AW4038
ADSL 11g AP Router

User's Manual

Version 1.0

TECOM CO., LTD.
23, R&D ROAD 2
SCIENCE-BASED INDUSTRIAL PARK
HSIN-CHU TAIWAN R.O.C.

Table of Contents

1. Introduction

Congratulations on becoming the owner of AW4038 4-port ADSL AP router. You will now be able to access the Internet using your high-speed ADSL connection. AW4038 has the following major features.

1.1 Features

- Built-in ADSL modem for high speed Internet access
- Network Address Translation (NAT) and IP filtering functions to provide network sharing and firewall protection for your computers
- 4-port switch to build your own local network
- Easy configuration via a web browser
- IEEE 802.11g 54Mbps Access Point

This User's Manual will guide you to install and configure your AW4038.

1.2 System Requirements

Before installing your AW4038, make sure that you have the following:

- ADSL 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 (NIC) or wireless network adapter.

For system configuration, use the supplied web-based program.

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

Note: Make sure that your computer has a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later.

The antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

2. Installation

In addition to this document, your AW4038 should arrive with the following:

- One standalone desktop AW4038
- One power adapter and power cord
- One Ethernet cable with RJ-45 connector
- One telephone cable with RJ-11 connector

Front Panel

The front panel LEDs indicate the status of the unit.

Label	Color	Function
PWR	Green	On: Power on Off: Power off
LAN1~4	Green	On: LAN link established and active Off: No LAN link Flashes during data transfer
DSL	Green	Flashes during the training mode. On: ADSL link established and active
Tx/Rx	Green	On: Router is active Flashes during data transfer through ADSL line
WLAN	Green	On: WLAN enabled Off: WLAN disabled Flashes during data transfer

Rear Panel

The connectors located at the rear panel have the following functions.

Interface	Function
Botton	Power switch on/off
Power (SNG 1- tec)	Connects to the power adapter cable
Reset	Resets unit's configuration to factory default
LAN1~4	RJ-45 connector: Connects AW4038 to your PC's Ethernet port, or to the uplink port on your LAN's hub
ADSL	RJ-11 connector: Connects AW4038 to ADSL line

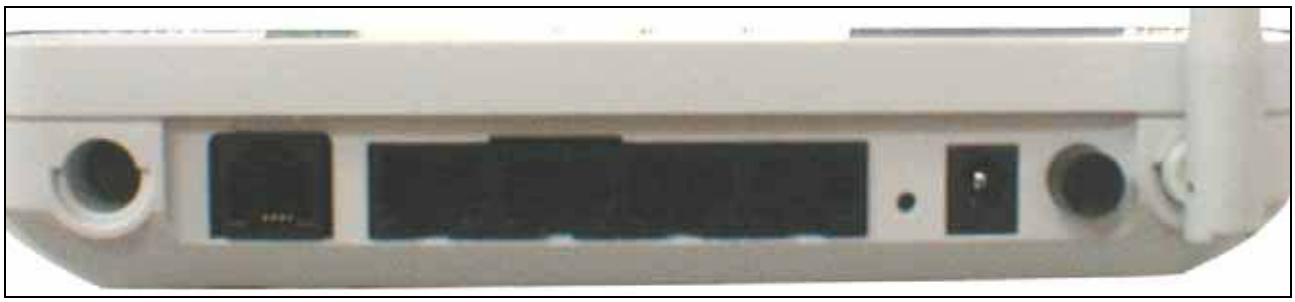


Figure 1. Rear view of AW4038

Connecting the Hardware

Connect AW4038 to the phone jack, the power outlet, and your computer or network.

WARNING

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and AW4038.*

Step 1. Connect the ADSL cable and optional telephone

Connect one end of the phone cable to the RJ-11 connector on the rear panel of AW4038. Connect the other end to the ADSL outlet provided by your service provider (normally MODEM port of the attached splitter).

Step 2. Connect the Ethernet cable

Connect one end of the Ethernet cable to the one of the four RJ-45 connectors on the rear panel of AW4038 and connect the other end to your PC's network adaptor (NIC). If you are connecting a LAN to AW4038, attach one end of the Ethernet cable to a regular hub port and the other end to the LAN port on AW4038.

Step 3. Attach the power connector

Connect the AC power adapter to the power connector on AW4038 and plug in the adapter to a wall outlet or power extension.

Step 4. Turn on AW4038 and power up your systems

Press the Power switch on the back panel of AW4038 to the ON (Low) position.
Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 5. Configure AW4038 through the WEB interface

Please refer to chapter 3.

Step 6. Save the configurations and Reboot

Save the changes you made on AW4038.

3. Configuration

3.1 Setup

- Connect AW4038 and PC with an RJ-45 Ethernet cable.
- Turn on AW4038.
- The default IP address of AW4038 is 192.168.1.1.

3.2 Establish The Connection

- Enter the IP address (default: 192.168.1.1) of AW4038 in the address line of Web Browser
- A Dialogue Box will pop up to request the user to login. (Figure 1)

Figure 2. 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 is valid, the home page “Device Info - Summary” will be displayed on the screen. (**Figure 3**)

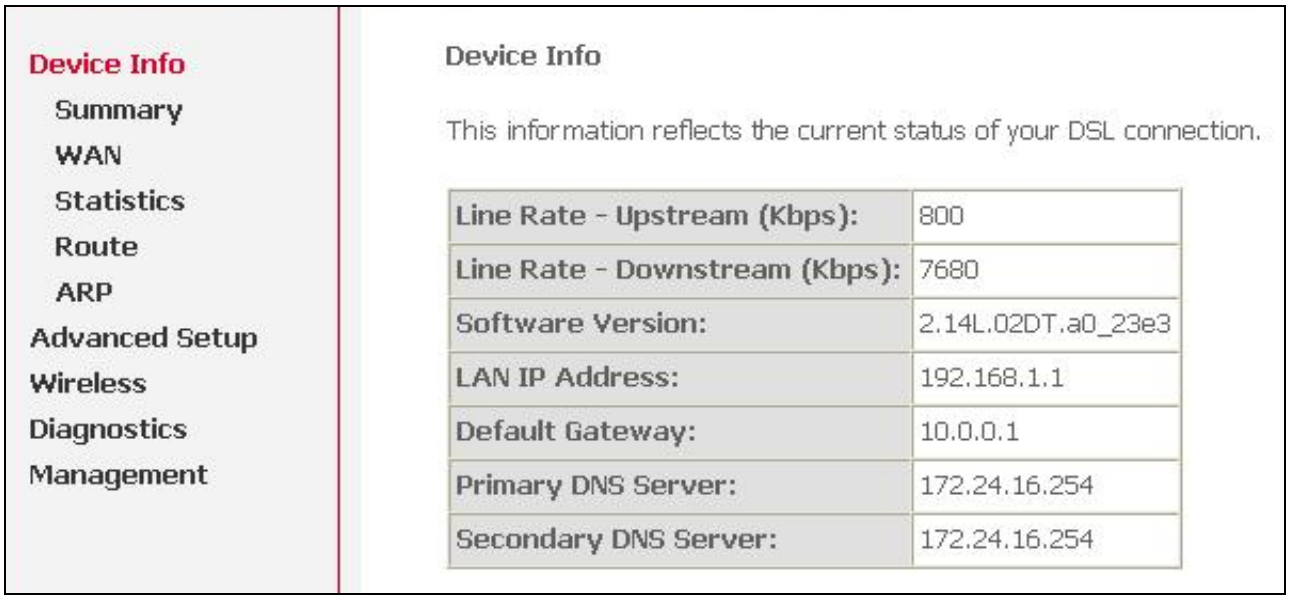


Figure 3. AW4038 Home Page

4. Quick Setup

The system administrator can configure AW4038 remotely or locally via a Web Browser. Network configuration needs to be planned and decided before starting the configuration procedure.

Quick Setup allows system administrator to select the appropriate operation mode and configure the corresponding settings step by step to create a connection. The following five operation modes are supported:

- PPP over Ethernet (PPPoE)
- IP over ATM (IPoA)
- Bridging
- MAC Encapsulation Routing (MER)
- PPP over ATM (PPPoA)

4.1 PPP over Ethernet (PPPoE) Configuration

Click on “Quick Setup” in the left frame, and follow the steps below to create a PPP over Ethernet (PPPoE) connection.

4.1.1 ATM PVC Configuration

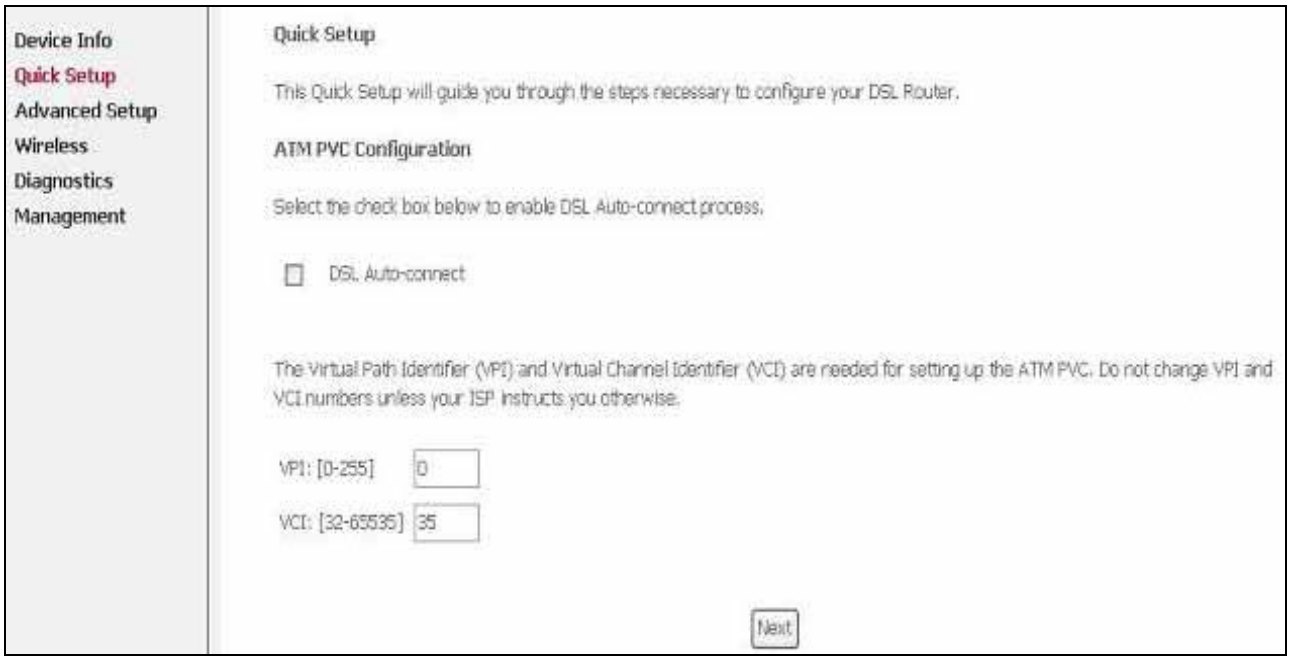


Figure 4. Quick Setup – ATM PVC Configuration

Enter the VPI/VCI values. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.1.2 Connection Type and Encapsulation Mode

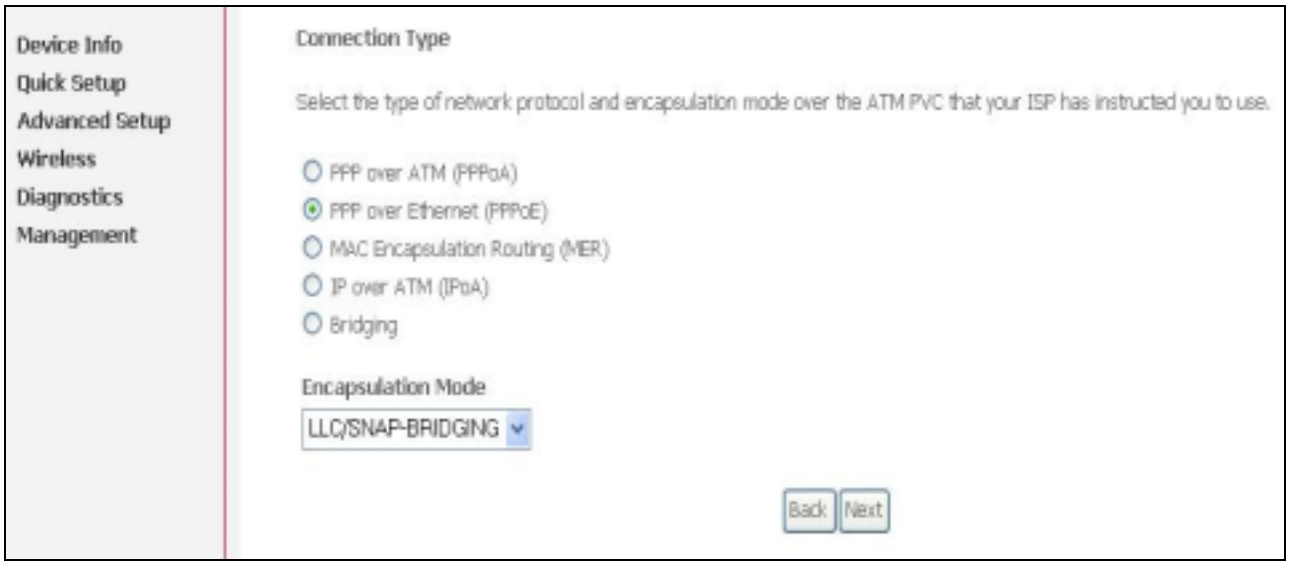


Figure 5. Quick Setup – Connection Type and Encapsulation Mode

Select “PPP over Ethernet (PPPoE)”, and the “Encapsulation Mode”. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.1.3 PPP Username and Password

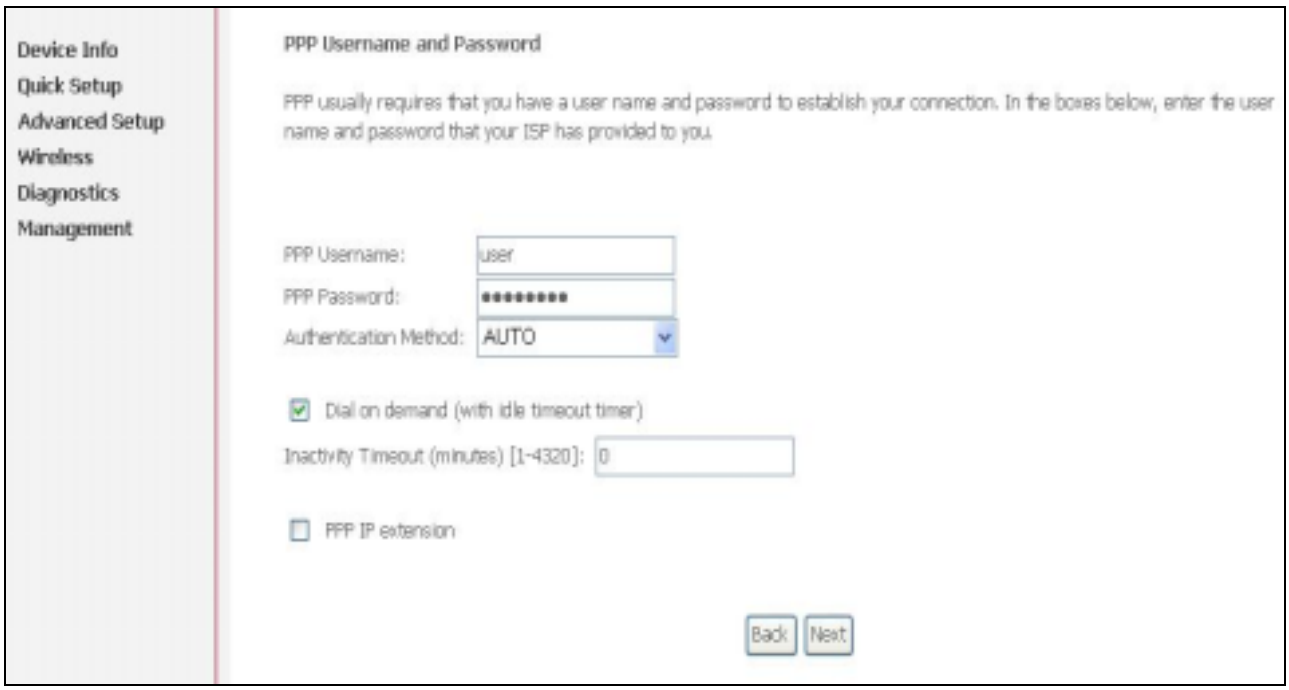


Figure 6. Quick Setup – PPP Username and Password

Enter “PPP Username”, “PPP Password”, and select “Authentication Method” (AUTO/PAP/CHAP). Please contact you ISP for the information.

The “Dial on demand” function, if checked, will tear down the PPP link automatically when there is no outgoing packet for the programmed period of time that is set below.

AW4038 activates PPPoE connection automatically when user wants to access Internet and there is no active PPPoE connection.

The users are able to assign some specific ATM PVC(s) to run PPPoE, if AW4038 has multiple ATM PVC connections.

The “PPP IP extension” is a special feature provided by some ISPs. Unless your service provider specifically requires this setup, do not select it.

Click on “Next” to go to next step.

4.1.4 IGMP Multicast, WAN service, and QoS

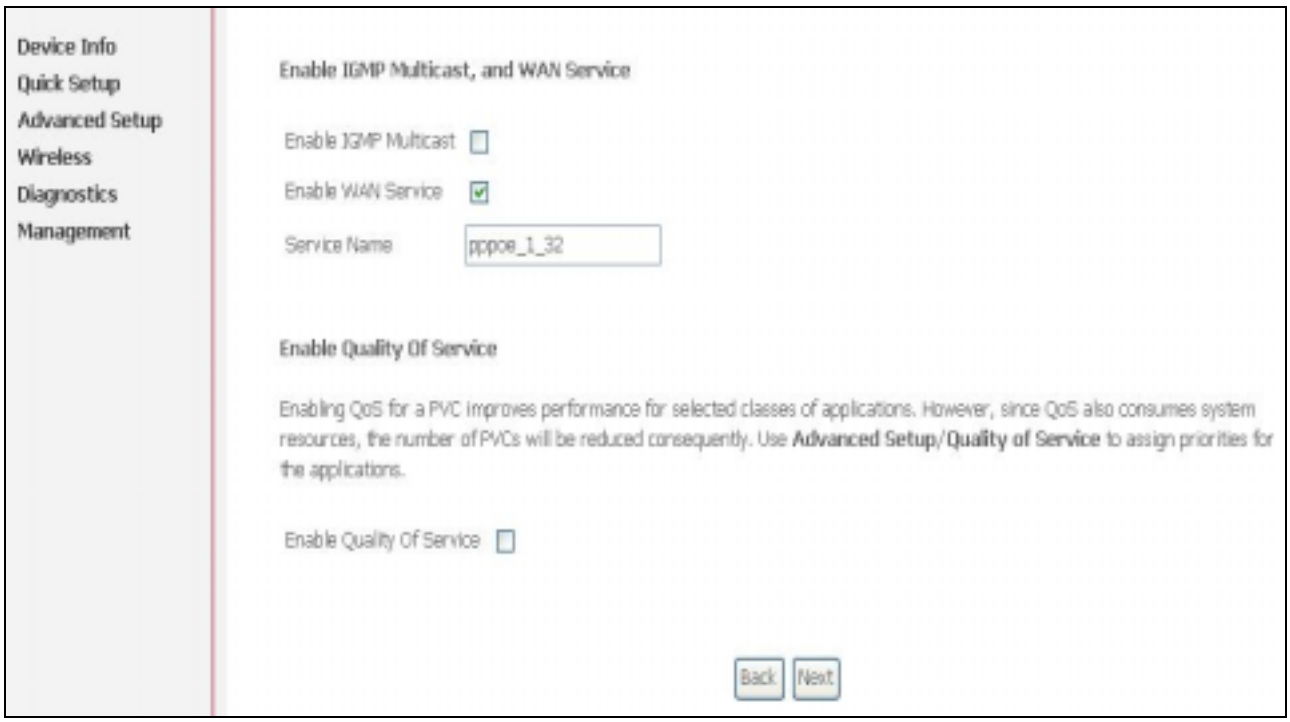


Figure 7. Quick Setup – IGMP Multicast, WAN service, and QoS

Check to Disable/Enable IGMP Multicast, WAN Service, and QoS.

Go to “Advanced Setup” > “Quality of Service” to assign priorities for the application. Click on “Next” to go to next step.

4.1.5 Device Setup

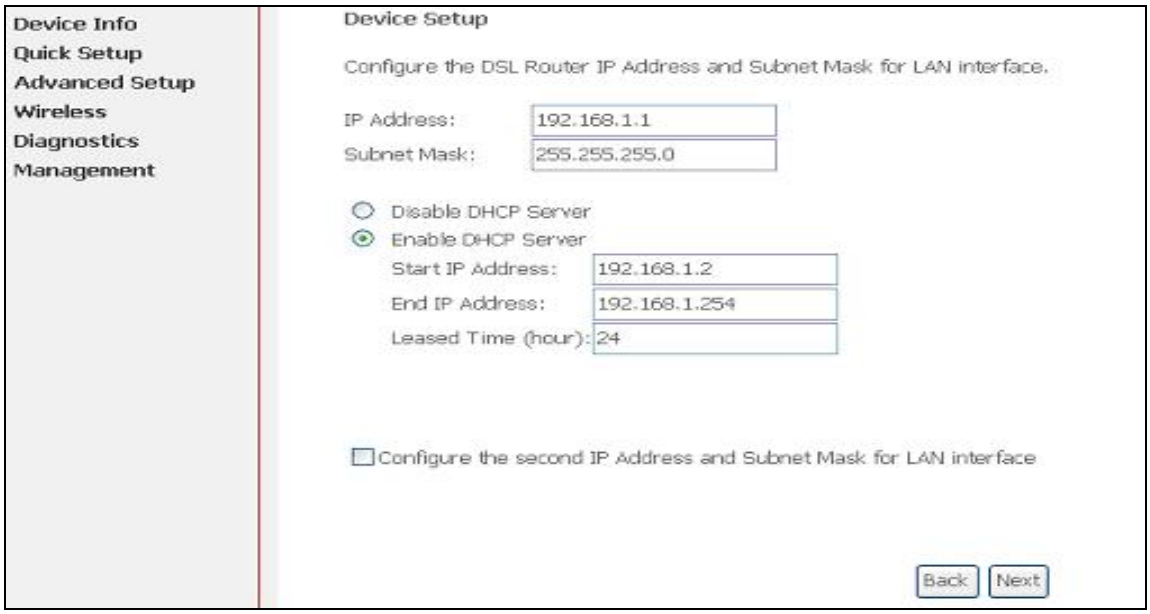


Figure 8. Quick Setup – Device Setup

Enter IP (LAN IP) and Subnet Mask.

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

AW1038 will assign IP address, subnet mask, Default gateway IP address and DNS server IP address to host PCs which connect to its LAN.

Select “Configure the second IP Address and Subnet Mask for LAN interface” and configure if second IP Address is used.

Note: 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.

4.1.6 Wireless Setup

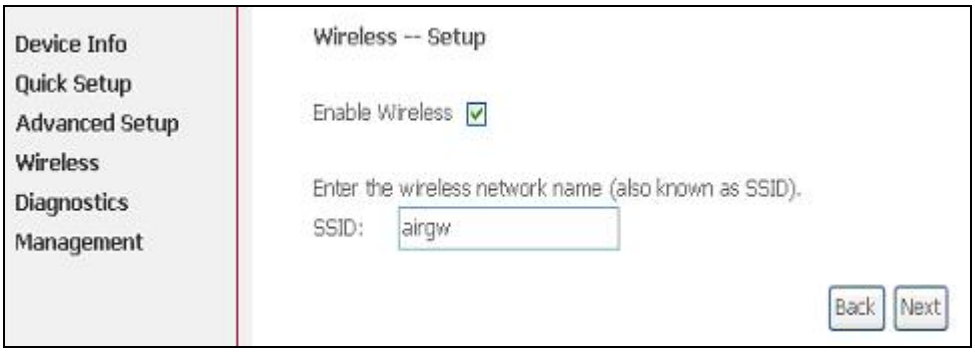


Figure 9. Quick Setup - Wireless Setup

Check “Enable Wireless” to enable wireless radio; or uncheck to disable.

“SSID” is the network name shared among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

Click on “Next” to go to next step.

4.1.7 WAN Setup – Summary

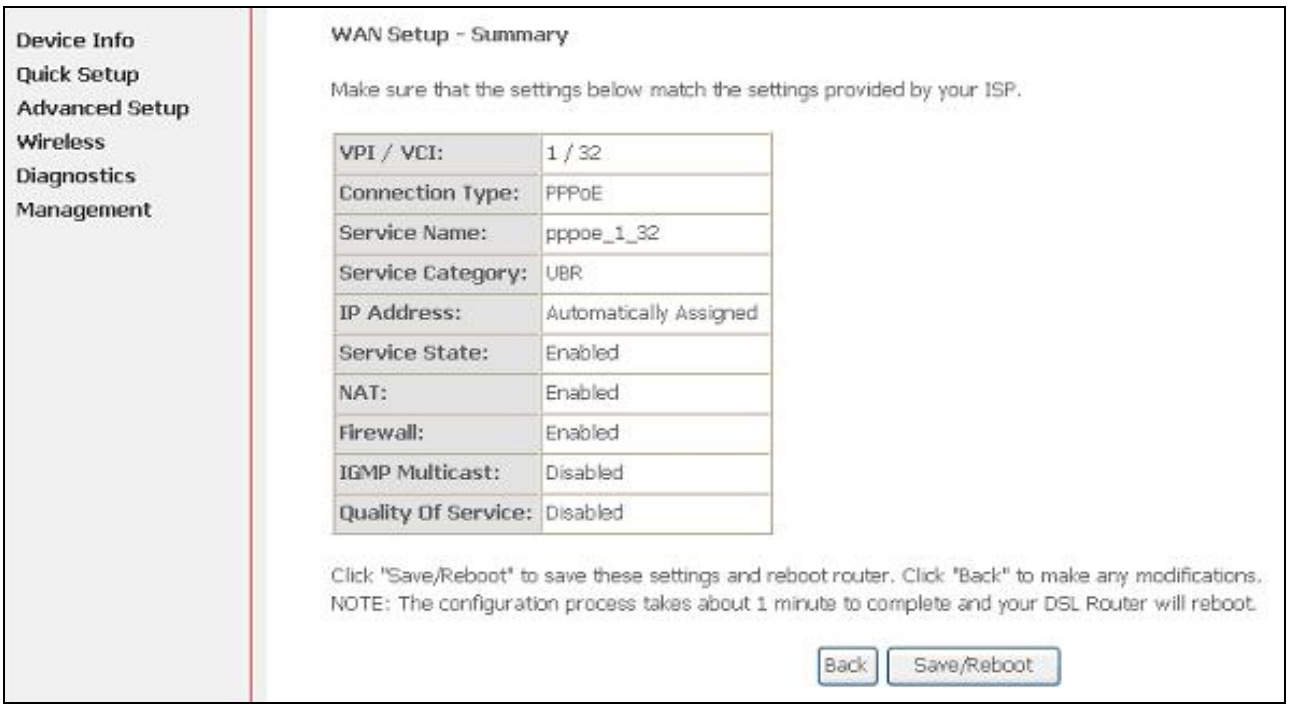


Figure 10. Quick Setup – WAN Setup – Summary

The last page displays a summary of previous settings. Make sure that the configurations match the settings provided by ISP, and then click on "Save/Reboot" button to complete the configuration procedure.

4.2 IP over ATM (IPoA) Configuration

Click on "Quick Setup" in the left frame, and follow the steps below to create an IP over ATM (Routed) connection.

4.2.1 ATM PVC Configuration

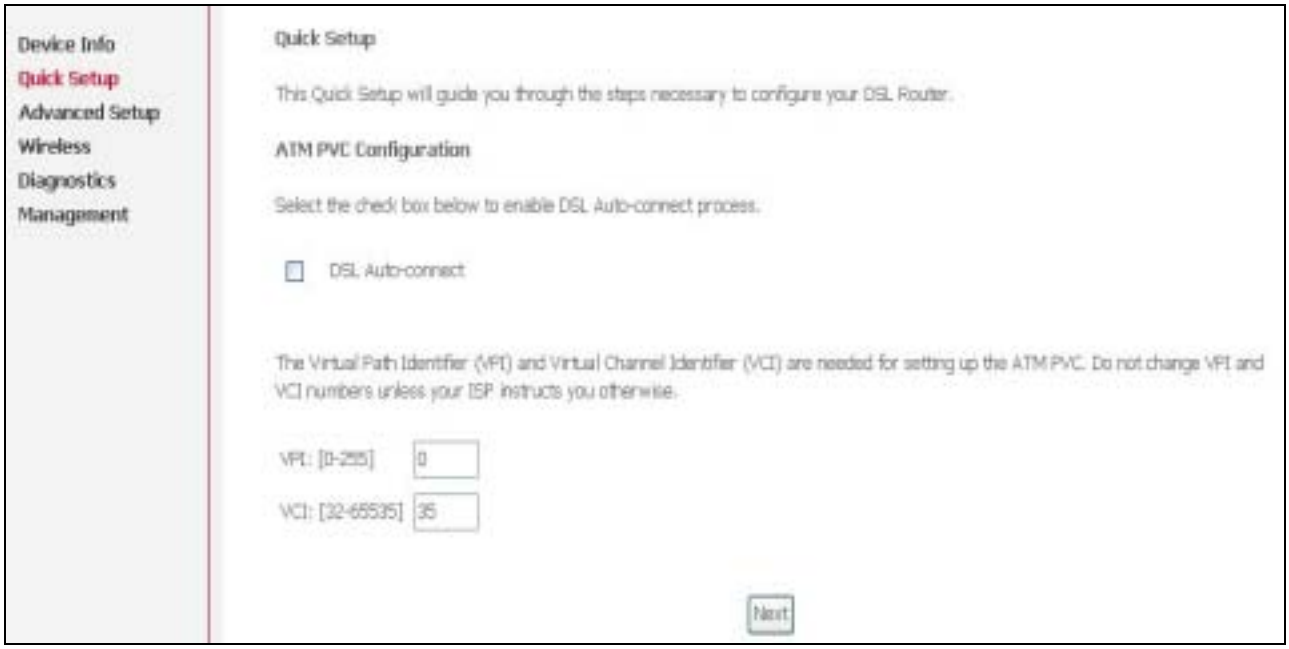


Figure 11. Quick Setup – ATM PVC Configuration

Enter the VPI/VCI values. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.2.2 Connection Type

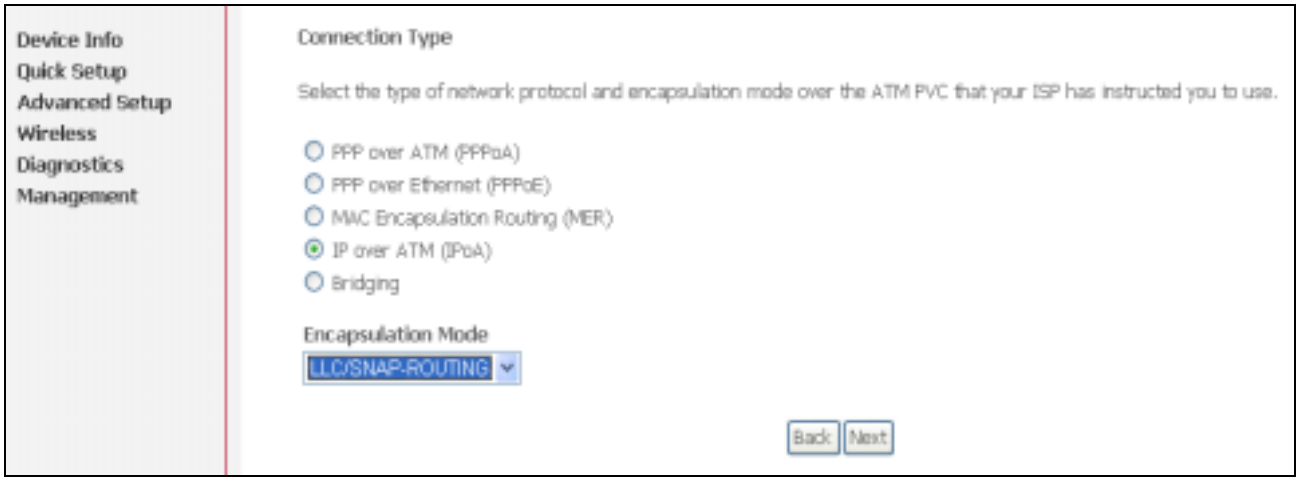


Figure 12. Quick Setup – Connection Type and Encapsulation Mode

Select “IP over ATM (IPoA)”, and the “Encapsulation Mode”. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.2.3 WAN IP Settings

Figure 13. Quick Setup– WAN IP Settings

WAN IP/Subnet Mask, default gateway, and DNS server settings. Please contact your ISP for the information.

Click on “Next” to go to next step.

4.2.4 NAT, IGMP Multicast, WAN Service, and QoS

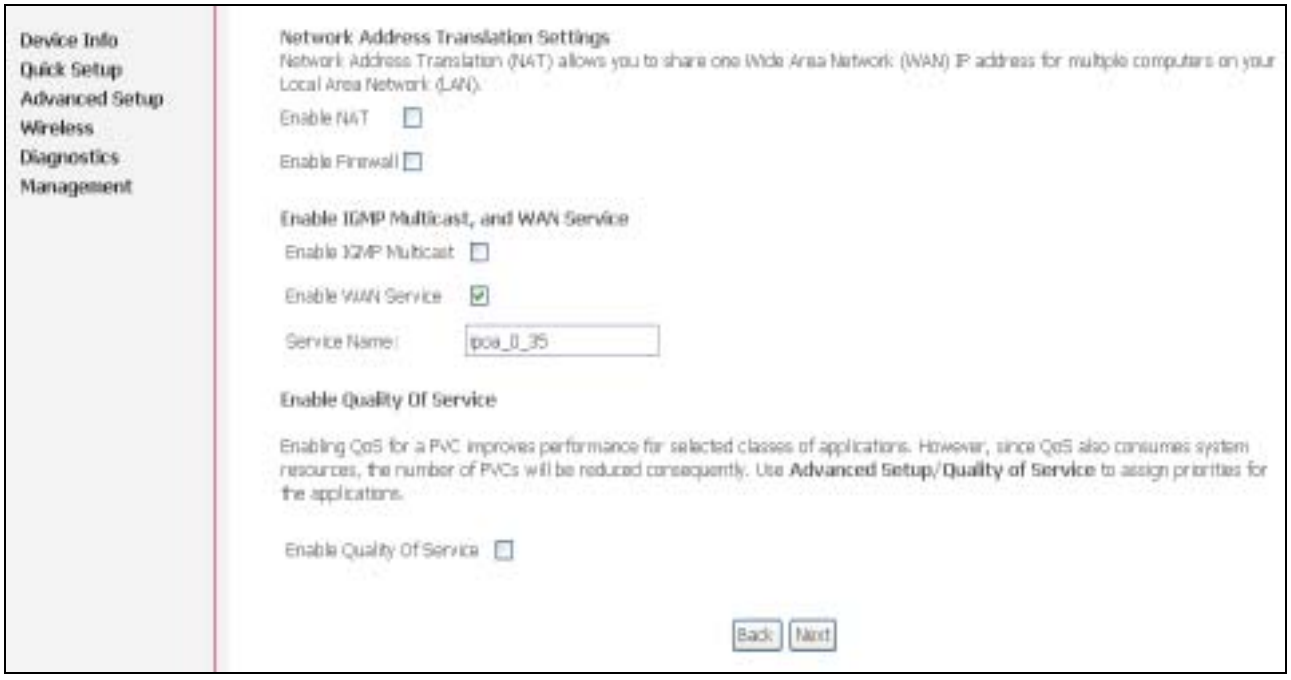


Figure 14. Quick Setup – IPoA – NAT, IGMP Multicast, WAN service, and QoS

Check to Enable/Disable NAT and Firewall functions.

Go to “Advanced Setup” > “Firewall” to assign filter rules.

Check to Enable/Disable IGMP Multicast, WAN Service, and QoS.

Go to “Advanced Setup” > “Quality of Service” to assign priorities for the application.

Click on “Next” to go to next step.

4.2.5 Device Setup

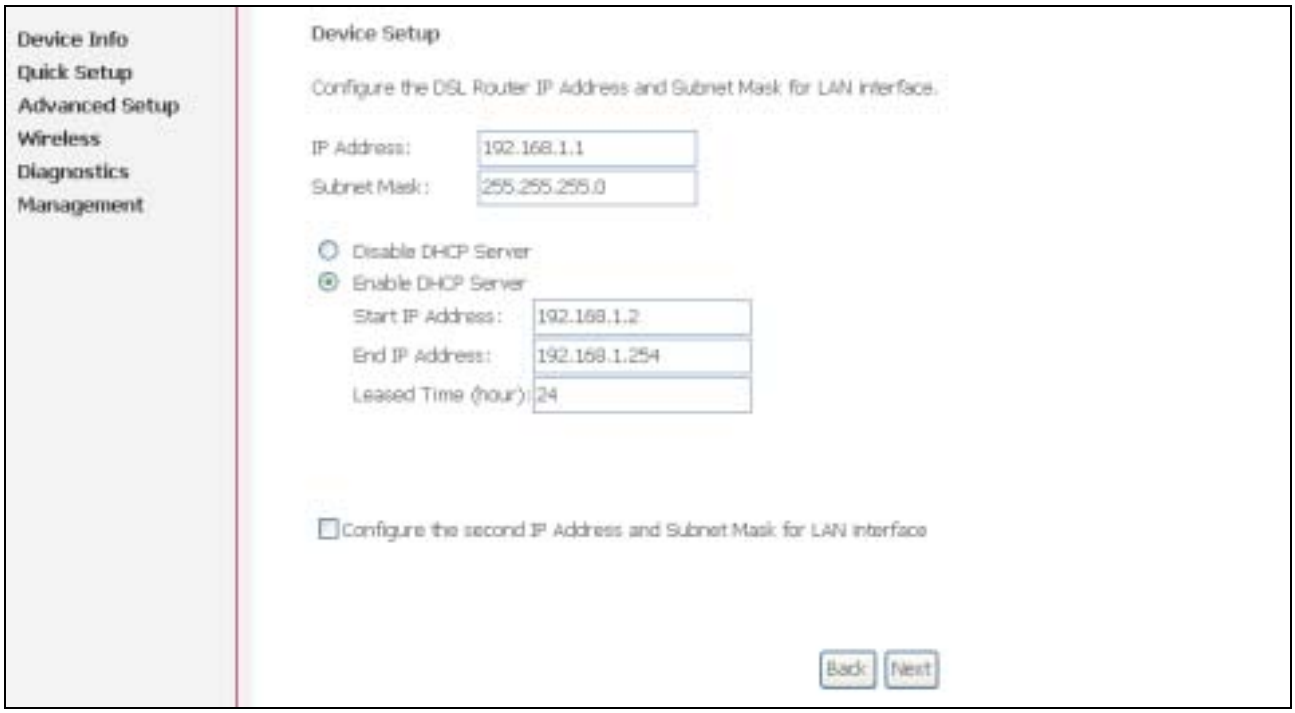


Figure 15. Quick Setup – Device Setup

Enter IP (LAN IP) Address and Subnet Mask to AW4038.

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

Select “Configure the second IP Address and Subnet Mask for LAN interface” and configure if second IP Address is used.

Click on “Next” to go to next step.

4.2.6 Wireless Setup

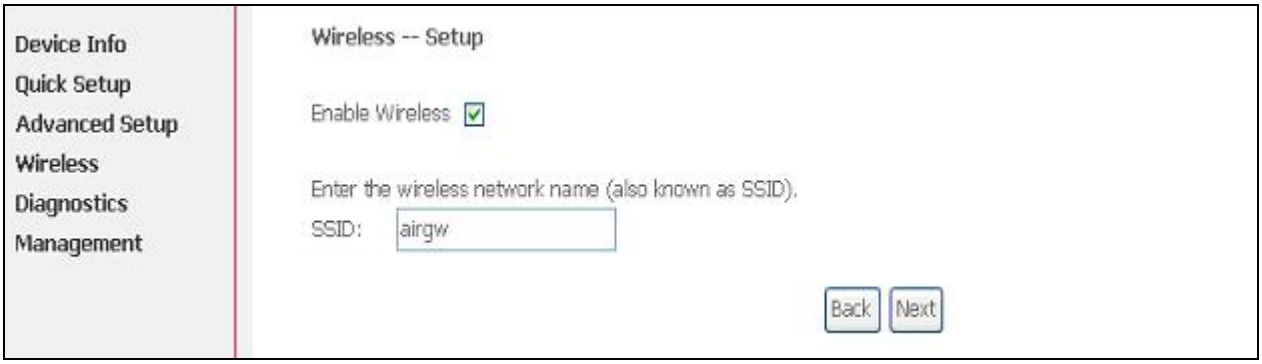


Figure 16. Quick Setup – Wireless Setup

Check “Enable Wireless” to enable wireless radio; or uncheck to disable.

“SSID” is the network name shared among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

Click on “Next” to go to next step.

4.2.7 WAN Setup – Summary

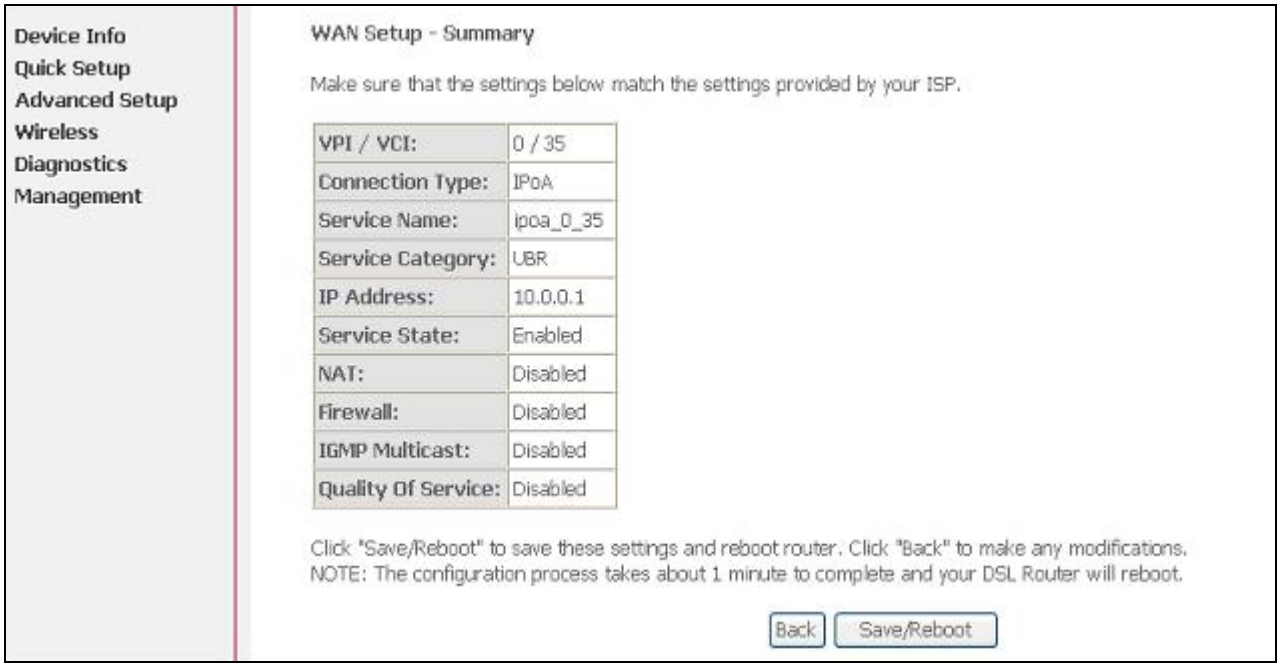


Figure 17. Quick Setup – WAN Setup – Summary

The last page gives a summary of previous steps. Make sure that the settings match the settings provided by ISP, and then click on “Save/Reboot” button to

complete the configuration procedure.

4.3 Bridge Configuration

Click on “Quick Setup” in the left frame, and follow the steps below to create a Bridging connection.

4.3.1 ATM PVC Configuration

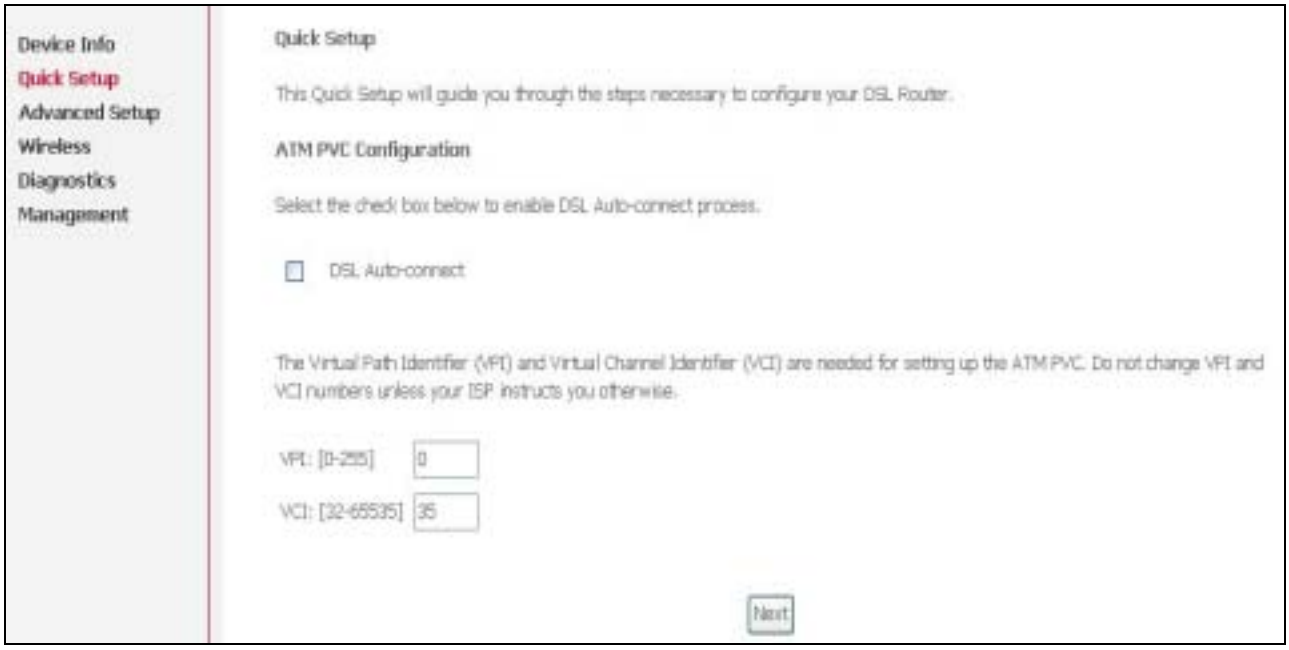


Figure 18. Quick Setup – ATM PVC Configuration

Enter the VPI/VCI values. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.3.2 Connection Type

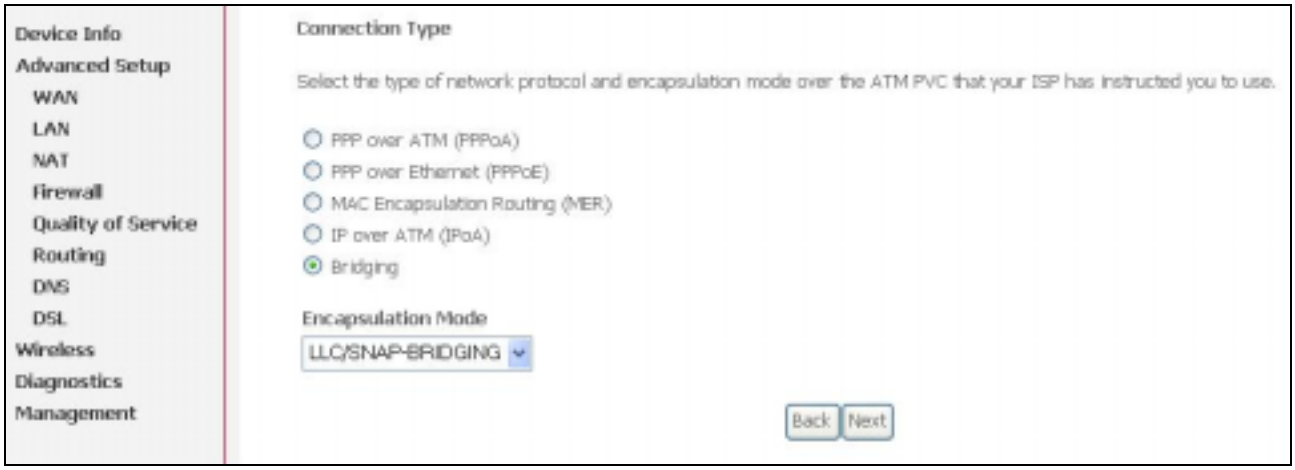


Figure 19. Quick Setup – Connection Type and Encapsulation Mode

Select “Bridging”, and the “Encapsulation Mode”. Please contact you ISP for the information.

Click on “Next” to go to next step.

4.3.3 WAN Service

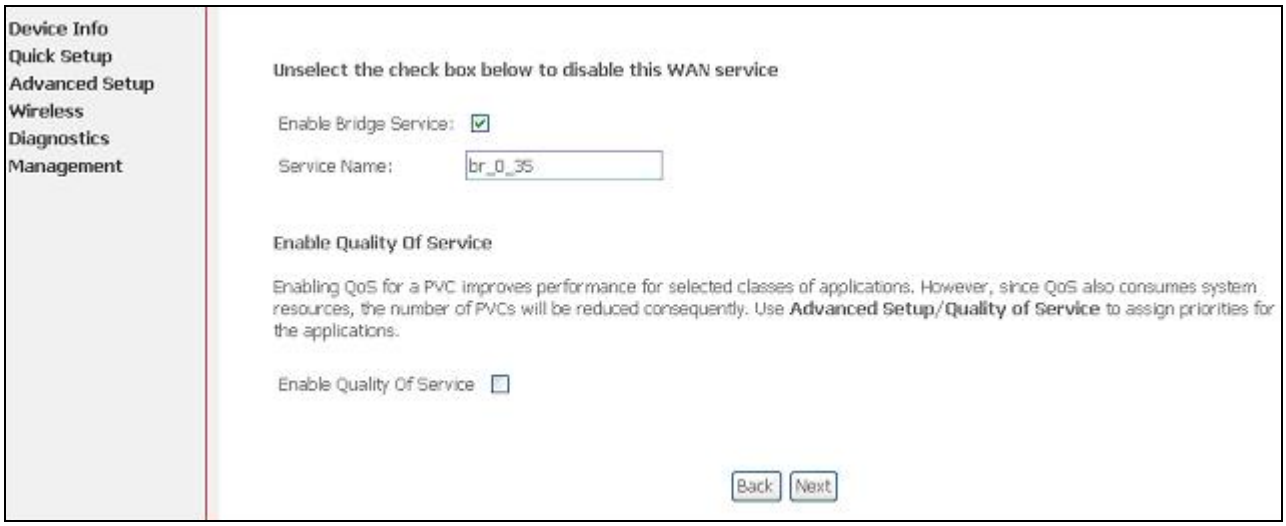


Figure 20. Quick Setup – WAN Service

Give a service name and check the box to enable this WAN service.

Check to Enable/Disable QoS.

Go to “Advanced Setup” > “Quality of Service” to assign priority for the application.

Click on “Next” to go to next step.

4.3.4 Device Setup

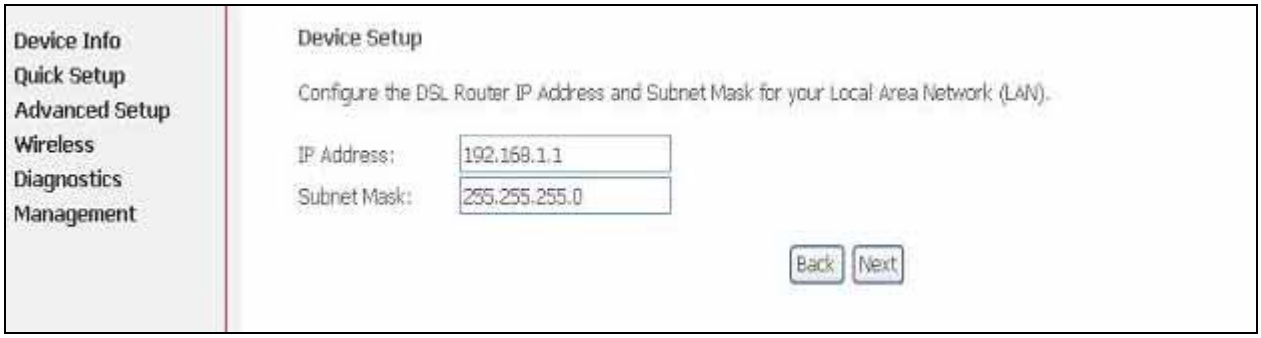


Figure 21. Quick Setup – Device Setup

Type LAN IP Address and Subnet Mask.

Click on “Next” to go to next step.

4.3.5 Wireless Setup

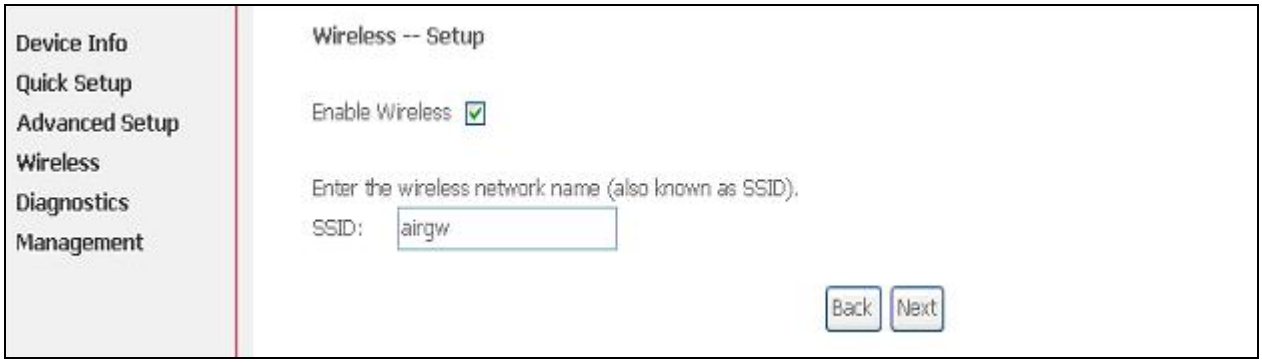


Figure 22. Quick Setup – Wireless Setup

Check “Enable Wireless” to enable wireless radio; or uncheck to disable.

“SSID” is the network name shared among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters.

Click on “Next” to go to next step.

4.3.6 WAN Setup – Summary

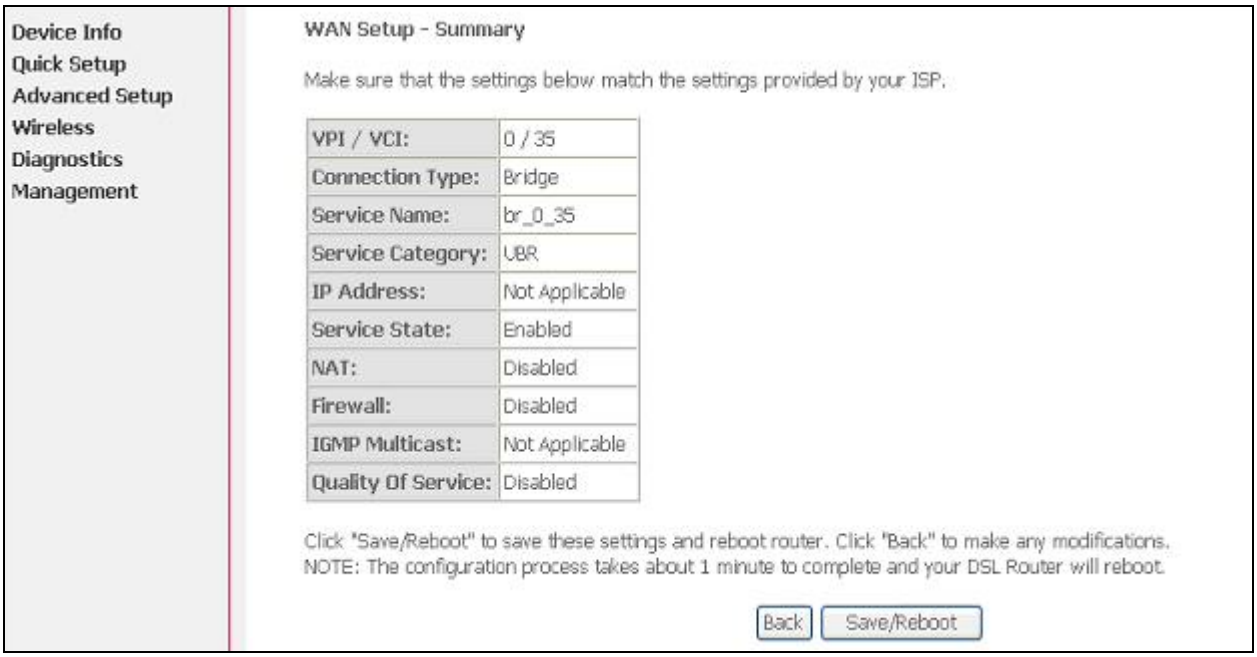


Figure 23. Quick Setup – WAN Setup – Summary

The last page gives a summary of previous steps. Make sure that the settings match the settings provided by ISP, and then click on “Save/Reboot” button to complete the configuration procedure.

4.4 MAC Encapsulation Routing (MER) Configuration

Configuration of MER is similar to IPoA. Select “MAC Encapsulation Routing (MER)” in “Connection Type”. For other configuration, please refer to IPoA settings (section **4.2**).

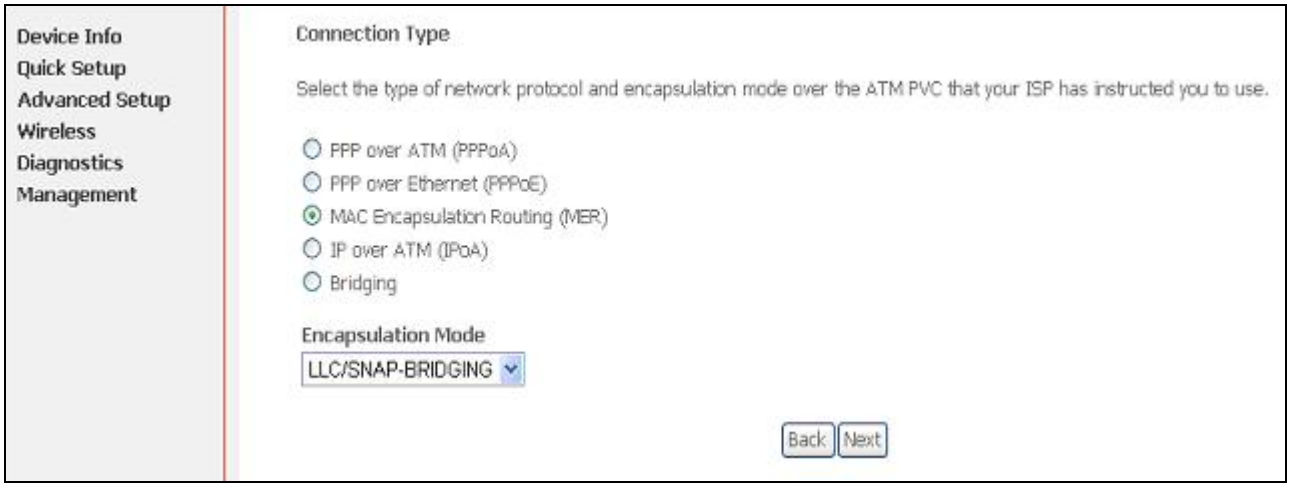


Figure 24. Quick Setup – Connection Type and Encapsulation Mode

4.5 PPP over ATM (PPPoA) Configuration

Configuration of PPPoA is similar to PPPoE. Select “PPP over ATM (PPPoA)” in “Connection Type”. For other configuration, please refer to PPPoE settings (section **4.1**).

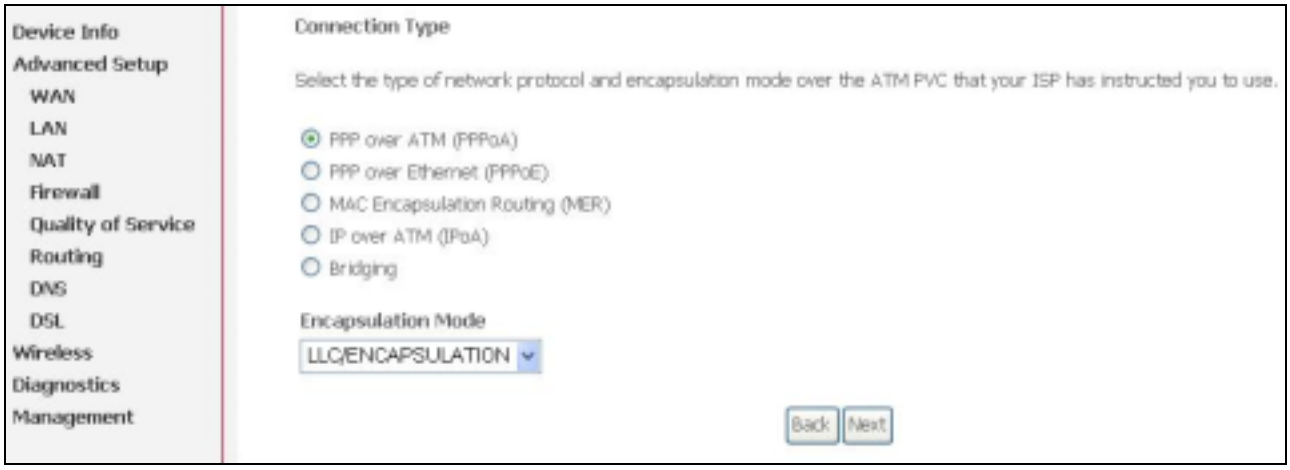


Figure 25. Quick Setup – Connection Type and Encapsulation Mode

5. Advanced Setup

Advanced Setup allows system administrator to configure the following topics:

- WAN
- LAN
- NAT
- Firewall
- Quality of Service
- Routing
- DNS
- DSL

5.1 WAN

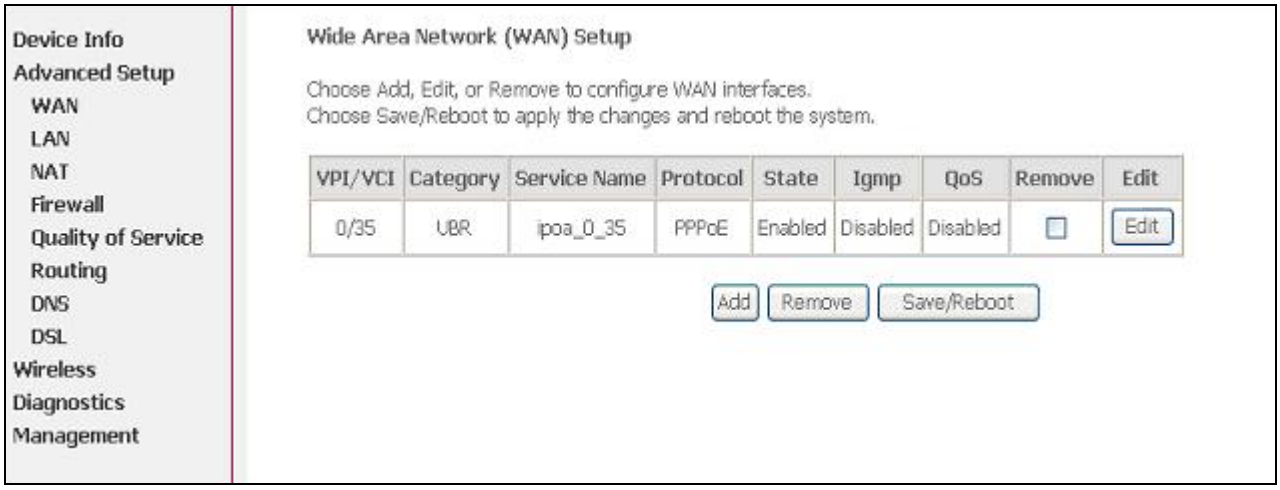


Figure 27. Advanced Setup – WAN

This page shows the current existing WAN interfaces in the system. User can choose Add, Edit, or Remove to configure WAN interfaces. For detail about Add and Edit procedure, please refer to ***4. Quick Setup***.

5.2 LAN

Please refer to **4.1.5.**

5.3 NAT

Three functions are supported in NAT: Virtual Servers, Port Triggering, and DMZ Host.

5.3.1 Virtual Servers

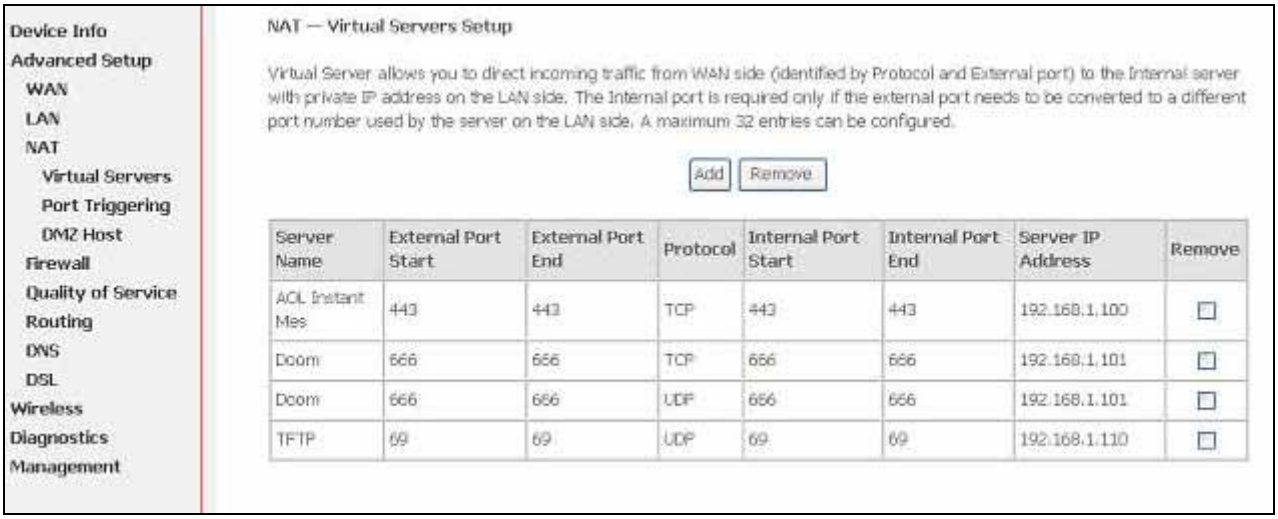


Figure 28. Advanced Setup – NAT

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. Maximum 32 entries can be configured.

Click on “Add” to enter configuration page to add your own rule(s). Some common used servers (Web, FTP, Mail, …etc.) are pre-defined in AW4038. User can simply select the desired server from the pull-down menu and assign the IP address of the local PC.

To delete the configured rule(s), check the “Remove” box of the specific rule(s) and click on “Remove”.

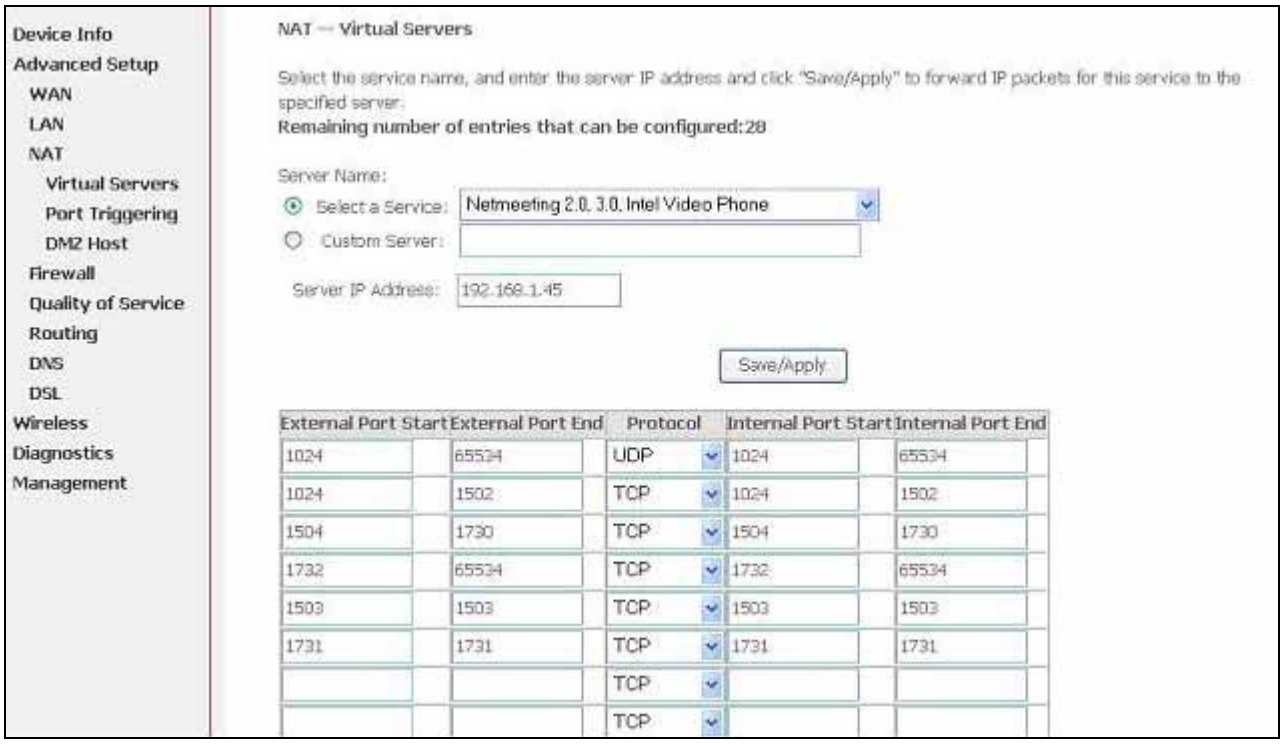


Figure 29. Advanced Setup – NAT – Virtual Servers

5.3.2 Port Triggering

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.

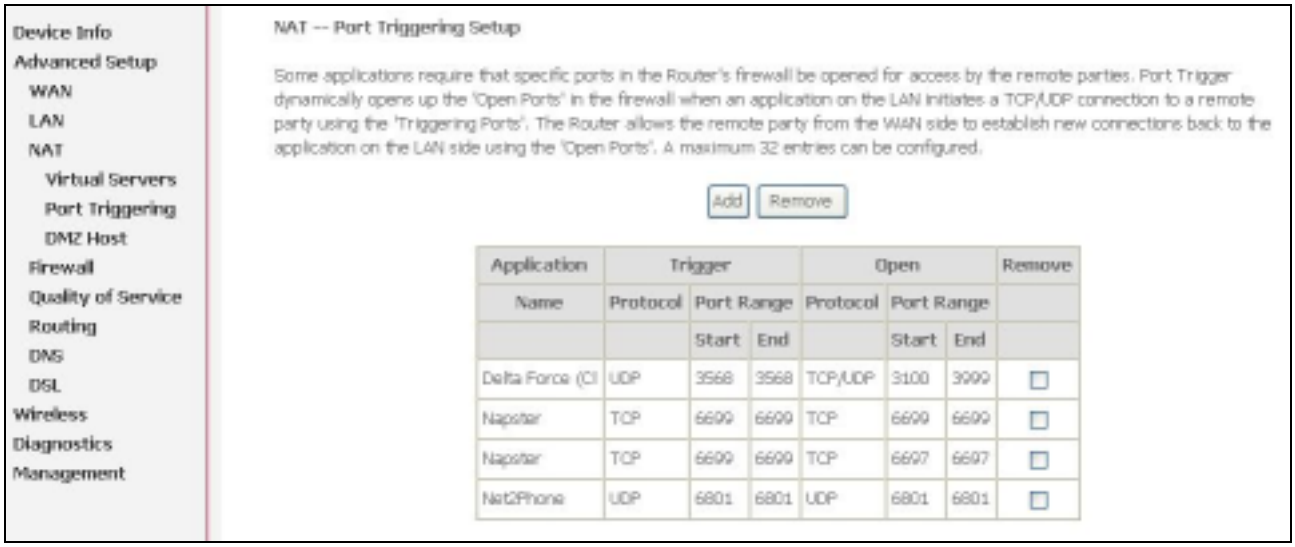


Figure 30. Advanced Setup – NAT – Port Triggering

Click on “Add” to enter configuration page to add your own rule(s). 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.

To delete the configured rule(s), check the “Remove” box of the specific rule(s) and click on “Remove”.

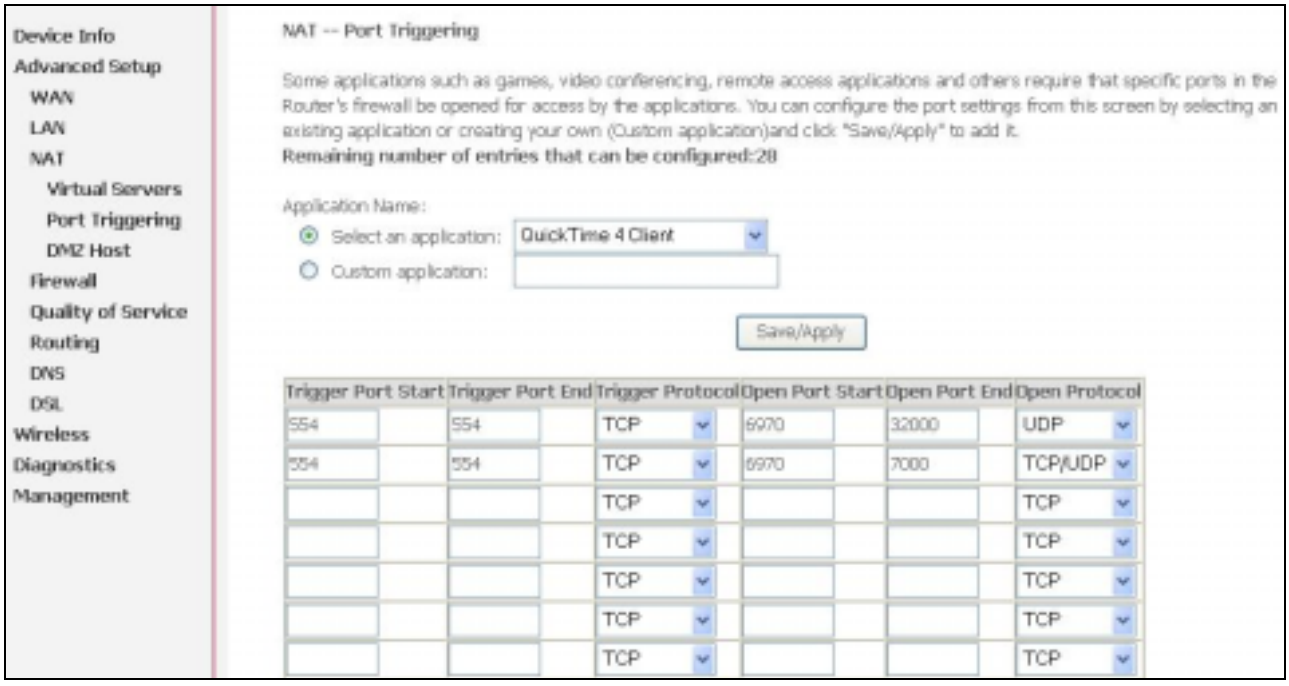


Figure 31. Advanced Setup – NAT – Add Port Triggering

5.3.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click “Apply” to activate the DMZ host.

Clear the IP address field and click “Apply” to deactivate the DMZ host.

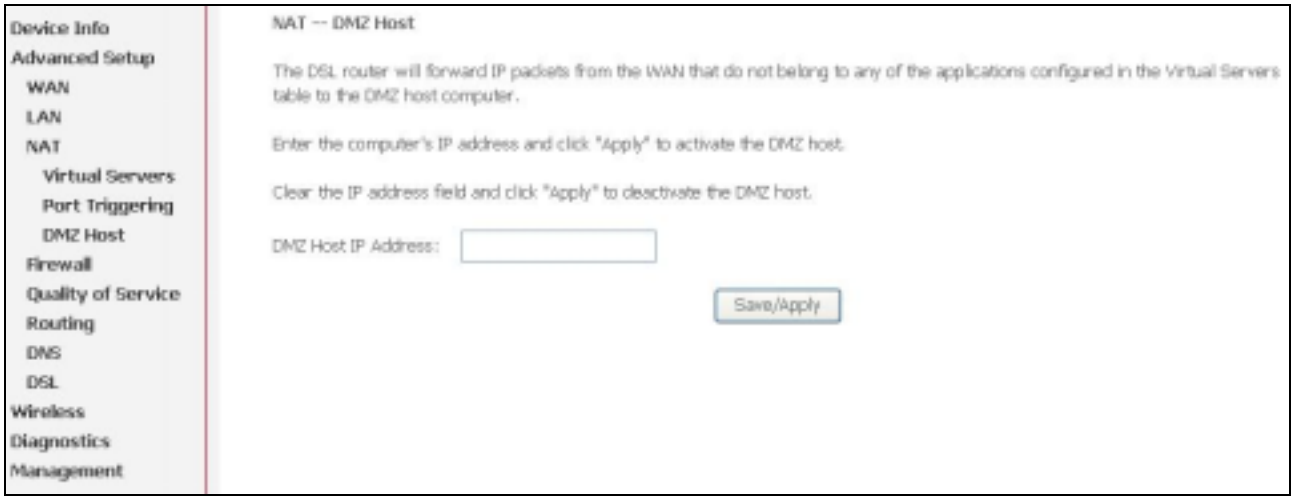


Figure 32. Advanced Setup – NAT – DMZ Host

5.4 Firewall

Two functions are supported in Firewall: Outgoing IP Filtering and MAC Filtering.

5.4.1 Firewall – Outgoing IP Filtering

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Choose “Add” to configure outgoing IP filters. To remove, check the item and click “Remove”.

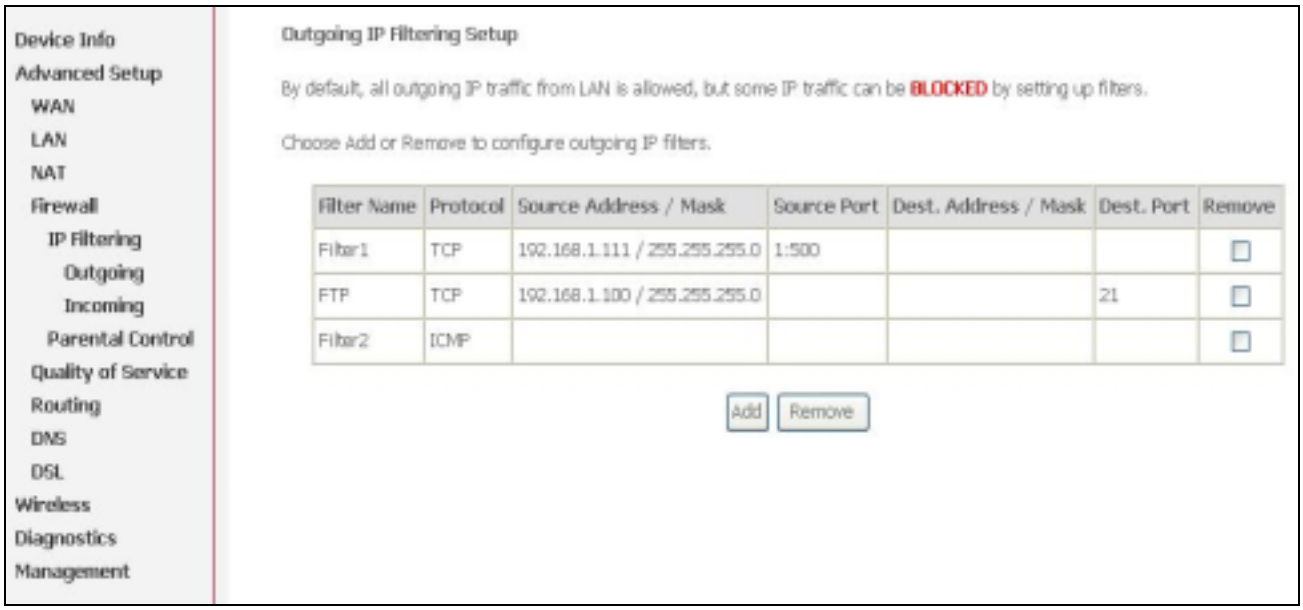


Figure 33. Advanced Setup – Firewall – Outgoing IP Filtering

The screen allows you to create a filter rule to identify outgoing IP traffic by

specifying a new filter name and at least one of the conditions 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. **Figure 34** shows the configuration that prevents a local PC (IP address: 192.168.1.100) from surfing the Internet.

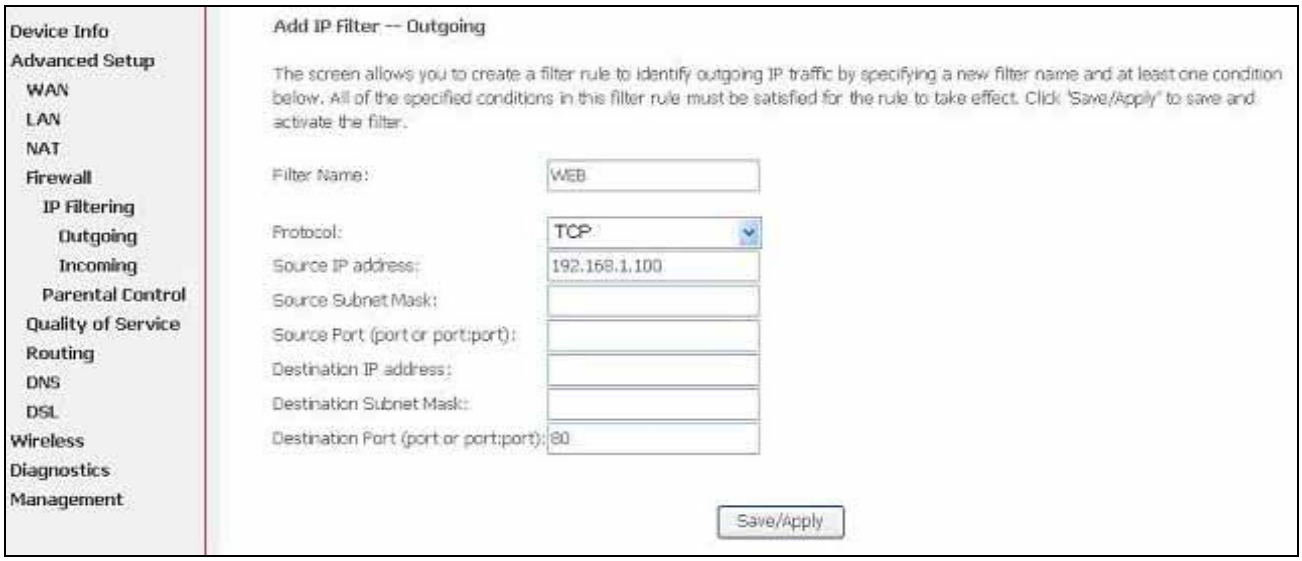


Figure 34. Advanced Setup – Firewall – Add new Outgoing IP Filter

5.4.2 Firewall – Incoming IP Filtering

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” to configure incoming IP filters. To remove, check the item and click “Remove”.

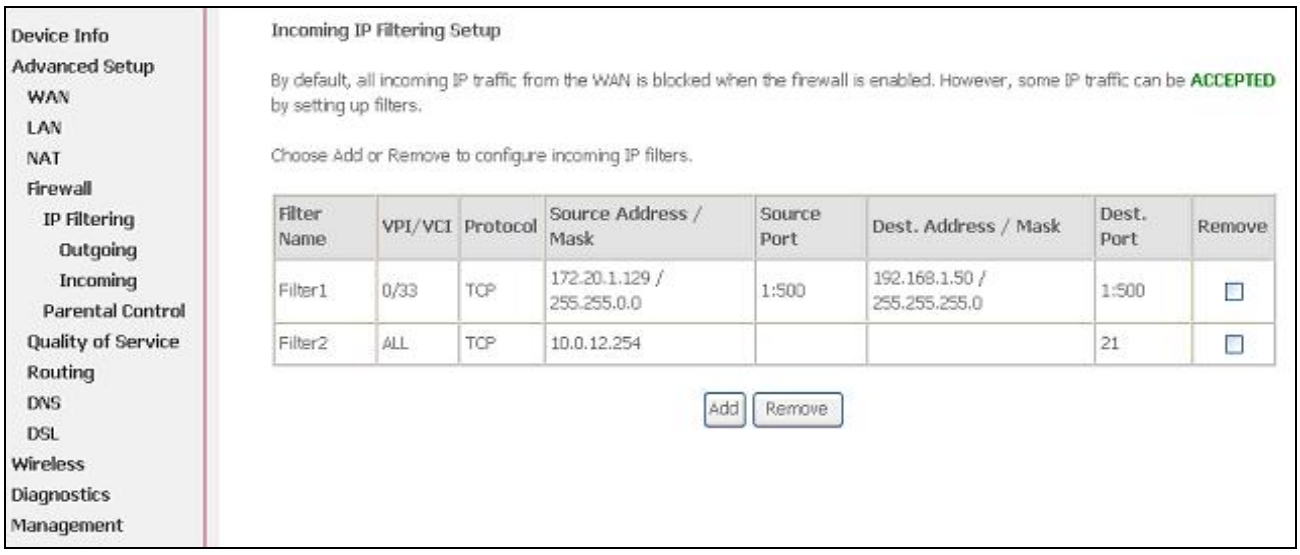


Figure 35. Advanced Setup – Firewall – Incoming IP Filter

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one of the conditions 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. **Figure 36** shows the configuration that allows a remote PC (IP address: 10.0.12.254) to access the local FTP server.

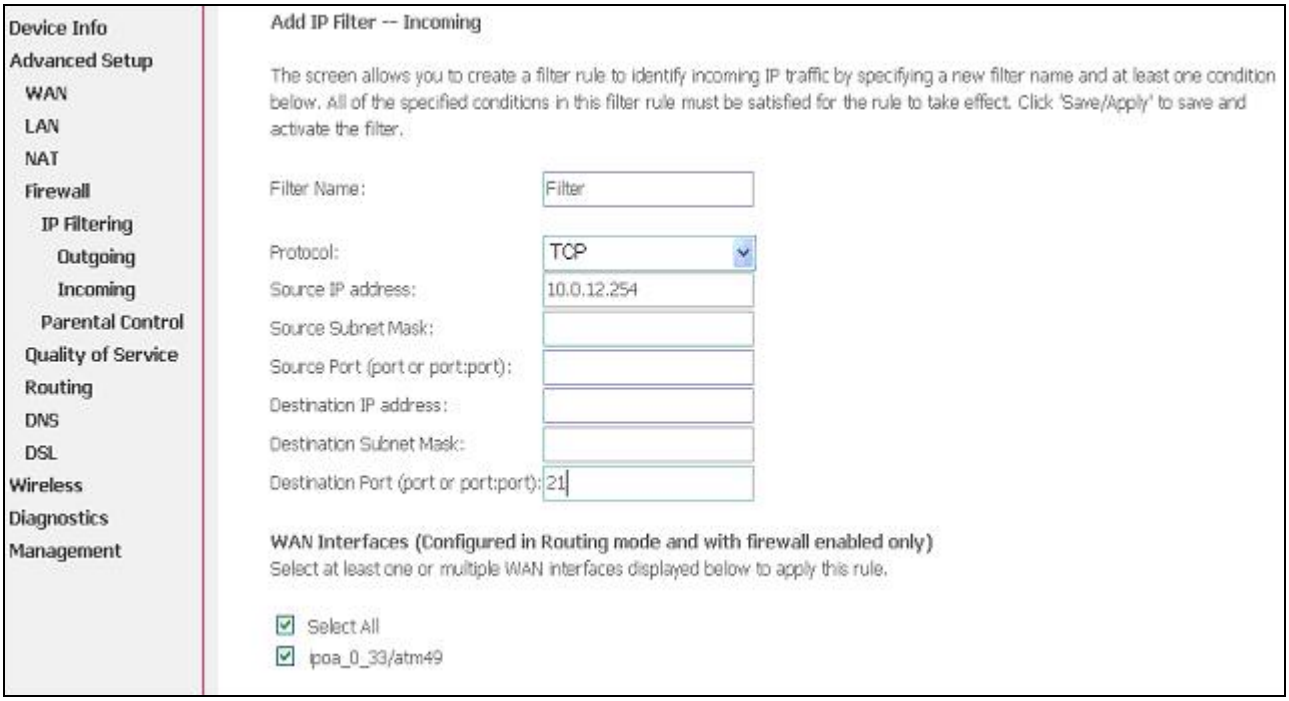


Figure 36. Advanced Setup – Firewall – Add new Incoming IP Filter

5.4.3 Firewall – Parental Control

Parental Control allows user to create time of day restriction to a special LAN device connected to the Router. Click “Add” to configure restriction rules. To remove, check the item and click “Remove”. Up to 16 entries can be configured and used.

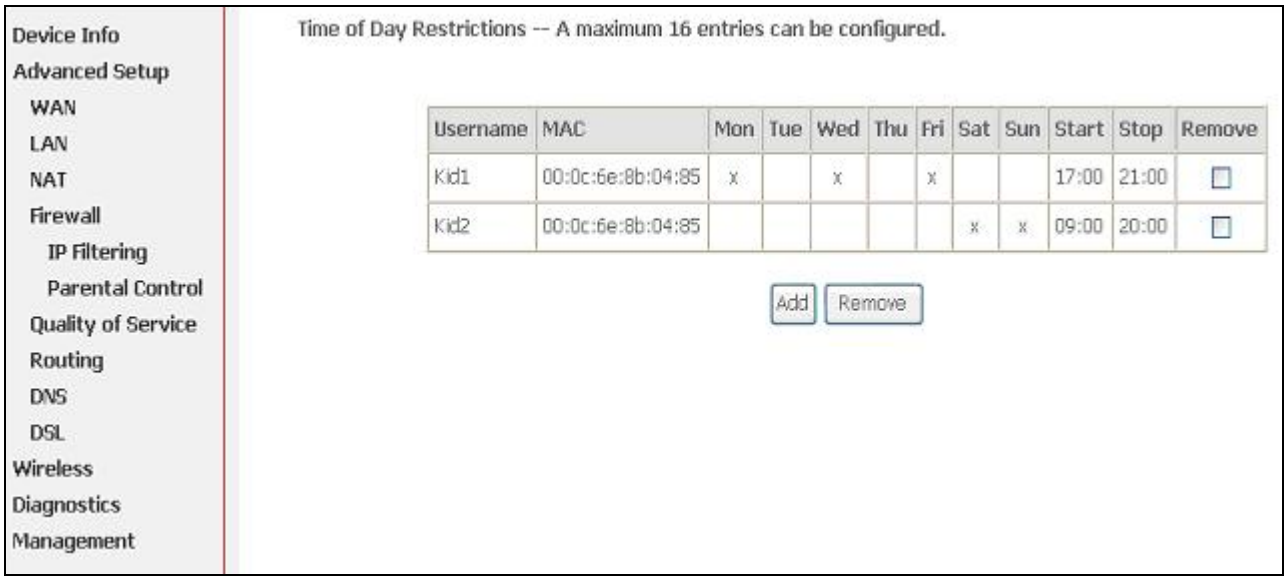


Figure 37. Advanced Setup – Firewall – Parental Control

The MAC Address of the “Browser” 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”. Click “Save/Apply” to save and activate the restriction rule.

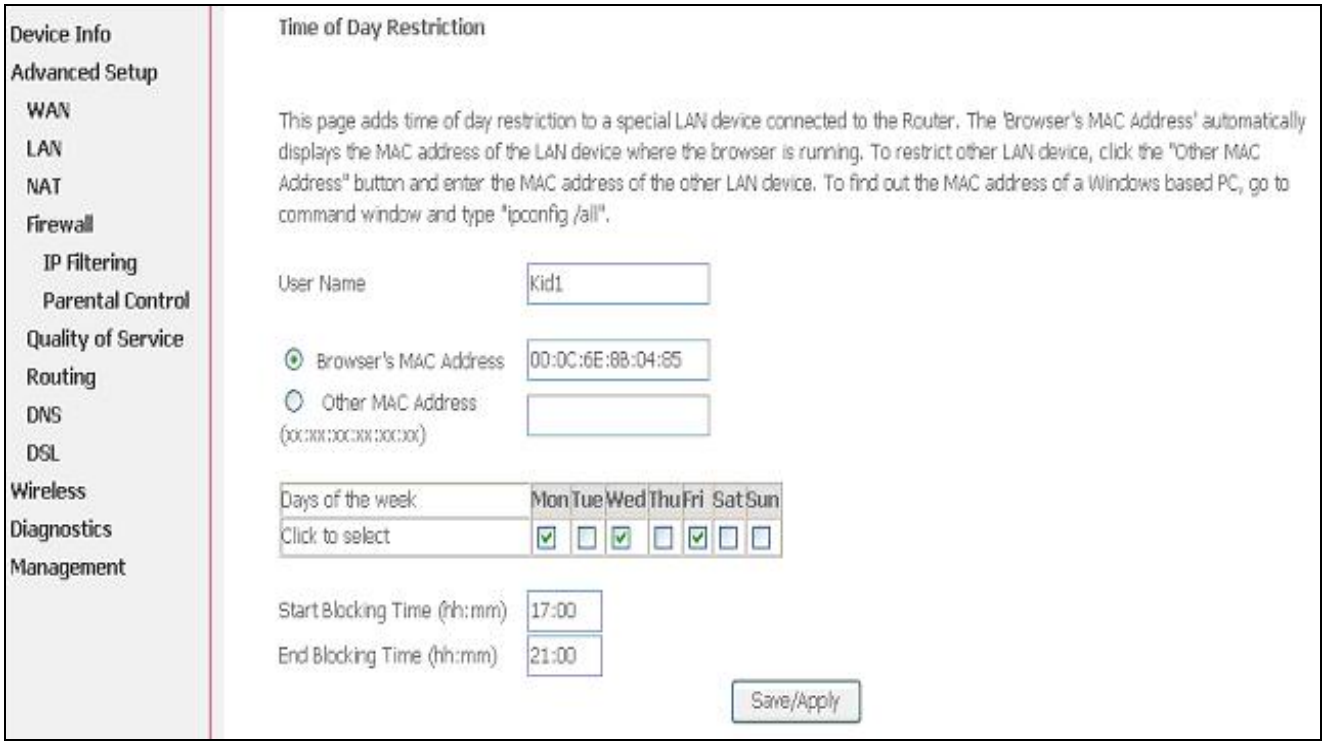


Figure 38. Advanced Setup – Firewall – Add new Parental Control

5.5 Quality of Service

Quality of Service (QoS) (including IP Precedence, IP TOS and IEEE 802.1P) refers to a combination of mechanisms that jointly provide a specific quality level to application traffic crossing a network or multiple, disparate networks.

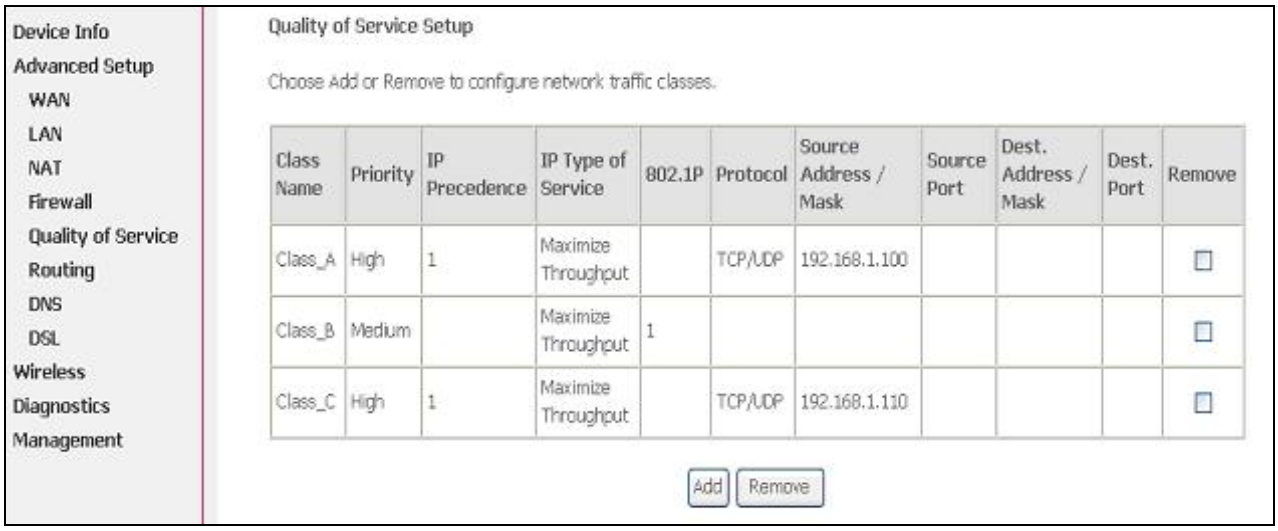


Figure 39. Advanced Setup – Quality of Service

Click on “Add” to create a class to identify the IP traffic by specifying at least one condition below. If multiple conditions are specified, all of them take effect.

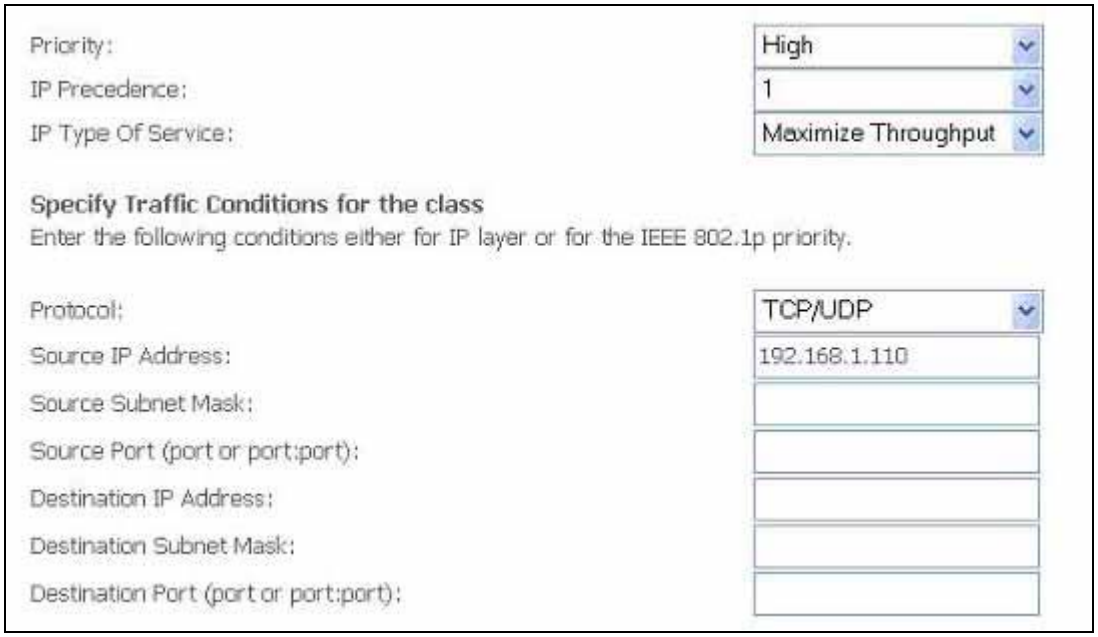


Figure 40. Advanced Setup – Add new QoS rule

5.6 Routing

There are three routing information related settings.

5.6.1 Routing – Default Gateway

If “Enable Automatic Assigned Default Gateway” checkbox is selected, AW4038 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 “Apply” button to save it.

NOTE: If changing the “Enable Automatic Assigned Default Gateway” from unselected to selected, You must reboot AW4038 to activate the automatic assigned default gateway.

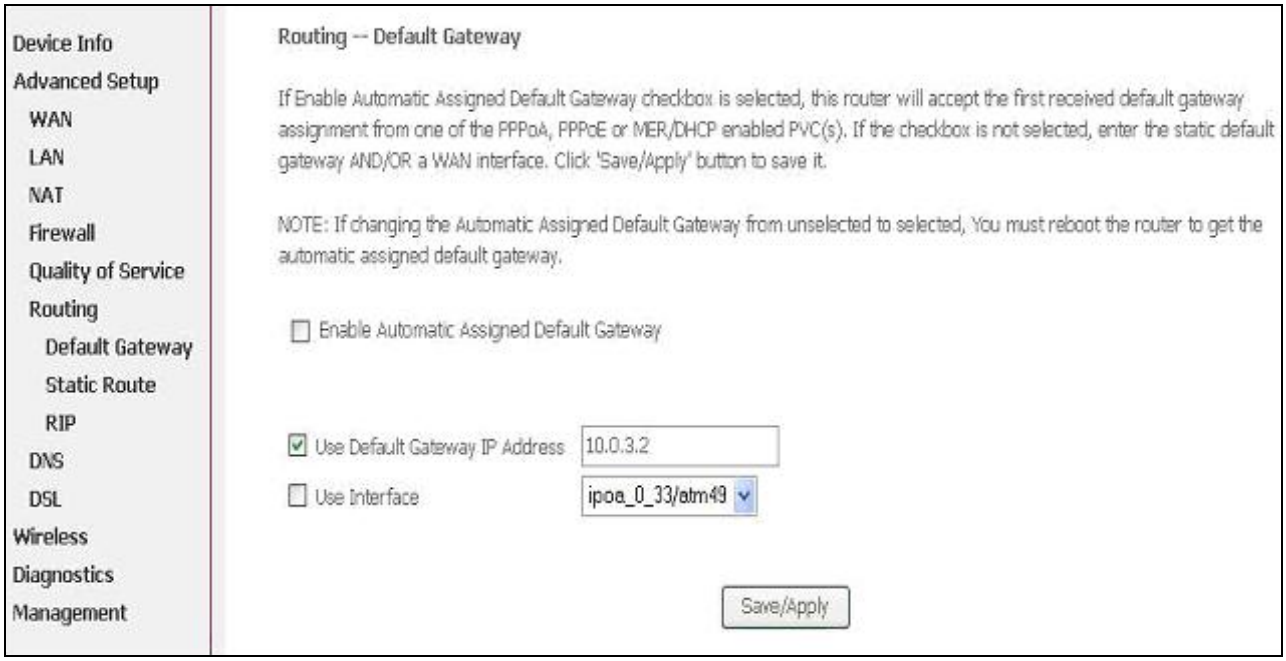


Figure 41. Advanced Setup – Routing – Default Gateway

5.6.2 Routing – Static Route

Click on “Add” to create a new Static Route. Up to 32 entries can be configured.

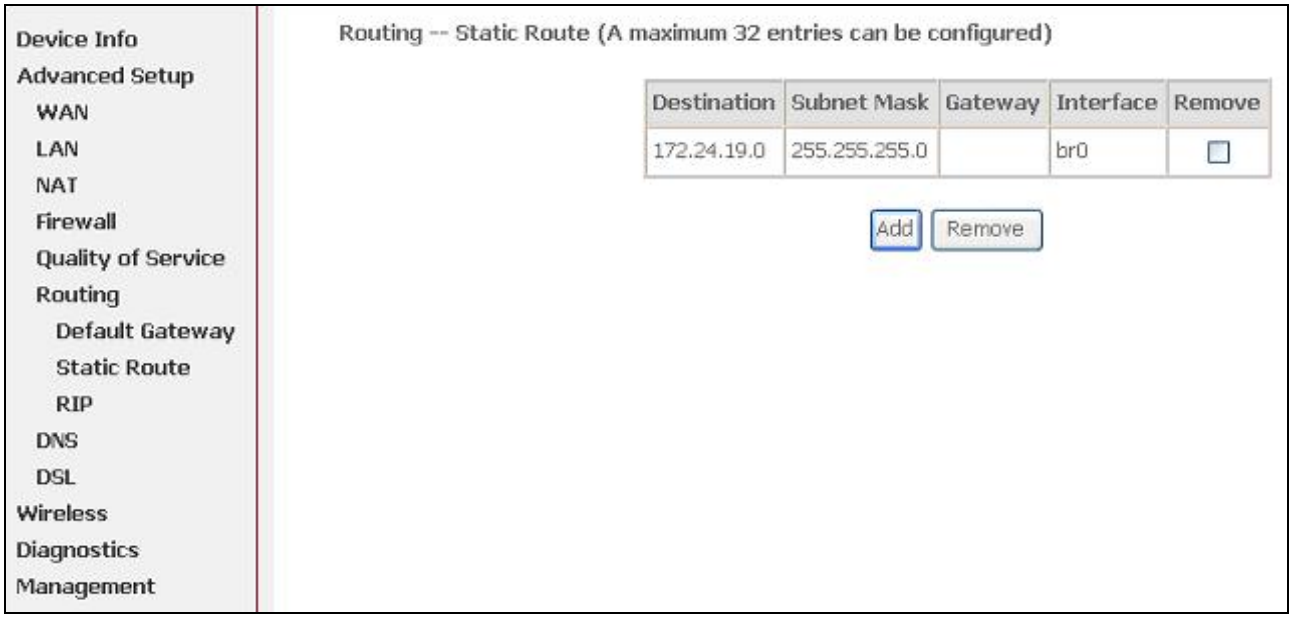


Figure 42. Advanced Setup – Routing – Static Route

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface, then click “Apply” to add the entry to the routing table.

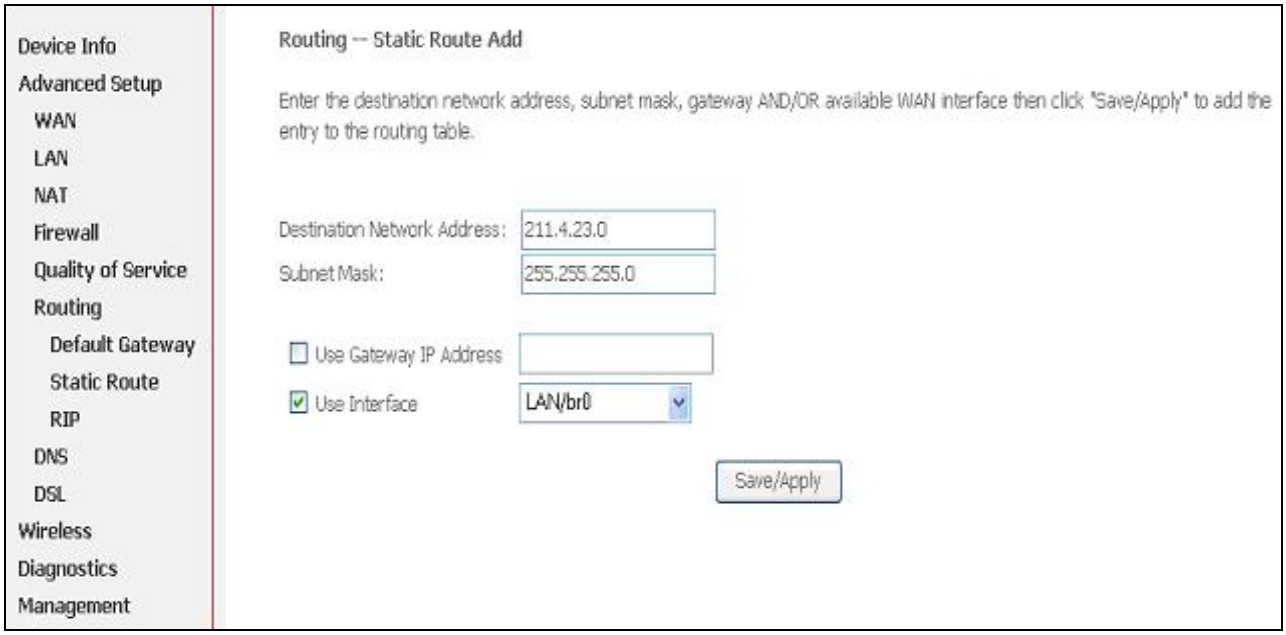


Figure 43. Advanced Setup – Routing – Add new Static Route

5.6.3 Routing – RIP

The Routing Information Protocol (RIP) is designed for exchanging routing

information within a small to medium-size Internetwork.

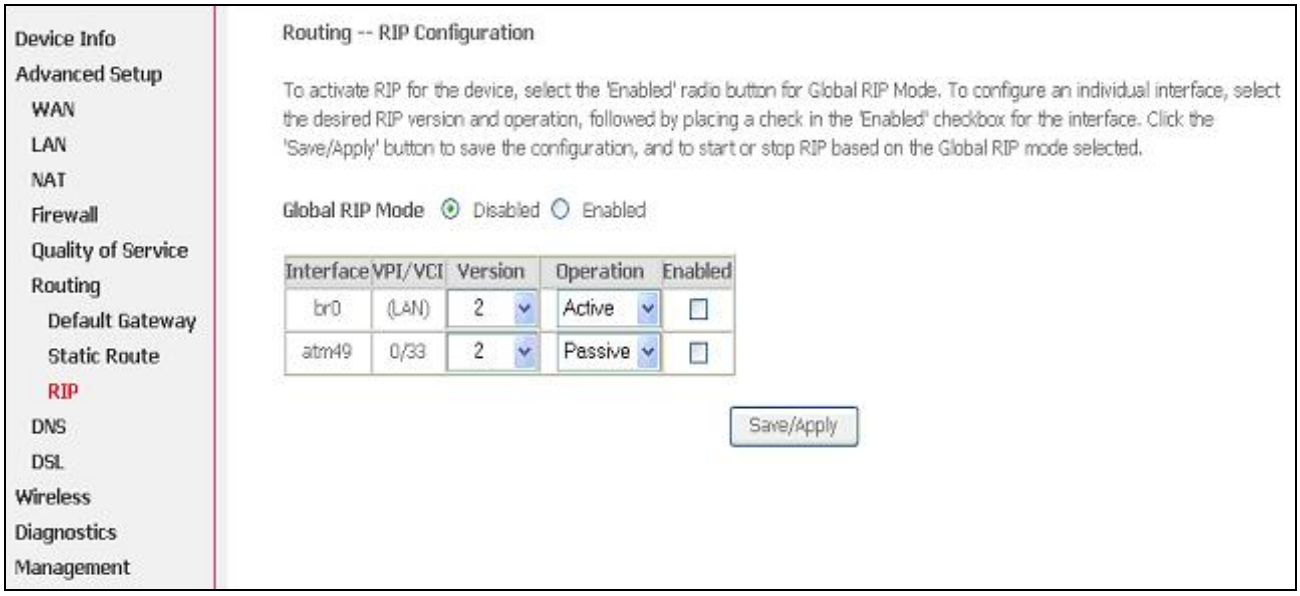


Figure 44. Advanced Setup – Routing – RIP

To configure an individual interface, select the desired RIP version and operation:

RIP Version 1: Class-based IP network.

RIP Version 2: Classless IP network.

Operation Active: Broadcast and listen to other RIP enabled devices.

Operation Passive: Listen only.

Placing a check in the “Enabled” checkbox for the interface to complete the configuration. Click the “Apply” button to save the configuration. To start/stop RIP for AW4038, select the “Enabled/Disabled” radio button for Global RIP Mode.

5.7 DNS

5.7.1 DNS Server

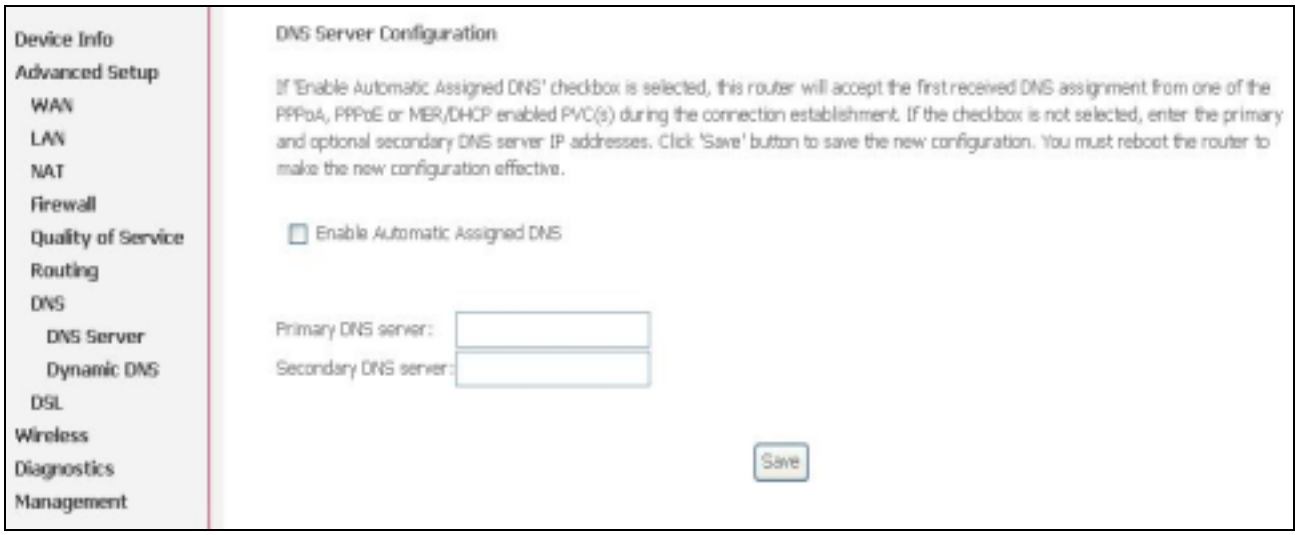


Figure 45. Advanced Setup – DNS Server

If “Enable Automatic Assigned DNS” checkbox is selected, AW4038 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 “Apply” button to save it.

NOTE: If changing from unselected “Enable Automatic Assigned DNS” to selected, you must reboot AW4038 to get the automatic assigned DNS addresses.

5.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the domains. This function allows your AW4038 to be more easily accessible from various locations of the Internet.
Choose “Add” to configure Dynamic DNS.

Before you proceed, please visit one of these two website to apply your own Dynamic DNS service: www.dnadns.org or www.tzo.com.

To remove, check the item and click “Remove”

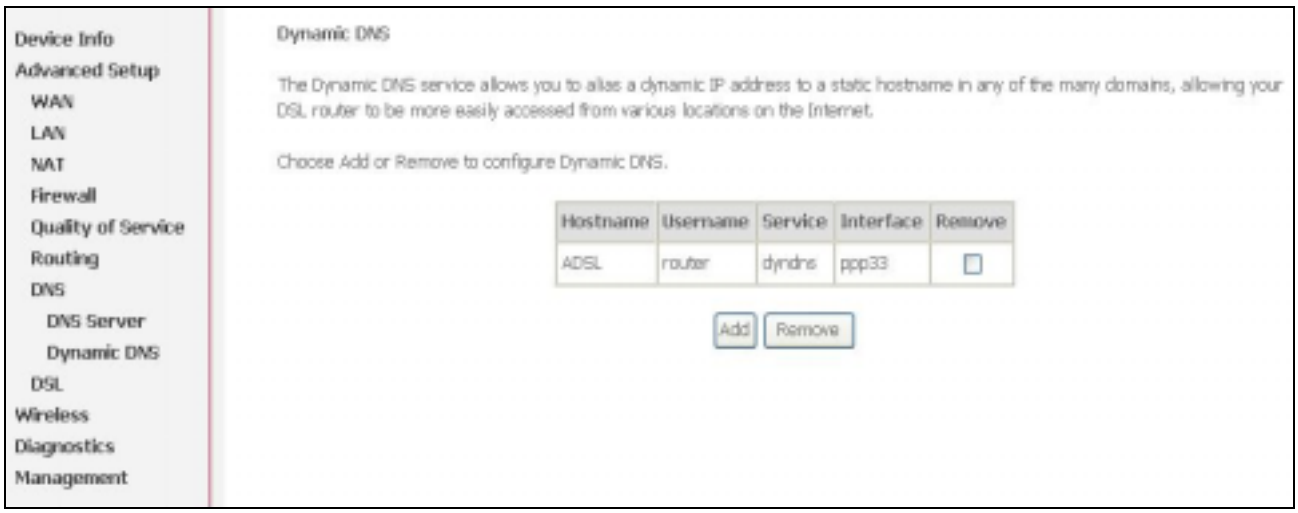


Figure 46. Advanced Setup – DNS – Dynamic DNS

Select your Dynamic DNS service provider from 'D-DNS provider', and enter your registration information. Click "Save/Apply" to save the configuration.

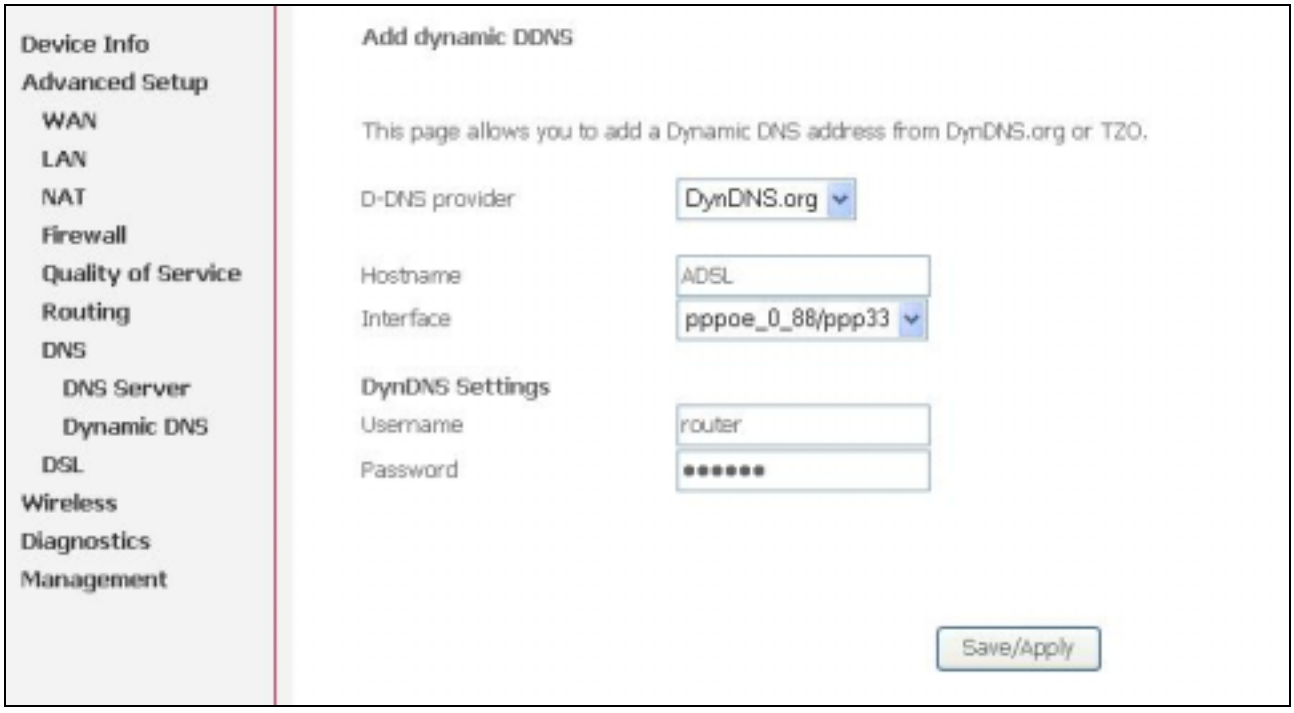


Figure 47. Advanced Setup – DNS – Add Dynamic DNS

6. Wireless Setup

6.1 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 (no broadcasting of your network name), set the wireless network name (also known as SSID, default: **airgw**), and restrict the channels based on nation's requirements. Click "Save/Apply" to save the configurations.

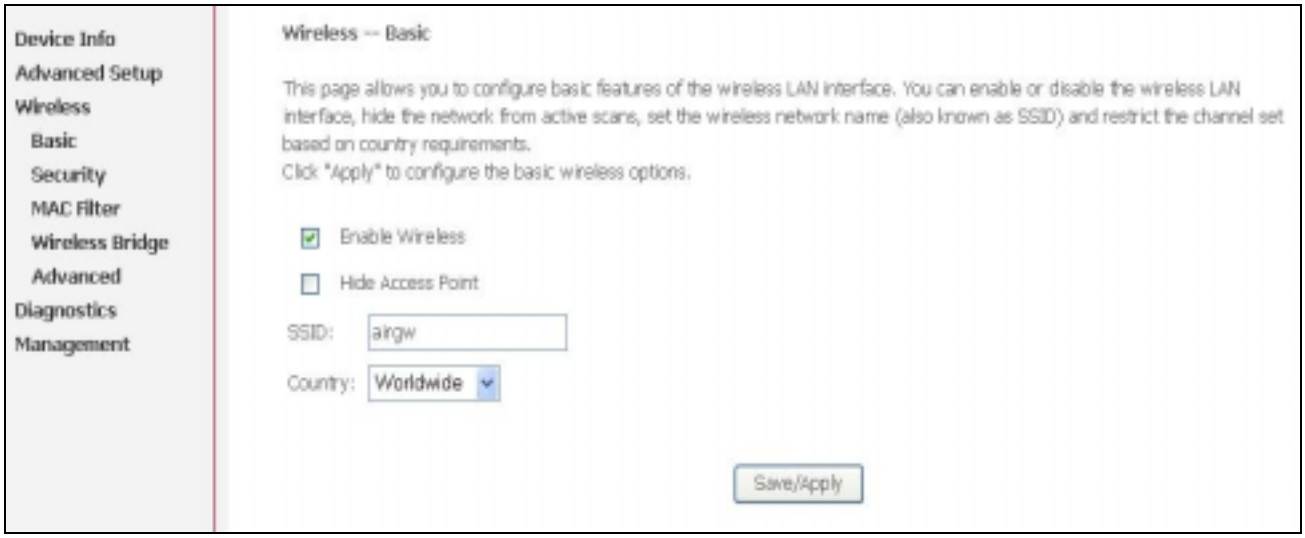


Figure 48. Wireless Setup – Basic

6.2 Security

Four types of wireless security are provided: Shared (WEP), 802.1x, WPA/WPA2, and WPA/WPA2-PSK.

6.2.1 WEP

WEP (**W**ired **E**quivalent **P**rivacy) provides security by encrypting data over radio waves when data is transmitted from one end point to another. WEP is the weakest security method but the easiest one to configure. To enable WEP, select the following items step by step:

Network Authentication: Shared

Data Encryption: Enabled

Encryption Strength: 128-bit (recommended for better security) or 64-bit

Click "Set Encryption Key" to enter your WEP keys.

Figure 49. Wireless Setup – Security – WEP

Four keys for both encryption strengths can be stored here. 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. Select which key (1 ~ 4) to use from “Current Network Key”. Click “Save/Apply” to save the configuration.

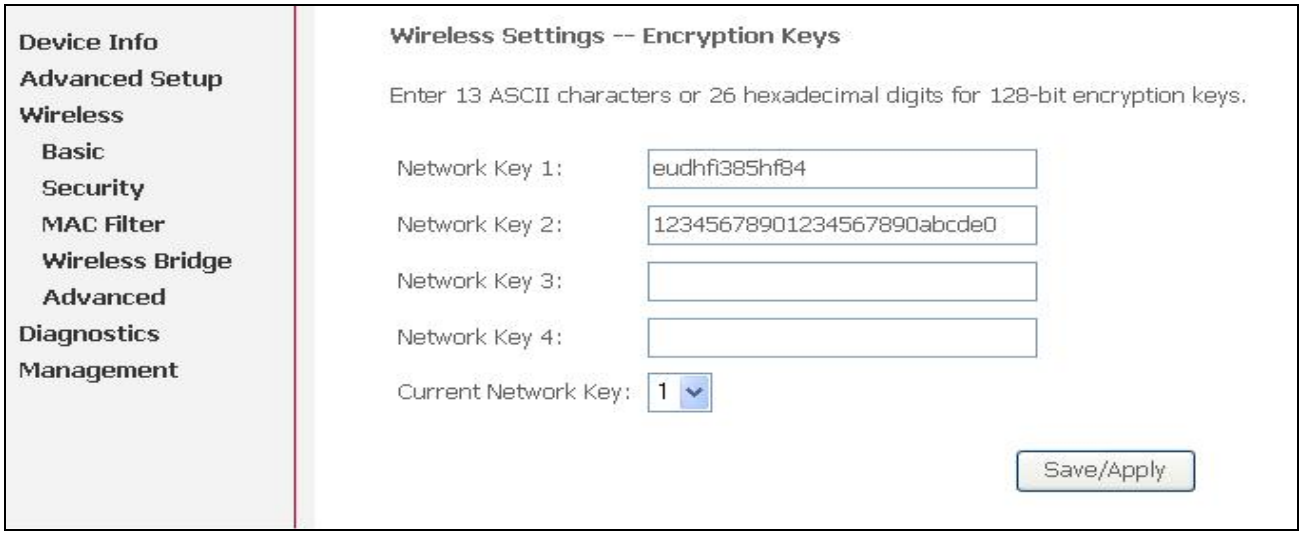


Figure 50. Wireless Setup – Security – WEP

6.2.2 802.1X

802.1X addresses the WEP weakness by adding user authentication, via RADIUS server. So you need to have your RADIUS server up and running before using 802.1X. To enable 802.1X, select “802.1X” in “Network Authentication”. Enter your RADIUS server IP address, port number (default: **1812**), and key. Follow section 6.2.1 to configure your WEP key and select “Save/Apply” to save your configuration.

Figure 51. Wireless Setup – Security – 802.1X

6.2.3 WPA/WPA2

WPA (Wi-Fi Protected Access) is the strongest wireless security provided by AW4038. Like 802.1X, WPA must co-work with RADIUS server as well. To enable WPA, select the following items step by step:

Network Authentication: WPA/WPA2

WPA Group Rekey Interval: in seconds. Default: **0** (no re-keying).

RADIUS Server IP Address/Port/Key: must match your RADIUS server.

WPA Encryption: TKIP (select AES or TKIP+AES for WPA2).

Check your supplicant capability before you decide which one to use.

Figure 52. Wireless Setup – Security – WPA

6.2.4 WPA/WPA2-PSK

WPA-PSK lets you take advantage of WPA without the hassle of setting up your own RADIUS server. To enable WPA-PSK, select “WPA-PSK” in “Network Authentication”. Enter 8 to 63 ASCII codes or 64 hexadecimal (0~9, A~F) digits in “WPA Pre-Shared Key”. Click “Save/Apply” to save the configuration.

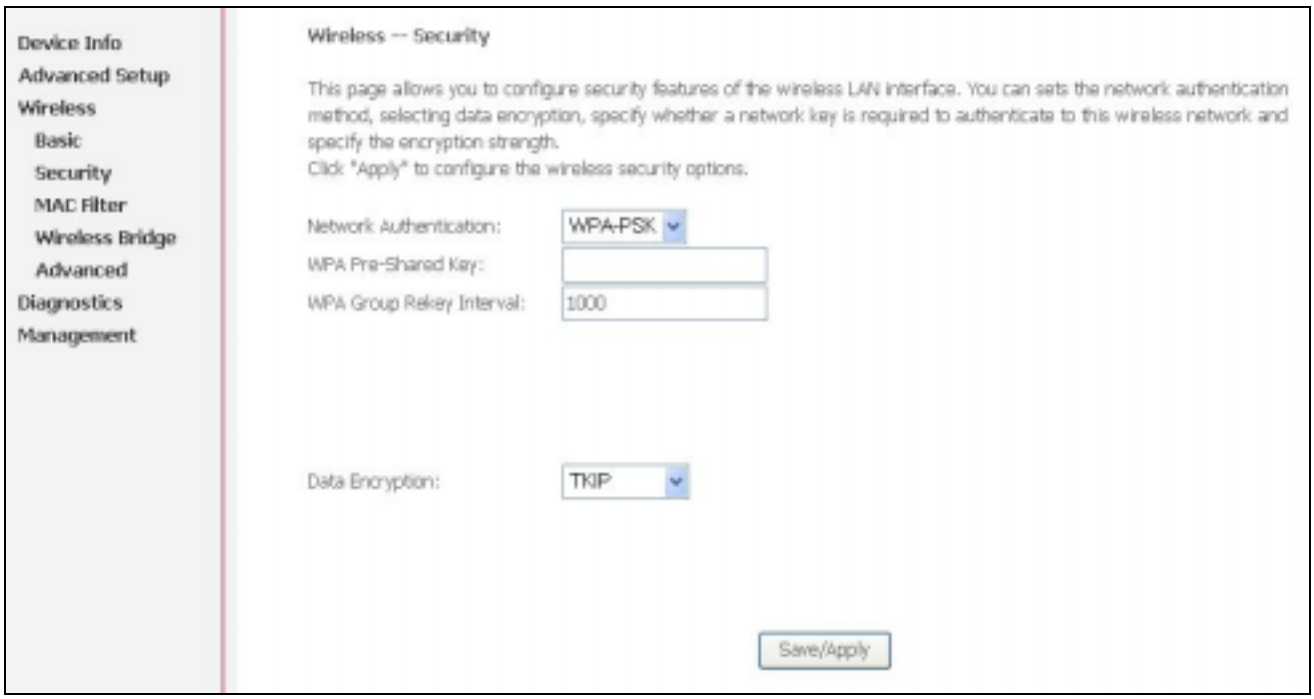


Figure 53. Wireless Setup – Security – WPA-PSK

6.3 MAC Filter

Wireless MAC filter allows you to implement access control based on device's MAC address.

When you select "Allow" in "MAC Restrict Mode", only data from devices with matching MAC addresses in filter table can access AW4038. If you select "Deny" in "MAC Restrict Mode", every device can access AW4038 except those which have matching MAC addresses in the filter table. To add filter entry, click on "Add" and enter the MAC address of AW4038. Click "Save/Apply" to save the configuration. To "delete" the entry, select the entry and click "Remove".

Figure 54. Wireless Setup – MAC Filter

6.4 Wireless Bridge

Wireless Bridge (also known as Wireless Distribution System) can bridge data between two APs, which is particularly useful while wired cabling is not available.

Note: only APs in same channel can be bridged.

AP Mode: Wireless Bridge- listens and answers other APs only

Access Point- Wireless Bridge also with AP functionality

Bridge Restrict: Disabled- any AP will be granted access

Enabled- only selected APs (Max. 4) with specified MAC address will be granted access

Enabled (Scan)- as above, but AW4038 will scan available AP for you to select.

Refresh: re-scan the available AP

Save/Apply: save the configuration

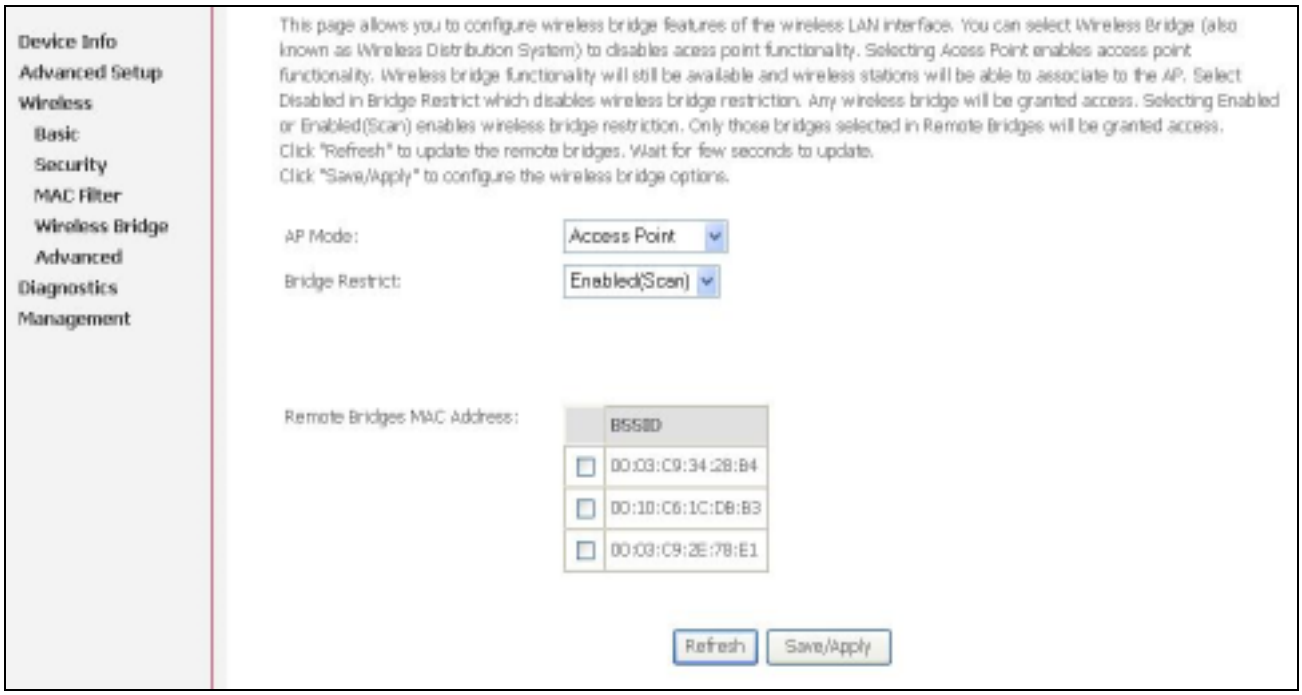


Figure 55. Wireless Setup – Wireless Bridge

6.5 Advanced

In most cases, AW4038 work well with wireless default settings. Modification is not recommended unless you are very familiar with these parameters.

Channel: Select the appropriate channel from the provided list to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly. Default: **7**.

Rate: The range is from 1 to 54Mbps. The data transmission rate should be set according to the speed of your wireless network. You can set one transmission speed, or keep the default setting “Auto” to have the router automatically detect the fastest possible data rate.

Basic Rate Set: Select the basic rate that wireless clients must support.

Fragmentation: This value should remain at its default setting of **2346**. The range is 256-2346 bytes. This value specifies the maximum packet size before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly lower the Fragmentation value. Setting the Fragmentation too low may result in poor network performance. Only slight adjustment of this value is recommended.

RTS Threshold: This value should remain at its default setting of **2347.** The range is 0-2347 bytes. Should you encounter inconsistent data flow, only

slight adjustment of this value is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. AW4038 sends Request to Send (RTS) frames to a particular receiving station and negotiates the transmission of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

DTIM Interval: This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM interval is a countdown field which is used to inform clients about the next window for listening to broadcast and multicast messages. When AW4038 has buffered broadcast or multicast for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast message. Default: **3**.

Beacon Interval: Enter a value between 1 and 65535 milliseconds. The Beacon Interval indicates the frequency interval of the beacon. A beacon is a packet broadcast by AW4038 to synchronize the wireless network. Default: **100**.

54g Mode: There are 3 selections. Select **54g Auto** for the widest compatibility. Select **54g Performance** for the fastest performance. Select **54g LRS** if you are experiencing difficulty with legacy 802.11b equipment.

54g protection: In **Auto** mode, AW4038 will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b network. Turn **off** protection to maximize 802.11g throughput under most conditions.

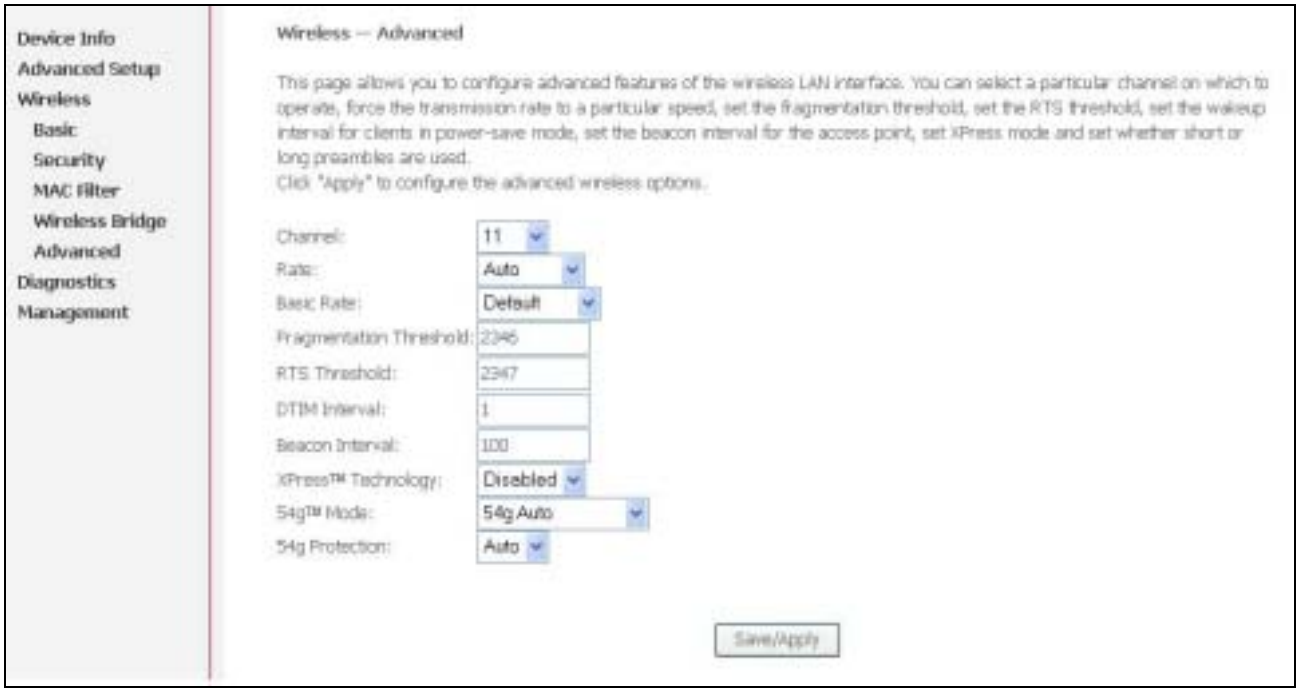


Figure 56. Wireless Setup – Advanced

6.6 Station Info

This page shows authenticated wireless stations and their status.

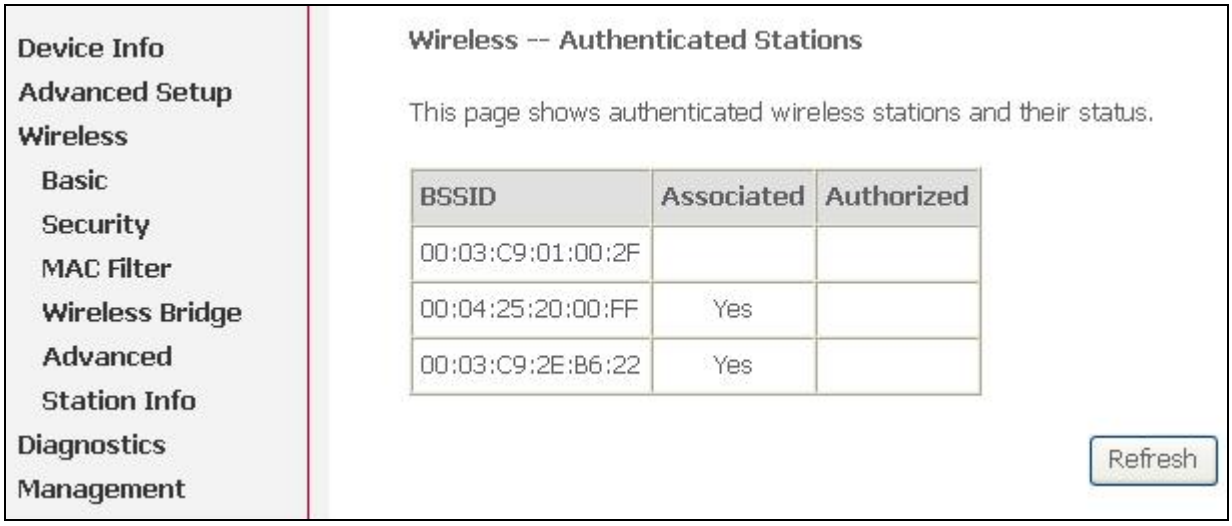


Figure 57. Wireless Setup – Station Info

7. Diagnostics

This page allows users to test the Ethernet port connection, DSL port connection, and connection to the Internet Service Provider. If a test displays a fail status, click “Return Diagnostic Tests” at the bottom of the page to make sure the fail status is consistent. If the test continues to show fail, click “Help” to go to the troubleshooting procedures.

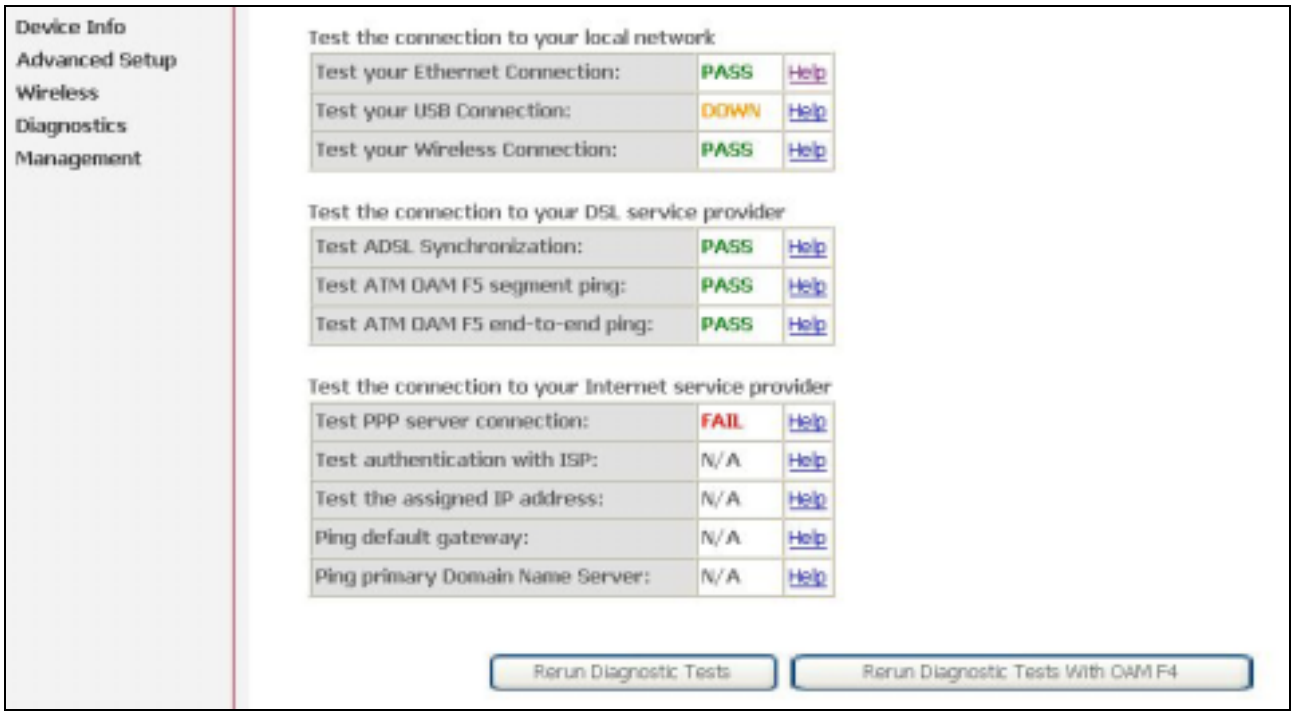


Figure 58. Diagnostics

8. Management

8.1 Settings

System Administrator can do the AW4038 settings backup, update, and restore default here. The settings can be saved from AW4038 to PC. The saved setting file can also be loaded from PC to AW4038. These 2 functions can help the system administrator to manage large amount of AW4038 efficiently. Restore Default would set the AW4038 with the factory default configuration.

To backup the current configurations, click on “Backup Settings”, and a File Download window will pop up.

Figure 59. Management – Settings – Backup Settings

Click on “Save” and select the destination of the backup file (backupsettings.cfg) in your local PC. Click on “Save” again to save your backup file.

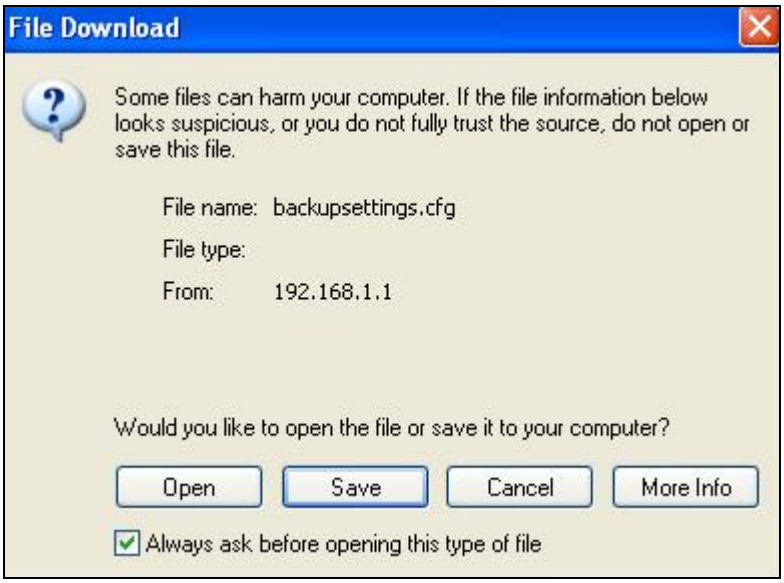


Figure 60. Management – Settings – File Download

To update the configuration, click on “Browse” and a Choose-File-window will pop up. Locate the saved file and click on “Update Settings”. AW4038 will modify its settings based on the update file.

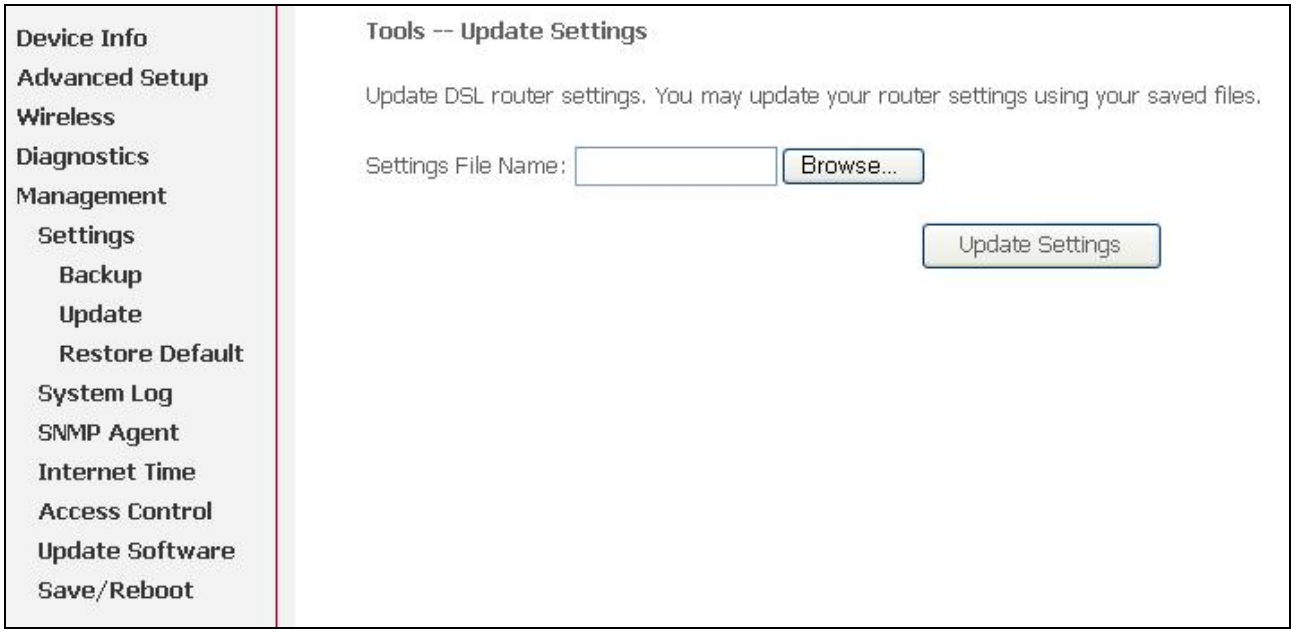


Figure 61. Management – Settings – Update

To restore the router to its factory default settings, click on “Restore Default Settings”.

Figure 62. Management – Settings – Restore Default

8.2 System Log

This allows System Administrator to view the System Log and configure the System Log options.

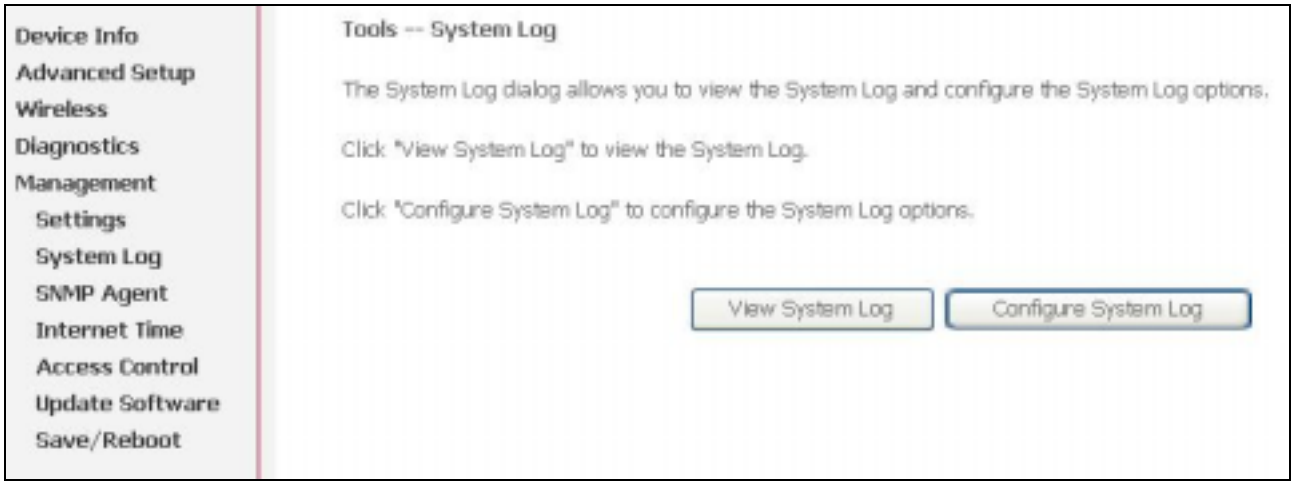


Figure 63. Management – System Log

Click on “Configure System Log” to configure the log options. There are 8 events of “Log Level” and “Display Level”: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, and **Debugging**. If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed.

If the selected mode is “Remote” or “Both”, events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is “Local” or “Both”, events will be recorded in the local memory. Click on “Save/Apply” to save the configuration.

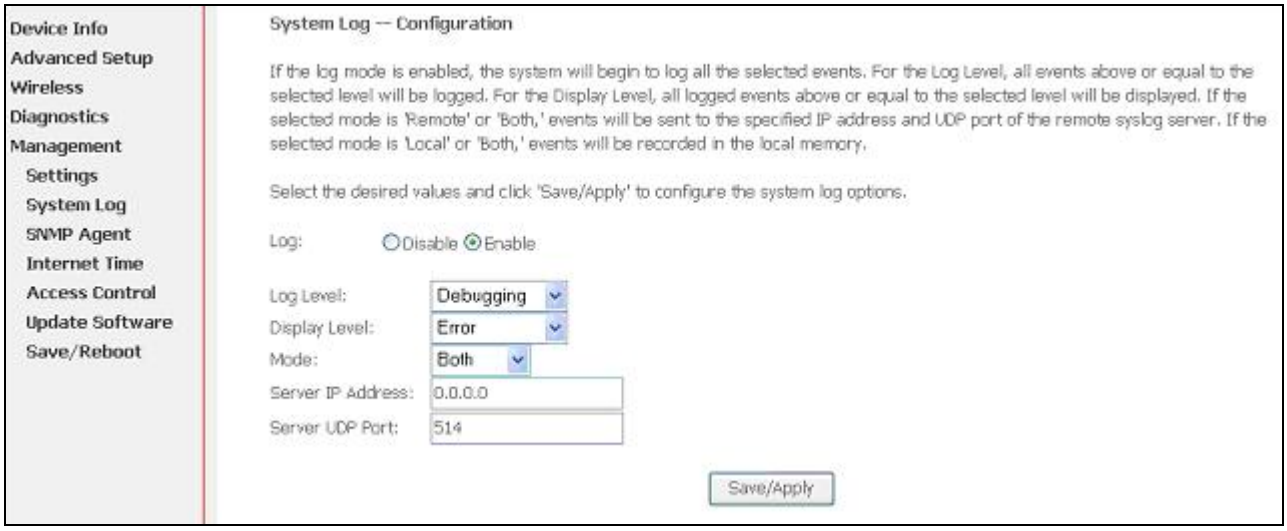


Figure 64. Management – System Log Configuration

Click on “View System Log” to see the router log based on your configuration.

8.3 SNMP Agent

System Administrator could enable or disable the embedded SNMP Agent here. SNMP Agent would allow a management application to retrieve AW4038 statistics and status.

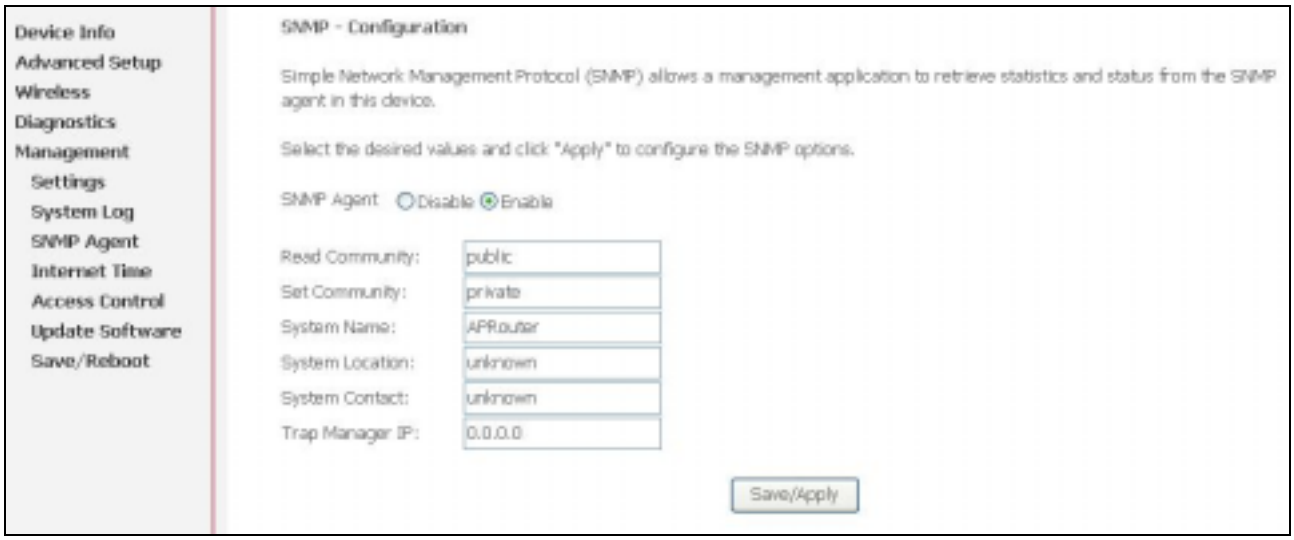


Figure 65. Management – SNMP Agent

8.4 Internet Time

AW4038 can synchronize its internal time with Internet time server when available. To enable this function, check “Automatically synchronize with Internet time servers”. Select First and Second NTP time server from the pull down menu. Or select “Other” and define your preferred NTP server. Choose the time zone from “Time zone offset”. Click on “Save/Apply” to save the configuration.

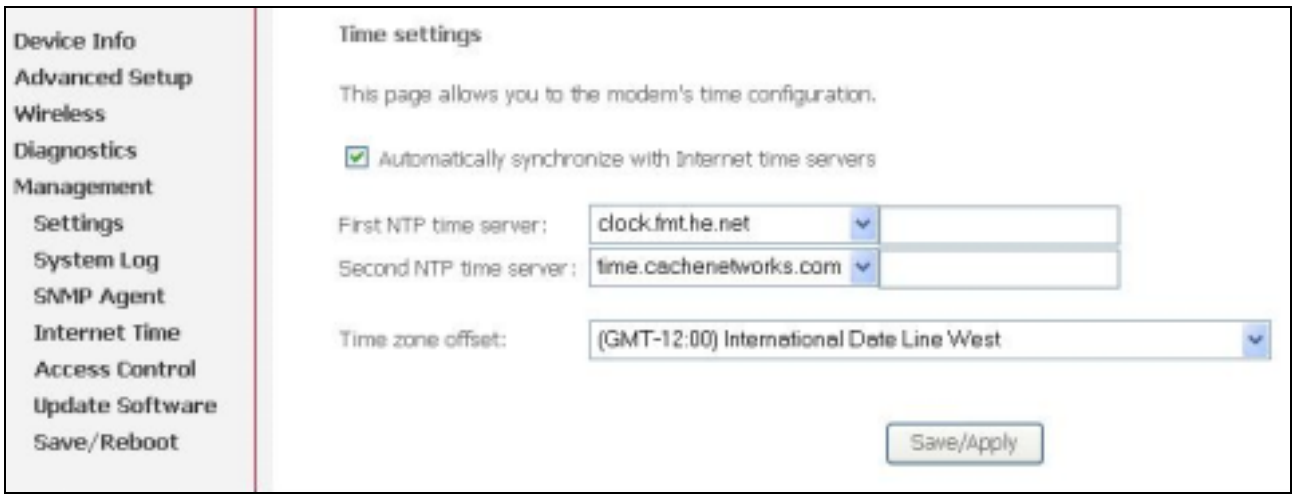


Figure 66. Management – Internet Time

8.5 Access Control

AW4038 browser management tool is protected by three categories: Services, IP addresses, and Passwords. All three must be matched, if configured, to gain access to the management tool.

All services are enabled from LAN side and disabled from WAN side by default.

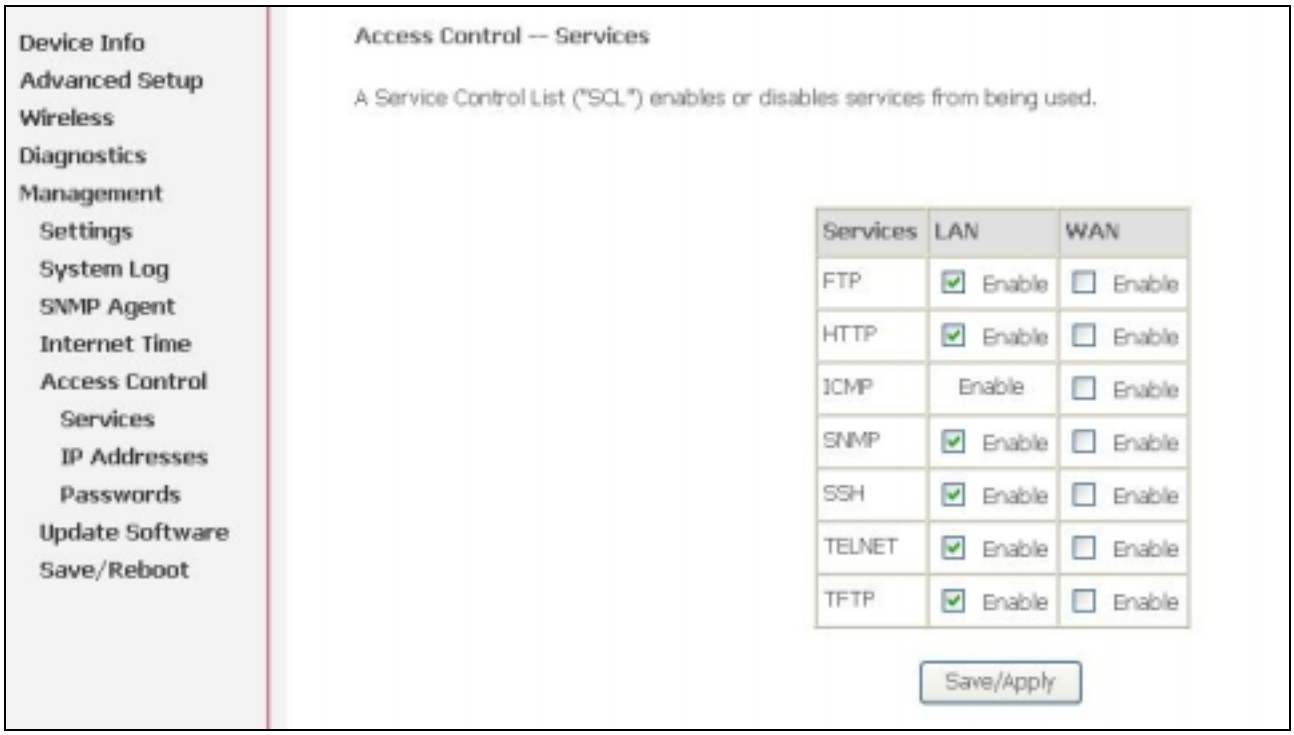


Figure 67. Management – Access Control - Service

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click “Add” to add an IP address to the Access Control List. To remove, mark the Remove option of the specified IP address, then click “Remove” to remove the IP address from the Access Control List. Up to 16 hosts can be configured here.

Figure 68. Management – Access Control – IP Addresses

Access to your router is controlled through three user accounts: **admin**, **support**, and **user**.

admin: has unrestricted access to change and view AW4038 configuration.

support: is used to allow an ISP technician to access AW4038 for maintenance and to run diagnostics.

user: can access AW4038 to view configuration settings and statistics, as well as,

update AW4038 software.

Use the fields below to enter up to 16 characters and click “Save/Apply” to change or create passwords.

Figure 69. Management – Access Control – Passwords

8.6 Update Software

The new software could be updated from the Local PC connected to AW4038 via Ethernet cable. Click on “Browse” to locate the new software image file in the PC. And then Click on “Update Software” to proceed the software update.

Note: The update process takes about 2 minutes to complete, and your AW4038 will reboot automatically.

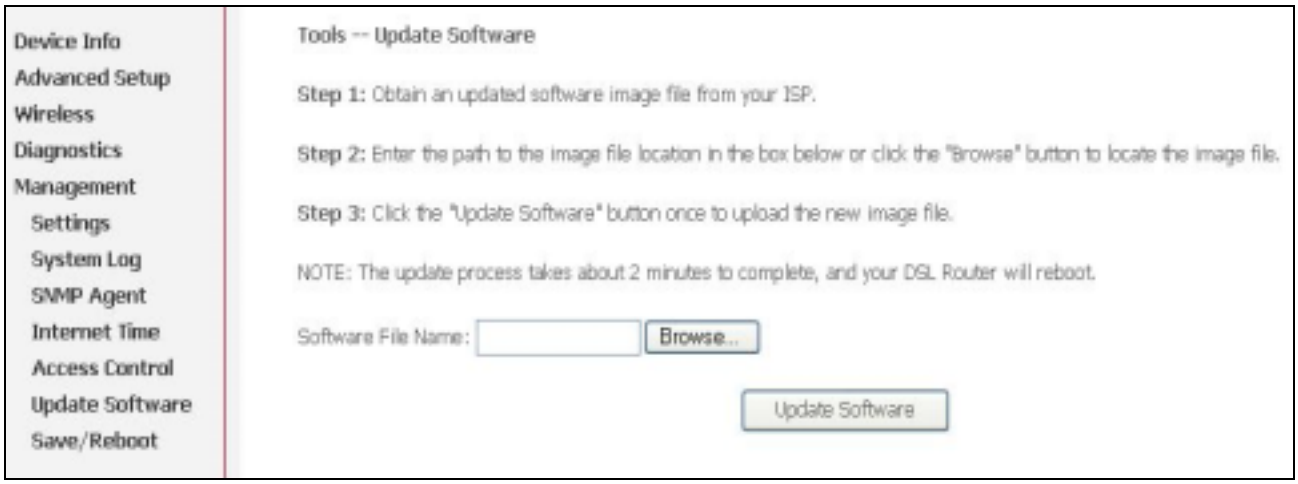


Figure 70. Management – Update Software

8.7 Save/Reboot

Click “Reboot Router” to reboot AW4038. AW4038 would automatically save the configuration before reboot, so that modified settings would take effect after reboot.

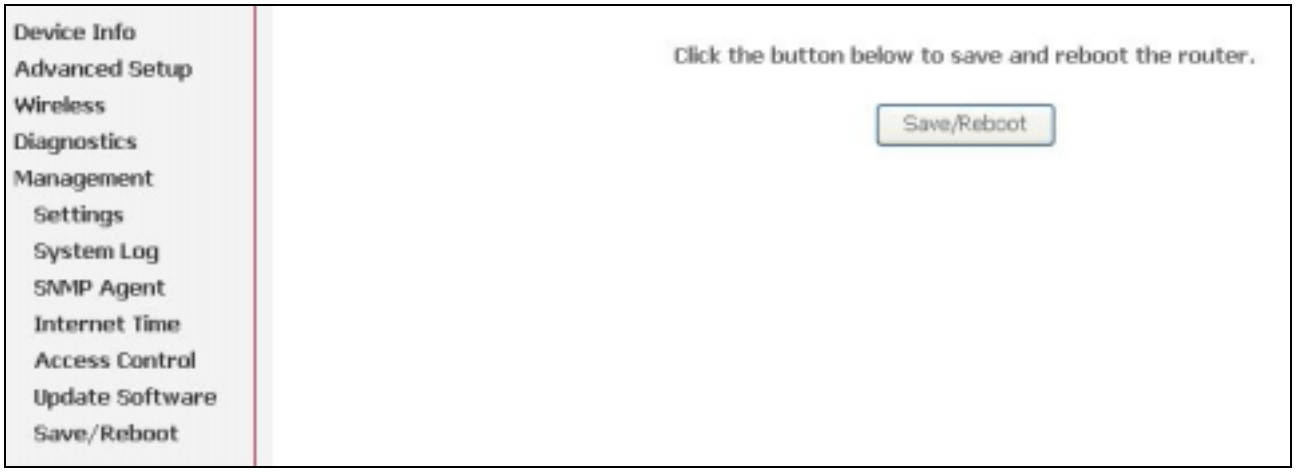


Figure 71. Management – Save and Reboot

9. Device Info

9.1 Summary

This page displays AW4038's hardware/software information and DSL connection status.

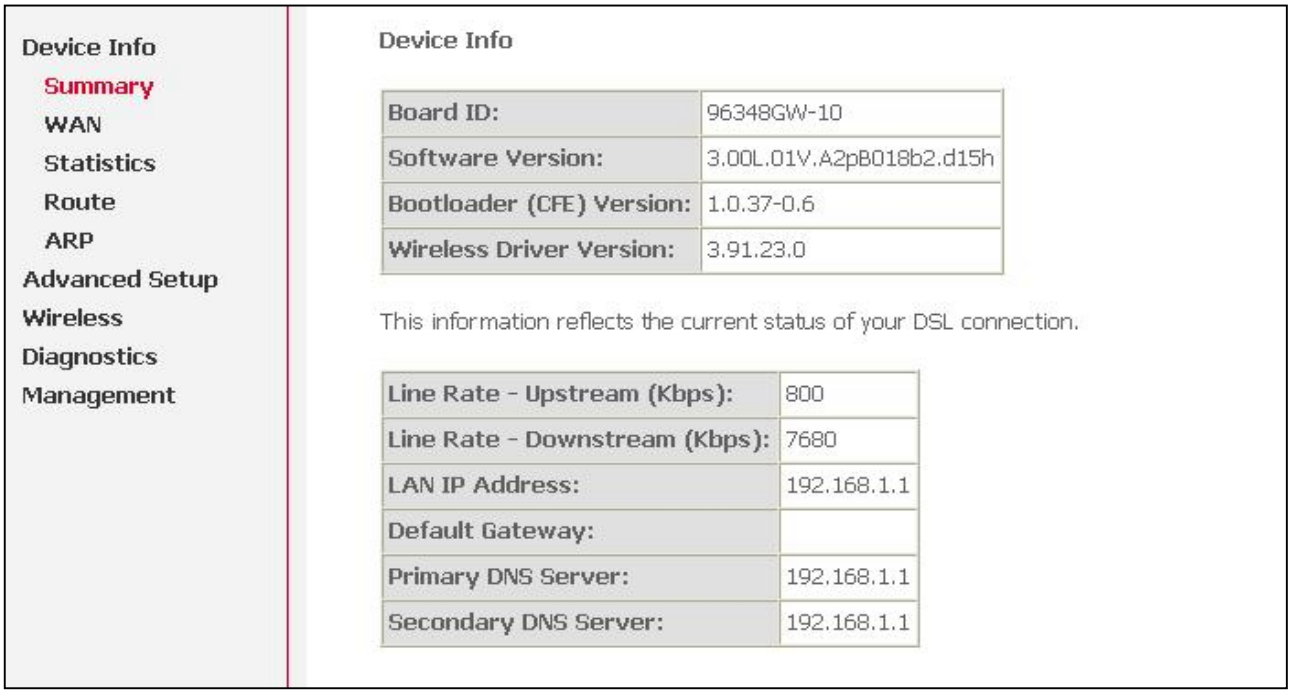


Figure 72. Device Info – Summary

9.2 WAN

This page displays AW4038's WAN interface information and connection status.

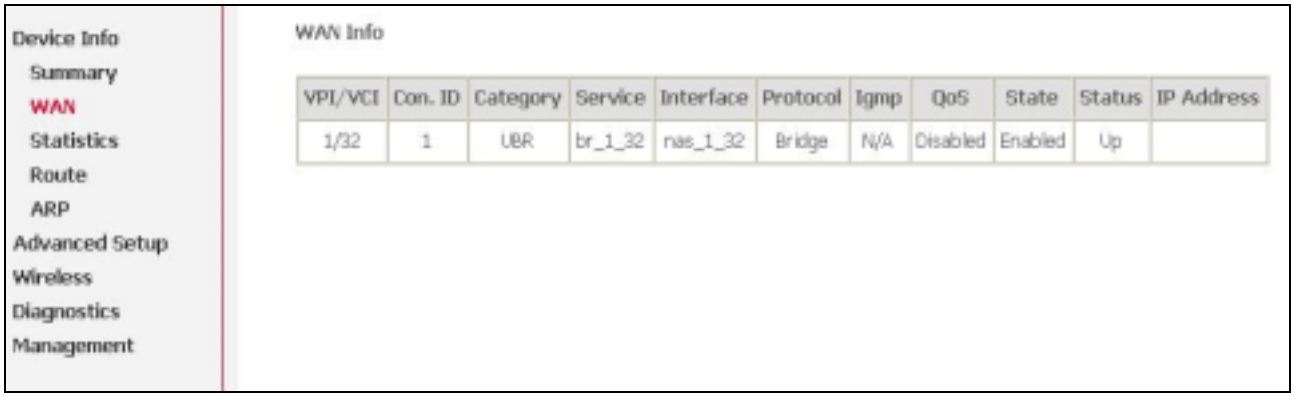


Figure 73. Device Info – WAN

9.3 Statistics

9.3.1 LAN/WAN

This page displays packets transmitted and received status of AW4038's LAN/WAN interfaces.

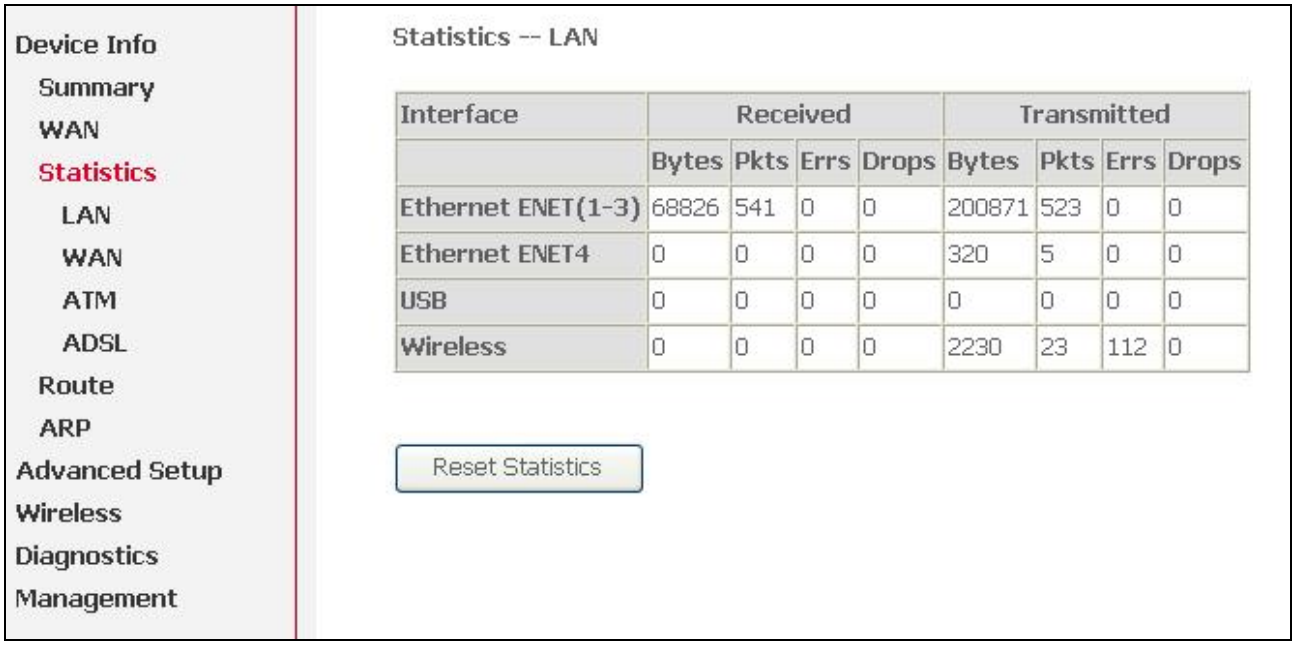


Figure 74. Device Info – Statistics – LAN

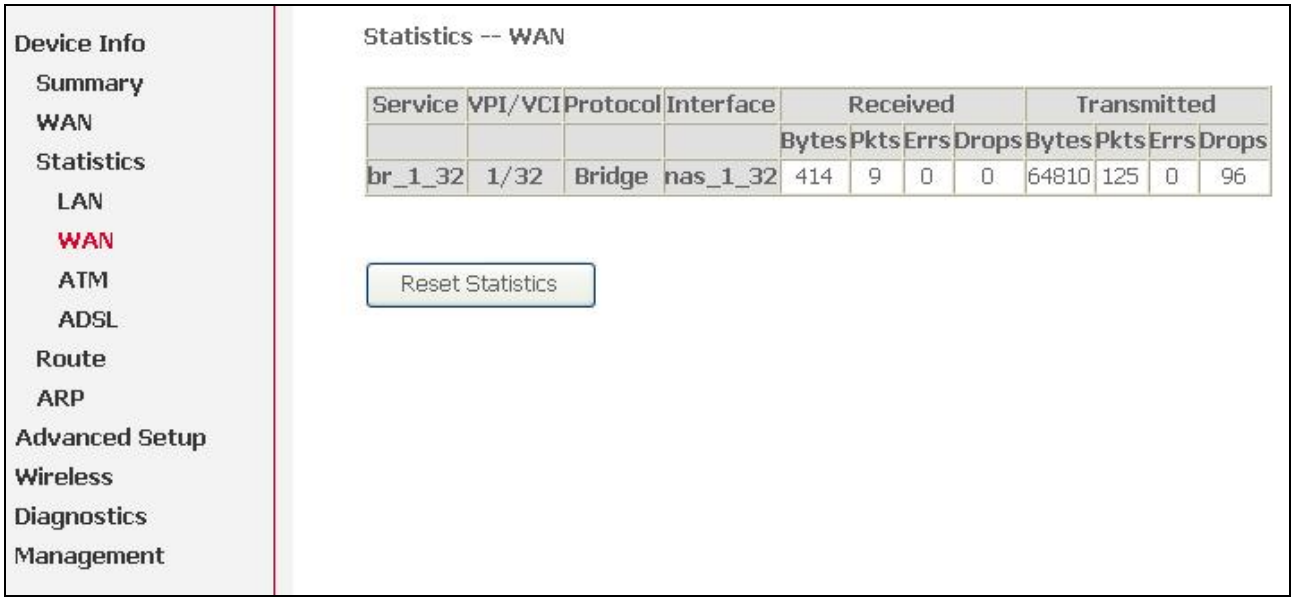


Figure 75. Device Info – Statistics – WAN

9.3.2 ATM

This page displays the statistics of AW4038's ATM interface (including AAL5).

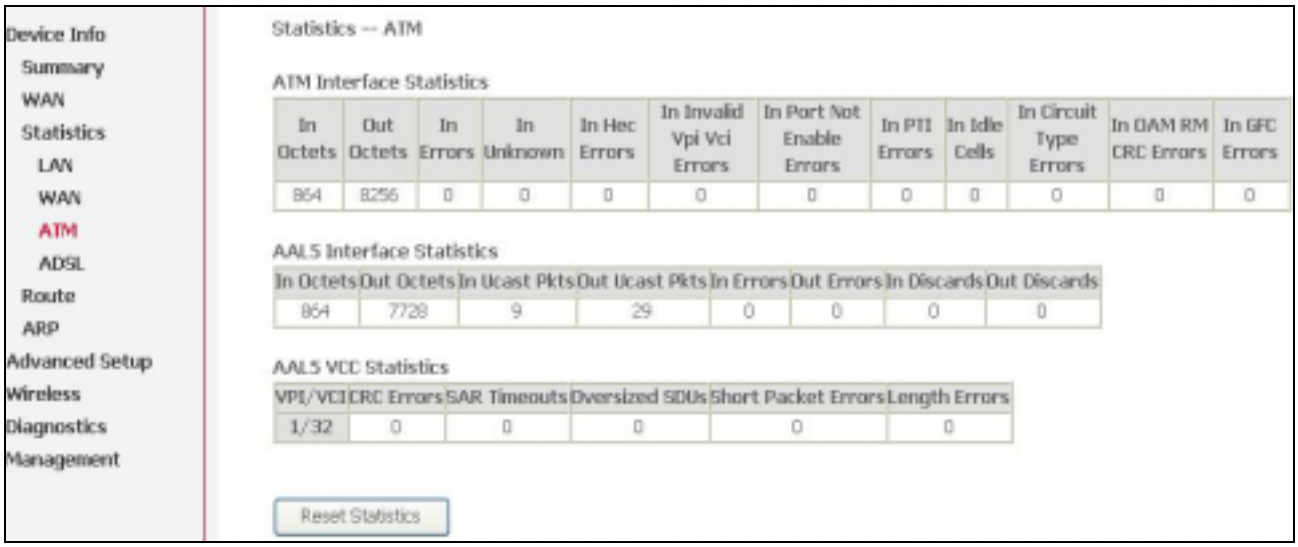
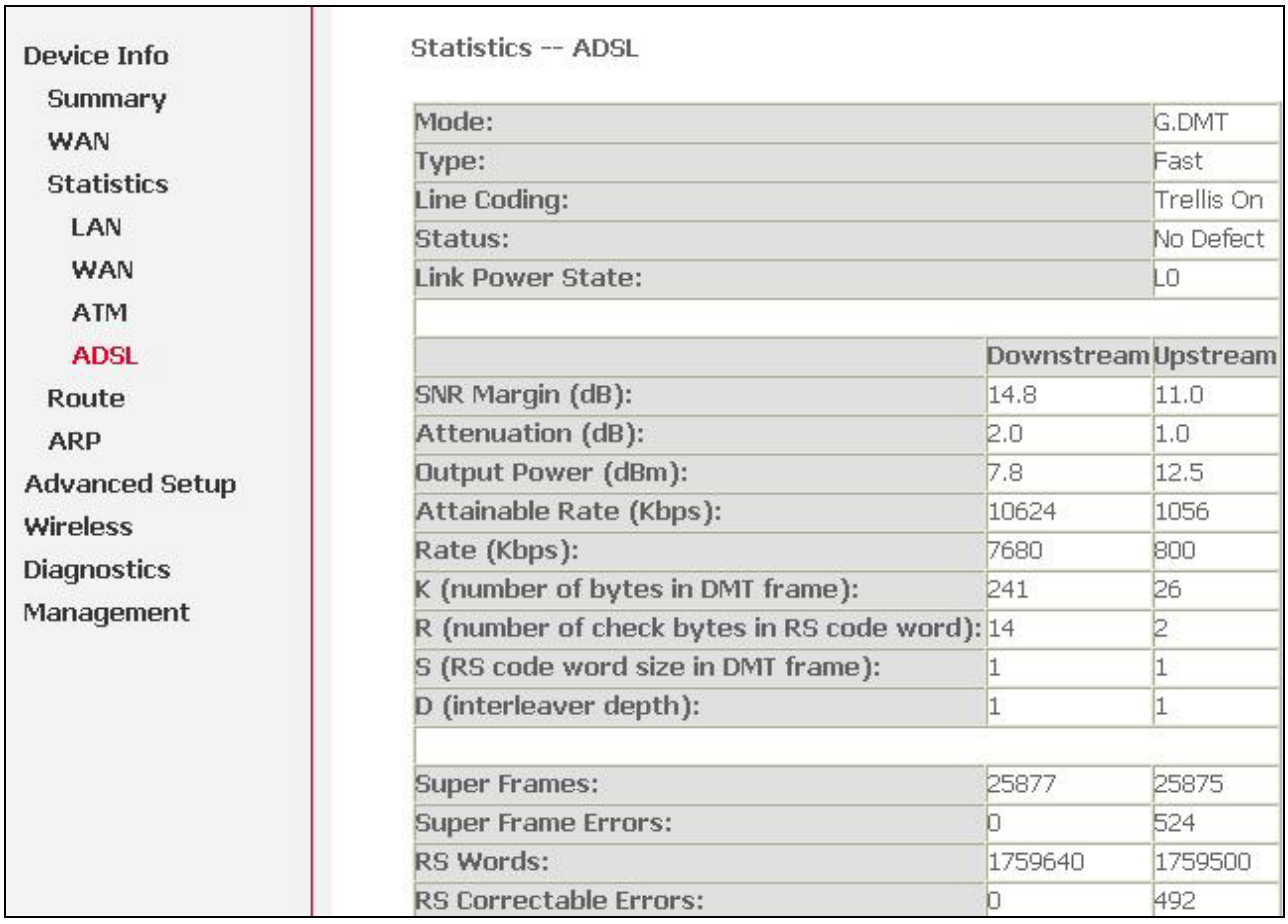
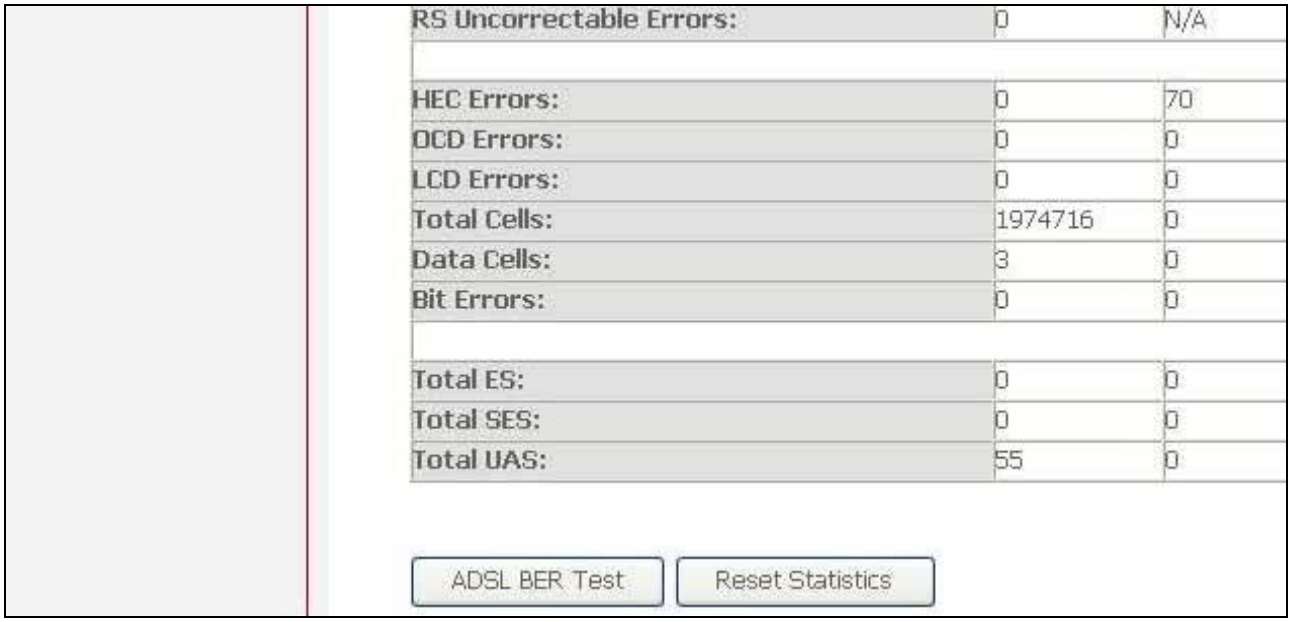


Figure 76. Device Info – Statistics – ATM

9.3.3 ADSL

This page displays AW4038's ADSL connection information and status, such as rate, SNR, ES (Error Second)…etc.



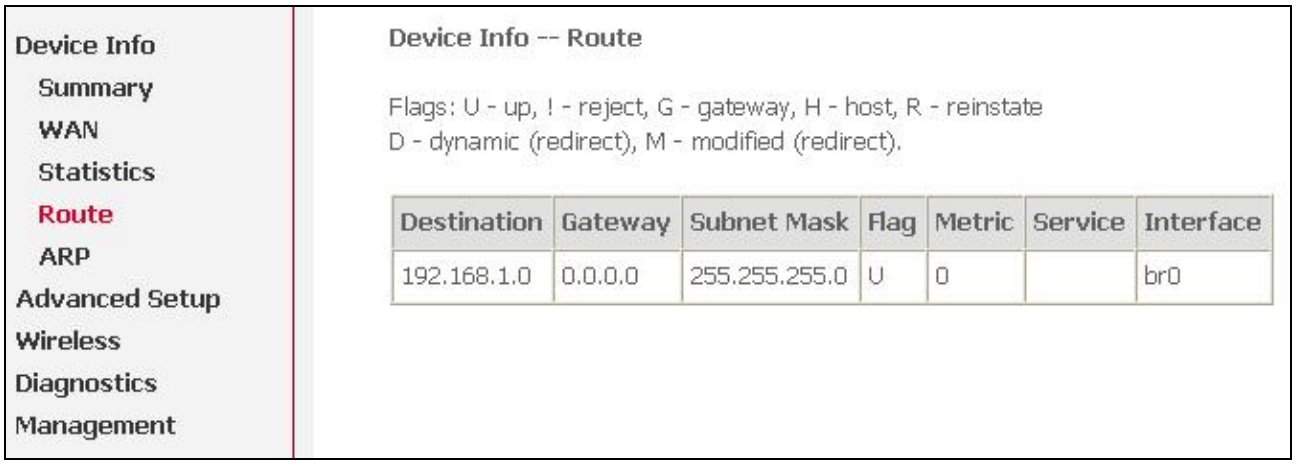


RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	70
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	1974716	0
Data Cells:	3	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	55	0

Figure 77. Device Info – Statistics – ADSL

9.4 Route

This page displays AW4038's routing table.



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 78. Device Info – Route

9.5 ARP

This page displays AW4038's ARP table.

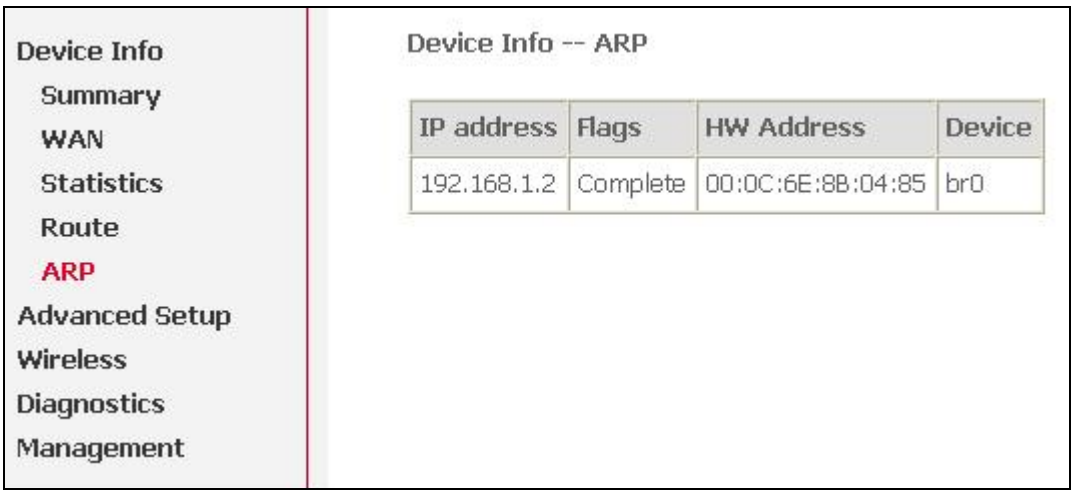


Figure 79. Device Info – ARP

NOTE: 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 or more 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.