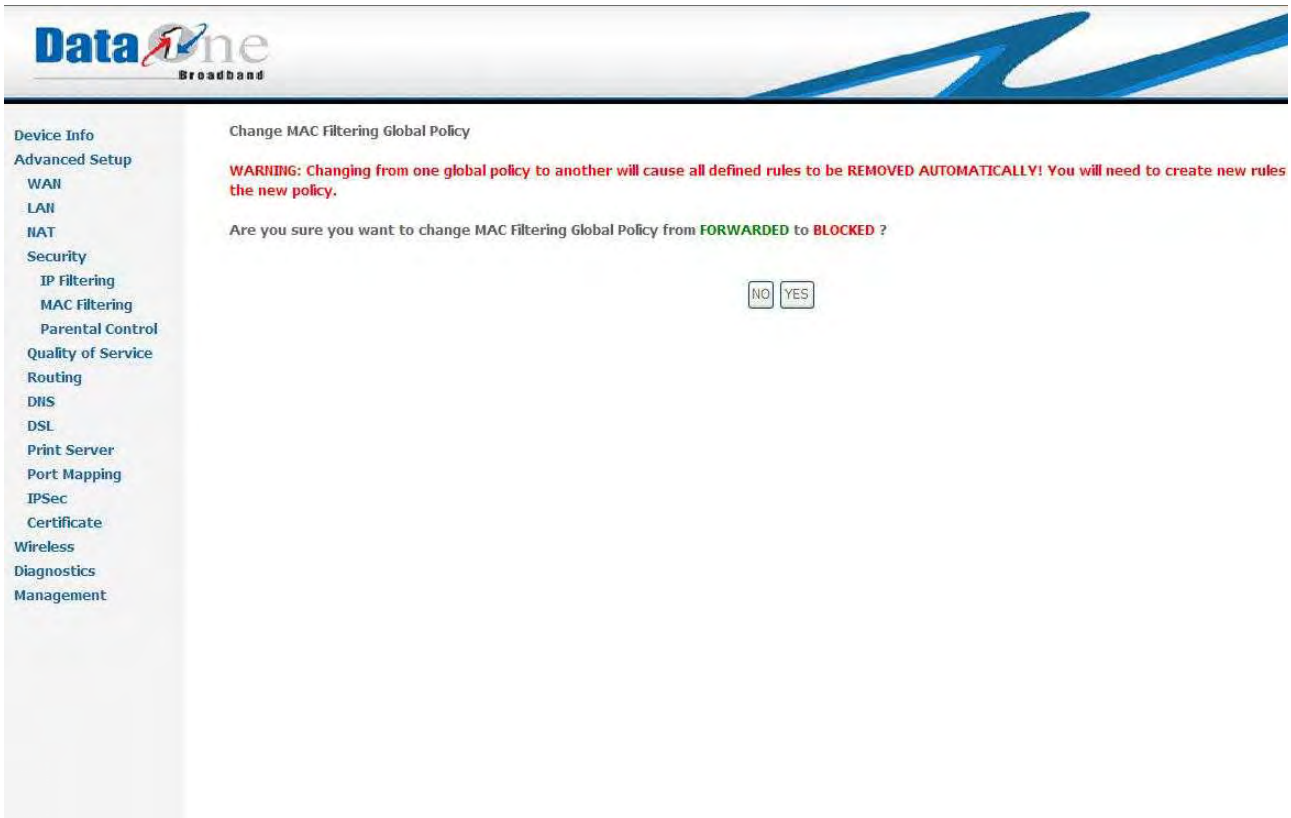


Figure 3.4.4.2.c Advanced Setup – Security – Clean MAC Filter Rules

3.4.4.3 Advanced Setup – Security – Parental Control

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

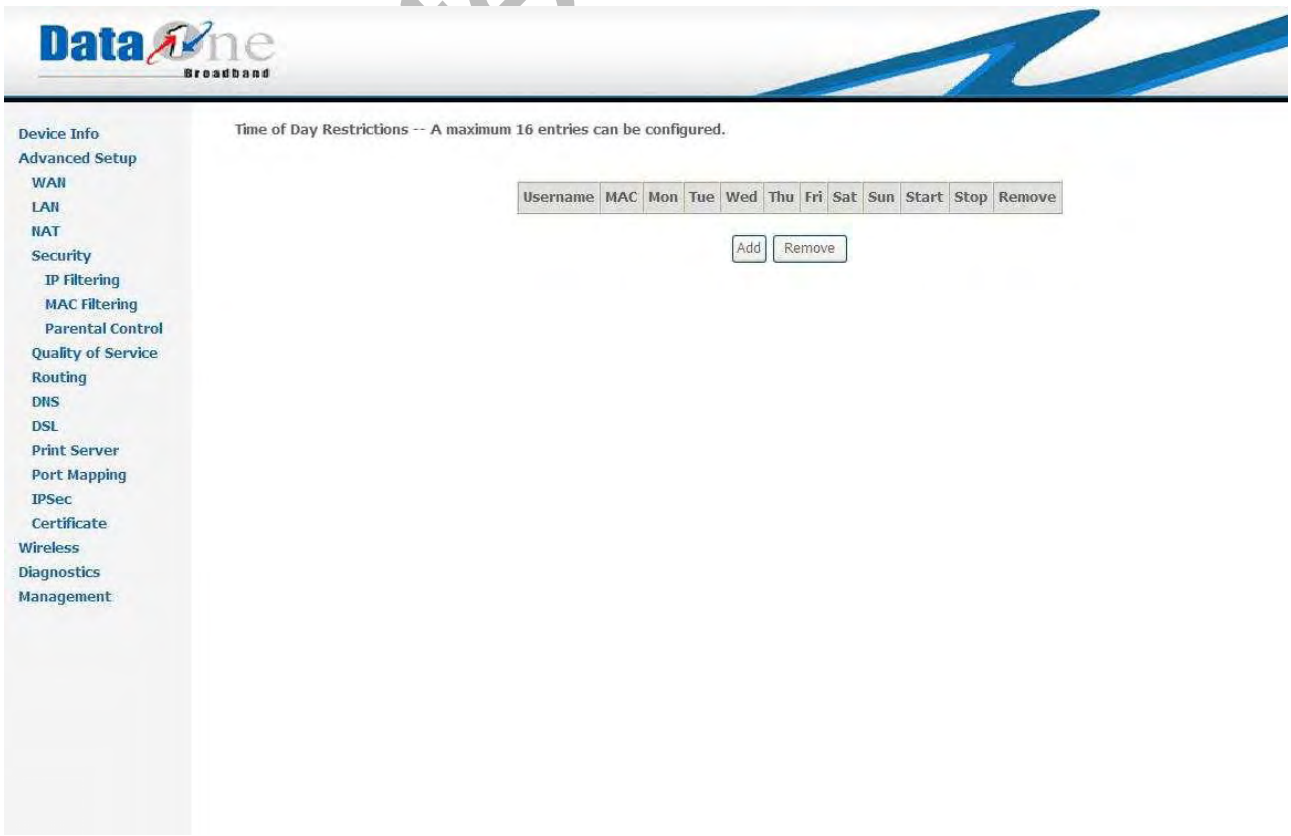


Figure 3.4.4.3.a Advanced Setup – Security – Parental Control

Click "***Add***" to set restriction rules as following:

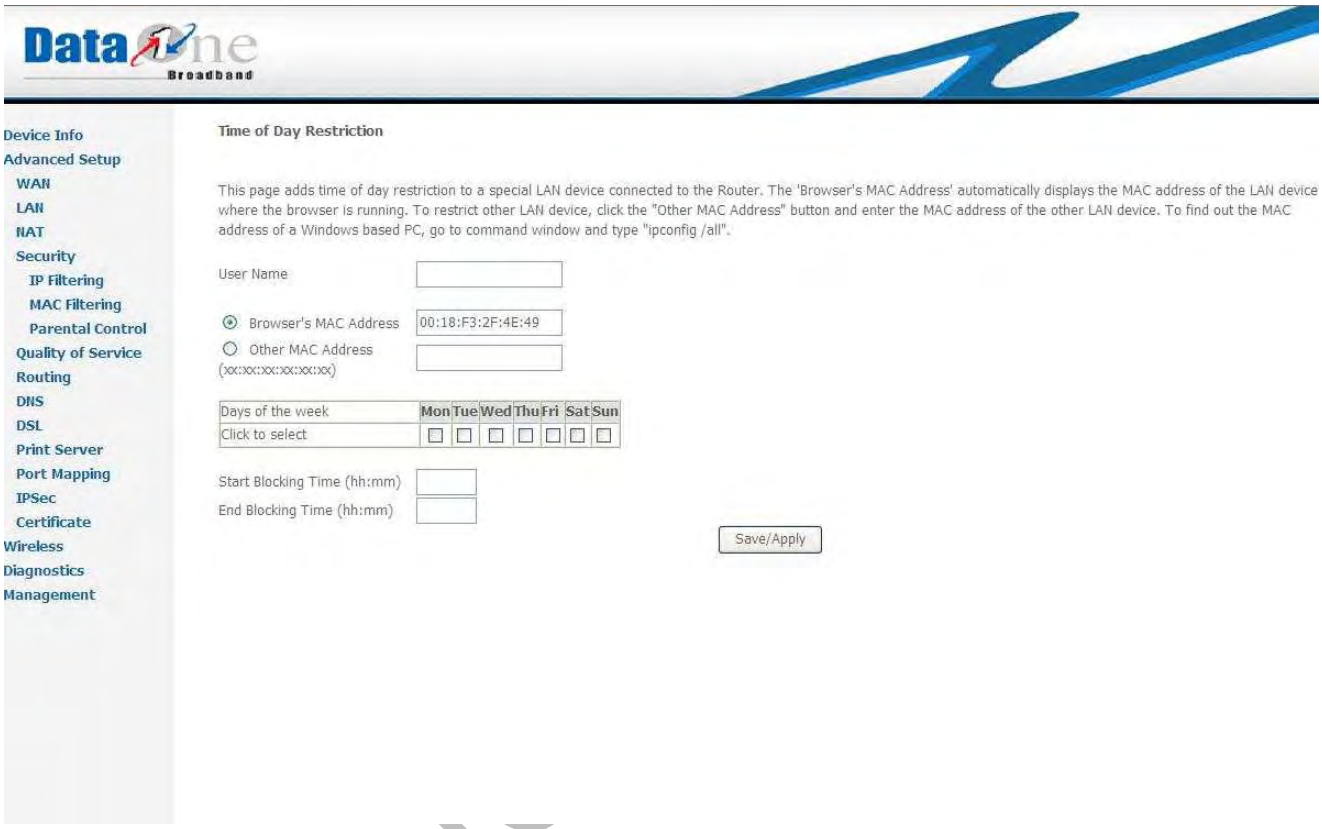


Figure 3.4.4.3.b Advanced Setup – Security – Parental Control – Add Restrictions

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.

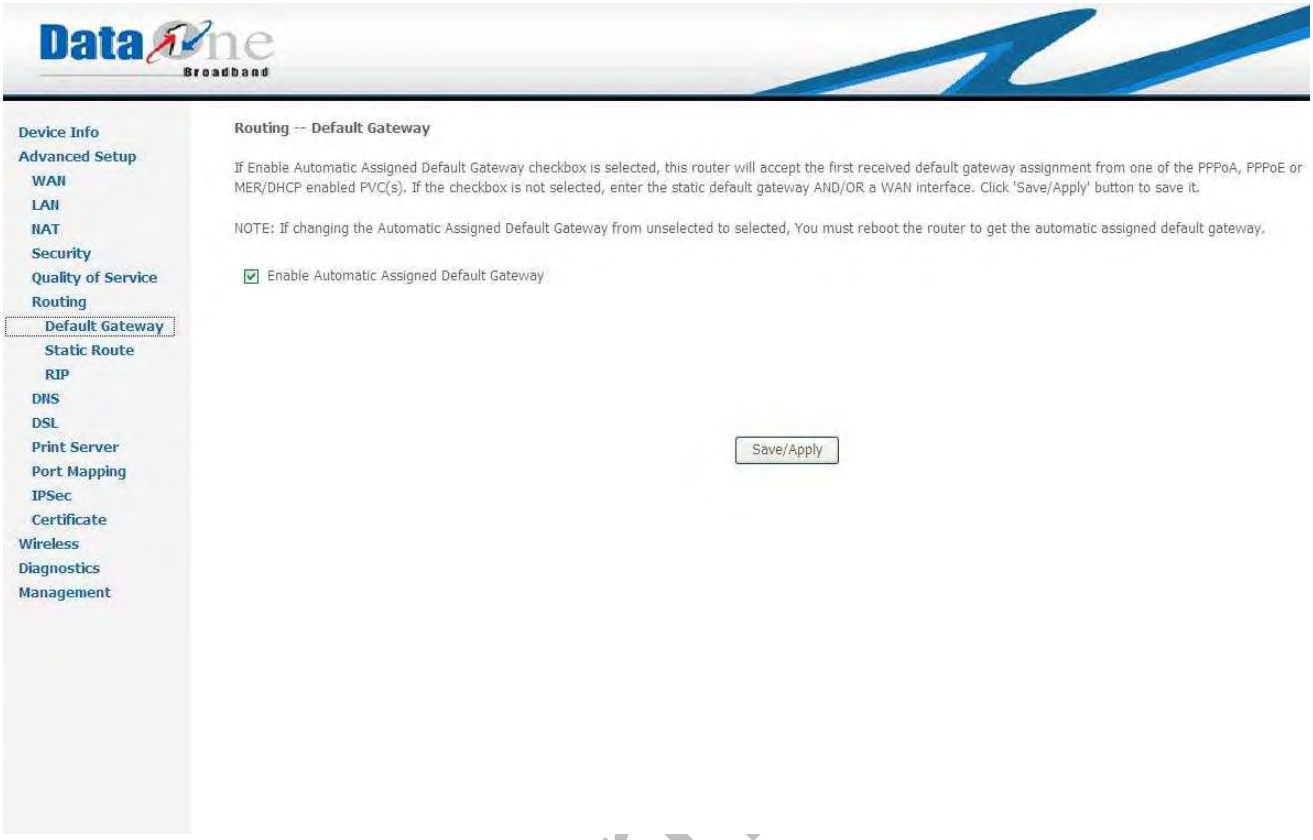


Figure 3.4.6.1 Advanced Setup – Routing – Default Gateway

3.4.6.2 Advanced Setup – Routing – Static Route

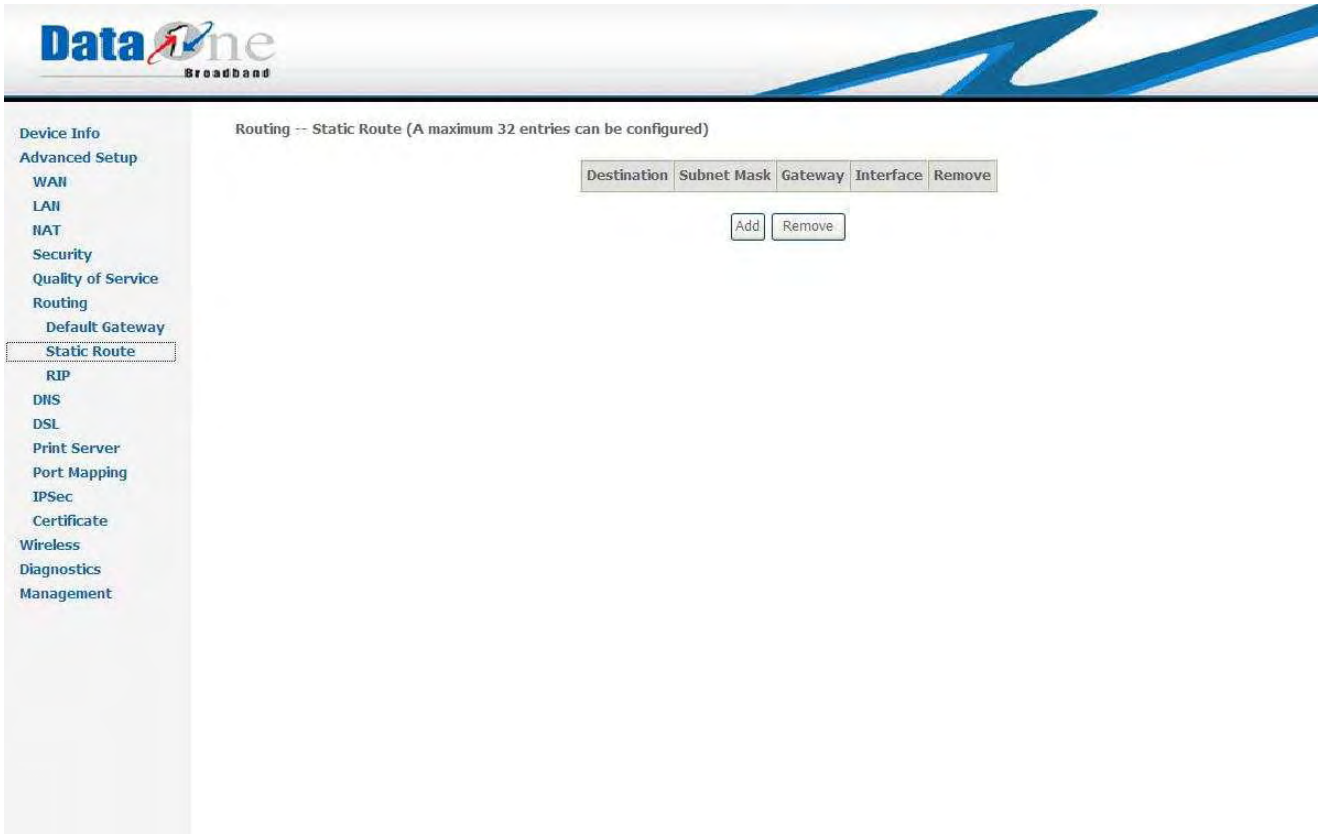


Figure 3.4.6.2.a Advanced Setup – Routing –Static Route

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

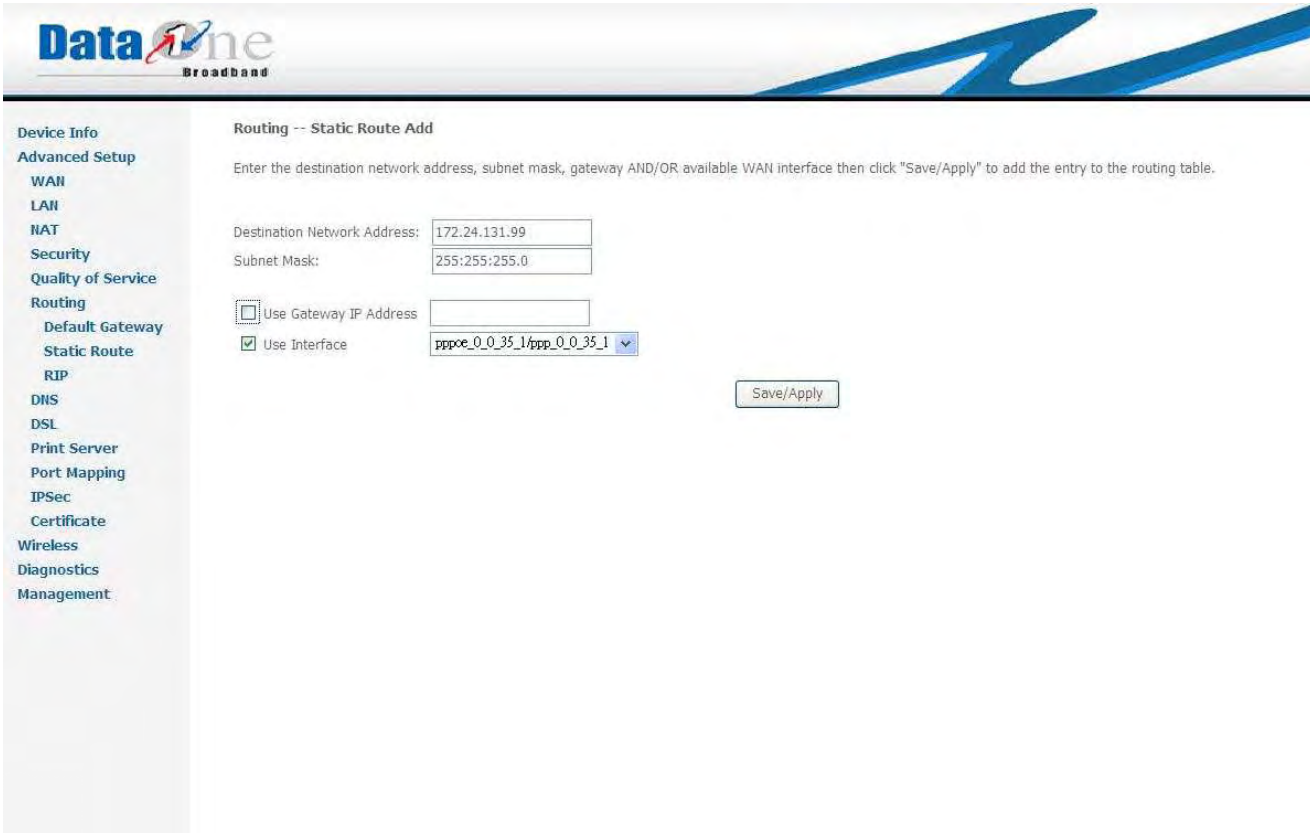


Figure 3.4.6.2.a Advanced Setup – Routing –Static Route

3.4.6.3 Advanced Setup – Routing – RIP

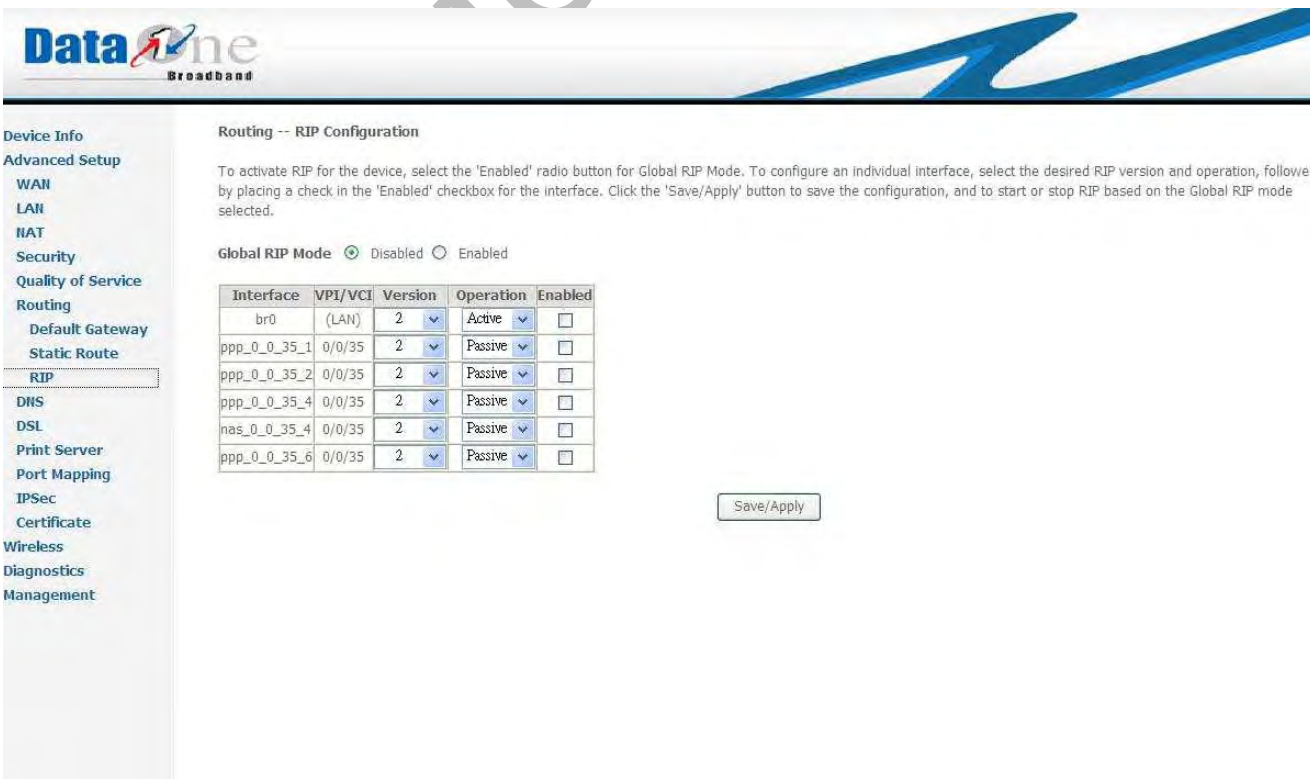


Figure 3.4.6.3 Advanced Setup – Routing –RIP

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

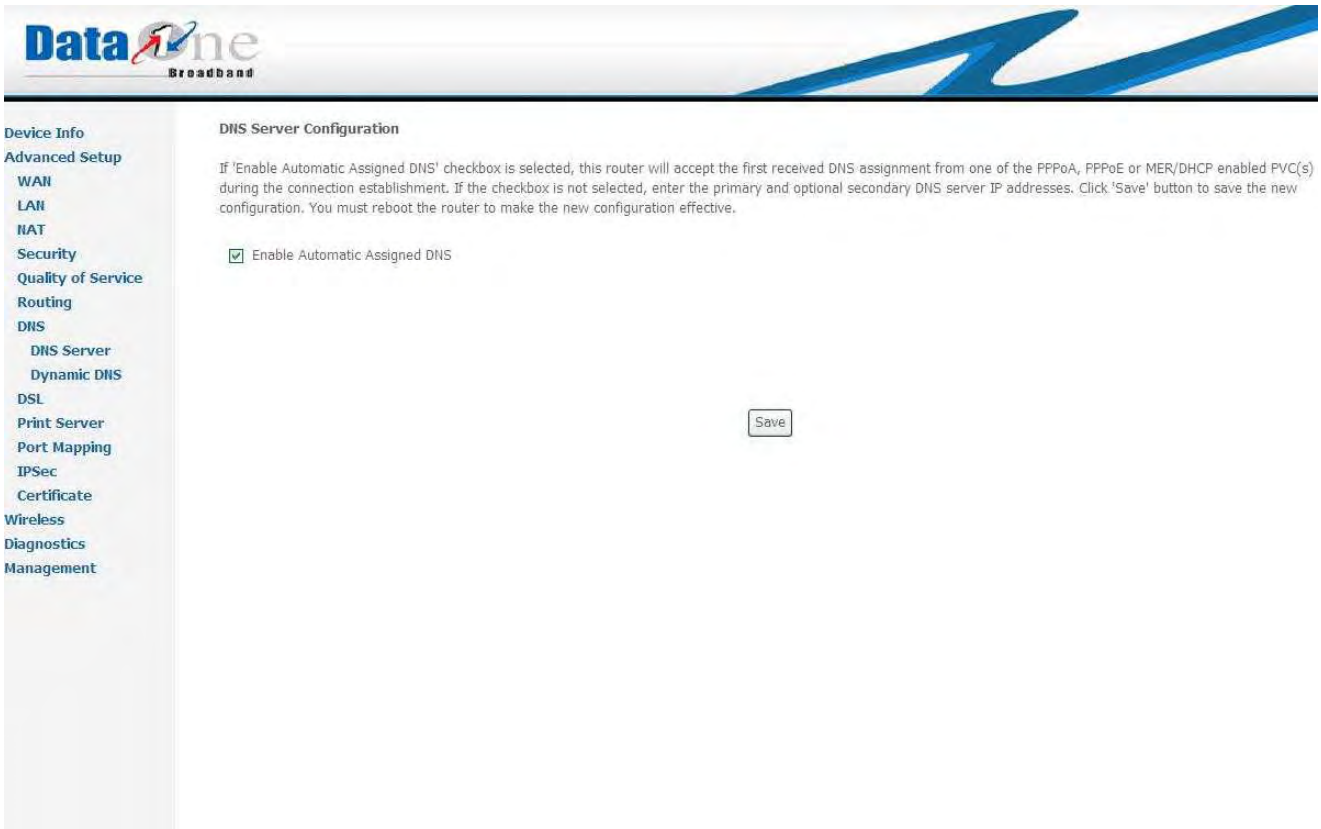


Figure 3.4.7.1 Advanced Setup –DNS – DNS Server

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.

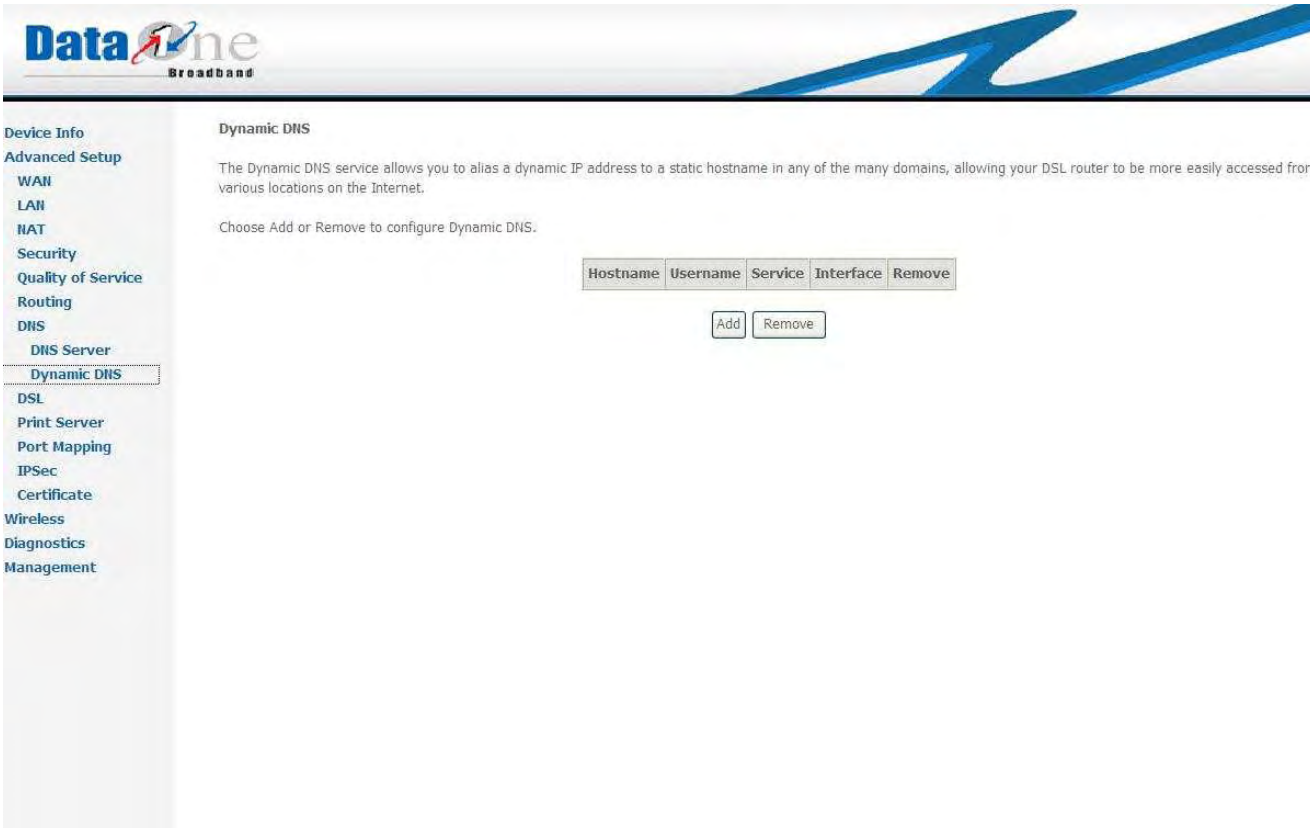


Figure 3.4.7.2.a Advanced Setup –DNS –Dynamic DNS

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

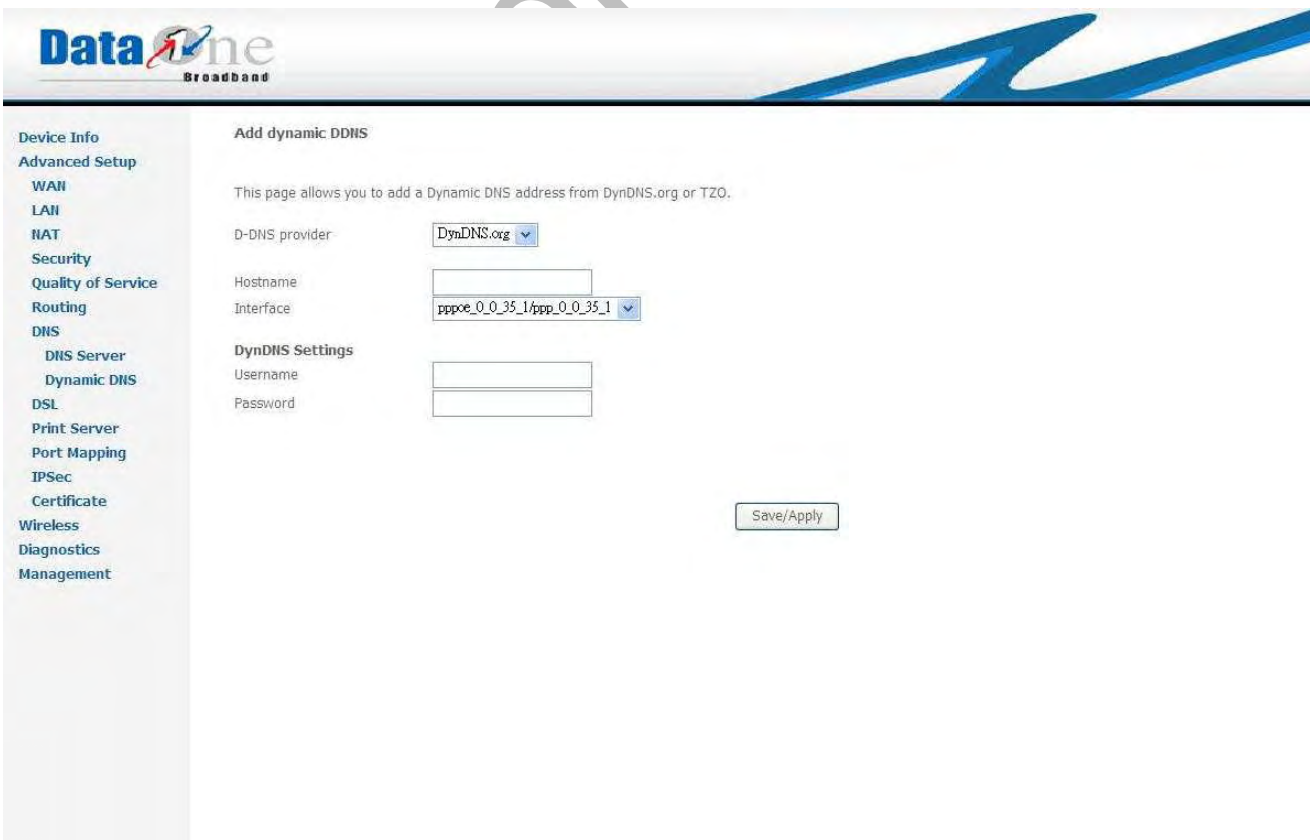


Figure 3.4.7.2.b Advanced Setup –DNS –Dynamic DNS

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

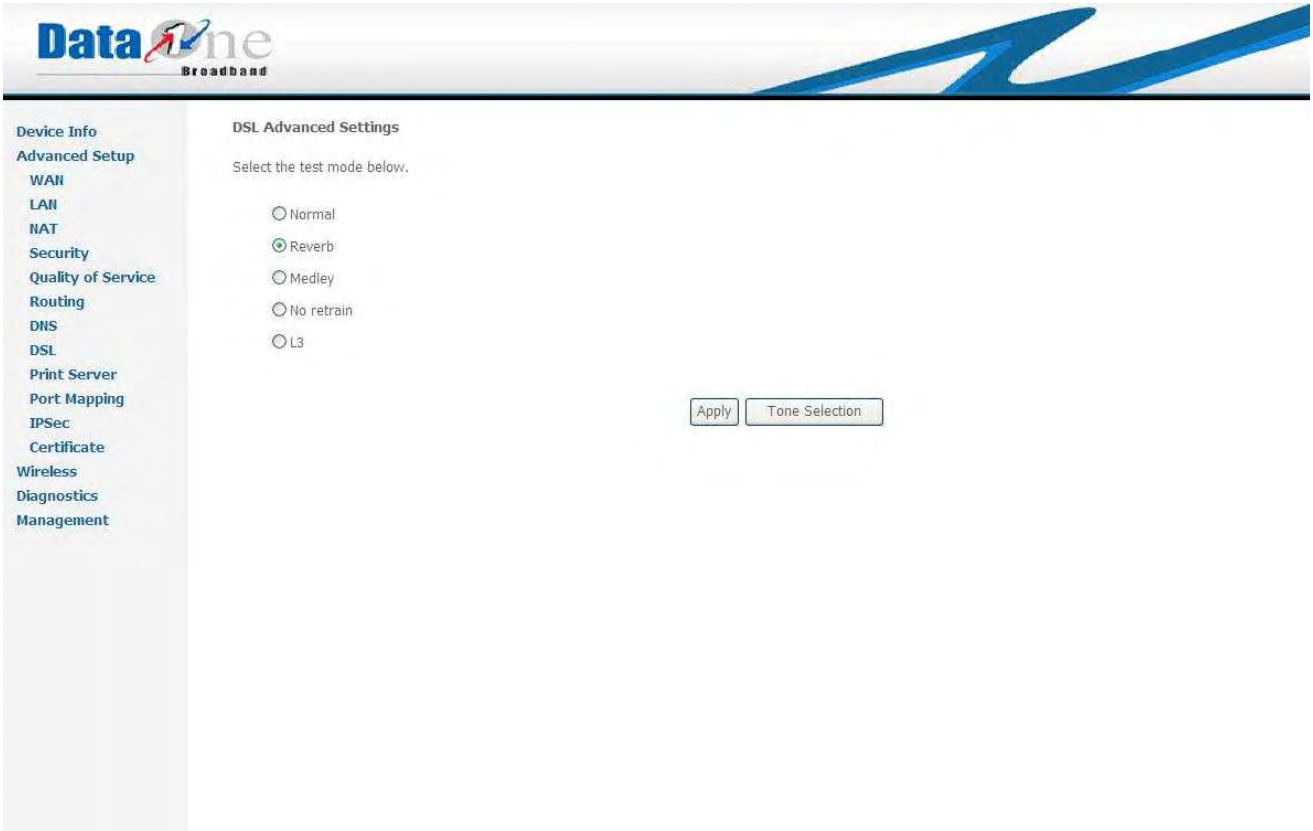


Figure 3.4.8.2 Advanced Setup – DSL Advanced Settings

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.

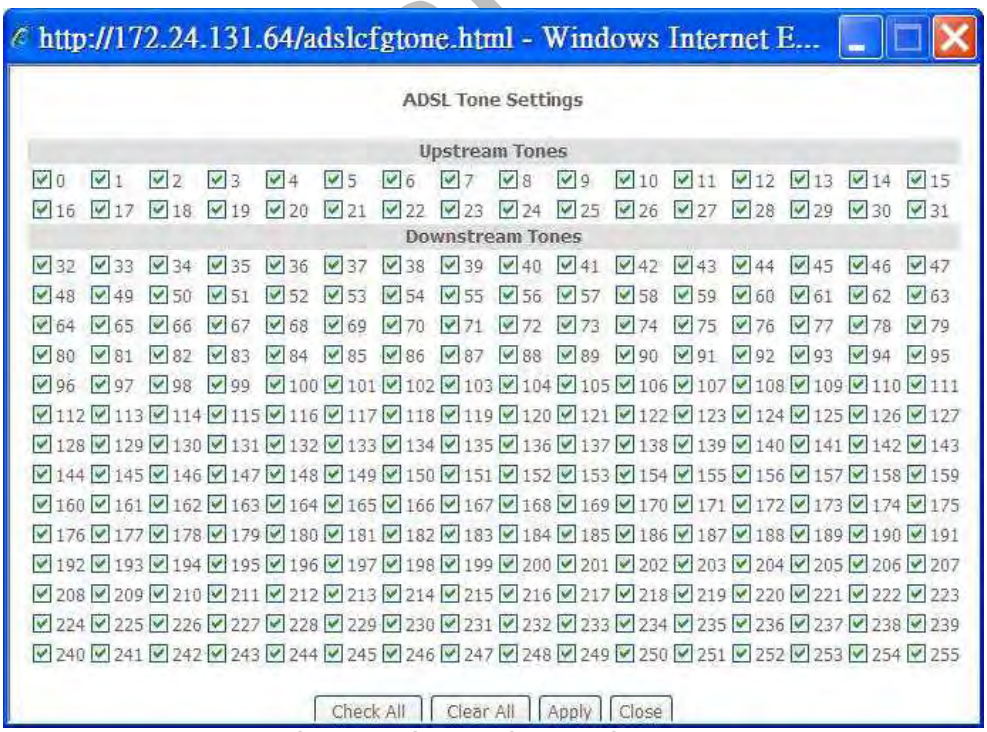


Figure 3.4.8.3 Advanced Setup – DSL -- ADSL Tone Settings

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.

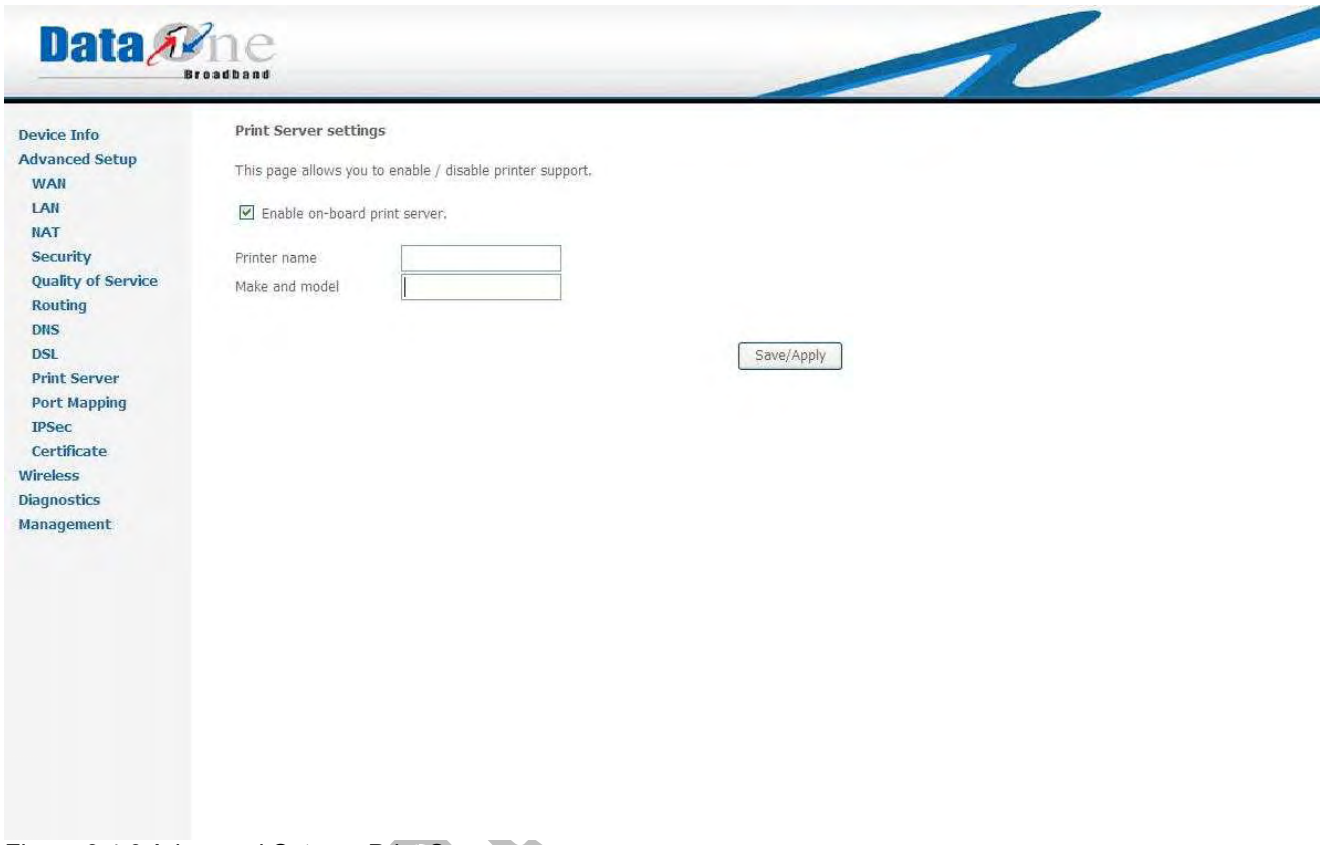


Figure 3.4.9 Advanced Setup – Print Server

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.

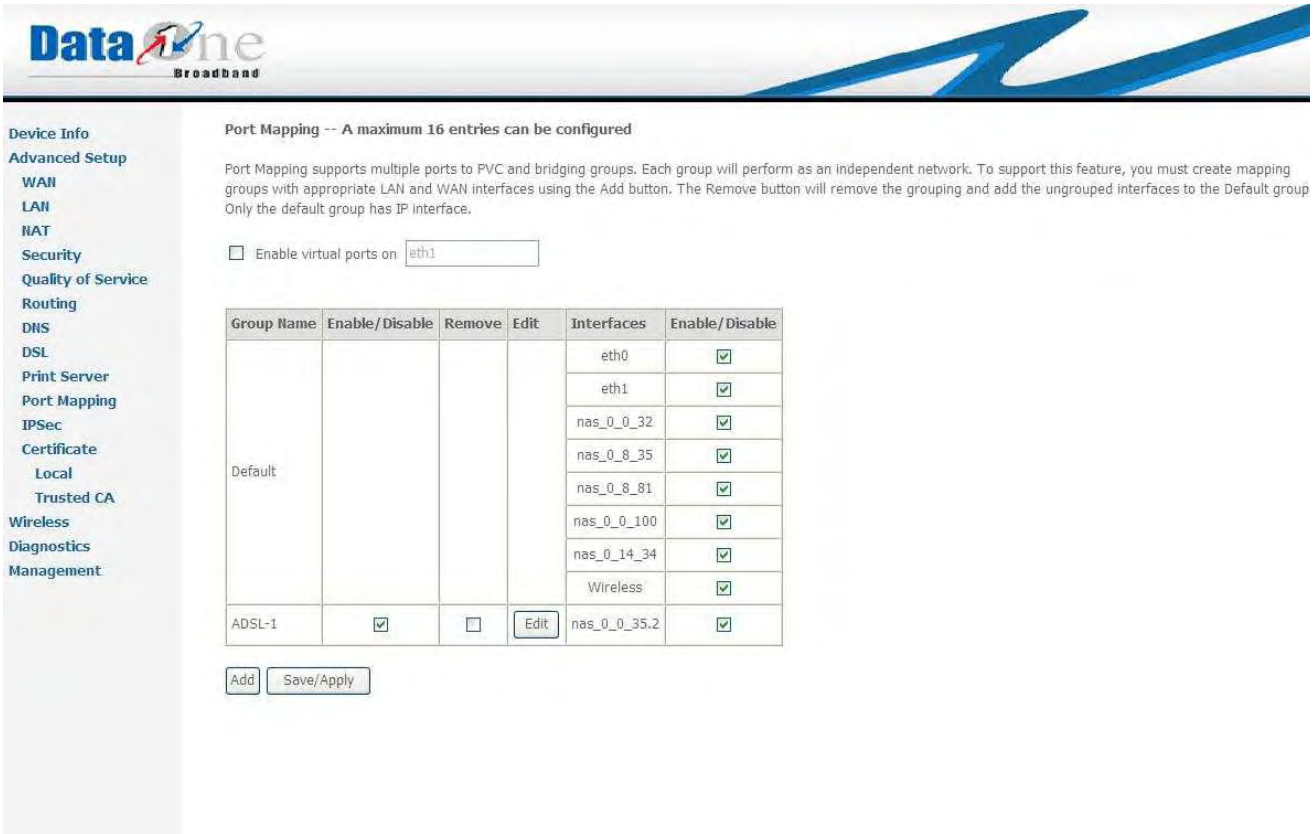


Figure 3.4.10.a Advanced Setup – Port Mapping

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.

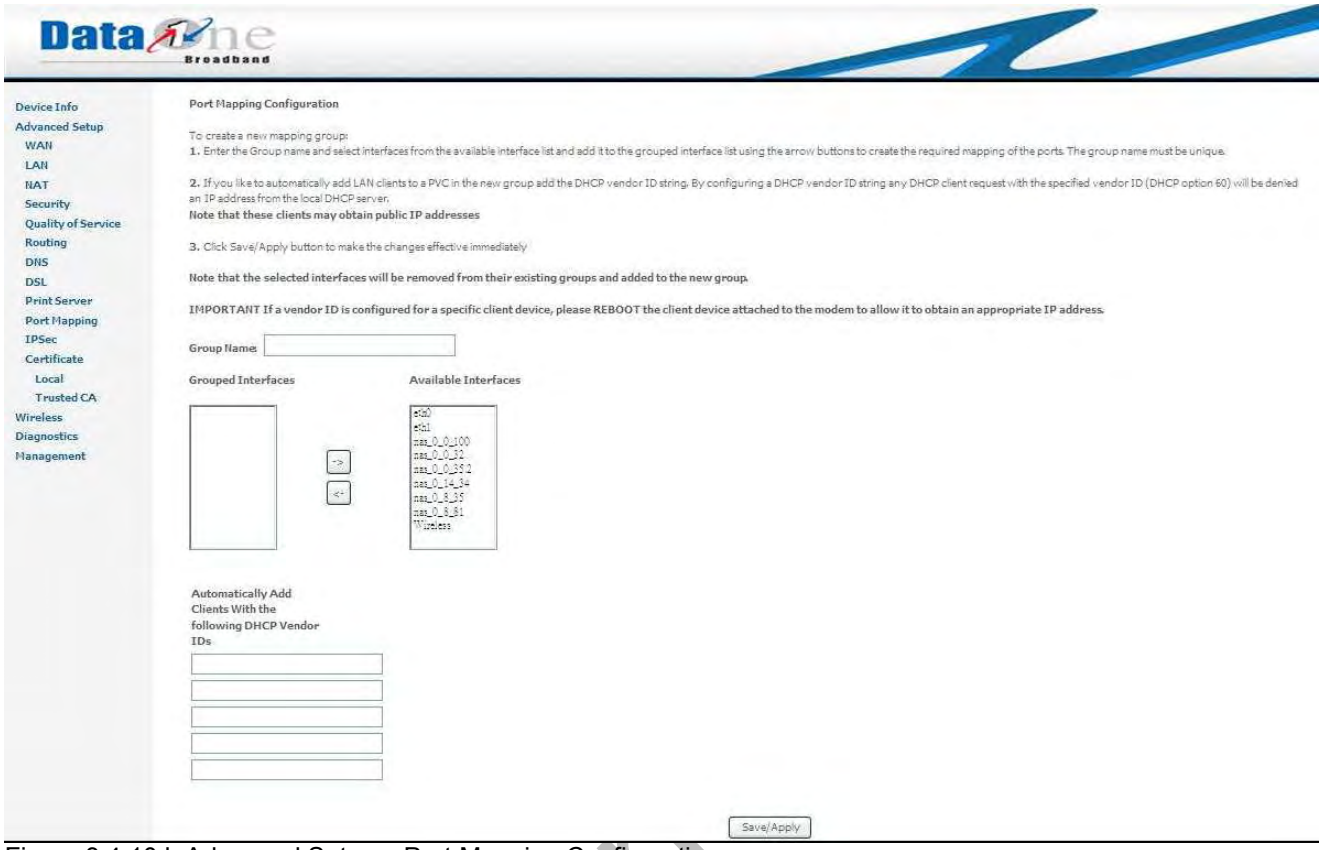


Figure 3.4.10.b Advanced Setup – Port Mapping Configuration.

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***"

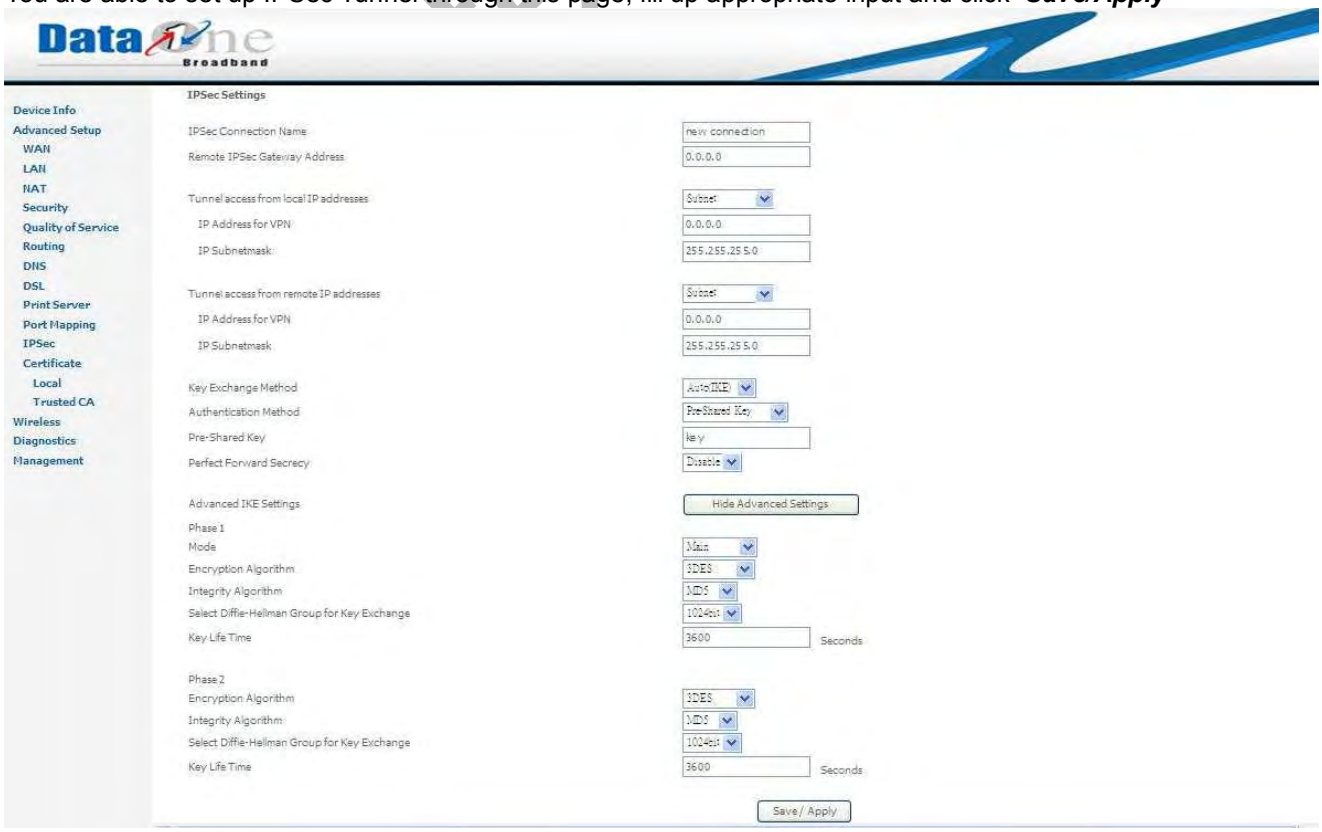
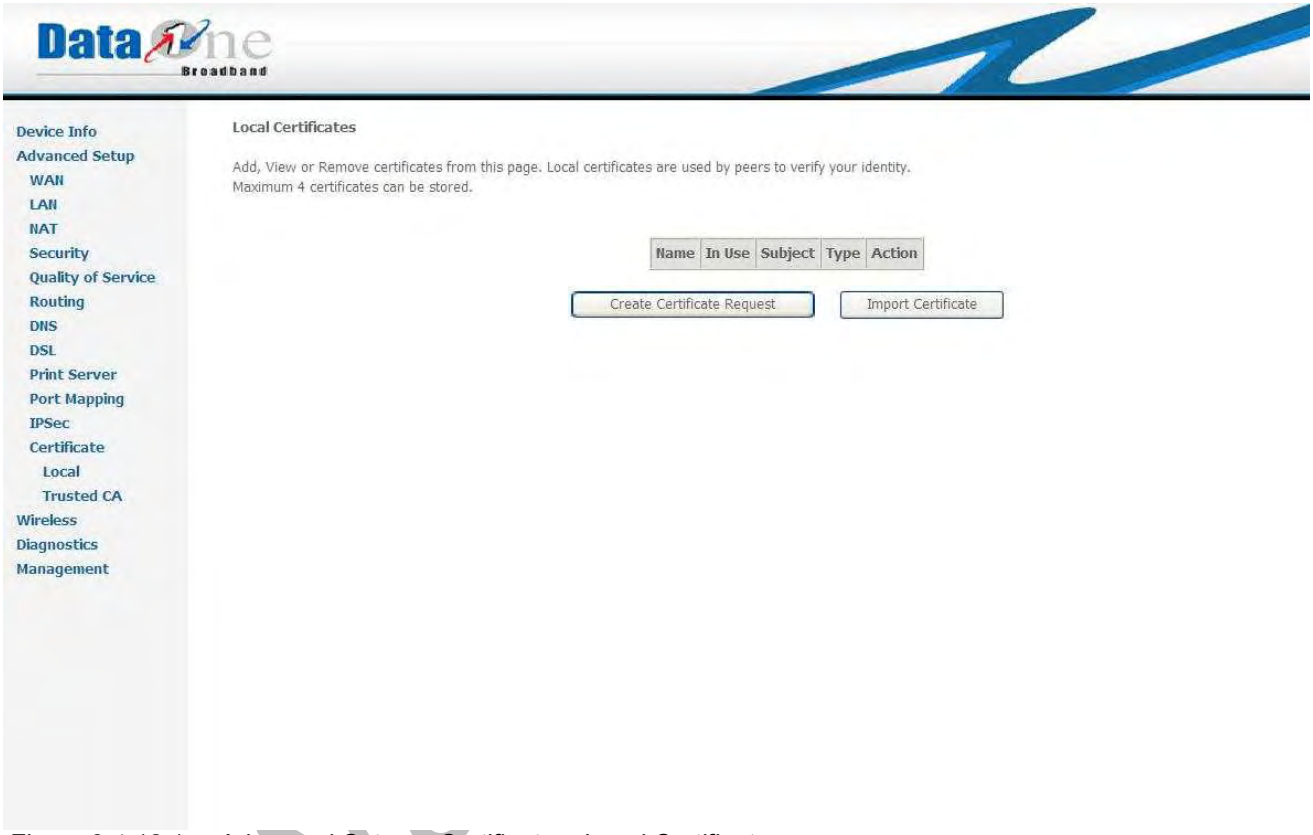


Figure 3.4.11 Advanced Setup – IPsec

3.4.12 Advanced Setup – Certificate

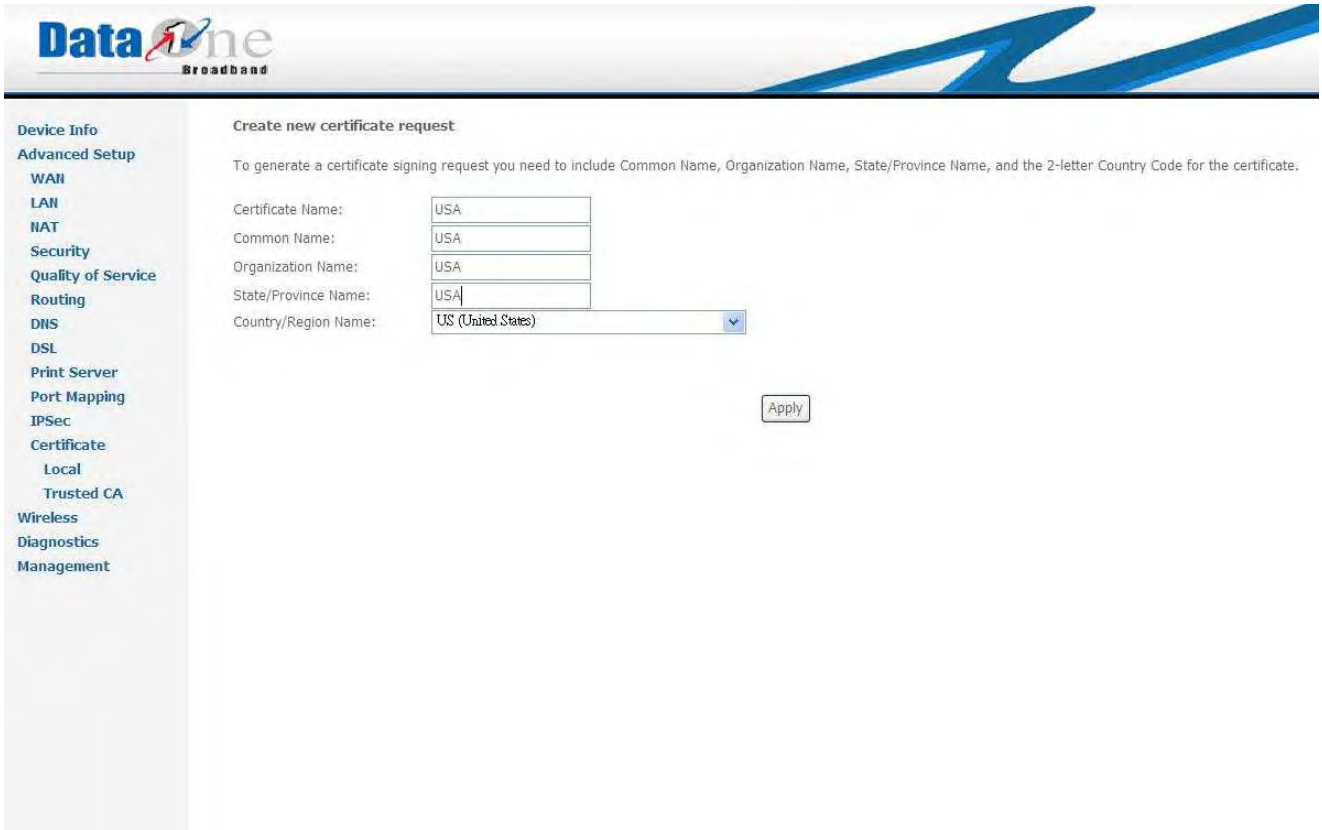
3.4.12.1 Advanced Setup – Certificate – Local Certificates

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.



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:

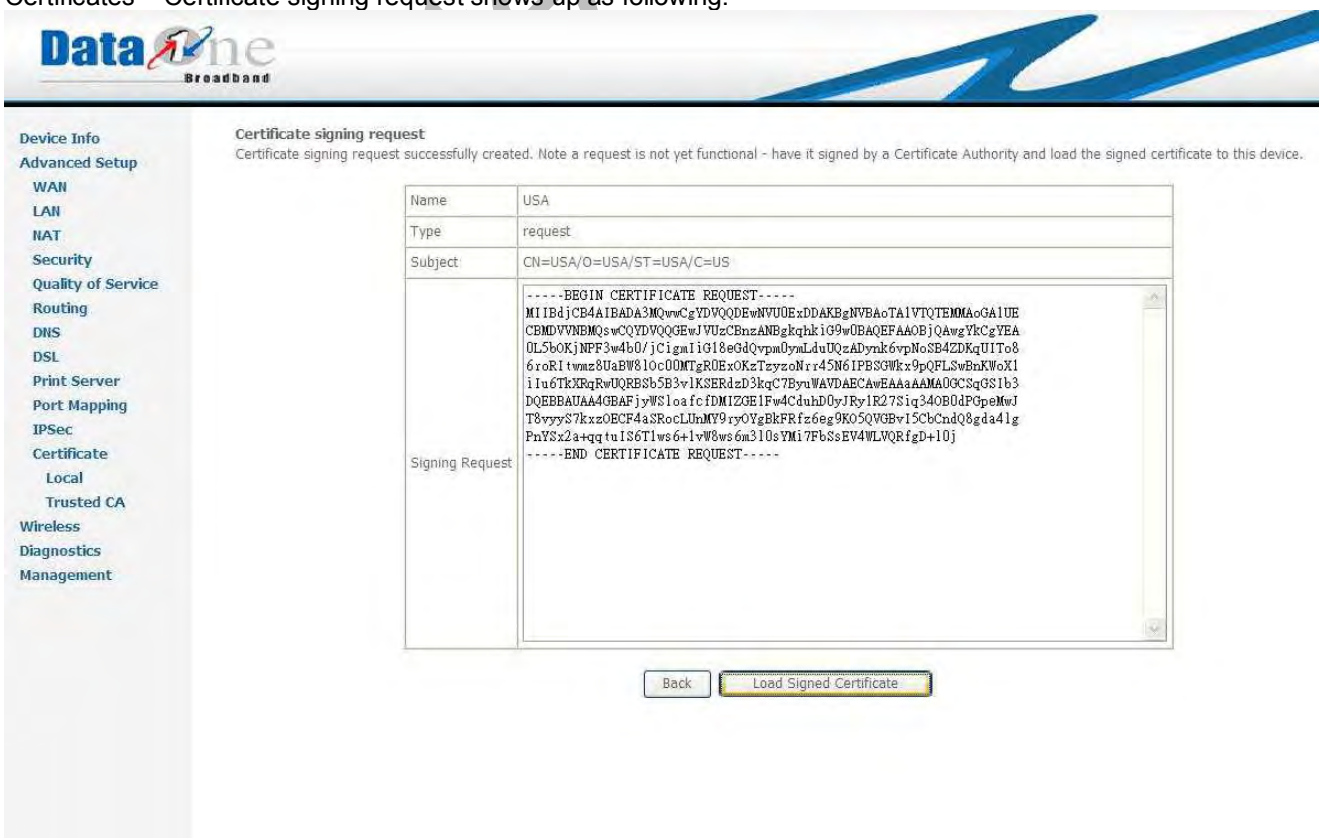


Figure 3.4.12.1.c Advanced Setup – Certificate – Local Certificates – Certificate signing request shows

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

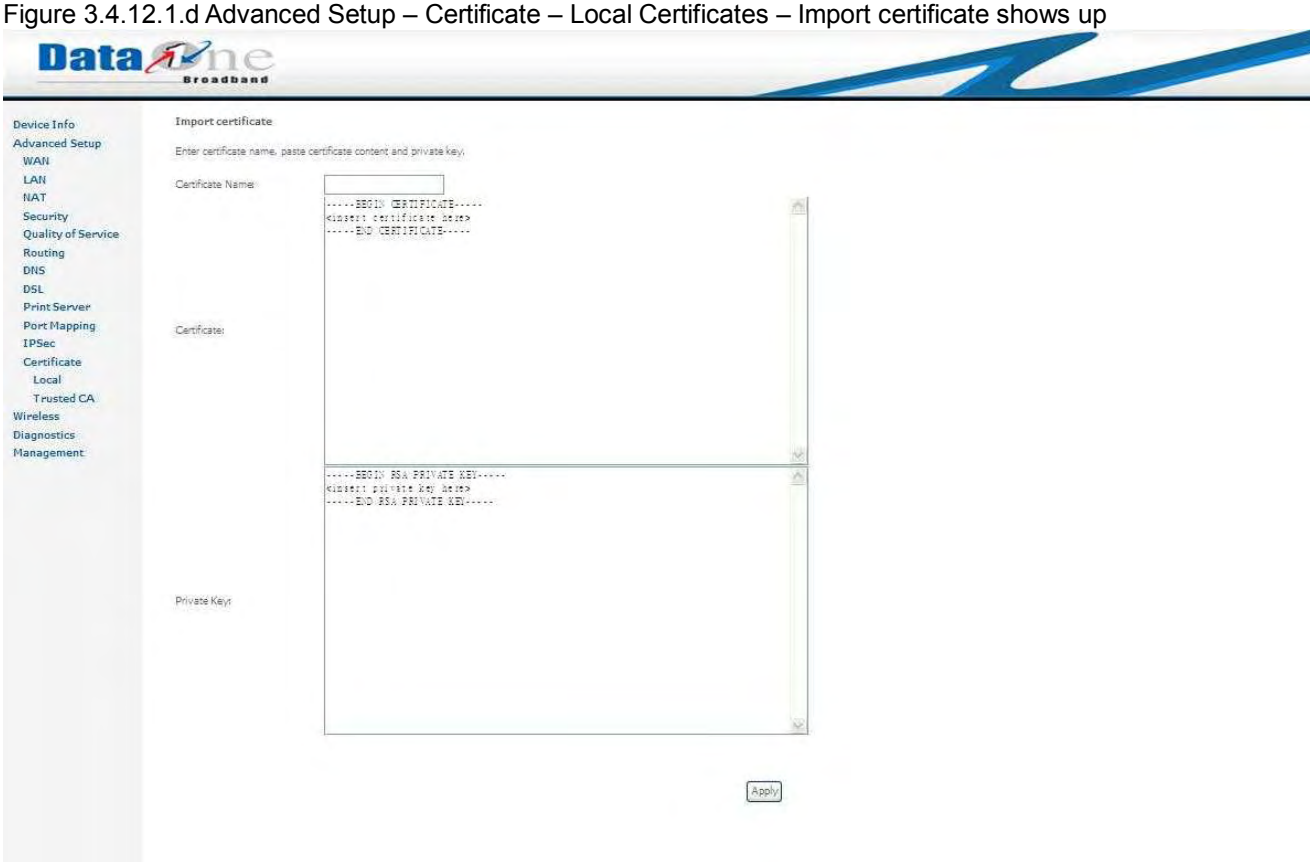
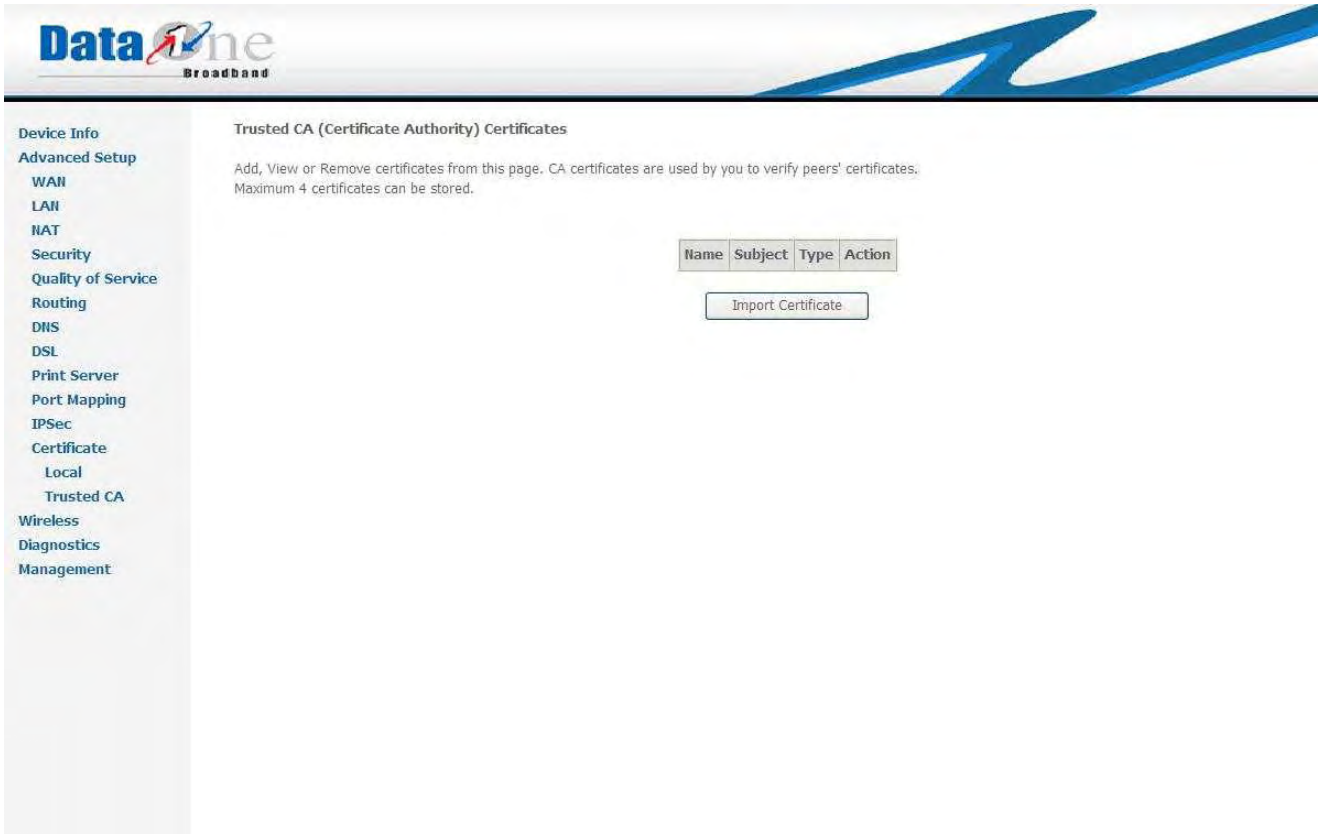


Figure 3.4.12.1.d Advanced Setup – Certificate – Local Certificates – Import certificate

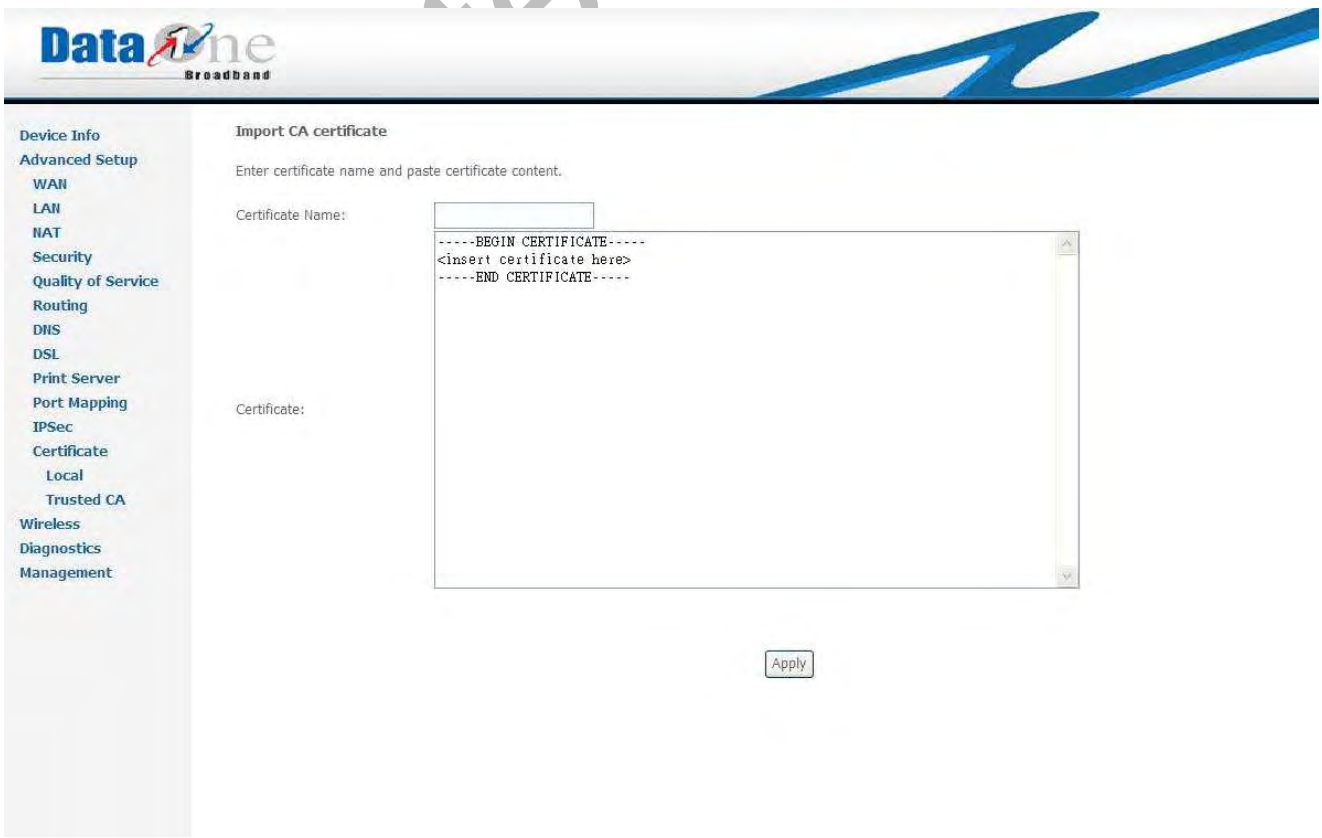
3.4.12.2 Advanced Setup – Certificate – Trusted CA

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



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.



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.

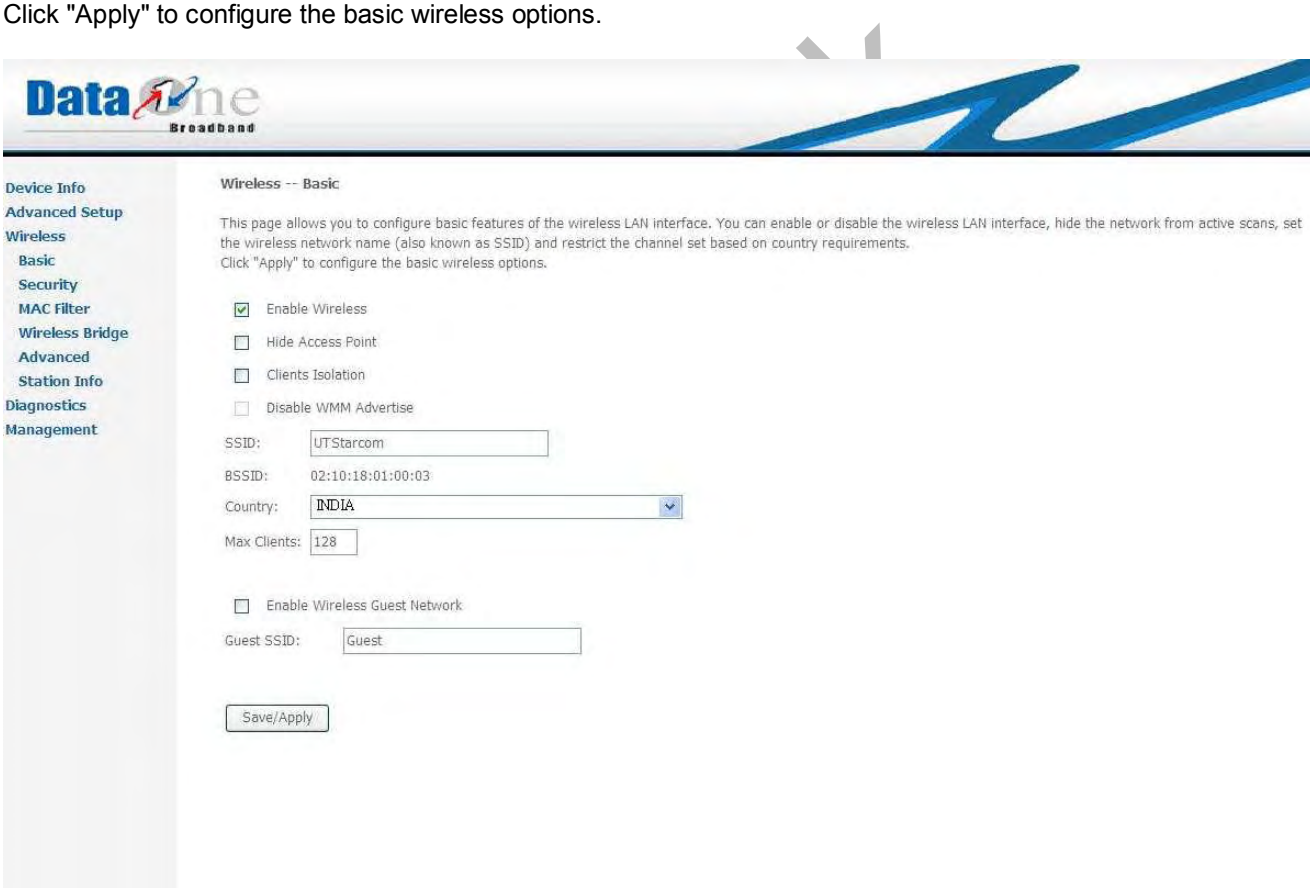


Figure 3.5.1 Wireless -- Basic

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

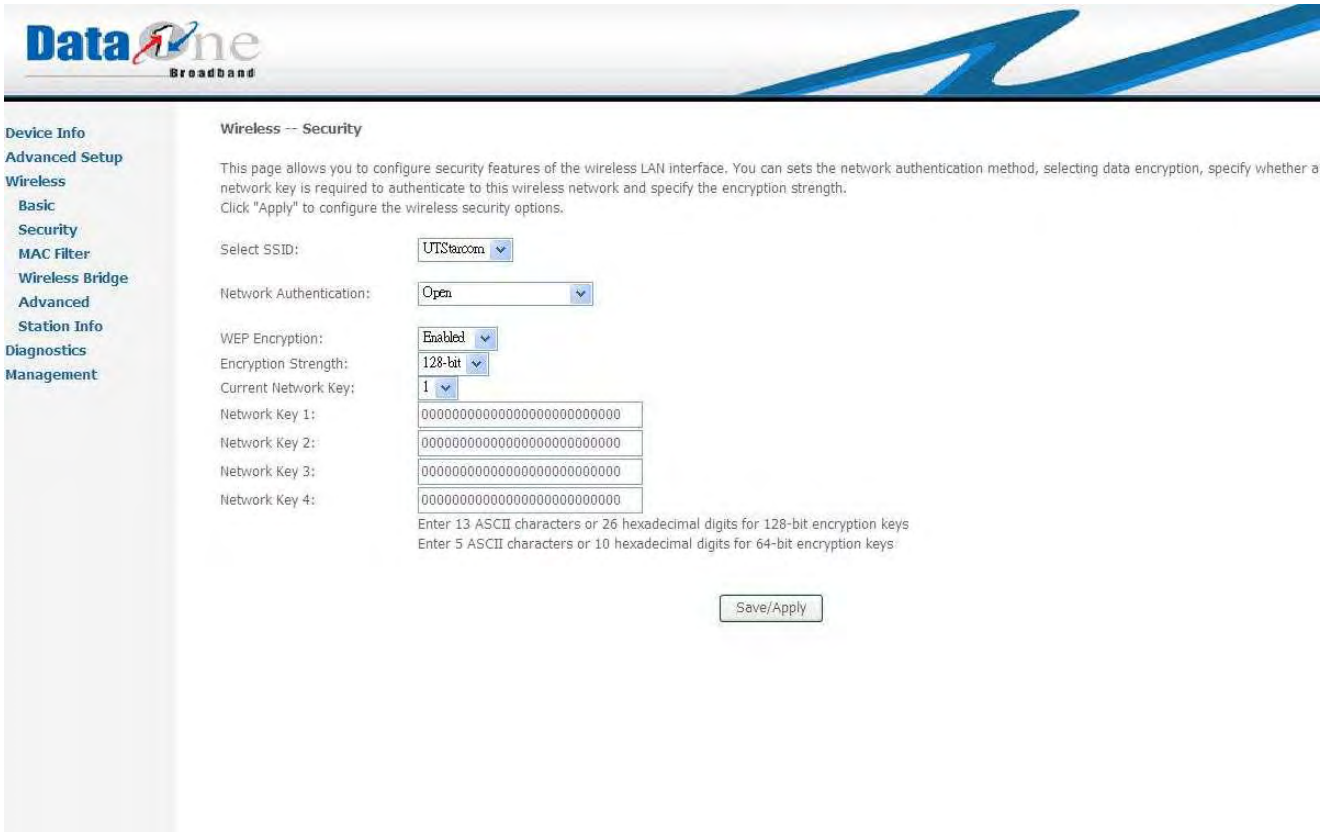
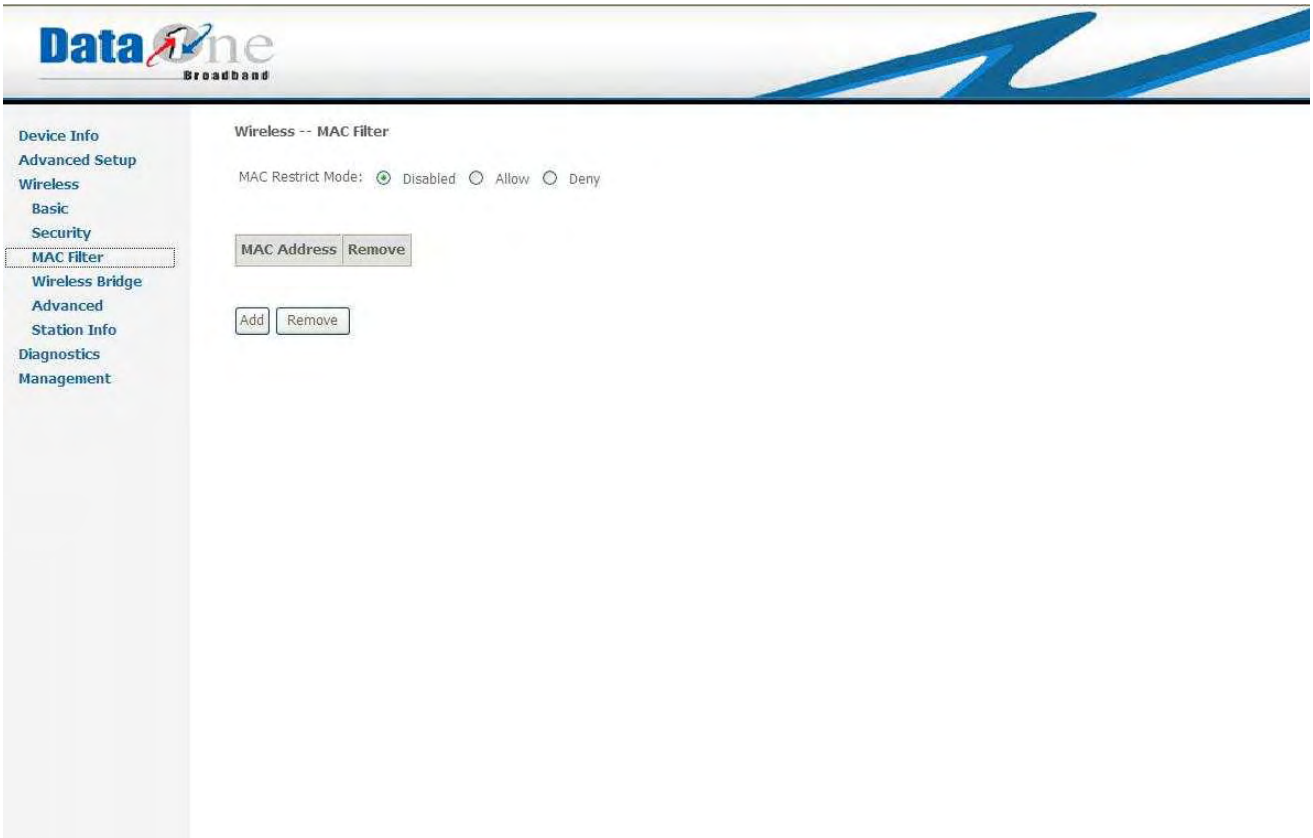


Figure 3.5.2 Wireless -- Security

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.



3.5.4 Wireless Bridge
3.5.5 Advanced
3.5.6 Station Info

3.6 Diagnostics
3.7 Management