ADD-NWAR3670

User Manual

Contents

1 Introduction

The ADD-NWAR3670 supports multiple line modes. It provides four 10/100 base-T Ethernet interfaces at the user end. The device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps. The ADD-NWAR3670 supports 3G WAN and 3G backup, Samba for USB storage.

The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with IEEE 802.11,802.11b/g/n and 802.11n specifications, WEP, WPA, and WPA2 security specifications. The WLAN of the device supports 2T2R.

1.1 Packing List

- 1 x ADD-NWAR3670
- 1 x external splitter
- 1 x power adapter
- 2 x telephone cables (RJ-11)
- 1 x Ethernet cable (RJ-45)
- 1 x USB cable
- 1 x user manual
- 1 x quality guarantee card
- 1 x certificate of quality

1.2 Safety Precautions

Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device

package.

- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.3 LEDs and Interfaces

Front Panel

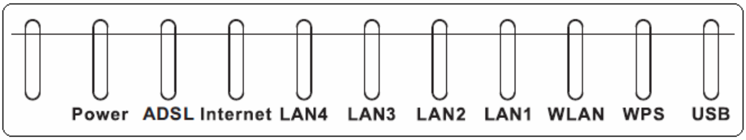


Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description

Power	Green	On	The device is powered on and the initialization is normal.
		Off	The power is off.
	Red	On	The device is self-testing, the self-test is failed.
ADSL	Green	On	Connection between the device and the physical layer of the office is established.
		Blinks	The device is handshaking with the physical layer of the office.
		Off	No signal is being detected.
Internet	Green	On	The Internet connection is normal in the routing mode (for example: PPP dial-up is successful), and no Internet data is being transmitted.
		Blinks	Internet data is being transmitted in the routing mode and bridge mode.
		Off	The device is in the bridge mode.
LAN4, LAN3, LAN2, LAN1	Green	On	The LAN connection is normal.
		Blinks	Data is being transmitted through the LAN interface, or the Internet data is being transmitted in the brige mode.
		Off	The LAN connection is not established.
WLAN	Green	On	The WLAN connection is normal.
		Blinks	Data is transmitted through the WLAN interface.
		Off	The WLAN connection is not established.
WPS	Green	Blinks	WPS negotiation is enabled, waiting for the clients.
		Off	WPS negotiation is not enabled on the device.
USB	Green	On	The USB connection is normal and

			activated.
		Blinks	Data is being transmitted through the USB interface.
		Off	The USB interface is not connected.

Rear Panel

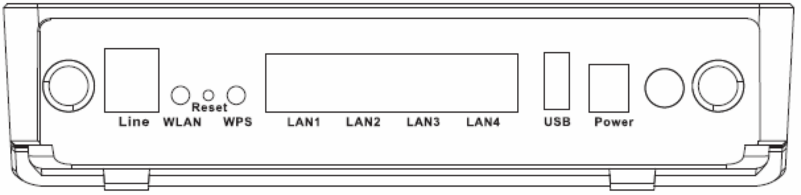


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
Line	RJ-11 interface, for connecting the interface of the telephone set through the telephone cable.
WLAN	Button to enable or disable WLAN.
Reset	Restore to factory defaults. To restore factory defaults, keep the device powered on, push a paper clip into the hole to press the button for over 5 seconds and then release.
WPS	Button to enable or disable WPS.
LAN1, LAN2, LAN3, LAN4	RJ-45 interface, for connecting the Ethernet interface of a computer or an Ethernet device.
USB	USB interface,for connecting to the USB interface of the 3G data card.
Power	Power interface, for connecting the interface of the power adapter.

Interface/Button	Description
○	Power switch, for turning on or off the power of the device.

1.4 System Requirements

Recommended system requirements are as follows:

- An 10 baseT/100BaseT Ethernet card is installed on your PC
- A hub or switch (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows 98SE, Windows 2000, Windows ME, or Windows XP
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.5 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade: Web, TFTP, FTP

- Reset to the factory defaults
- DNS relay
- Virtual server
- DMZ
- Two-level passwords and user names
- Web user interface
- Telnet CLI
- System status display
- PPP session PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management (telnet and HTTP, TR069))
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP
- 3G WAN and 3G Backup
- Samba for USB storage
- USB printer

2 Hardware Installation

Step 1 Connect the Line port of the device and the Modem port of the splitter with a telephone cable. Connect the phone to the Phone port of the splitter through a telephone cable. Connect the incoming line to the Line port of the splitter.

The splitter has three ports:

- Line: Connect to a wall phone port (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connectto a telephone set.

Step 2 Connect the LAN port of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:

Use twisted-pair cables to connect with the Hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the device.

Connection 1: Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.

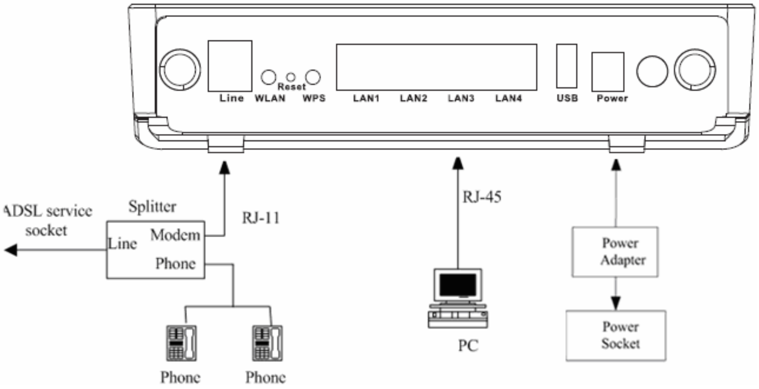


Figure 3 Connection diagram (without telephone sets before the splitter)

Connection 2: Figure 4 displays the application diagram for the connection of the device, PC, splitter and telephone sets when a telephone set is placed before the splitter.

As illustrated in the following figure, the splitter is installed close to the device.

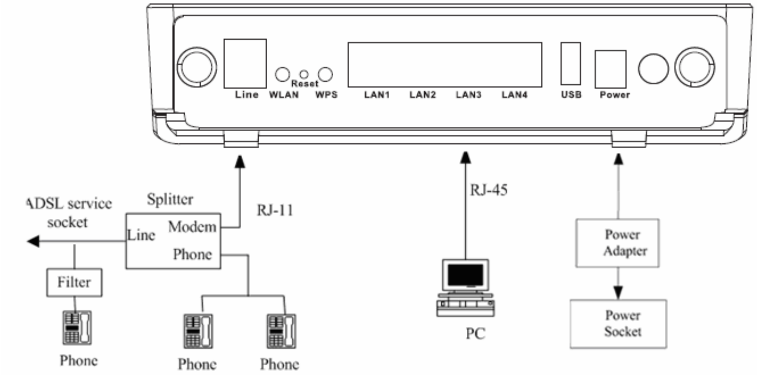


Figure 4 Connection diagram (with a telephone set before the splitter)

Connection 1 is recommended.

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

3 About the Web Configurator

This chapter describes how to configure the device by using the Web-based configuration utility.

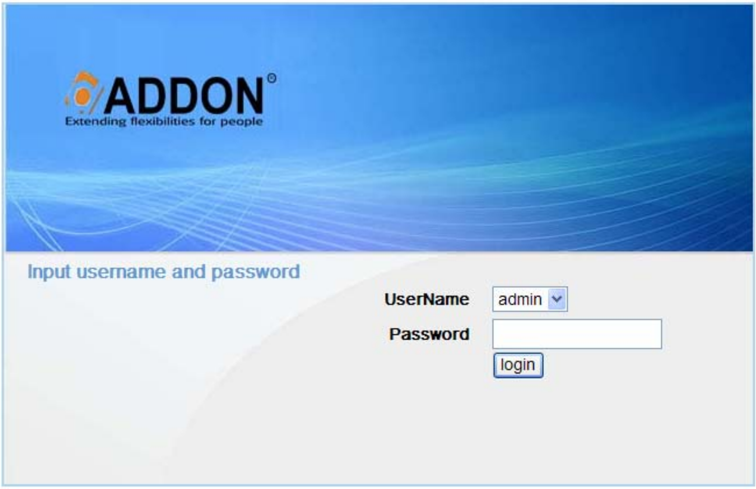
3.1 Access the Device

The following is the detailed description of accesing the device for the first time.

Step 1 Open the Internet Explorer (IE) browser and enter **http://192.168.1.1**.

Step 2 The **Login** page shown in the following figure appears. Enter the user name and password.

- The user name and password of the super user are **admin** and **admin.**
- The user name and password of the normal user are **user** and **user.**

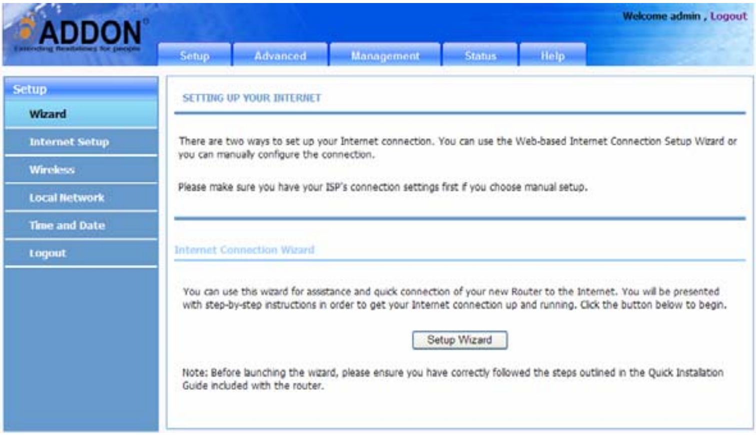


Input username and password

UserName: admin

Password

If you log in as the super user successfully, the page shown in the following figure appears.



SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose manual setup.

Internet Connection Wizard

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

If the login information is incorrect, click **Try Again** in the page that pops up to log in again.

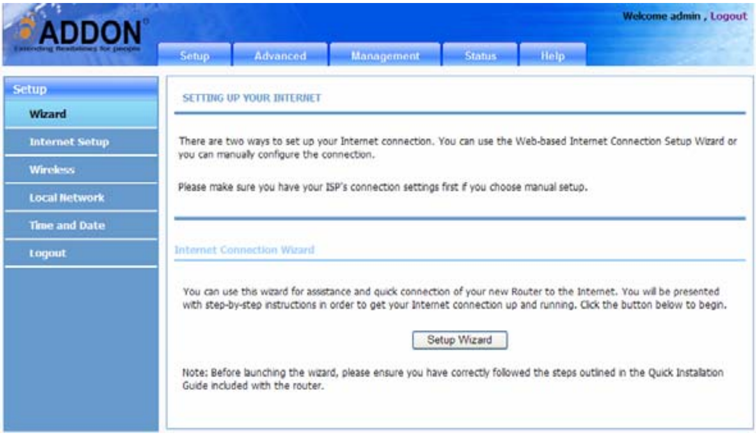
3.2 Setup

3.2.1 Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe these various configuration parameters.

When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

Step 1 Choose **Setup** > **Wizard**. The page shown in the following figure appears.



SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

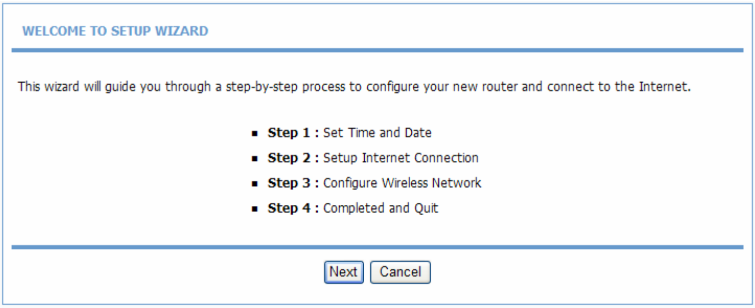
Please make sure you have your ISP's connection settings first if you choose manual setup.

Internet Connection Wizard

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

Step 2 Click **Setup Wizard**. The page shown in the following figure appears.



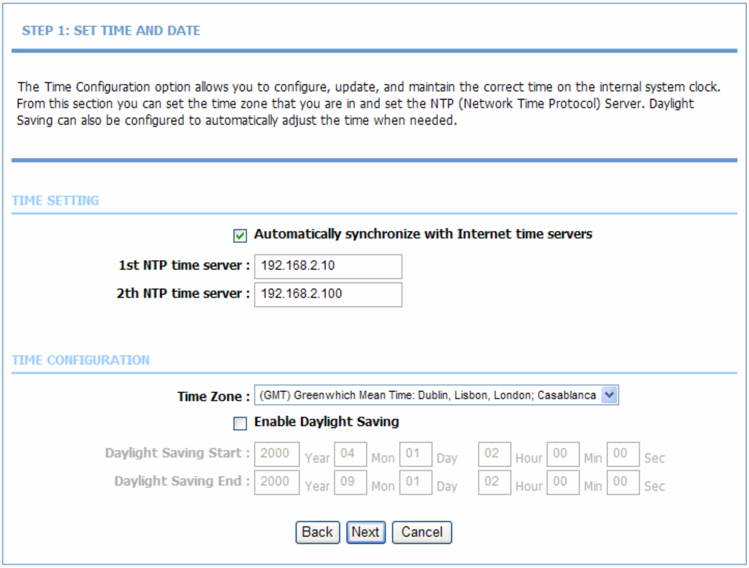
WELCOME TO SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

- **Step 1 :** Set Time and Date
- **Step 2 :** Setup Internet Connection
- **Step 3 :** Configure Wireless Network
- **Step 4 :** Completed and Quit

Step 3 There are four steps to configure the device. Click **Next** to continue.

Step 4 Set the time and date.



STEP 1: SET TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTING

☑ **Automatically synchronize with Internet time servers**

1st NTP time server : 192.168.2.10

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Time Zone : (GMT) Greenwhich Mean Time: Dublin, Lisbon, London; Casablanca

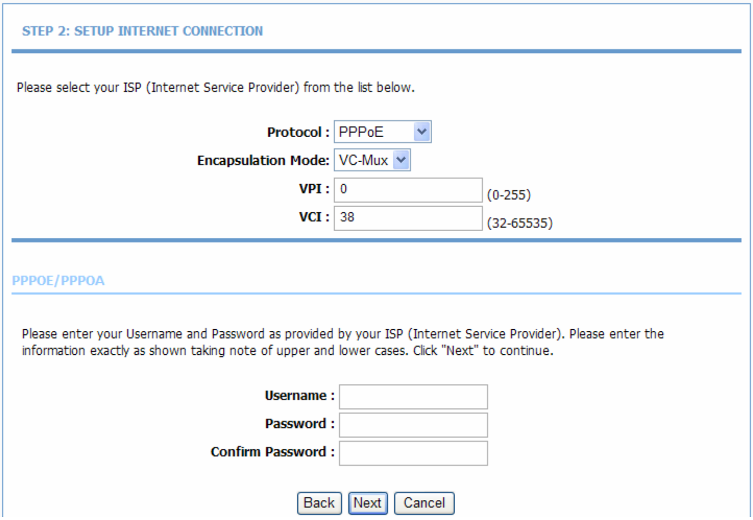
□ **Enable Daylight Saving**

Daylight Saving Start : 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec

Daylight Saving End : 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec

Step 5 Configure the Internet connection.

Select the country and ISP. Set the VPI and VCI. If you fail to find the country and ISP from the drop-down lists, select **Others**. Click **Next**. If the **Protocol** is **PPPoE** or **PPPoA,** the page shown in either of the two following figures appears.



STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol : PPPoE

Encapsulation Mode: VC-Mux

VPI : 0 (0-255)

VCI : 38 (32-65535)

PPPOE/PPPOA

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

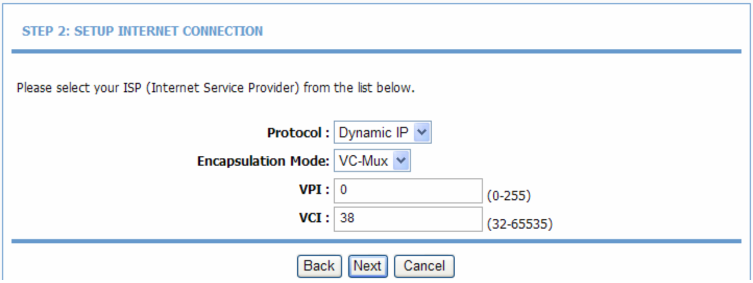
Username :

Password :

Confirm Password :

In this page, enter the user name and password.

If the Protocol is **Dynamic IP**, the page shown in the following figure appears.



STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

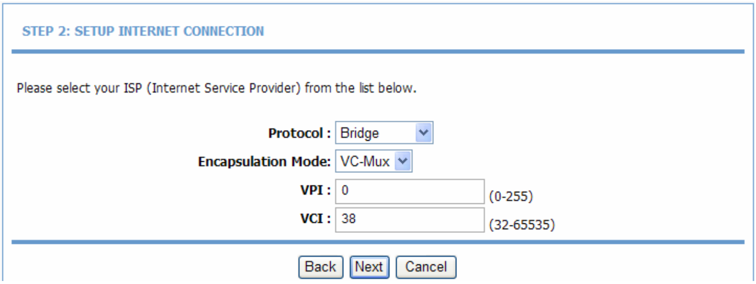
Protocol : Dynamic IP

Encapsulation Mode: VC-Mux

VPI : 0 (0-255)

VCI : 38 (32-65535)

If the Protocol is **Bridge**, the page shown in the following figure appears.

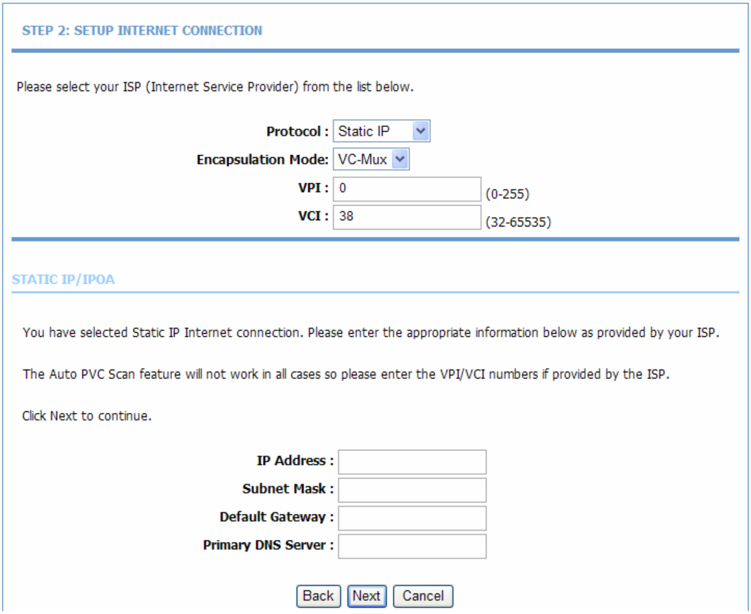


STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol :	Bridge
Encapsulation Mode:	VC-Mux
VPI :	0 (0-255)
VCI :	38 (32-65535)

If the Protocol is **Static IP**, the page shown in the following figure appears.



STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol :	Static IP
Encapsulation Mode:	VC-Mux
VPI :	0 (0-255)
VCI :	38 (32-65535)

STATIC IP/IPOA

You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

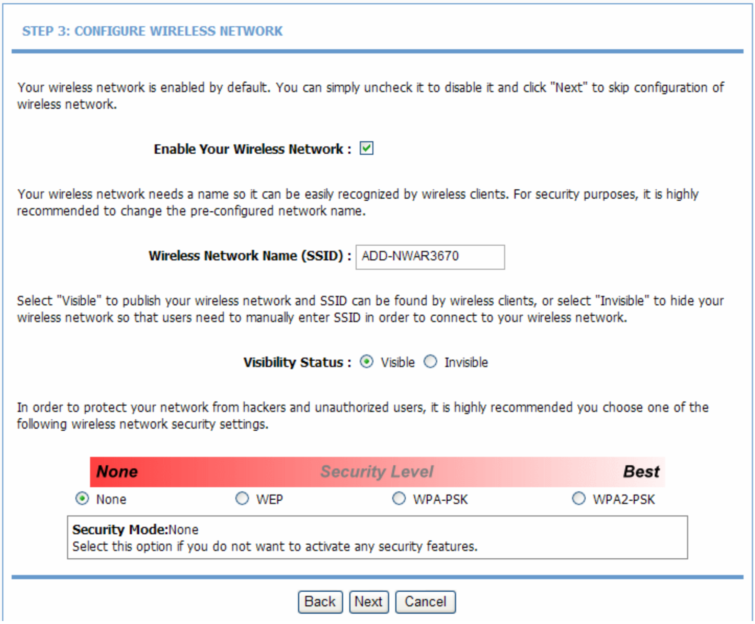
IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**. Click **Next**. The page shown in the following page appears.



STEP 3: CONFIGURE WIRELESS NETWORK

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

Enable Your Wireless Network : ☑

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) : ADD-NWAR3670

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

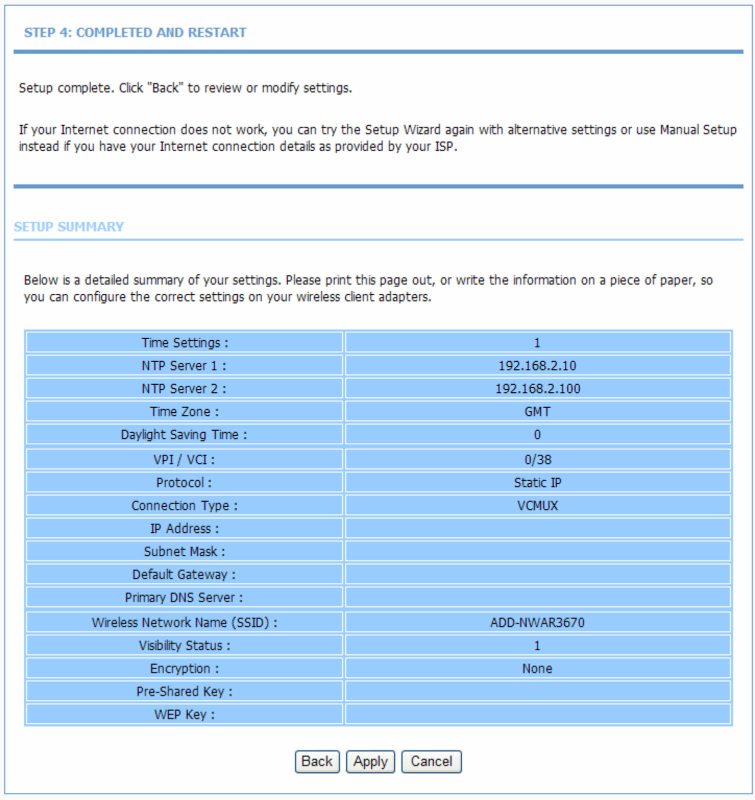
Visibility Status : ● Visible ○ Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

● None ○ WEP ○ WPA-PSK ○ WPA2-PSK

Security Mode:None
Select this option if you do not want to activate any security features.

Step 6 Configure the wireless network. Enter the information and click **Next**.



STEP 4: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings.

If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

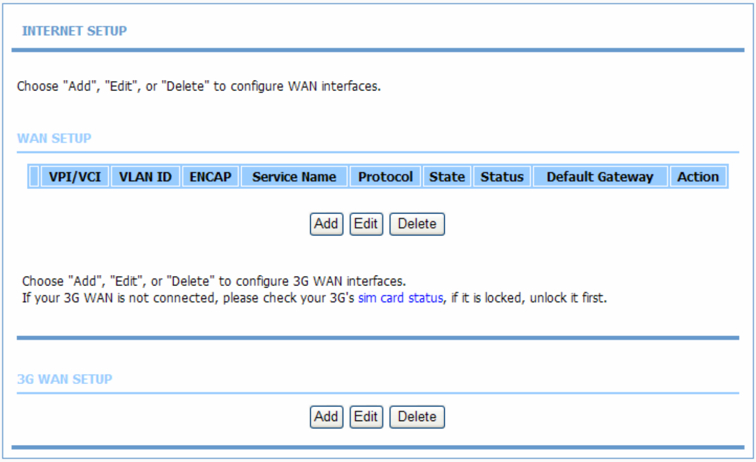
Time Settings :	1
NTP Server 1 :	192.168.2.10
NTP Server 2 :	192.168.2.100
Time Zone :	GMT
Daylight Saving Time :	0
VPI / VCI :	0/38
Protocol :	Static IP
Connection Type :	VCMUX
IP Address :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	
Wireless Network Name (SSID) :	ADD-NWAR3670
Visibility Status :	1
Encryption :	None
Pre-Shared Key :	
WEP Key :	

Note:

In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.

3.2.2 Internet Setup

Choose **Setup** > **Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.



INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

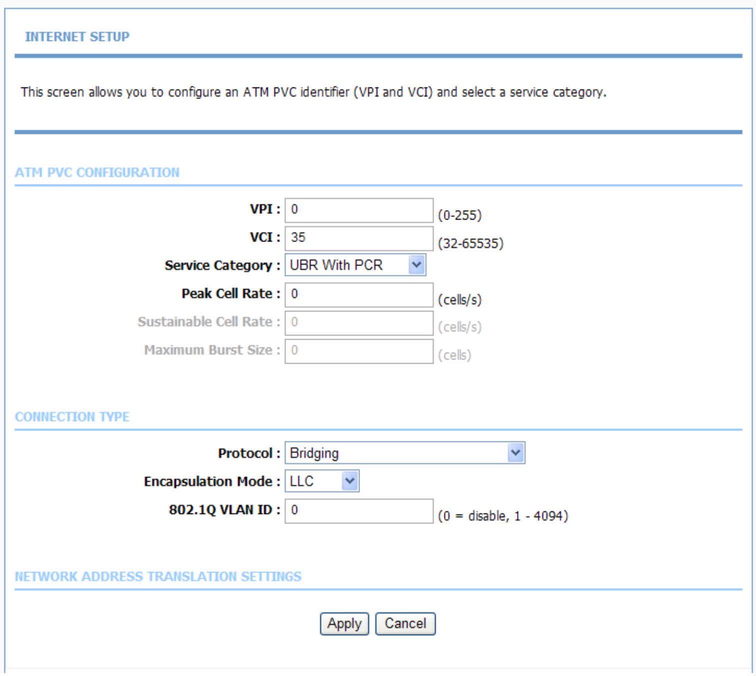
WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.
If your 3G WAN is not connected, please check your 3G's sim card status, if it is locked, unlock it first.

3G WAN SETUP

Click **Add in “WAN SETUP”**. The page shown in the following figure appears.



INTERNET SETUP

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

ATM PVC CONFIGURATION

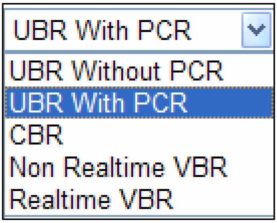
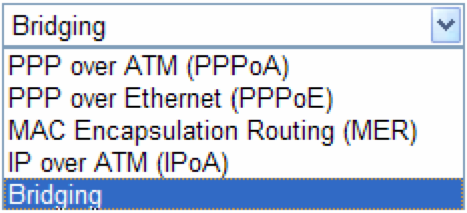
VPI :	0	(0-255)
VCI :	35	(32-65535)
Service Category :	UBR With PCR	
Peak Cell Rate :	0	(cells/s)
Sustainable Cell Rate :	0	(cells/s)
Maximum Burst Size :	0	(cells)

CONNECTION TYPE

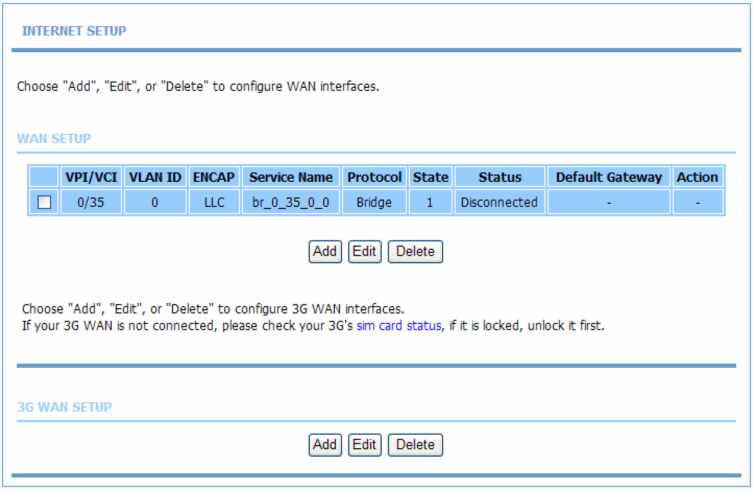
Protocol :	Bridging	
Encapsulation Mode :	LLC	
802.1Q VLAN ID :	0	(0 = disable, 1 - 4094)

NETWORK ADDRESS TRANSLATION SETTINGS

Field	Description
PVC Settings	● The virtual path between two points in an ATM network, and its valid value is from 0 to 255. ● The virtual channel between two points in an ATM network, ranging from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).
Service Category	You can select from the drop-down list.

Field	Description
	 UBR With PCR UBR Without PCR UBR With PCR CBR Non Realtime VBR Realtime VBR
Protocol	You can select from the drop-down list.  Bridging PPP over ATM (PPPoA) PPP over Ethernet (PPPoE) MAC Encapsulation Routing (MER) IP over ATM (IPoA) Bridging
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.

Click **Apply**, the page shown in the following figure appears.



INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
□	0/35	0	LLC	br_0_35_0_0	Bridge	1	Disconnected	-	-

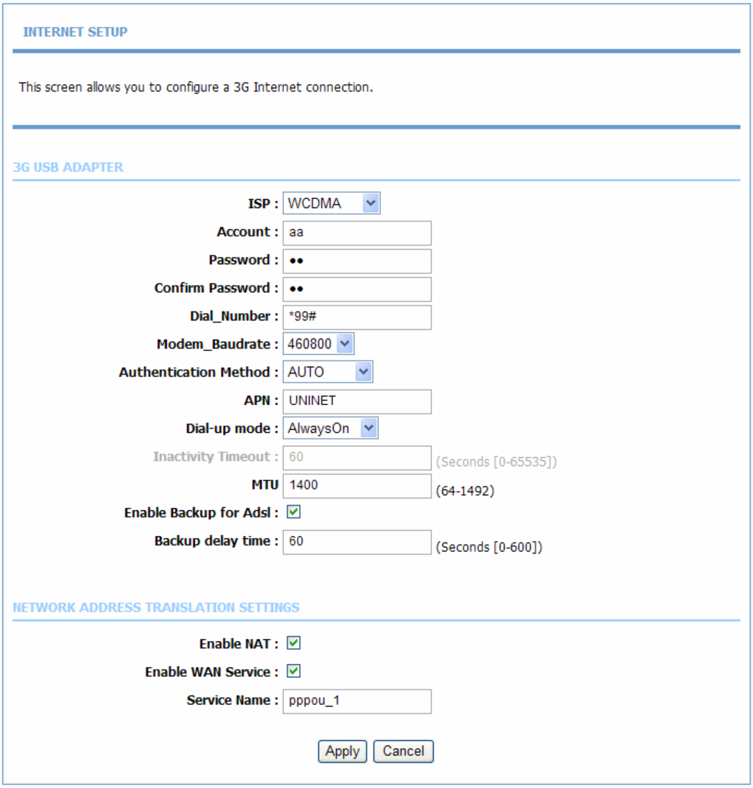
Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.
If your 3G WAN is not connected, please check your 3G's sim card status, if it is locked, unlock it first.

3G WAN SETUP

The device supports the following three types of 3G USB dongle: WCDMA, CDMA2000, and TD-SCDMA. You can access the PPP dialup through 3G and manage the pin code of 3G.

You need to configure the parameters, including the ISP, Account, password, Dial_number, and APN, which can be obtained from the ISP. To perform 3G backup, you need to select enable backup for ADSL. Before dialing, ensure to check whether the 3G card is locked with PIN/PUK code.

Click **Add** in**“3G WAN SETUP”**.The page shown in the following figure appears.



INTERNET SETUP

This screen allows you to configure a 3G Internet connection.

3G USB ADAPTER

ISP :	WCDMA
Account :	aa
Password :	••
Confirm Password :	••
Dial_Number :	*99#
Modem_Baudrate :	460800
Authentication Method :	AUTO
APN :	UNINET
Dial-up mode :	AlwaysOn
Inactivity Timeout :	60 (Seconds [0-65535])
MTU	1400 (64-1492)
Enable Backup for Adsl :	☑
Backup delay time :	60 (Seconds [0-600])

NETWORK ADDRESS TRANSLATION SETTINGS

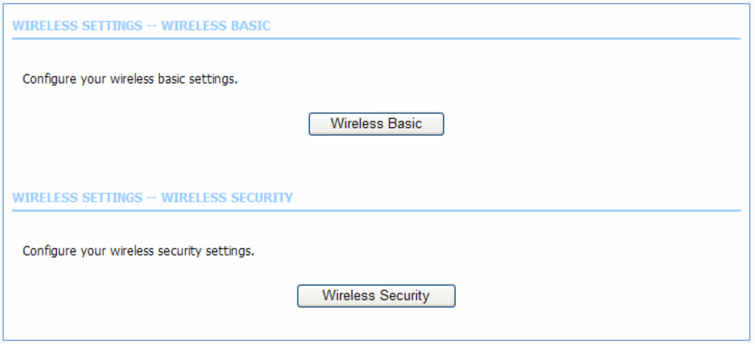
Enable NAT :	☑
Enable WAN Service :	☑
Service Name :	pppou_1

Click **Apply** to save the settings.

3.2.3Wireless

This section describes the wireless LAN and some basic configuration. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a pear-to-pear network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup** > **Wireless** . The **Wireless** page shown in the following figure appears.



WIRELESS SETTINGS -- WIRELESS BASIC

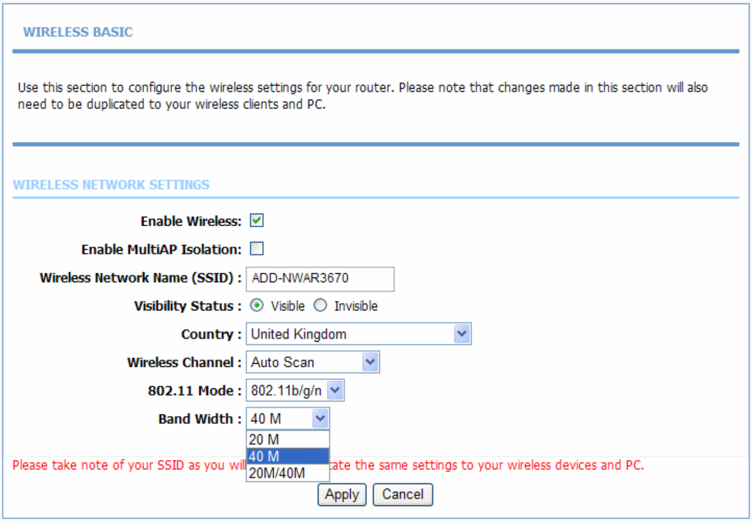
Configure your wireless basic settings.

WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

3.2.3.1 Wireless Basics

In the **Wireless** page, click **Wireless Basic**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.



WIRELESS BASIC

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

Enable Wireless: ☑

Enable MultiAP Isolation: □

Wireless Network Name (SSID) : ADD-NWAR3670

Visibility Status : ● Visible ○ Invisible

Country : United Kingdom

Wireless Channel : Auto Scan

802.11 Mode : 802.11b/g/n

Band Width : 40 M

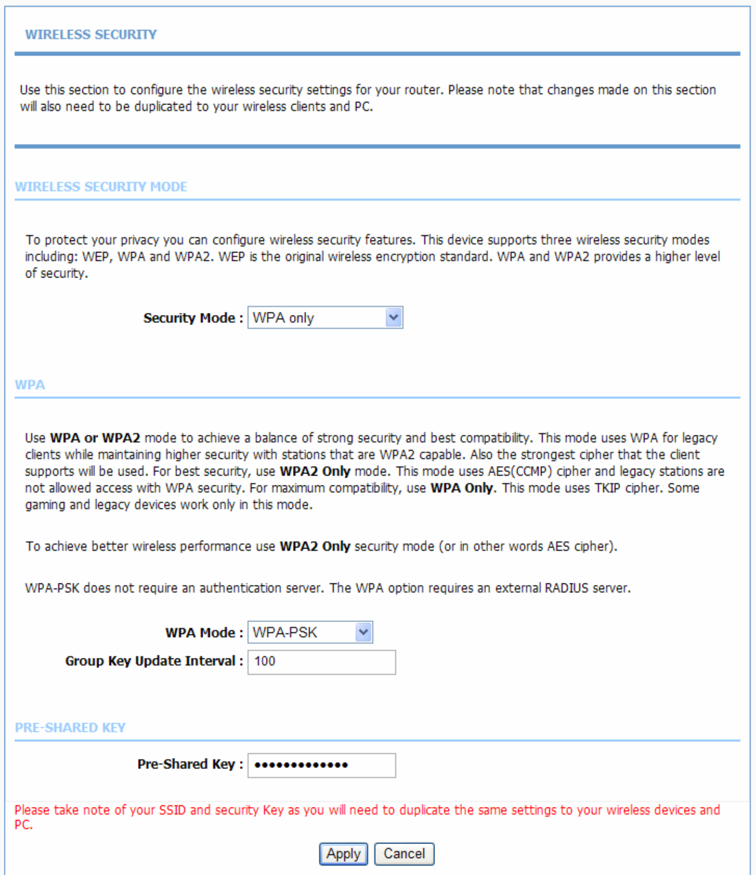
Please take note of your SSID as you wil ate the same settings to your wireless devices and PC.

- **Enable Wireless**: Select this to turn Wi-Fi on and off.
- **Enable MultiAP Isolation**: Select this to turn MultiAP isolation on and off.
- **Wireless Network Name (SSID)**: The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
- **Visibility Status**: You can select visible or invisible.
- **Country**: Select the country from the drop-down list.
- **Wireless Channel**: Select the wireless channel from the pull-down menu. It is different for different country.
- **802.11 Mode**: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are, 802.11b Only, 802.11g Only, 802.11n Only, or 802.11b/g ,802.11b/g/n,802.11n/g.
- **Band Width**: Select the appropriate band width from the pull-down menu.

Click **Apply** to save the settings.

3.2.3.2 Wireless Security

In the **Wireless** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA only

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : WPA-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : •••••••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

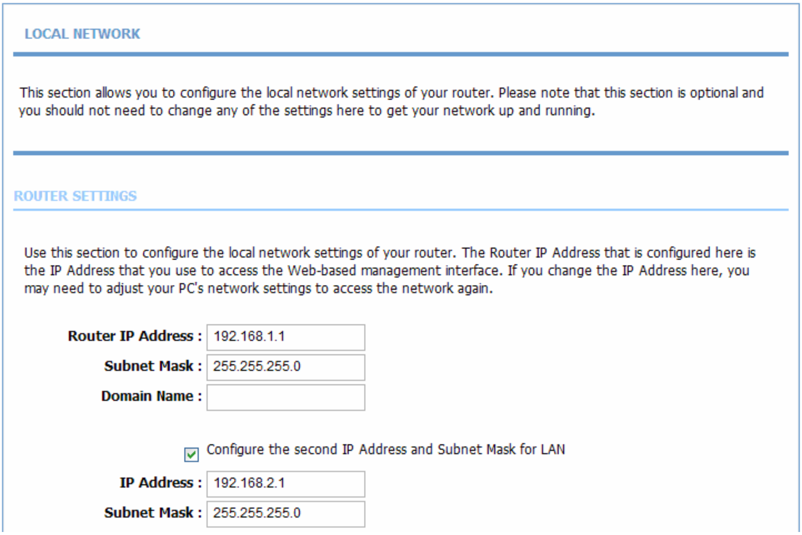
Click **Apply** to save the settings.

3.2.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup** > **Local Network**. The **Local Network** page shown in the following figure appears.



LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

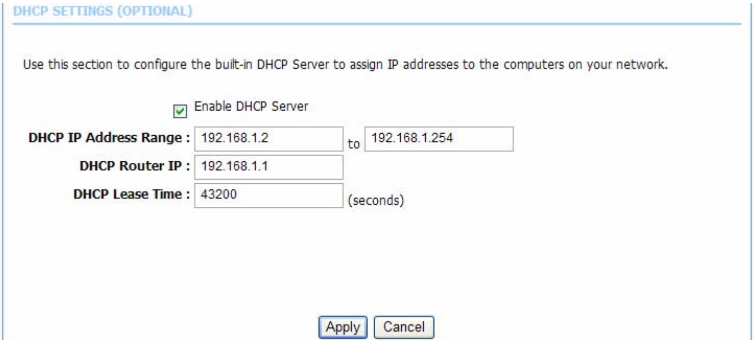
Domain Name :

☑ Configure the second IP Address and Subnet Mask for LAN

IP Address : 192.168.2.1

Subnet Mask : 255.255.255.0

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplys IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.



DHCP SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

☑ Enable DHCP Server

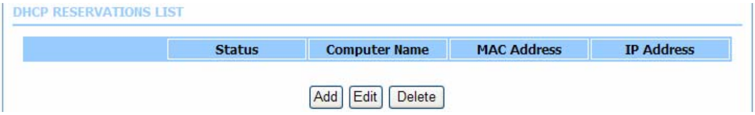
DHCP IP Address Range : 192.168.1.2 to 192.168.1.254

DHCP Router IP : 192.168.1.1

DHCP Lease Time : 43200 (seconds)

Click **Apply** to save the settings.

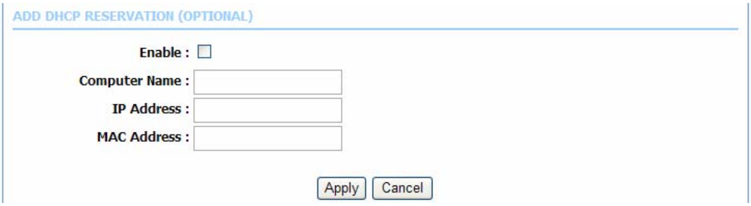
In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.



DHCP RESERVATIONS LIST

	Status	Computer Name	MAC Address	IP Address

Click **Add** to add static DHCP (optional). The page shown in the following figure appears.



ADD DHCP RESERVATION (OPTIONAL)

Enable : □

Computer Name :

IP Address :

MAC Address :

Select **Enable** to reserve the IP address for the designated PC with the configured MAC address.

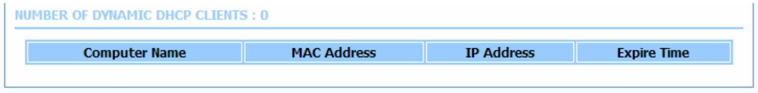
The **Computer Name** helps you to recognize the PC with the MAC address. For example, Father’s Laptop.

Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

If the DHCP reservations list table is not empty, you can select one or more items and click **Edit** or **Delete**.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer(s).

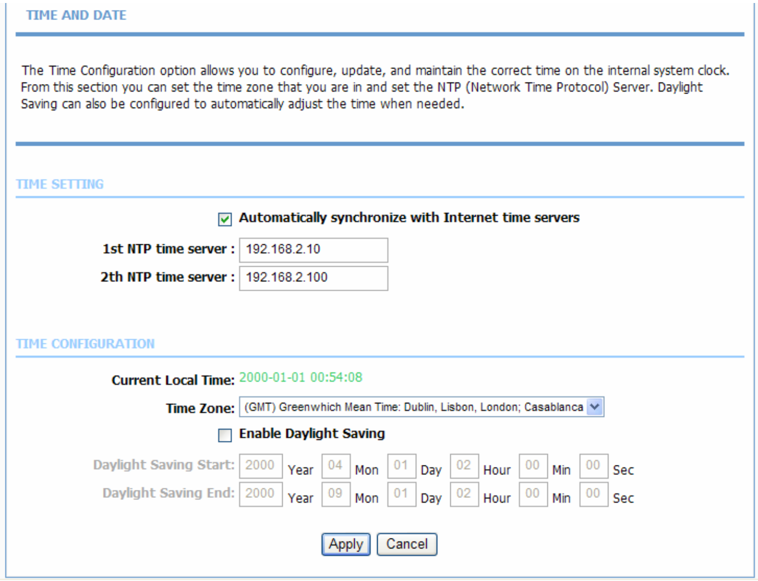


NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time

3.2.5Time and Date

Choose **Setup** > **Time and Date**. The page shown in the following figure appears.



TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTING

☑ Automatically synchronize with Internet time servers

1st NTP time server : 192.168.2.10

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Current Local Time: 2000-01-01 00:54:08

Time Zone: (GMT) Greenwhich Mean Time: Dublin, Lisbon, London; Casablanca

□ Enable Daylight Saving

Daylight Saving Start: 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec

Daylight Saving End: 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

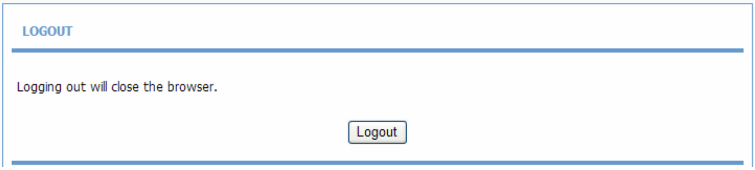
Select the specific time server and the time zone from the corresponding drop-down lists.

Select **Enable Daylight Saving** if necessary. Set the daylight as you want.

Click **Apply** to save the settings.

3.2.6 Logout

Choose **Setup** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



LOGOUT

Logging out will close the browser.

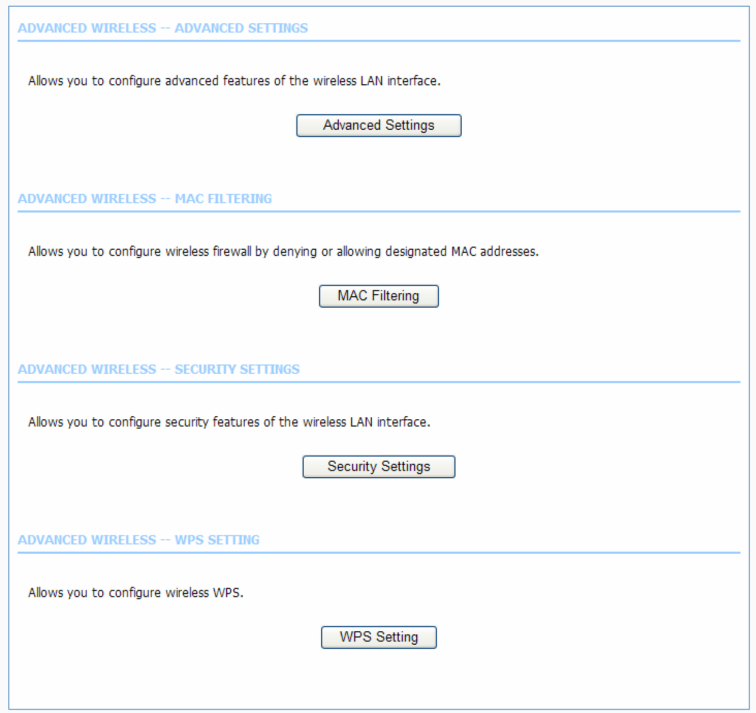
3.3 Advanced

This section includes advanced features used for network management, security and administrative tools to manage the device. You can view status and other information that are used to examine performance and troubleshoot.

3.3.1 Advanced Wireless

This function is used to modify the standard 802.11g wireless radio settings. It is recommend not to change the default settings, because incorrect settings may impair the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **ADVANCED** > **Advanced Wireless**. The page shown in the following figure appears.



ADVANCED WIRELESS -- ADVANCED SETTINGS

Allows you to configure advanced features of the wireless LAN interface.

ADVANCED WIRELESS -- MAC FILTERING

Allows you to configure wireless firewall by denying or allowing designated MAC addresses.

ADVANCED WIRELESS -- SECURITY SETTINGS

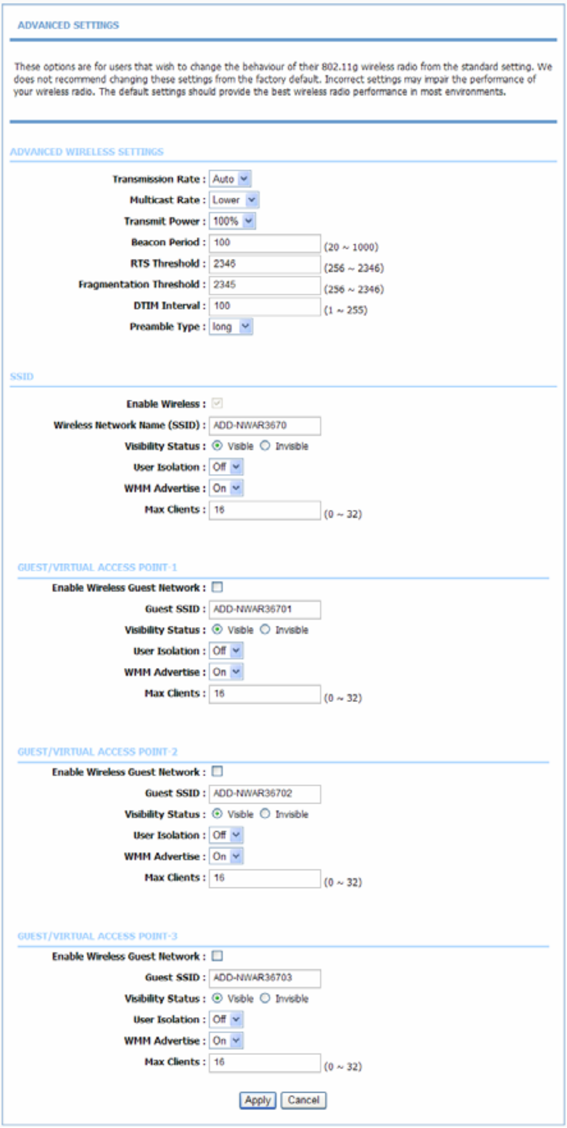
Allows you to configure security features of the wireless LAN interface.

ADVANCED WIRELESS -- WPS SETTING

Allows you to configure wireless WPS.

3.3.1.1 Advanced Settings

Select **Advance Settings.** The page shown in the following figure appears.



ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. We does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate : Auto

Multicast Rate : Lower

Transmit Power : 100%

Beacon Period : 100 (20 ~ 1000)

RTS Threshold : 2346 (256 ~ 2346)

Fragmentation Threshold : 2345 (256 ~ 2346)

DTIM Interval : 100 (1 ~ 255)

Preamble Type : long

SSID

Enable Wireless : ☑

Wireless Network Name (SSID) : ADD-NWAR3670

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □

Guest SSID : ADD-NWAR36701

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □

Guest SSID : ADD-NWAR36702

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : □

Guest SSID : ADD-NWAR36703

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WMM Advertise : On

Max Clients : 16 (0 ~ 32)

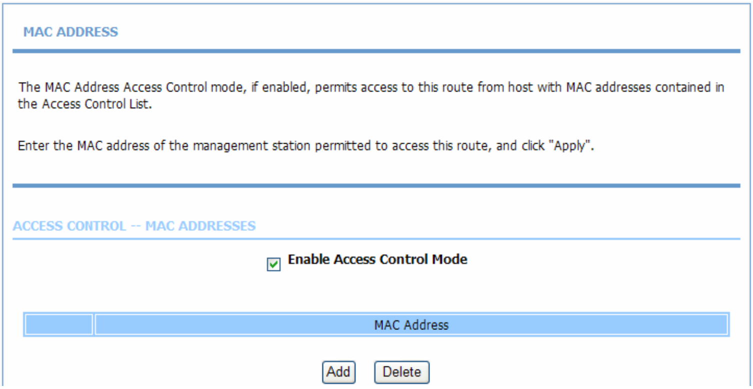
Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Click **Apply** to save the settings.

3.3.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.



MAC ADDRESS

The MAC Address Access Control mode, if enabled, permits access to this route from host with MAC addresses contained in the Access Control List.

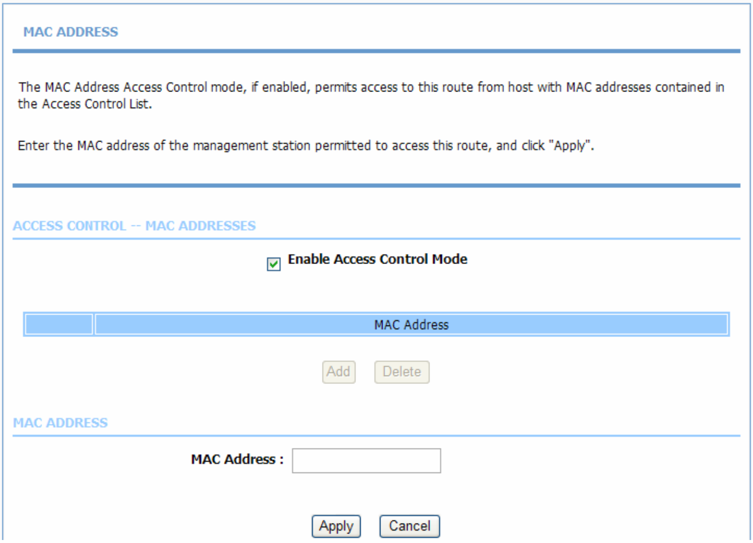
Enter the MAC address of the management station permitted to access this route, and click "Apply".

ACCESS CONTROL -- MAC ADDRESSES

☑ Enable Access Control Mode

	MAC Address

Click **Add** and the **MAC ADDRESS** pane appears below the **ACCESS CONTROL - MAC ADDRESSES** table. See the following figure:



MAC ADDRESS

The MAC Address Access Control mode, if enabled, permits access to this route from host with MAC addresses contained in the Access Control List.

Enter the MAC address of the management station permitted to access this route, and click "Apply".

ACCESS CONTROL -- MAC ADDRESSES

☑ Enable Access Control Mode

	MAC Address

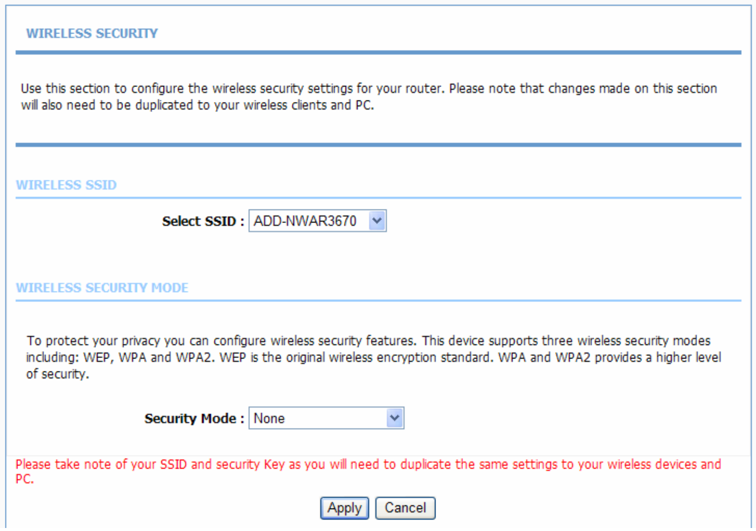
MAC ADDRESS

MAC Address :

Enter the MAC address in the corresponding field and click **Apply**. The newly added MAC address is displayed in the **ACCESS CONTROL - MAC ADDRESSES** table.

3.3.1.3 Security Settings

Select **Security Settings**. The page shown in the following figure appears.



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SSID

Select SSID : ADD-NWAR3670

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

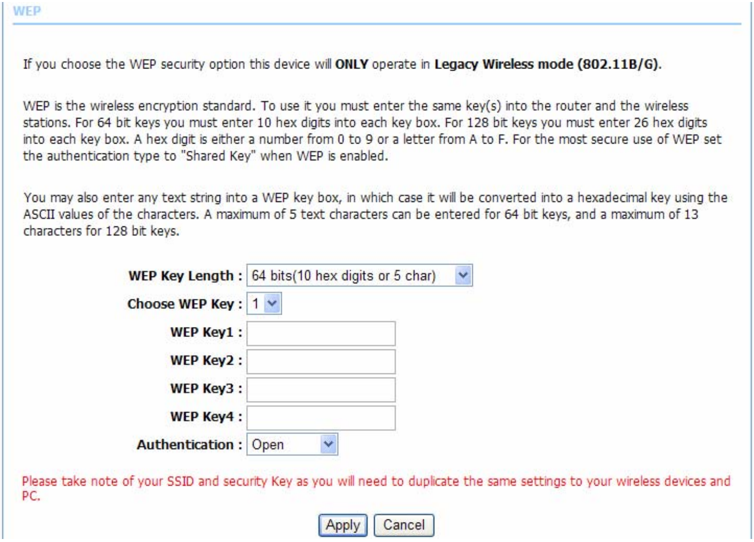
Security Mode : None

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Select the SSID that you want to configure from the drop-down list.

Select the encryption type from the **Security Mode** drop-down list.You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**.

If you select **WEP**, the page shown in the following figure appears.



WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 64 bits(10 hex digits or 5 char)

Choose WEP Key : 1

WEP Key1 :

WEP Key2 :

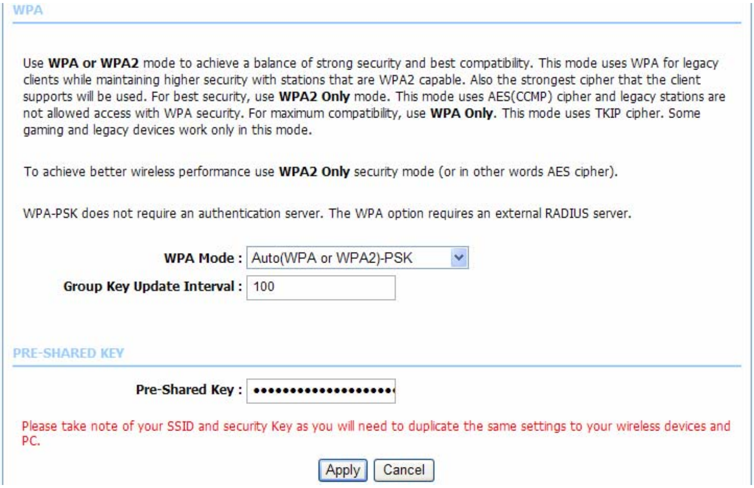
WEP Key3 :

WEP Key4 :

Authentication : Open

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select **AUTO (WPA or WPA2)**, the page shown in the following figure appears.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : Auto(WPA or WPA2)-PSK

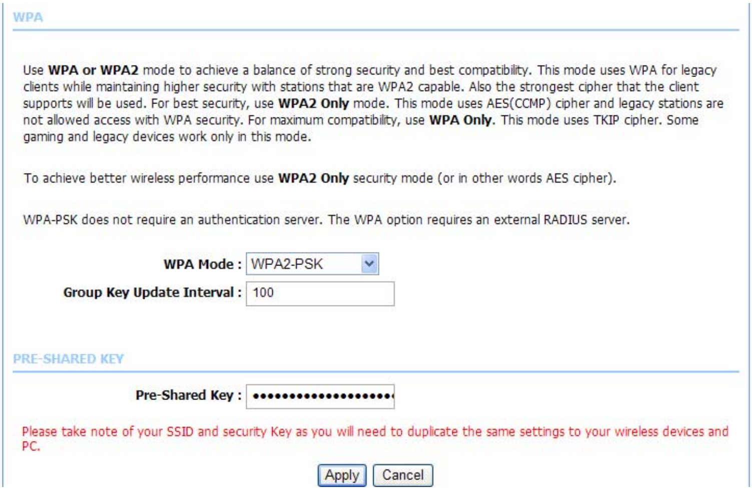
Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : ••••••••••••••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select **WPA2 only**, the page shown in the following figure appears.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : WPA2-PSK

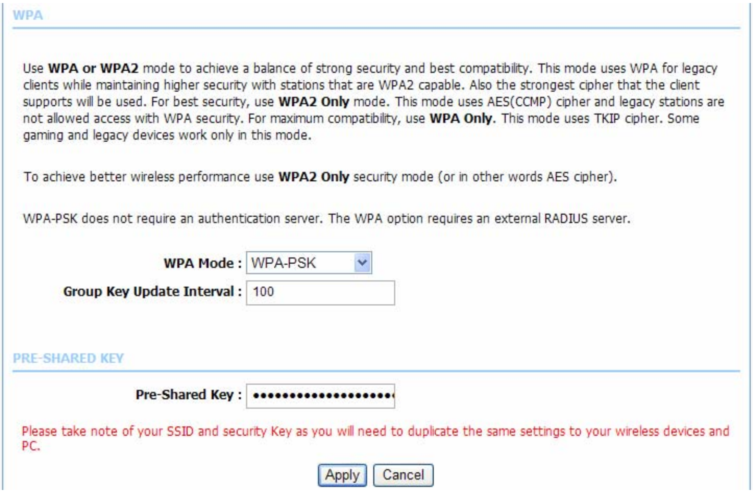
Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : ••••••••••••••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select **WPA only**, the page shown in the following figure appears.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : WPA-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

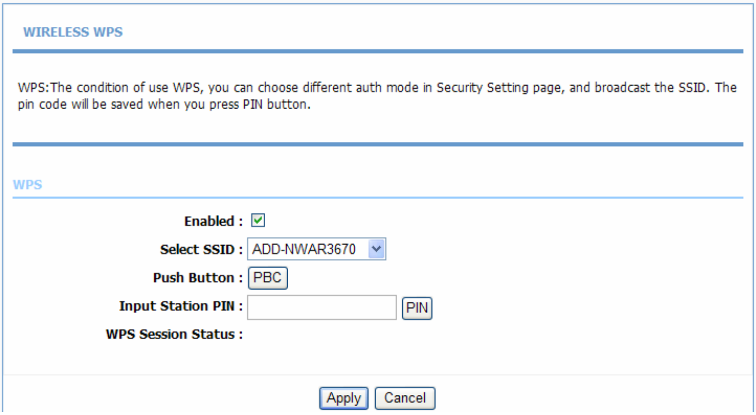
Pre-Shared Key : •••••••••••••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Click **Apply** to save the settings.

3.3.1.4 WPS Settings

In the **ADVANCED WIRELESS** page, click **WPS Setting**. The **WIRELESS WPS** page as shown in the following figure appears:



WIRELESS WPS

WPS:The condition of use WPS, you can choose different auth mode in Security Setting page, and broadcast the SSID. The pin code will be saved when you press PIN button.

WPS

Enabled : ☑

Select SSID : ADD-NWAR3670

Push Button : PBC

Input Station PIN : PIN

WPS Session Status :

Enabled: The WPS service is enabled by default.

Note:

Ensure that the network card supports the WPS function.

You can use one of the following there methods to use WPS authentication:

- Press the **WPS** button on the side panel for 3 seconds.
- In the **WIRELESS WPS** page, click **PBC**. It has the same function of the **WPS** button on the side panel. This is an optional method on wireless clients.

  Note:

  You need a Registrar when using the PBC method in a special case in which the PIN is all zeros.

- In the **WIRELESS WPS** page, enter the **PIN** code provided by the station and click **PIN**. PIN entry is a mandatory method of setup for all WPS certified devices.

  Note:

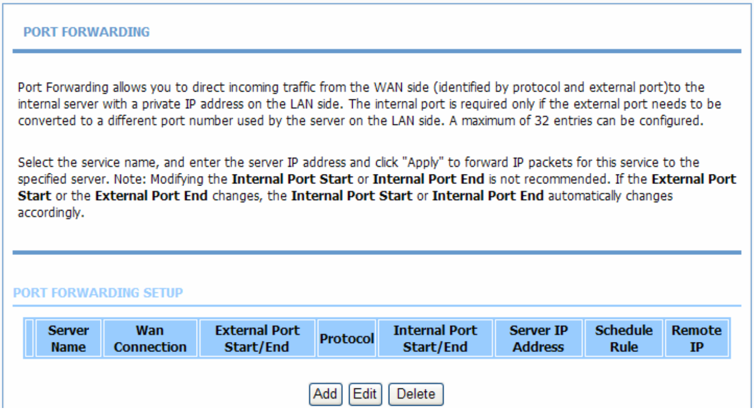
  If you are using the PIN method, you need a Registrar, either an access point or a wireless router, to initiate the registration between a new device and an active access point or a wireless router.

3.3.2Port Forwarding

This function is used to open ports in your device and re-direct data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the

LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in.

Choose **ADVANCED** > **Port Forwarding**. The page shown in the following figure appears.



PORT FORWARDING

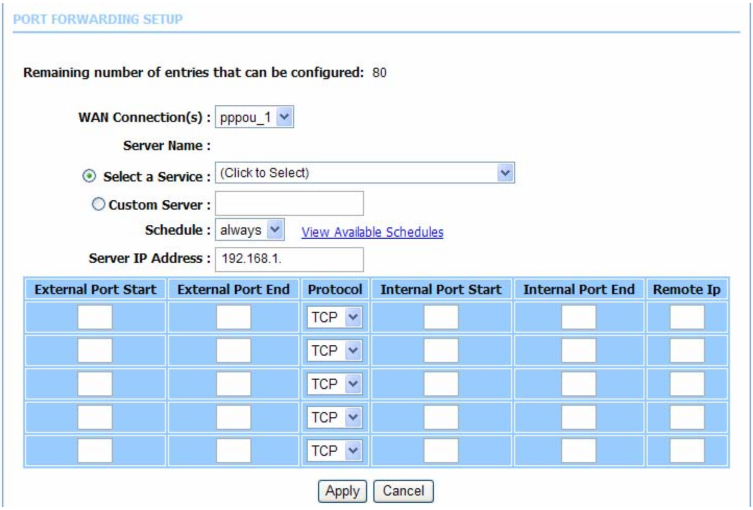
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server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

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

PORT FORWARDING SETUP

	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP

Click **Add** to add a virtual server.



PORT FORWARDING SETUP

Remaining number of entries that can be configured: 80

WAN Connection(s) : pppou_1

Server Name :

● Select a Service : (Click to Select)

○ Custom Server :

Schedule : always View Available Schedules

Server IP Address : 192.168.1.

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

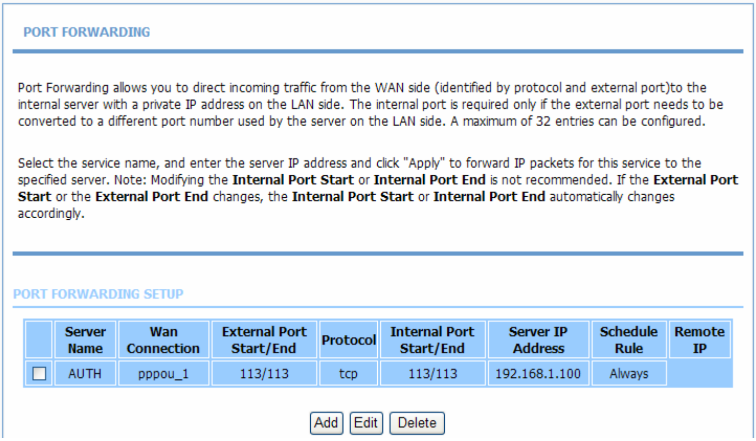
Select a service for a preset application, or enter a name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.

The Ports show the ports that you want to open on the device.

The **TCP/UDP** means the protocol type of the opened ports.

Click Apply to save the settings. The page shown in the following figure appears. A virtual server is added.



PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a 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 of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

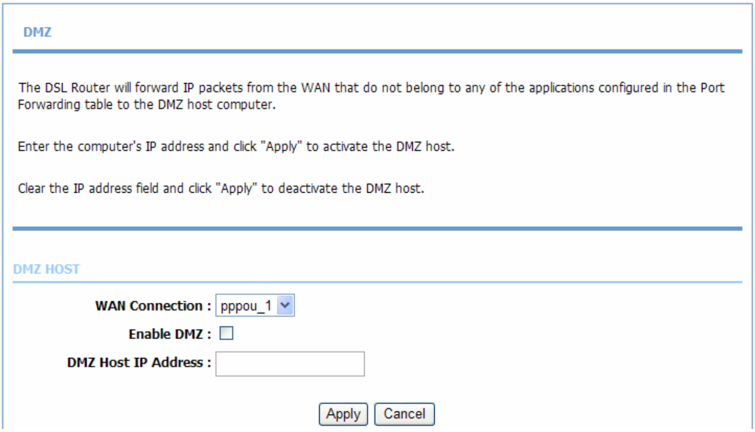
PORT FORWARDING SETUP

	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
□	AUTH	pppou_1	113/113	tcp	113/113	192.168.1.100	Always	

3.3.3 DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

Choose **ADVANCED** > **DMZ**. The page shown in the following figure appears.



DMZ

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding 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.

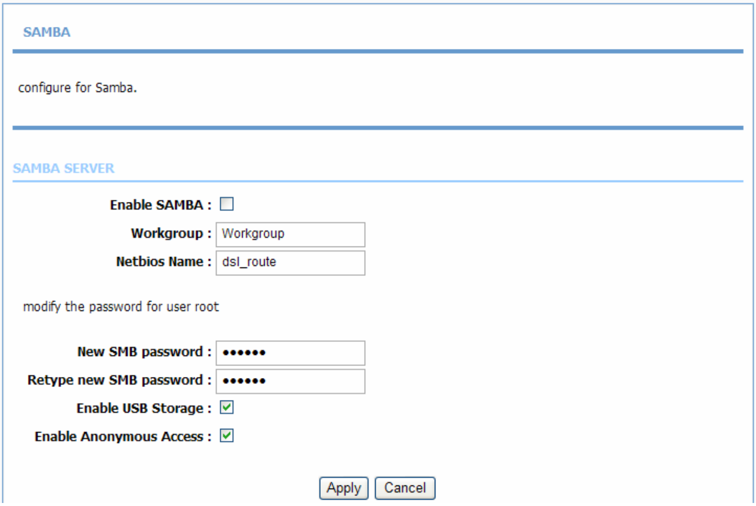
DMZ HOST

WAN Connection :	pppou_1
Enable DMZ :	□
DMZ Host IP Address :	

Click **Apply** to save the settings.

3.3.4 SAMBA

Select **SAMBA**.The page shown in the following figure appears.



SAMBA

configure for Samba.

SAMBA SERVER

Enable SAMBA :	□
Workgroup :	Workgroup
Netbios Name :	dsl_route

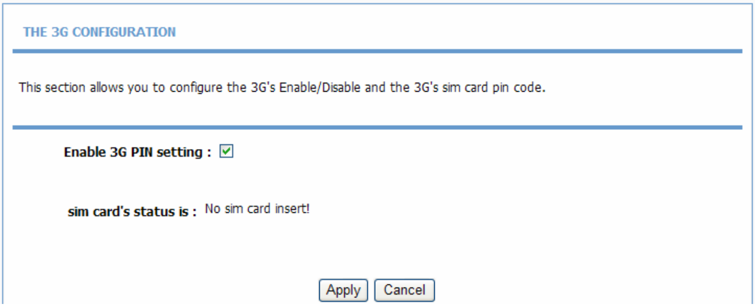
modify the password for user root

New SMB password :	••••••
Retype new SMB password :	••••••
Enable USB Storage :	☑
Enable Anonymous Access :	☑

- **Enable SAMBA**: Select the check box to enable the samba service.
- **Workgroup**: Enter the name of your local area network (LAN).
- **Netbios Name**: Enter your netbios name which is an identifier used by netbios services running on a computer.
- **New SMB password**: Enter your samba password for user root.
- **Retype new SMB password**: Reconfirm your samba password here.
- **Enable USB Storage**: Select the check box to support USB storage.
- **Enable Anonymous Access**: Select the check box to allow anonymous users access.

3.3.5 3G Configuration

Choose **ADVANCED** > **3G Configuration**. The page shown in the following figure appears. In this page, you can manage the 3G pin, including modifying, enabling, disabling, and unlocking it.



THE 3G CONFIGURATION

This section allows you to configure the 3G's Enable/Disable and the 3G's sim card pin code.

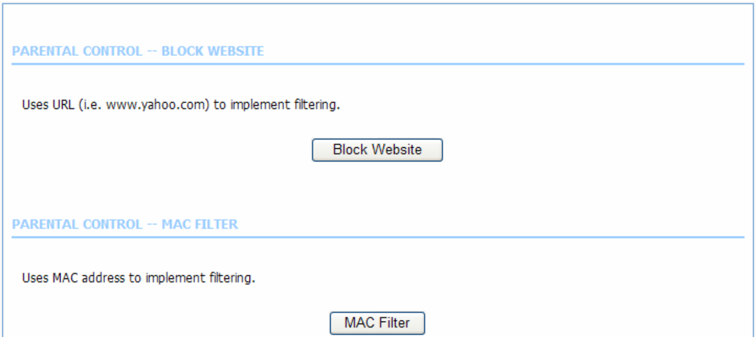
Enable 3G PIN setting : ☑

sim card's status is : No sim card insert!

Click **Apply** to save the settings.

3.3.6Parental Control

Choose **ADVANCED** > **Parental Control**. The **Parent Control** page shown in the following figure appears.



PARENTAL CONTROL -- BLOCK WEBSITE

Uses URL (i.e. www.yahoo.com) to implement filtering.

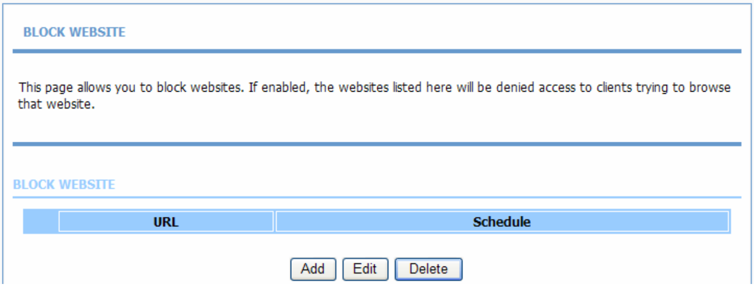
PARENTAL CONTROL -- MAC FILTER

Uses MAC address to implement filtering.

This page provides two useful tools for restricting the Internet access. **Block Websites** allows you to quickly create a list of all websites that you wish to stop users from accessing. **Block MAC Address** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

3.3.6.1 Block Website

In the **Parent Control** page, click **Block Website**. The page shown in the following figure appears.



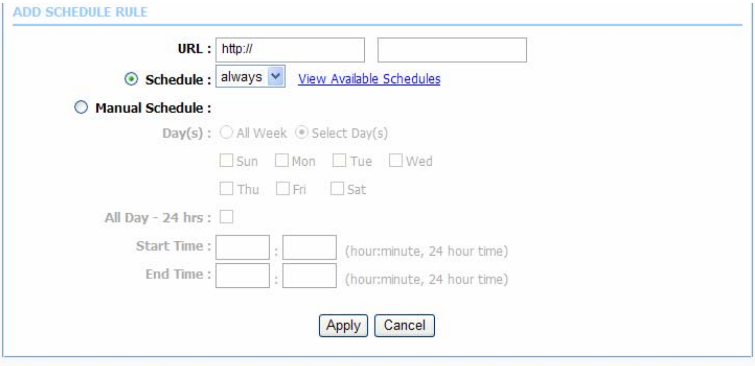
BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule

Click **Add**. The page shown in the following page appears.



ADD SCHEDULE RULE

URL : http://

● Schedule : always

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

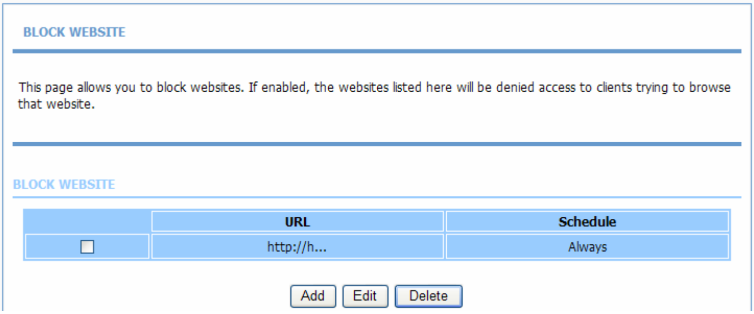
All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Enter the website in the **URL** field. Select the **Schedule** from drop-down list, or select **Manual Schedule** and select the corresponding time and days.

Click **Apply** to add the website to the **BLOCK WEBSITE Table**. The page shown in the following figure appears.



BLOCK WEBSITE

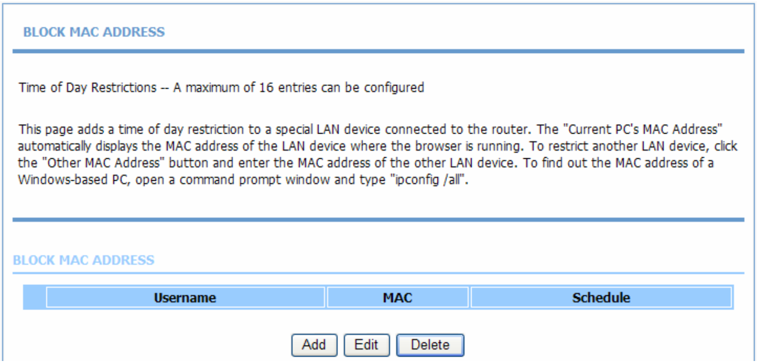
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule
□	http://h...	Always

3.3.6.2 MAC Filter

In the **Parent Control** page, click **MAC Filter**. The page shown in the following figure appears.



BLOCK MAC ADDRESS

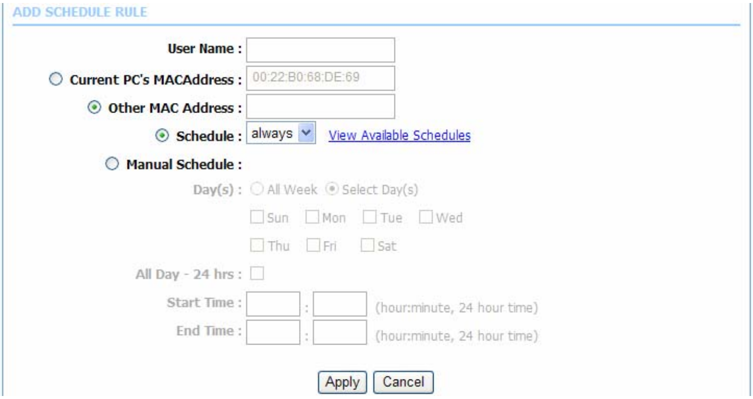
Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

BLOCK MAC ADDRESS

	Username	MAC	Schedule

Click **Add**. The page shown in the following figure appears.



ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:22:B0:68:DE:69

● Other MAC Address :

● Schedule : always View Available Schedules

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

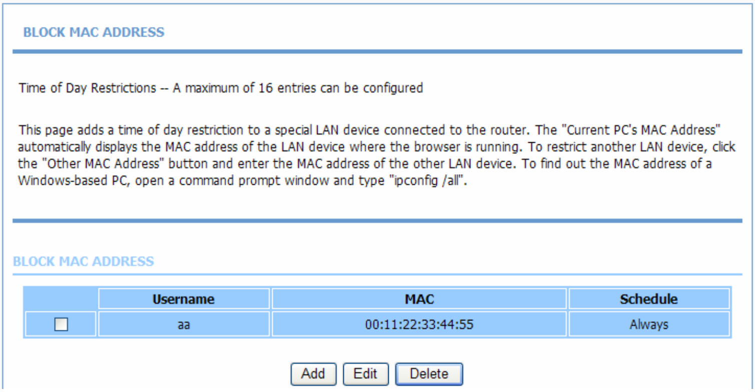
□ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS Table**. The page shown in the following figure appears.



BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

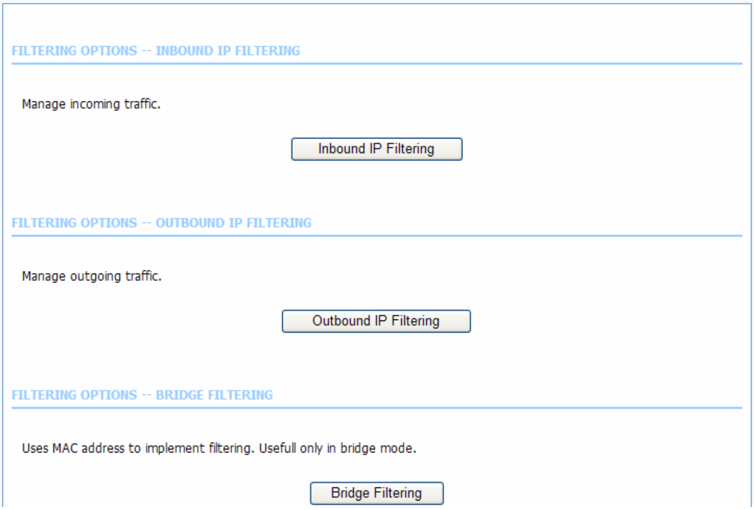
This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address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

BLOCK MAC ADDRESS

	Username	MAC	Schedule
□	aa	00:11:22:33:44:55	Always

3.3.7 Filtering Options

Choose **ADVANCED** > **Filtering Options**. The **Filtering Options** page shown in the following figure appears.



FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

FILTERING OPTIONS -- OUTBOUND IP FILTERING

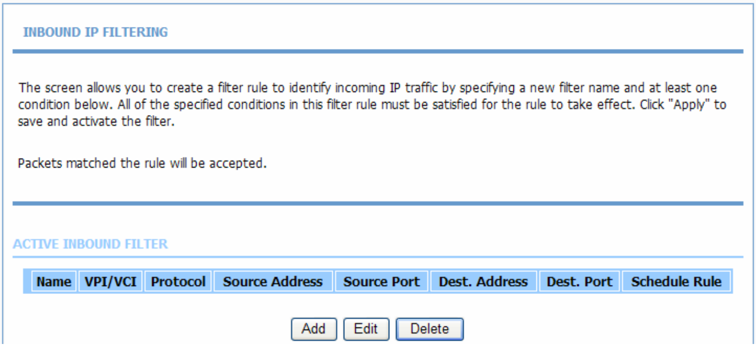
Manage outgoing traffic.

FILTERING OPTIONS -- BRIDGE FILTERING

Uses MAC address to implement filtering. Usefull only in bridge mode.

3.3.7.1 Inbound IP Filtering

In the **Filtering Options** page, click **Inbound IP Filtering**. The page shown in the following figure appears.



INBOUND IP FILTERING

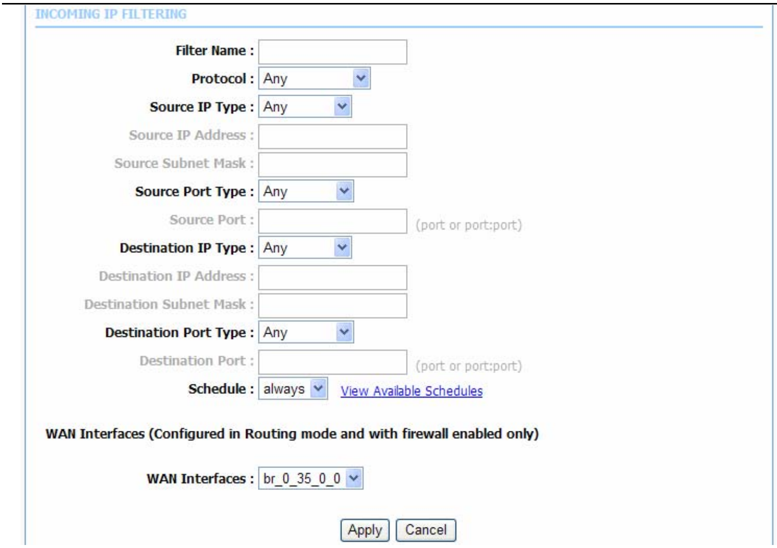
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

Packets matched the rule will be accepted.

ACTIVE INBOUND FILTER

Name	VPI/VCI	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Click **Add** to add an inbound IP filter. The page shown in the following figure appears.



INCOMING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : always View Available Schedules

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

WAN Interfaces : br_0_35_0_0

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port.

Click **Apply** to save the settings.

Note:

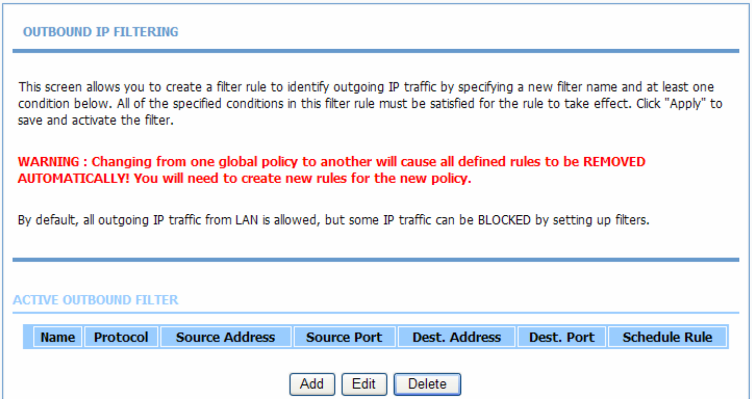
The settings only apply when the firewall is enabled.

The **ACTIVE INBOUND FILTER** shows detailed information about each created inbound IP filter. Click **Delete** to remove an IP filter (only appears when an IP filter exists).

3.3.7.2 Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition.

In the **Filtering Options** page, click **Outbound IP Filtering**. The page shown in the following figure appears.



OUTBOUND IP FILTERING

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

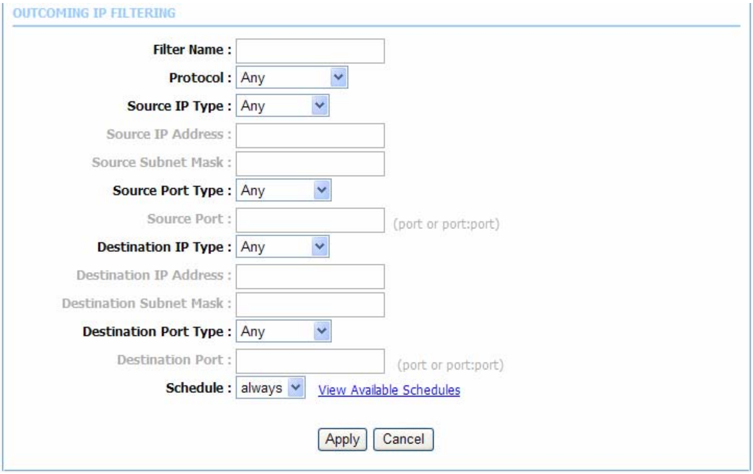
WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

ACTIVE OUTBOUND FILTER

Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Click **Add** to add an outbound IP filter. The page shown in the following figure appears.



OUTCOMING IP FILTERING

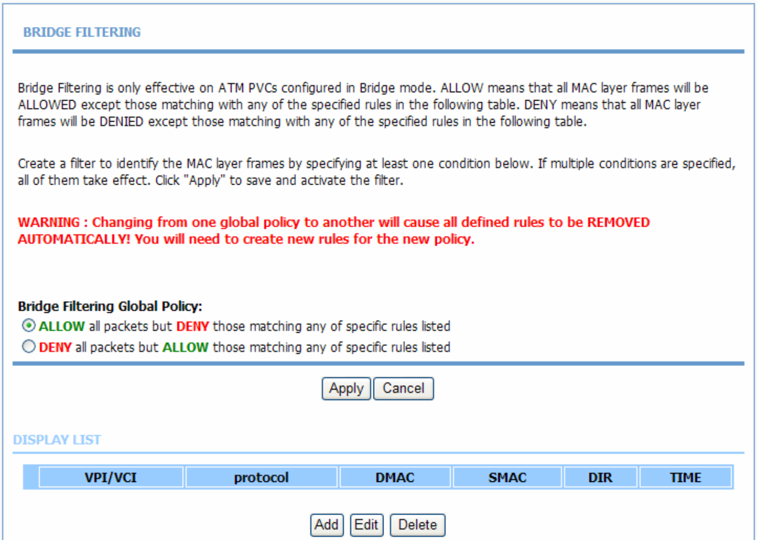
Filter Name :	
Protocol :	Any
Source IP Type :	Any
Source IP Address :	
Source Subnet Mask :	
Source Port Type :	Any
Source Port :	(port or port:port)
Destination IP Type :	Any
Destination IP Address :	
Destination Subnet Mask :	
Destination Port Type :	Any
Destination Port :	(port or port:port)
Schedule :	always View Available Schedules

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Click **Apply** to save the settings.

The **ACTIVE OUTBOUND IP FILTER** shows detailed information about each created outbound IP filter. Click **Delete** to delete an IP filter (only appears when an IP filter exists).

3.3.7.3 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page shown in the following figure appears.This page is used to configure bridge parameters. In this page, you can change the settings or view some information of the bridge and its attached ports.



BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

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

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

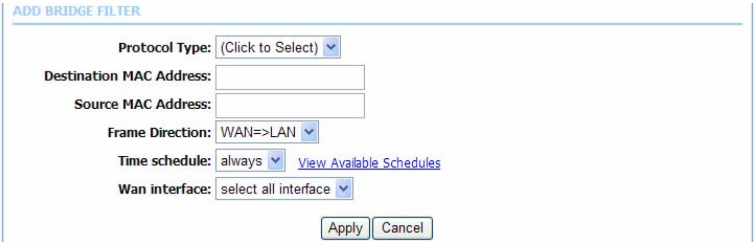
● ALLOW all packets but DENY those matching any of specific rules listed

○ DENY all packets but ALLOW those matching any of specific rules listed

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME

Click **Add** to add a bridge filter. The page shown in the following figure appears.



ADD BRIDGE FILTER

Protocol Type: (Click to Select)

Destination MAC Address:

Source MAC Address:

Frame Direction: WAN=>LAN

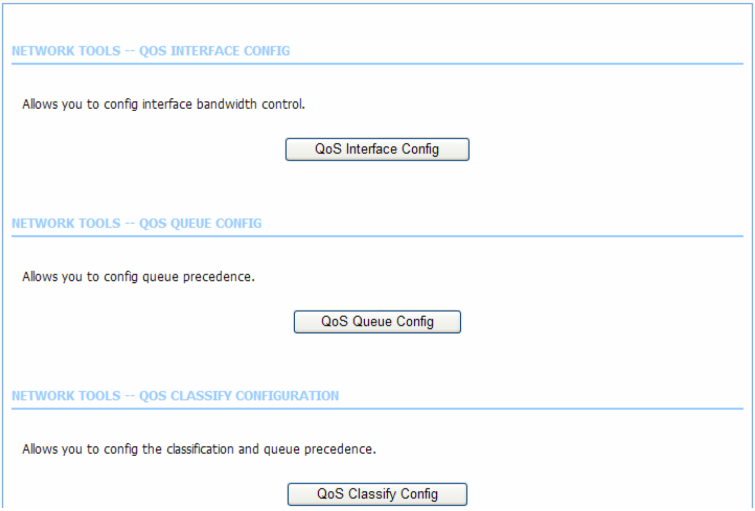
Time schedule: always

Wan interface: select all interface

Click **Apply** to save the settings.

3.3.8 Qos Config

Choose **ADVANCED** >**Qos Config**. The page shown in the following figure appears.



NETWORK TOOLS -- QOS INTERFACE CONFIG

Allows you to config interface bandwidth control.

NETWORK TOOLS -- QOS QUEUE CONFIG

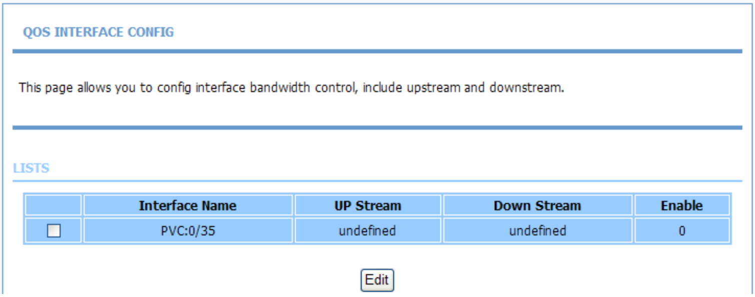
Allows you to config queue precedence.

NETWORK TOOLS -- QOS CLASSIFY CONFIGURATION

Allows you to config the classification and queue precedence.

3.3.8.1 QoS Interface Config

In the **QoS CONFIG** page, click **QoS Interface Config**. The page as shown in the following figure appears:



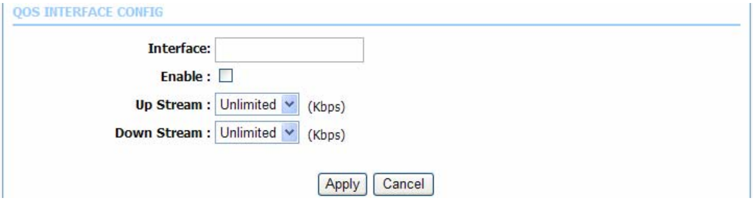
QOS INTERFACE CONFIG

This page allows you to config interface bandwidth control, include upstream and downstream.

LISTS

	Interface Name	UP Stream	Down Stream	Enable
□	PVC:0/35	undefined	undefined	0

Click **Edit** and the page as shown in the following figure appears:



QOS INTERFACE CONFIG

Interface:

Enable : □

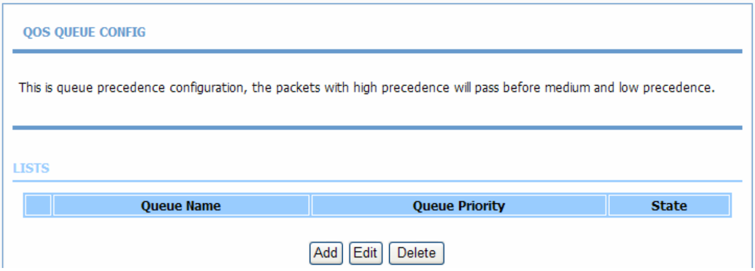
Up Stream : Unlimited (Kbps)

Down Stream : Unlimited (Kbps)

In this page, you can configure the uplink bandwidth and downlink bandwidth of each interface. The uplink rate and the downlink rate are limited according to the configured bandwidth. Click **Apply** to save the settings.

3.3.8.2 Queue Configuration

In the **QoS CONFIG** page, click **Qos Queue Config**. The page as shown in the following figure appears:



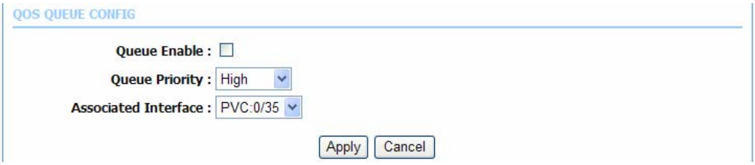
QOS QUEUE CONFIG

This is queue precedence configuration, the packets with high precedence will pass before medium and low precedence.

LISTS

	Queue Name	Queue Priority	State

In this page, you can configure the priority of the queue. The device supports the following three priority levels: high, medium, low. The device handles packets of the high queue priority first, then packets of medium, and finally packets of low priority. Click **Add**. The page as shown in the following figure appears:



QOS QUEUE CONFIG

Queue Enable : □

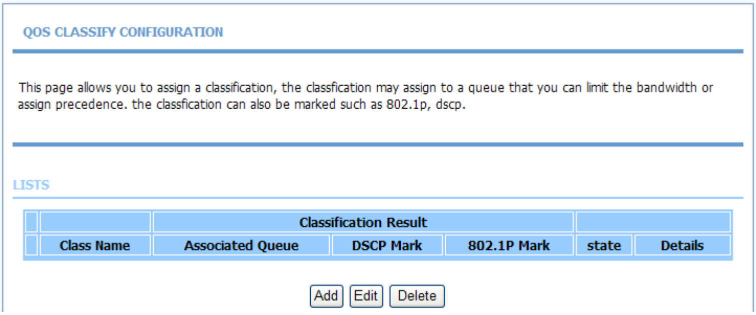
Queue Priority : High

Associated Interface : PVC:0/35

Click **Apply** to save the settings.

3.3.8.3 Classification Configuration

In the **QoS CONFIG** page, click **QoS Classify Configuration**. The page as shown in the following figure appears:



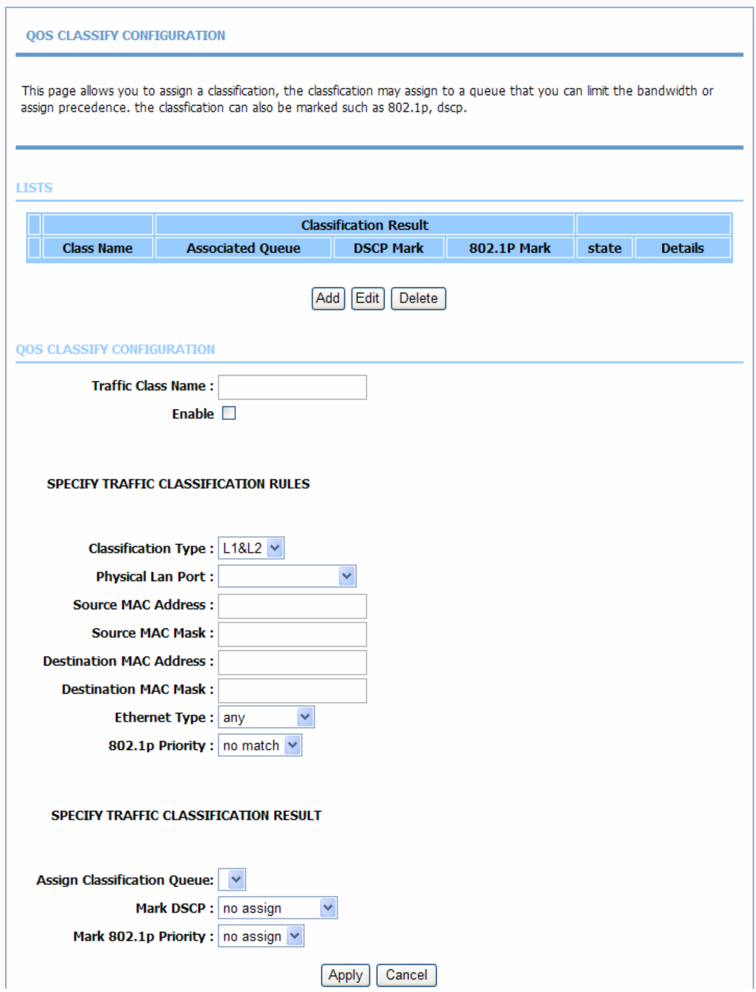
QOS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classfication may assign to a queue that you can limit the bandwidth or assign precedence. the classfication can also be marked such as 802.1p, dscp.

LISTS

		Classification Result				
	Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details

This page displays the classes. Click **Add** and the page as shown in the following figure appears:



QOS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classfication may assign to a queue that you can limit the bandwidth or assign precedence. the classfication can also be marked such as 802.1p, dscp.

LISTS

		Classification Result				
	Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details

QOS CLASSIFY CONFIGURATION

Traffic Class Name :

Enable □

SPECIFY TRAFFIC CLASSIFICATION RULES

Classification Type : L1&L2

Physical Lan Port :

Source MAC Address :

Source MAC Mask :

Destination MAC Address :

Destination MAC Mask :

Ethernet Type : any

802.1p Priority : no match

SPECIFY TRAFFIC CLASSIFICATION RESULT

Assign Classification Queue:

Mark DSCP : no assign

Mark 802.1p Priority : no assign

The following table describes the parameters in this page.

Field	Description
Traffic Class Name	Enter the name of the traffic class.
Enable	Select or deselect the check box to enable or

Field	Description
	disable QoS classification.
SPECIFY TRAFFIC CLASSIFICATION RULES	
Classification Type	Select **L1&L2** or **L3&L4** from the drop-down list. ● **L1&L2** maps to the features of layer 1 and layer 2, such as the MAC address. ● **L3&L4** maps to the features of layer 3 and layer 4, such as the IP address and the port.
Physical Lan Port	Select the physical port of the packet from the drop-down list. For example, ethernet1, ethernet2, ethernet3, and ethernet4.
Source MAC Address	Enter the source MAC address of the packet.
Source MAC Mask	Use mask 000000ffffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
Destination MAC Address	Enter the destination MAC address of the packet.
Destination MAC Mask	Use mask 000000ffffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped
Ethernet Type	Select the layer 2 protocol type from the drop-down list. For example, IP protocol and IPX protocol.
802.1p Priority	Select the 802.1p priority of the packet from the drop-down list. You can select **no match** or a value in the range of 0—7. Note that this function is not supported at the moment.
SPECIFIC TRAFFIC CLASSIFICATION RESULT	
Assign Classification Queue	Specify the queue to which the packet belongs. You can set the queue in the classification configuration.
Mark DSCP	Attach the DSCP mark to the mapped packet.
Mark 802.1p Priority	Attach the 802.1p mark to the mapped packet.

Click **Apply** to save the settings.

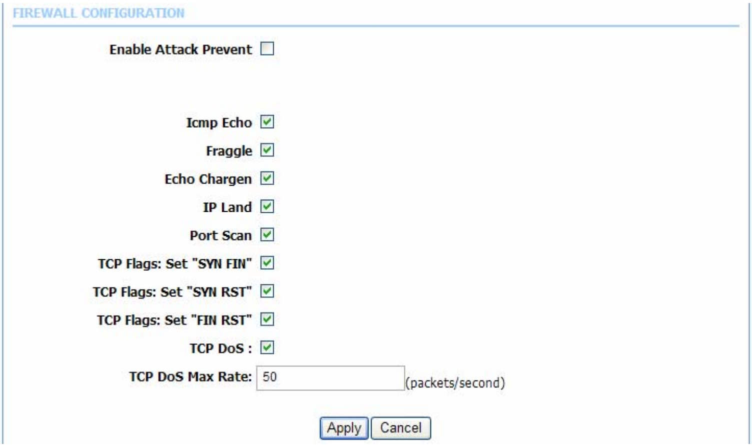
.

3.3.9 Firewall Settings

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Choose **ADVANCED** > **Firewall Settings**. The page shown in the following figure appears.



FIREWALL CONFIGURATION

Enable Attack Prevent □

Icmp Echo ☑

Fraggle ☑

Echo Chargen ☑

IP Land ☑

Port Scan ☑

TCP Flags: Set "SYN FIN" ☑

TCP Flags: Set "SYN RST" ☑

TCP Flags: Set "FIN RST" ☑

TCP DoS : ☑

TCP DoS Max Rate: 50 (packets/second)

Click **Apply** to save the settings.

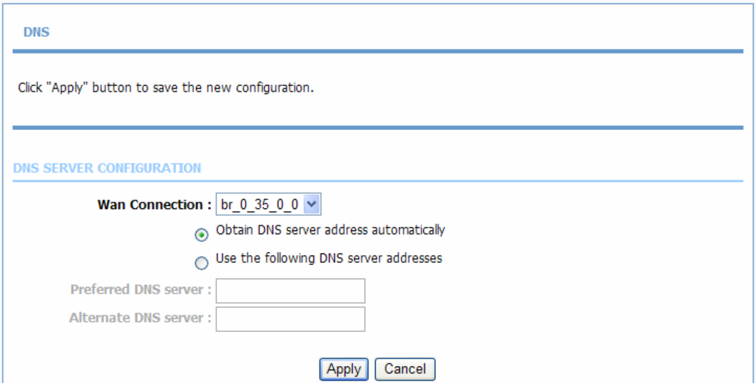
3.3.10 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The

Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **ADVANCED** > **DNS**. The page shown in the folllowin g figure appears.



DNS

Click "Apply" button to save the new configuration.

DNS SERVER CONFIGURATION

Wan Connection : br_0_35_0_0

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Preferred DNS server :

Alternate DNS server :

DNS SERVER CONFIGURATION

If you are using the device for DHCP service on the LAN or if you are using DNS servers on the ISP network, select **Obtain DNS server address automatically**.

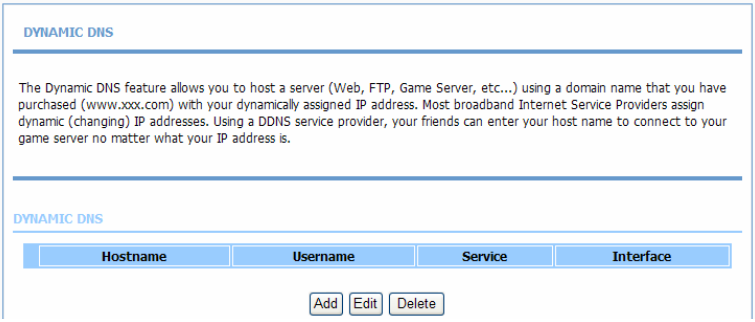
If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

Click **Apply** to save the settings.

3.3.11Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers.

Choose **ADVANCED** > **Dynamic DNS**. The page shown in the following page appears.



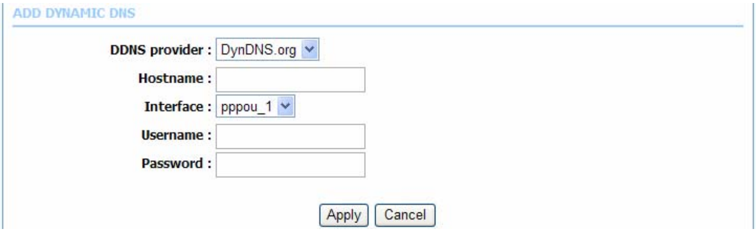
DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

DYNAMIC DNS

Hostname	Username	Service	Interface

Click **Add** to add dynamic DNS. The page shown in the following figure appears.



ADD DYNAMIC DNS

DDNS provider : DynDNS.org

Hostname :

Interface : pppou_1

Username :

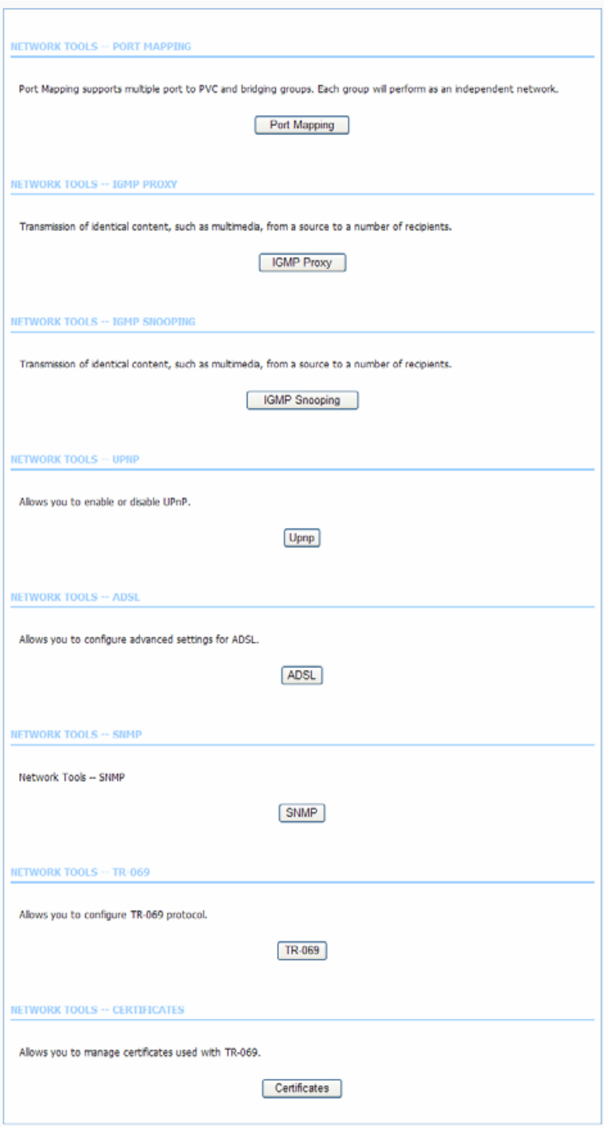
Password :

- **DDNS provider**: Select one of the DDNS registration organizations from the down-list drop. Available servers include DynDns.org and dlinkddns.com.
- **Host Name**: Enter the host name that you registered with your DDNS service provider.
- **Username**: Enter the user name for your DDNS account.
- **Password**: Enter the password for your DDNS account.

Click **Apply** to save the settings.

3.3.12 Network Tools

Choose **ADVANCED** > **Network Tools**. The page shown in the following figure appears.



NETWORK TOOLS -- PORT MAPPING

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

NETWORK TOOLS -- IGMP PROXY

Transmission of identical content, such as multimedia, from a source to a number of recipients.

NETWORK TOOLS -- IGMP SNOOPING

Transmission of identical content, such as multimedia, from a source to a number of recipients.

NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.

NETWORK TOOLS -- ADSL

Allows you to configure advanced settings for ADSL.

NETWORK TOOLS -- SNMP

Network Tools -- SNMP

NETWORK TOOLS -- TR-069

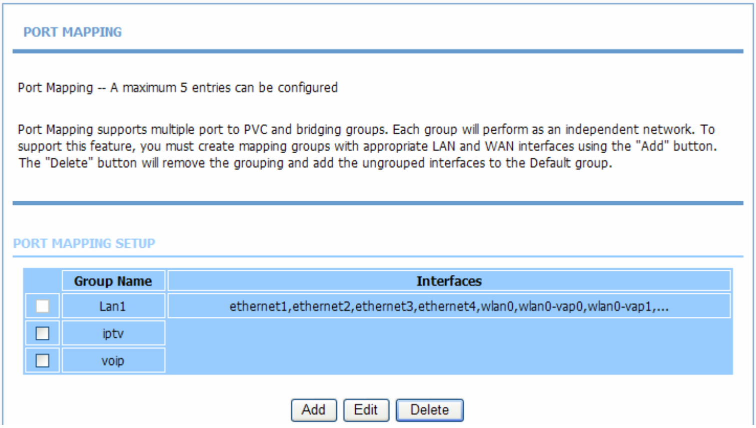
Allows you to configure TR-069 protocol.

NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

3.3.12.1 Port Mapping

Choose **ADVANCED** > **Network Tools** and click **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.



PORT MAPPING

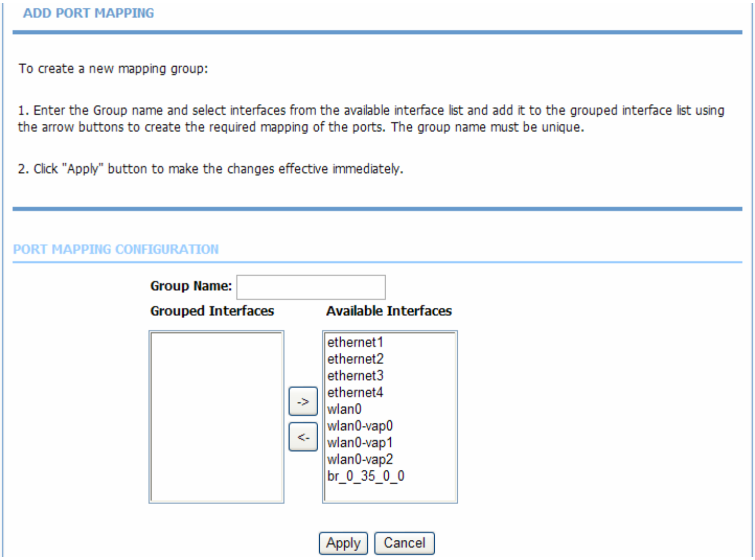
Port Mapping -- A maximum 5 entries can be configured

Port Mapping supports multiple port 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 "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

PORT MAPPING SETUP

	Group Name	Interfaces
□	Lan1	ethernet1,ethernet2,ethernet3,ethernet4,wlan0,wlan0-vap0,wlan0-vap1,...
□	iptv	
□	voip	

Click **Add** to add port mapping. The page shown in the following figure appears.



ADD PORT MAPPING

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. Click "Apply" button to make the changes effective immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces

Available Interfaces

ethernet1
ethernet2
ethernet3
ethernet4
wlan0
wlan0-vap0
wlan0-vap1
wlan0-vap2
br_0_35_0_0

The procedure for creating a mapping group is as follows:

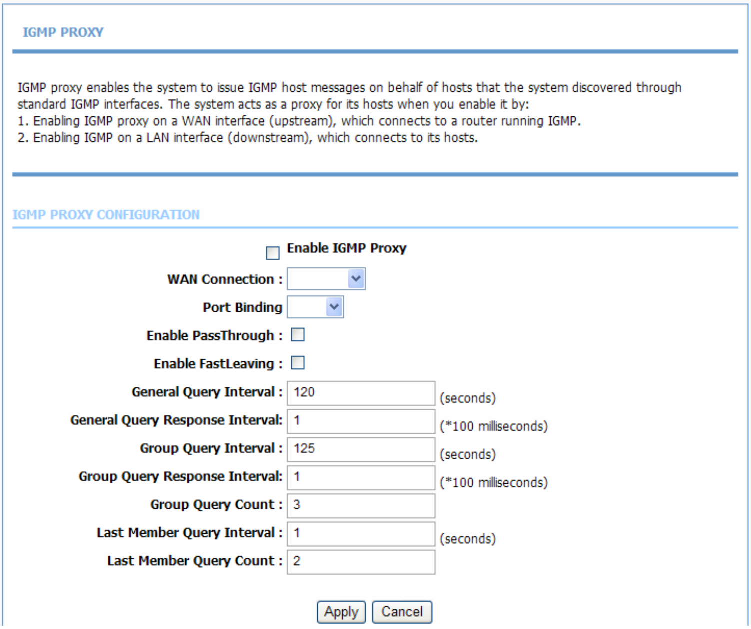
Step 1 Enter the group name.

Step 2 Select interfaces from the **Available Interface** list and click the **<-** arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 3 Click **Apply** to save the settings.

3.3.12.2 IGMP Proxy

Choose **ADVANCED** > **Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.



IGMP PROXY

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:
1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its hosts.

IGMP PROXY CONFIGURATION

□	Enable IGMP Proxy	
WAN Connection :		
Port Binding		
Enable PassThrough :	□	
Enable FastLeaving :	□	
General Query Interval :	120	(seconds)
General Query Response Interval:	1	(*100 milliseconds)
Group Query Interval :	125	(seconds)
Group Query Response Interval:	1	(*100 milliseconds)
Group Query Count :	3	
Last Member Query Interval :	1	(seconds)
Last Member Query Count :	2	

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.

Following are the parameters which can be configured:

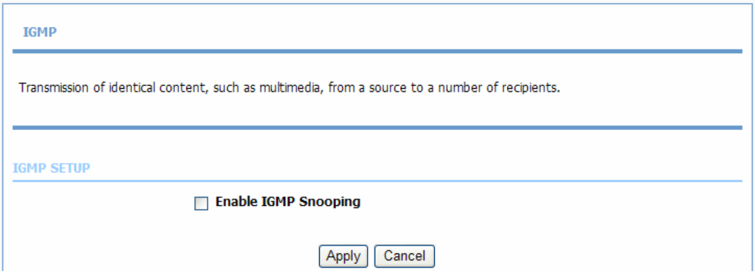
- **WAN Connection**: Select the WAN Connection which used to transmit the IGMP packets. You need to create WAN connection first.
- **Enable PassThrough**: The device preserve IP address field of the IGMP packets when sent in upstream direction to the DSLAM.
- **Enable FastLeaving**: Enable the IGMP user disconnected from particular multicast group immediately without performing the verification procedure with IGMP GSQ messages.

- **General Query Interval**: The device will send query messages to check IGMP user periodically. The unit is second.
- **General Query Response Interval**: The device waits for the IGMP user's replying. The unit is 100 * millisecond.
- **Group Query Interval**: The device will send multicast group query message to check if the IGMP user is still alive. The unit is second.
- **Group Query Response Interval**: The device waits for the IGMP user's replying. The unit is 100 * millisecond.
- **Group Query Count**: This parameter specifies how many times that the device sends the multicast group query message.
- **Last Member Query Interval**: When the last member left, the device sent the query messages periodically. The unit is second.
- **Last Member Query Count**: This parameter specifies how many times that the device sends the query message.

Click **Apply** to save the settings.

3.3.12.3 IGMP Snooping

When enable IGMP Snooping, the multicast data transmits through the specific LAN port which has received the request report.



IGMP

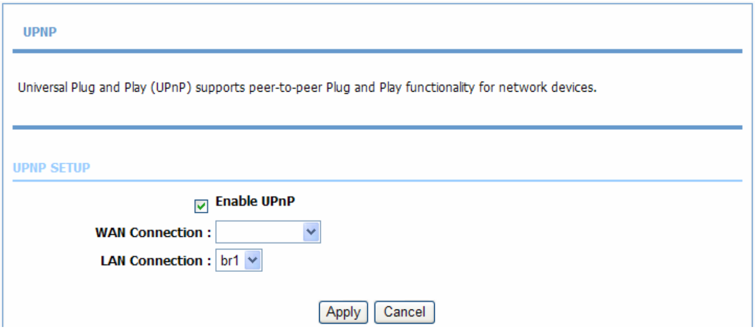
Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

☐ Enable IGMP Snooping

3.3.12.4 UPnP

Choose **ADVANCED** > **Network Tools** and click **UPnP**. The page shown in the following figure appears.



UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPNP SETUP

☑ Enable UPnP

WAN Connection :

LAN Connection : br1

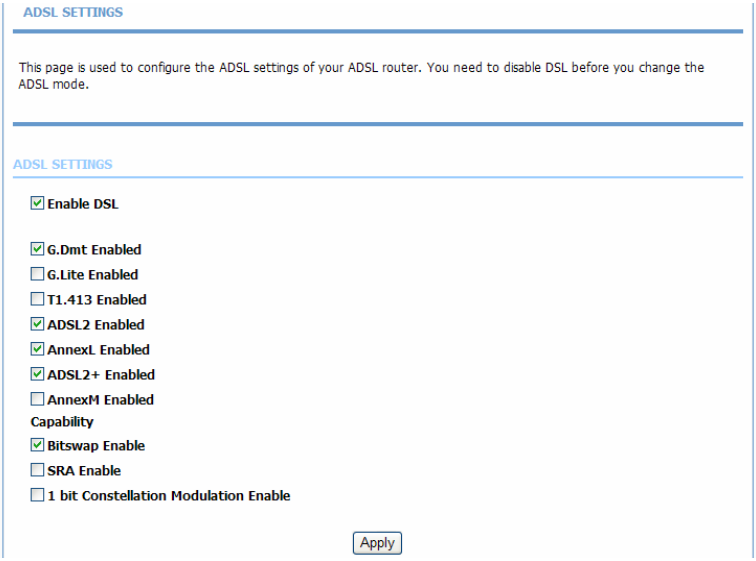
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

3.3.12.5 ADSL Settings

Choose **ADVANCED** > **Network Tools** and click **ADSL Settings**. The page shown in the following figure appears.



ADSL SETTINGS

This page is used to configure the ADSL settings of your ADSL router. You need to disable DSL before you change the ADSL mode.

ADSL SETTINGS

☑ Enable DSL

☑ G.Dmt Enabled
□ G.Lite Enabled
□ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

Capability

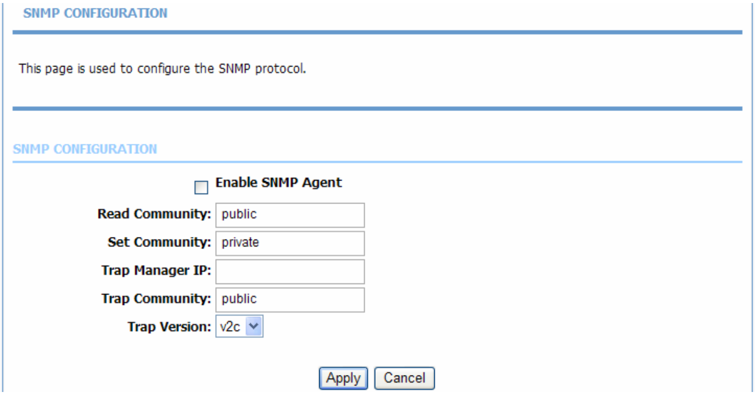
☑ Bitswap Enable
□ SRA Enable
□ 1 bit Constellation Modulation Enable

In this page, you can select the DSL modulation. Normally, you can remain this factory default setting. The device negotiates the modulation mode with DSLAM.

Click **Apply** to save the settings.

3.3.12.6 SNMP

Choose **ADVANCED** > **Network Tools** and click **SNMP**. The page shown in the following figure appears. In this page, you can set SNMP parameters.



SNMP CONFIGURATION

This page is used to configure the SNMP protocol.

SNMP CONFIGURATION

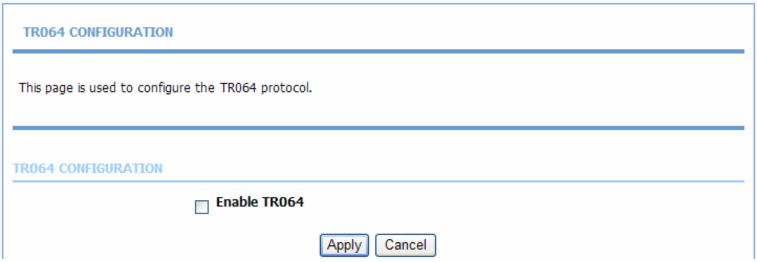
□ Enable SNMP Agent

Read Community:	public
Set Community:	private
Trap Manager IP:	
Trap Community:	public
Trap Version:	v2c

Click **Apply** to save the settings.

3.3.12.7 TR-064

Choose **ADVANCED > Network Tools** and click **TR-064.** The page shown in the following figure appears. In this page, you can enable the **TR064** service.



TR064 CONFIGURATION

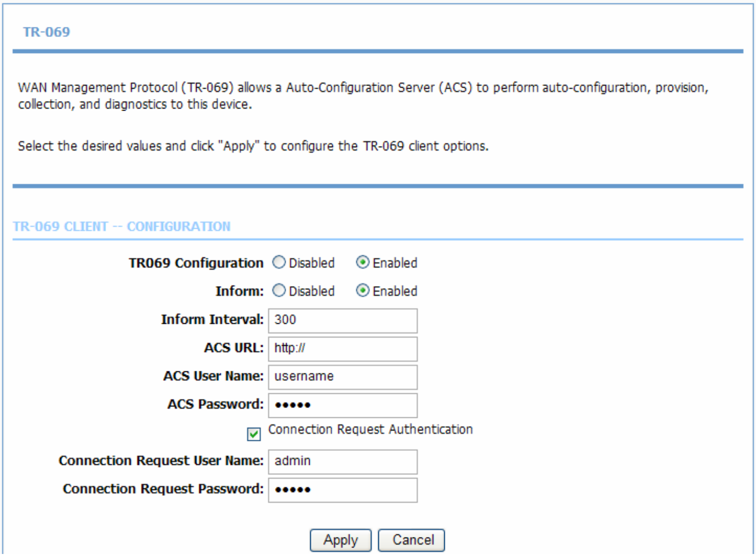
This page is used to configure the TR064 protocol.

TR064 CONFIGURATION

□ Enable TR064

3.3.12.8 TR-069

Choose **ADVANCED** > **Network Tools** and click **TR069**. The page shown in the following figure appears. In this page, you can configure the TR069 CPE.



TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

TR-069 CLIENT -- CONFIGURATION

TR069 Configuration ○ Disabled ● Enabled

Inform: ○ Disabled ● Enabled

Inform Interval: 300

ACS URL: http://

ACS User Name: username

ACS Password: •••••

☑ Connection Request Authentication

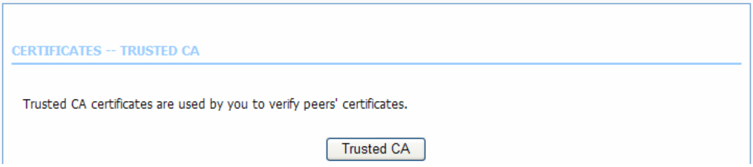
Connection Request User Name: admin

Connection Request Password: •••••

Click **Apply** to save settings.

3.3.12.9 Certificates

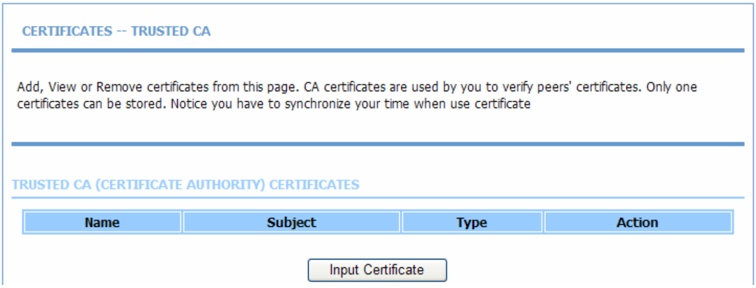
Choose **ADVANCED** > **Network Tools** and click **Certificates**. The **Certificates** page shown in the following figure appears.



CERTIFICATES -- TRUSTED CA

Trusted CA certificates are used by you to verify peers' certificates.

Press **Trusted CA** button to import a certificate



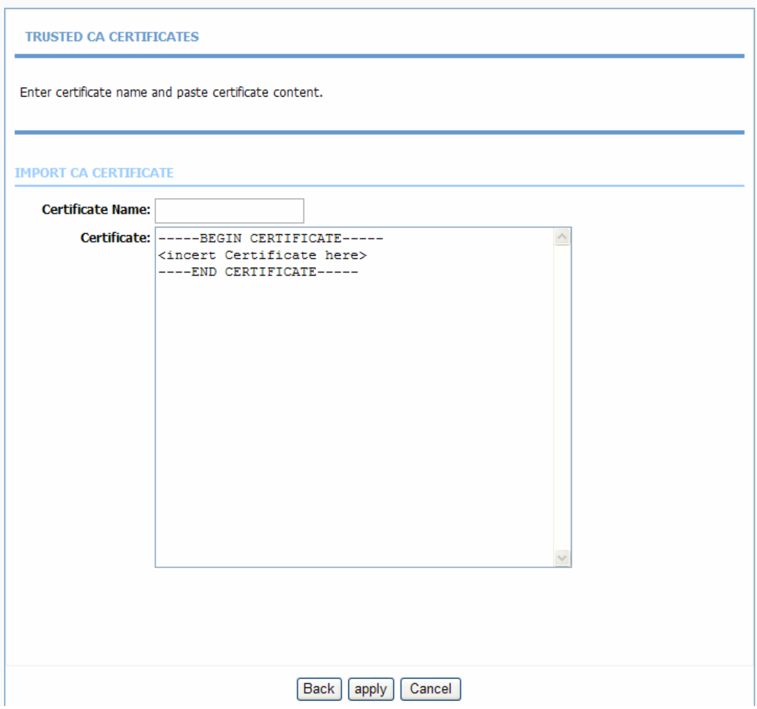
CERTIFICATES -- TRUSTED CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificates can be stored. Notice you have to synchronize your time when use certificate

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action

Press **Input Certificate** button to import a certification



TRUSTED CA CERTIFICATES

Enter certificate name and paste certificate content.

IMPORT CA CERTIFICATE

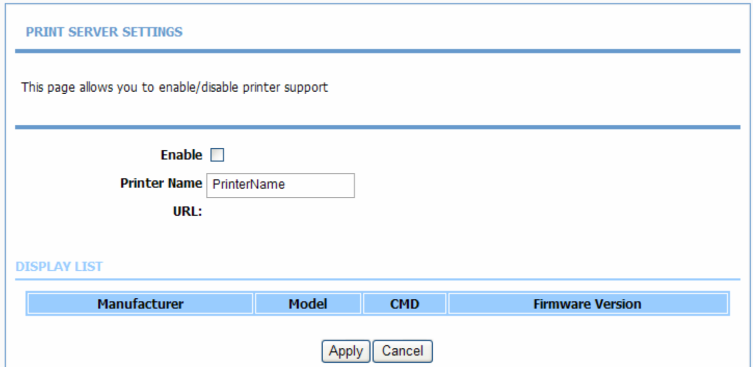
Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<incert Certificate here>
----END CERTIFICATE-----
```

3.3.12.10 Printer

This page allows you to config network printer, if you have an usb interface.



PRINT SERVER SETTINGS

This page allows you to enable/disable printer support

Enable □

Printer Name: PrinterName

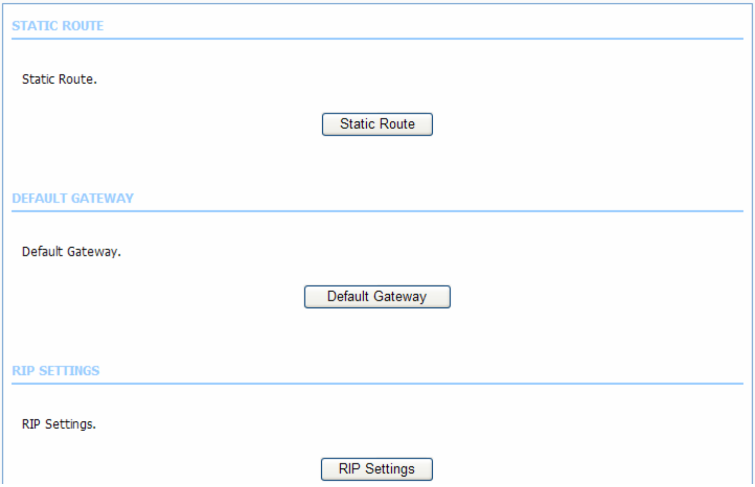
URL:

DISPLAY LIST

Manufacturer	Model	CMD	Firmware Version

3.3.13 Routing

Choose **ADVANCED** > **Routing**. The page shown in the following page appears.



STATIC ROUTE

Static Route.

DEFAULT GATEWAY

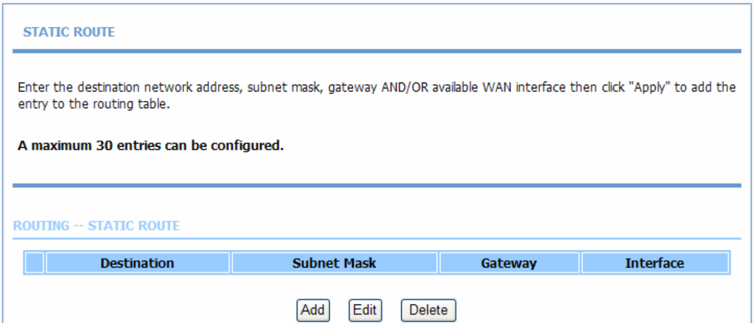
Default Gateway.

RIP SETTINGS

RIP Settings.

3.3.13.1 Static Route

Choose **ADVANCED** > **Routing** and click **Static Route**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.



STATIC ROUTE

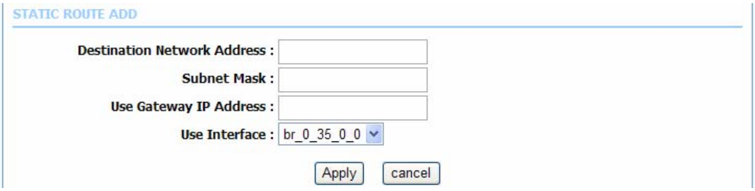
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

Click **Add** to add a static route. The page shown in the following figure appears.



STATIC ROUTE ADD

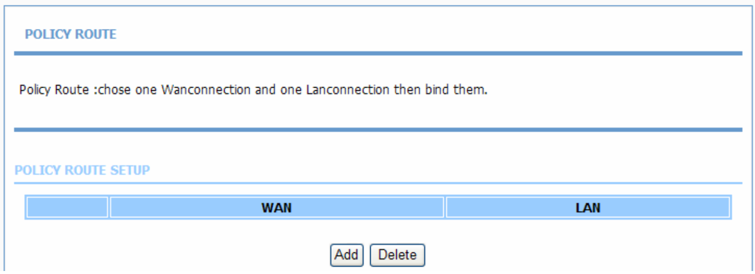
Destination Network Address :	
Subnet Mask :	
Use Gateway IP Address :	
Use Interface :	br_0_35_0_0

- **Destination Network Address**: The destination IP address of the router.
- **Subnet Mask**: The subnet mask of the destination IP address.
- **Use Gateway IP Address**: The gateway IP address of the router.
- **Use Interface**: The interface name of the router output port.

Click **Apply** to save the settings.

3.3.13.2 Policy Route

The policy route binds one WAN connection and one LAN interface.



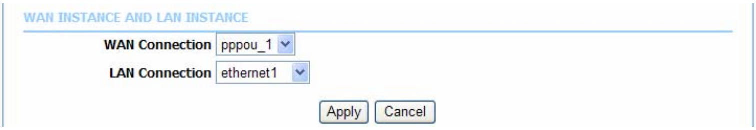
POLICY ROUTE

Policy Route :chose one Wanconnection and one Lanconnection then bind them.

POLICY ROUTE SETUP

	WAN	LAN

Click **add**, the page shown in the following figure appears.



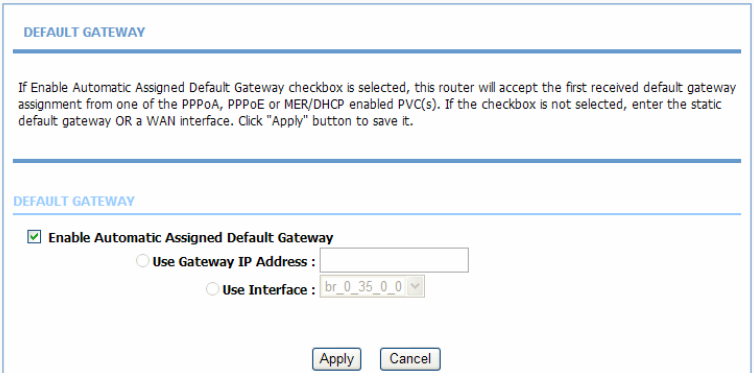
WAN INSTANCE AND LAN INSTANCE

WAN Connection pppou_1

LAN Connection ethernet1

3.3.13.3 Default Gateway

Choose **ADVANCED** > **Routing** and click **Default Gateway**. The page shown in the following figure appears.



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 OR a WAN interface. Click "Apply" button to save it.

DEFAULT GATEWAY

☑ Enable Automatic Assigned Default Gateway

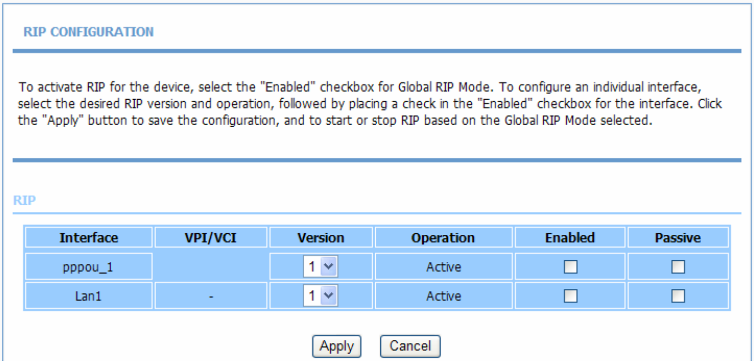
○ Use Gateway IP Address :

○ Use Interface : br_0_35_0_0

Click **Apply** to save the settings.

3.3.13.4 RIP Settings

Choose **ADVANCED** > **Routing** and click **RIP Settings**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.



RIP CONFIGURATION

To activate RIP for the device, select the "Enabled" checkbox 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 "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

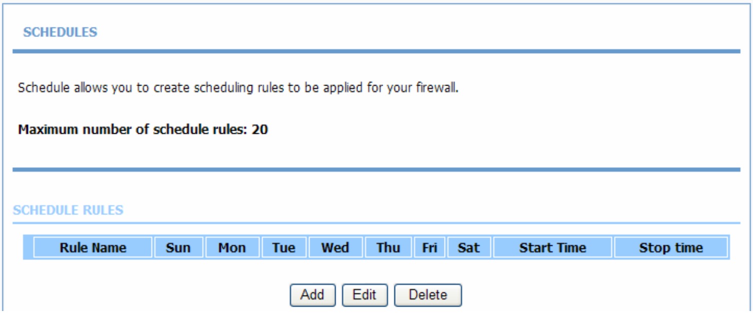
RIP

Interface	VPI/VCI	Version	Operation	Enabled	Passive
pppou_1		1	Active	□	□
Lan1	-	1	Active	□	□

If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

3.3.14 Schedules

Choose **ADVANCED** > **Schedules**. The page shown in the following figure appears.



SCHEDULES

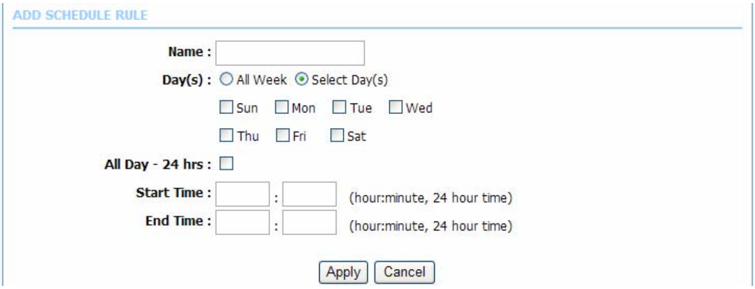
Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

SCHEDULE RULES

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time

Click **Add** to add schedule rule. The page shown in the following figure appears.



ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

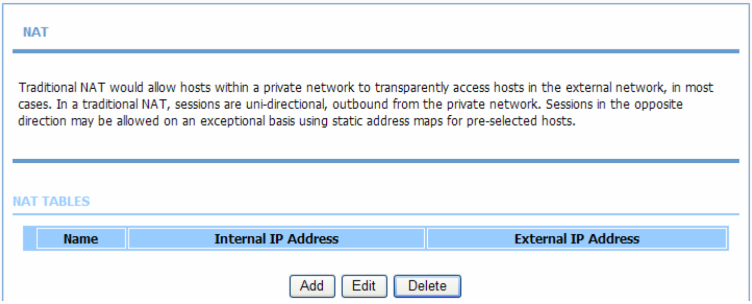
Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Click **Apply** to save the settings.

3.3.15 NAT

Network address translation (NAT) is the process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. The packets which source IP address match “Internal IP Address” in the NAT table come to the router, the router changes source IP of this packet by the IP address that set in “External IP Address”, then transmit the packet into Internet.



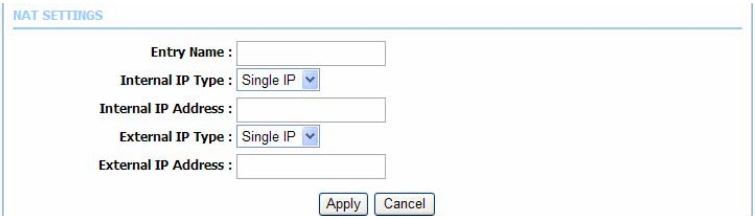
NAT

Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.

NAT TABLES

Name	Internal IP Address	External IP Address

Click **add**, the page shown in the following figure appears.



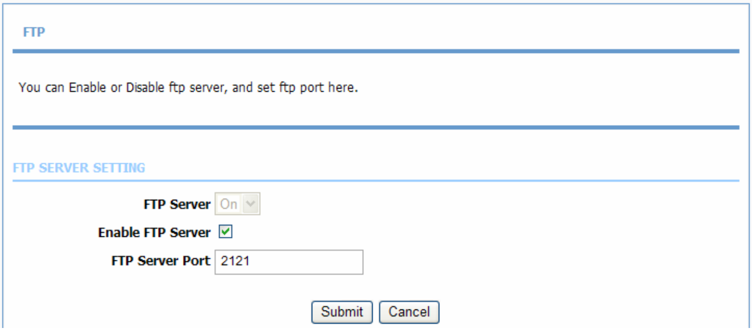
NAT SETTINGS

Entry Name :	
Internal IP Type :	Single IP
Internal IP Address :	
External IP Type :	Single IP
External IP Address :	

- **Entry Name**: A string that names this entry.
- **Internal IP Type**: By changing this setting, can change the single IP address type to input the IP range type in “Internal IP Address”.
- **Internal IP Address**:This IP Address should be set by a private network IP address ,
- **External IP Type**: By changing this setting, can change the single IP address type to input the IP range type in “External IP Address”.
- **External IP Address**: This should be set by an internal IP address.

3.3.16 FTPD Setting

Choose **ADVANCED** > **Logout**. The page shown in the following figure appears. In this page, you can Enable or Disable ftp server, and set ftp port here.



FTP

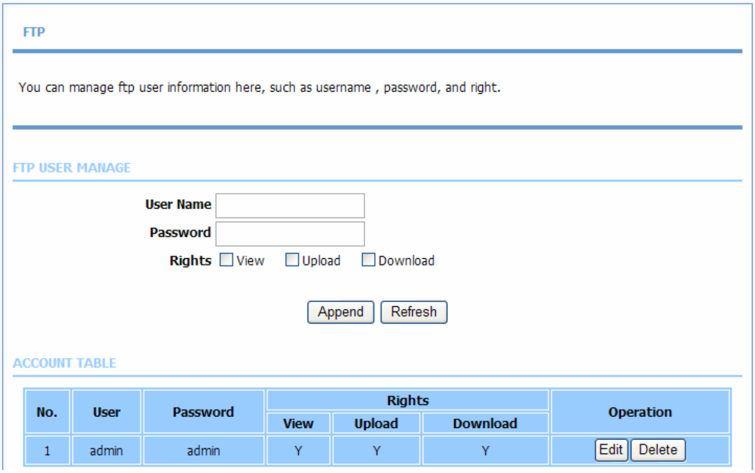
You can Enable or Disable ftp server, and set ftp port here.

FTP SERVER SETTING

FTP Server	On
Enable FTP Server	☑
FTP Server Port	2121

3.3.17FTPD Account

Choose **ADVANCED** > **Logout.** The page shown in the following figure appears. In this page, You can manage ftp user information here, such as username , password, and right.



FTP

You can manage ftp user information here, such as username , password, and right.

FTP USER MANAGE

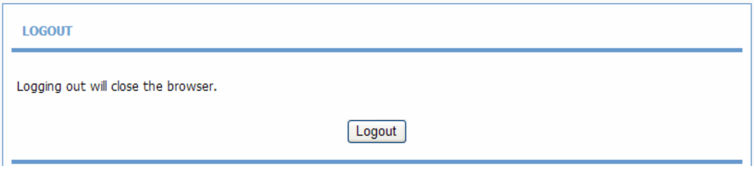
User Name	
Password	
Rights	□ View □ Upload □ Download

ACCOUNT TABLE

No.	User	Password	Rights			Operation
			View	Upload	Download	
1	admin	admin	Y	Y	Y	Edit Delete

3.3.18Logout

Choose **ADVANCED** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



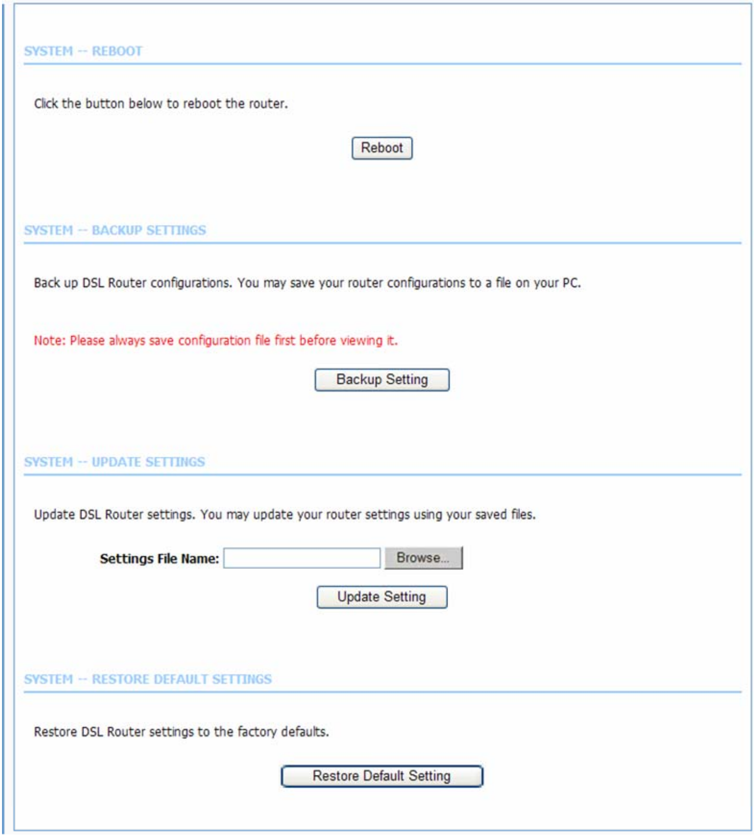
LOGOUT

Logging out will close the browser.

3.4 Management

3.4.1 System Management

Choose **MANAGEMENT** > **System Management**. The **System** page shown in the following figure appears.



SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.

Note: Please always save configuration file first before viewing it.

SYSTEM -- UPDATE SETTINGS

Update DSL Router settings. You may update your router settings using your saved files.

Settings File Name:

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

In this page, you can reboot device, back up the current settings to a file, restore the settings from the file saved previously, and restore the factory default settings.

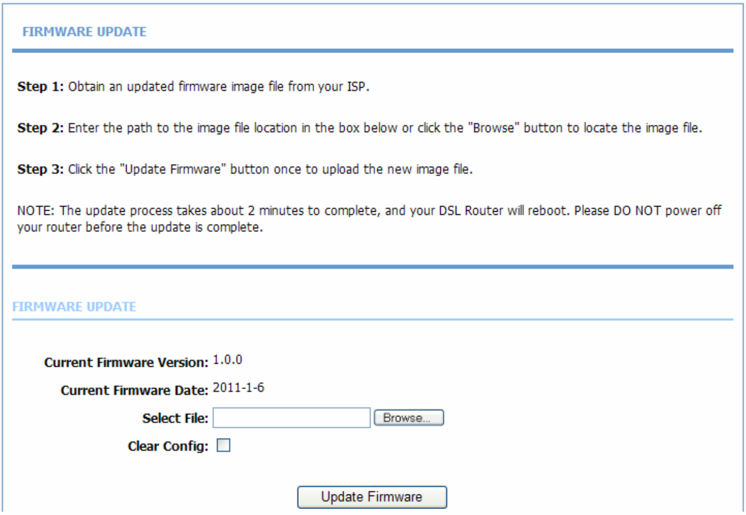
The buttons in this page are described as follows:

- **Reboot**: Reboot the device.
- **Backup Setting**: Save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
- **Update setting**: Click **Browse** to select the configuration file of device and click **Update Settings** to begin restoring the device configuration..
- **Restore Default Setting**: Reset the device to default settings.

***Notice**: Do not turn off your device or press the **Reset** button while an operation in this page is in progress.*

3.4.2 Firmware Update

Choose **MANAGEMENT** > **Firmware Update**. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.



FIRMWARE UPDATE

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

FIRMWARE UPDATE

Current Firmware Version: 1.0.0

Current Firmware Date: 2011-1-6

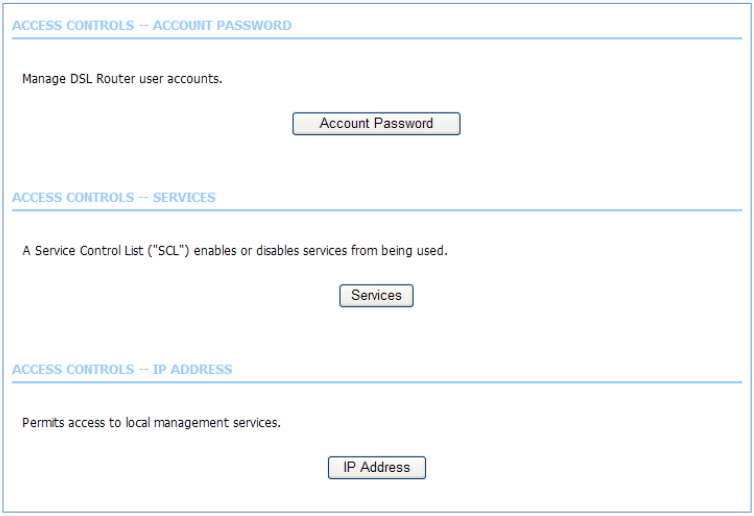
Select File:

Clear Config: □

The procedure for updating the firmware is as follows:
Step 1 Click **Browse…**to search the file.
Step 2 Select **Click Config**.
Step 3 Click **Update Firmware** to copy the file.
The device loads the file and reboots automatically.
Notice*: Do not turn off your device or press the reset button while this procedure is in progress.*

3.4.3 Access Controls

Choose **MANAGEMENT** > **Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **Account Password**, **Services**, and **IP Address**.



ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

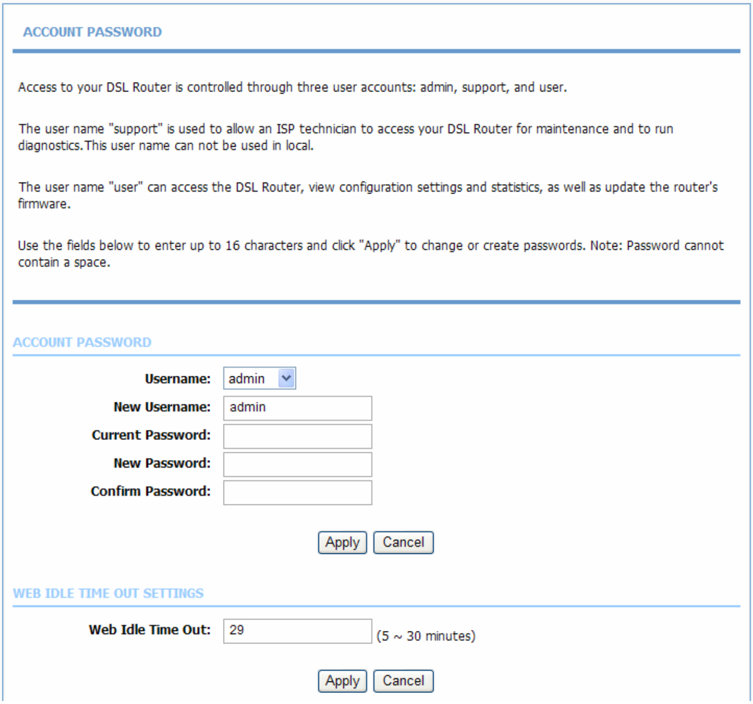
A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROLS -- IP ADDRESS

Permits access to local management services.

3.4.3.1 User Management

In the **Access Controls** page, click **User Management**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.



ACCOUNT PASSWORD

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.This user name can not be used in local.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username:	admin
New Username:	admin
Current Password:	
New Password:	
Confirm Password:	

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out: 29 (5 ~ 30 minutes)

You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

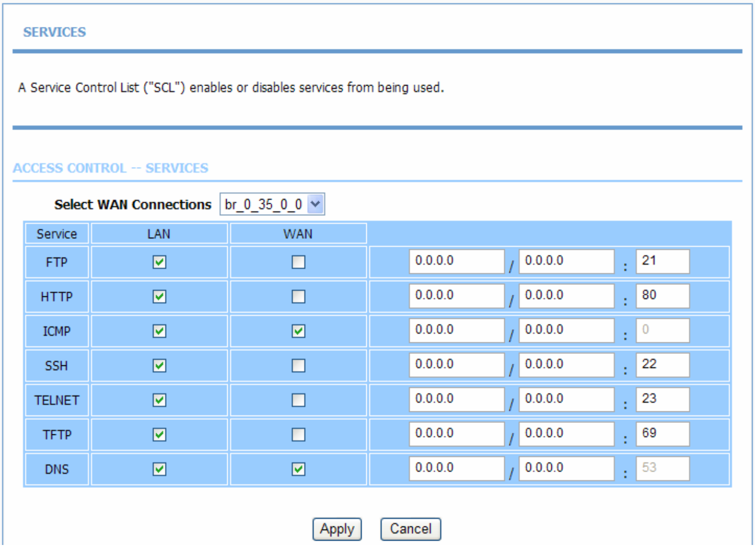
Select the **Username** from the drop-down list. You can select **admin,**, **support**, or **user**.

Enter the current and new passwords and confirm the new password, to change the password.

Click **Apply** to apply the settings.

3.4.3.2 Services

In the **Access Controls** page, click **Services**. The page shown in the following figure appears.



SERVICES

A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROL -- SERVICES

Select WAN Connections: br_0_35_0_0

Service	LAN	WAN	
FTP	☑	□	0.0.0.0 / 0.0.0.0 : 21
HTTP	☑	□	0.0.0.0 / 0.0.0.0 : 80
ICMP	☑	☑	0.0.0.0 / 0.0.0.0 : 0
SSH	☑	□	0.0.0.0 / 0.0.0.0 : 22
TELNET	☑	□	0.0.0.0 / 0.0.0.0 : 23
TFTP	☑	□	0.0.0.0 / 0.0.0.0 : 69
DNS	☑	☑	0.0.0.0 / 0.0.0.0 : 53

In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

Select the management services that you want to enable or disable on the LAN or WAN interface.

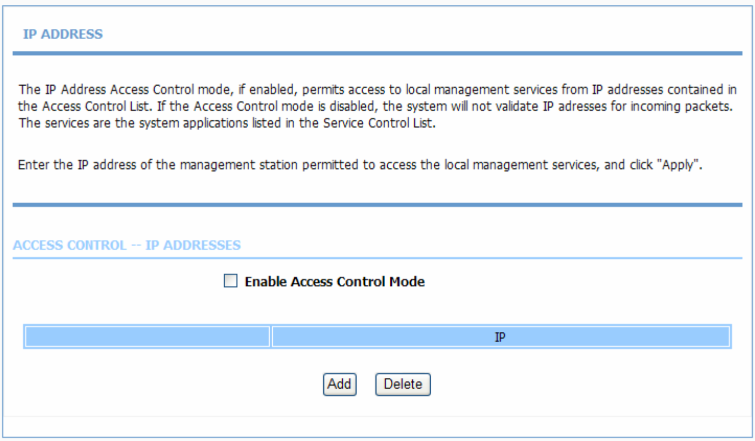
Click **Apply** to apply the settings.

Note:

If you disable HTTP service, you cannot access the configuration page of the device any more.

3.4.3.3 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.



IP ADDRESS

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 adresses for incoming packets. The services are the system applications listed in the Service Control List.

Enter the IP address of the management station permitted to access the local management services, and click "Apply".

ACCESS CONTROL -- IP ADDRESSES

☐ Enable Access Control Mode

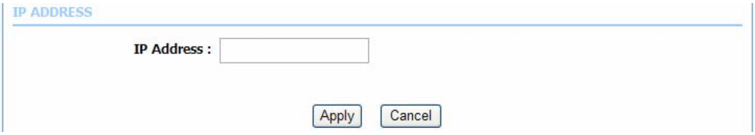
	IP

In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.
Select **Enable Access Control Mode** to enable ACL.

Note:

If you enable the ACL capability, ensure that IP address of the host is in ACL list.

Click **Add**. The page shown in the following figure appears.



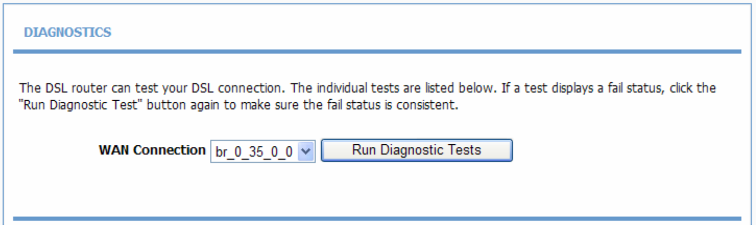
IP ADDRESS

IP Address :

Click **Apply** to apply the settings.

3.4.4 Diagnosis

Choose **MANAGEMENT**> **Diagnosis**. The page shown in the following figure appears. In this page, you can test the device.

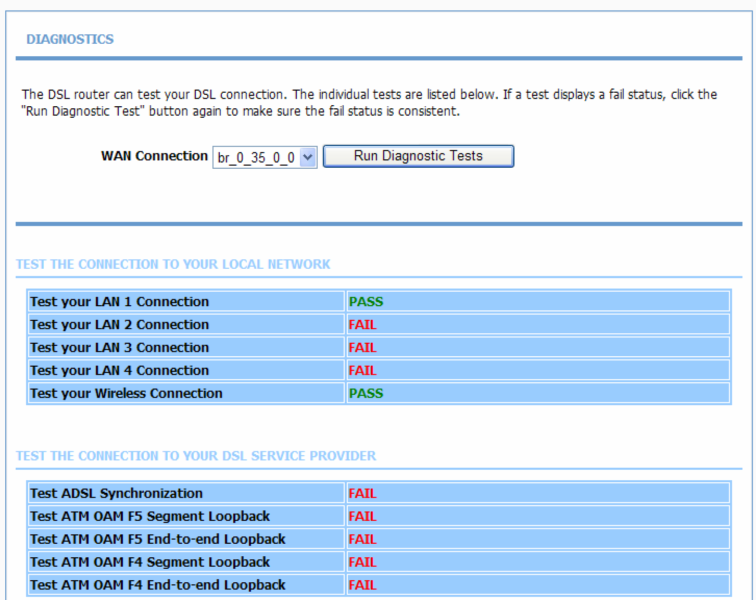


DIAGNOSTICS

The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection br_0_35_0_0

Click **Run Diagnostics Tests** to run diagnostics. The page shown in the following figure appears.



DIAGNOSTICS

The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection br_0_35_0_0

TEST THE CONNECTION TO YOUR LOCAL NETWORK

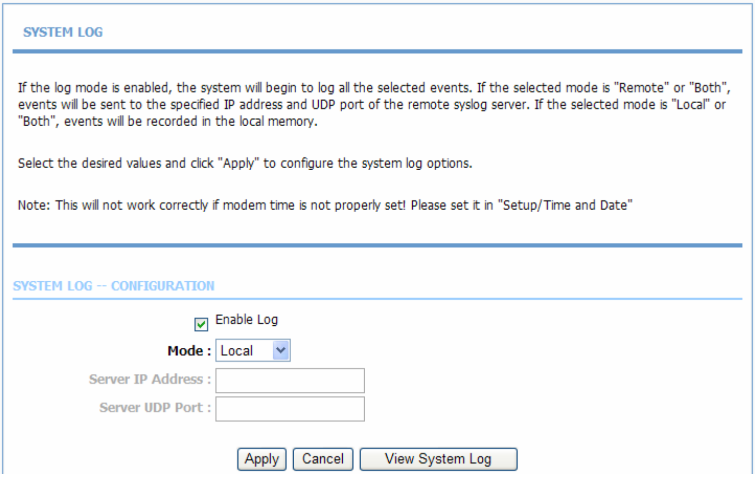
Test your LAN 1 Connection	PASS
Test your LAN 2 Connection	FAIL
Test your LAN 3 Connection	FAIL
Test your LAN 4 Connection	FAIL
Test your Wireless Connection	PASS

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

Test ADSL Synchronization	FAIL
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	FAIL
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

3.4.5 System Log

Choose **MANAGEMENT** > **Log Configuration**. The **System Log** page shown in the following figure appears.



SYSTEM LOG

If the log mode is enabled, the system will begin to log all the selected events. 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.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

SYSTEM LOG -- CONFIGURATION

☑ Enable Log

Mode : Local

Server IP Address :

Server UDP Port :

This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.

The procedure for logging the events is as follows:

Step 1 Select **Enable Log** check box.

Step 2 Select the display mode from the **Mode** drop-down list.

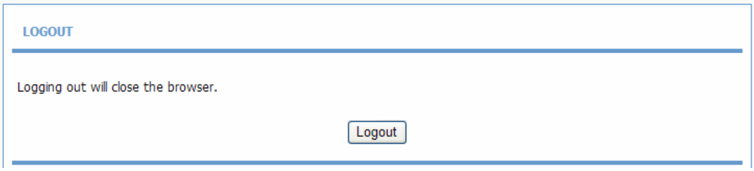
Step 3 Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

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

Step 5 Click **View System Log** to view the detail information of system log.

3.4.6 Logout

Choose **MANAGEMENT** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



LOGOUT

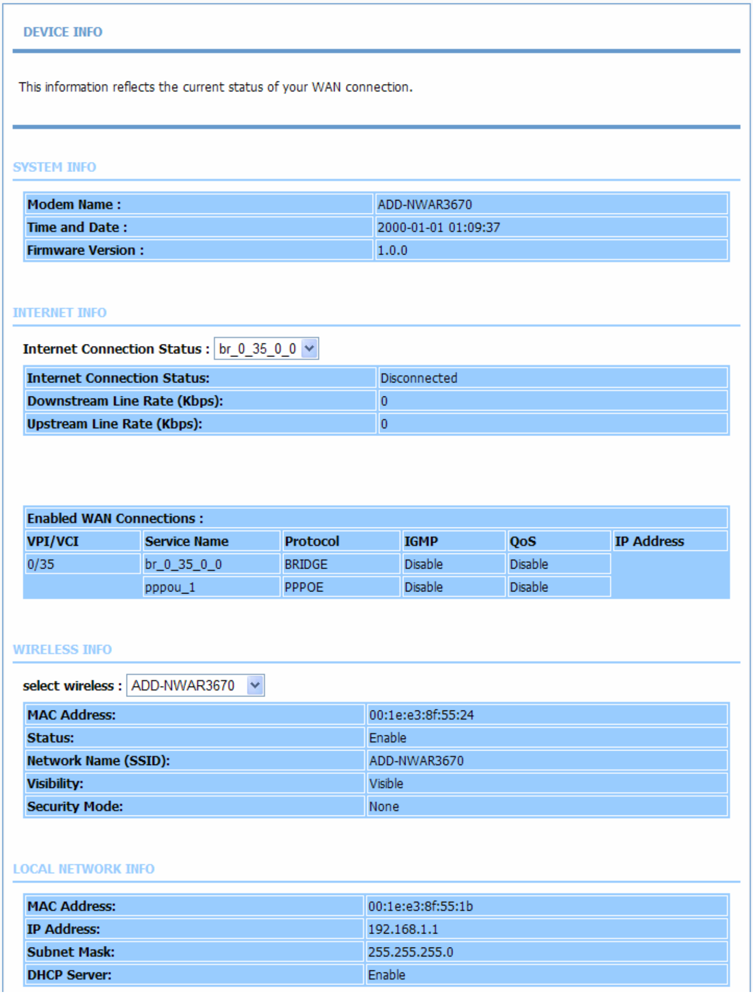
Logging out will close the browser.

3.5 Status

You can view the system information and monitor performance.

3.5.1 Device Info

Choose **STATUS** > **Device Info**. The page shown in the following figure appears.



DEVICE INFO

This information reflects the current status of your WAN connection.

SYSTEM INFO

Modem Name :	ADD-NWAR3670
Time and Date :	2000-01-01 01:09:37
Firmware Version :	1.0.0

INTERNET INFO

Internet Connection Status : br_0_35_0_0

Internet Connection Status:	Disconnected
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
0/35	br_0_35_0_0	BRIDGE	Disable	Disable	
	pppou_1	PPPOE	Disable	Disable	

WIRELESS INFO

select wireless : ADD-NWAR3670

MAC Address:	00:1e:e3:8f:55:24
Status:	Enable
Network Name (SSID):	ADD-NWAR3670
Visibility:	Visible
Security Mode:	None

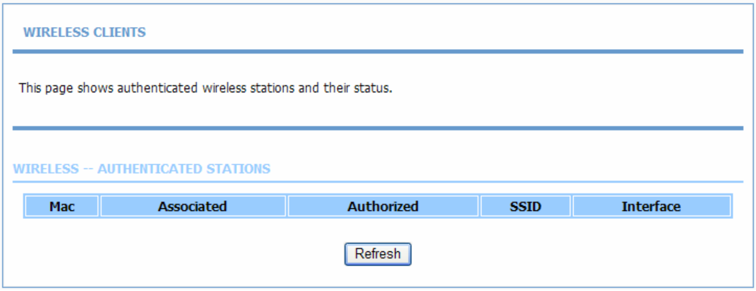
LOCAL NETWORK INFO

MAC Address:	00:1e:e3:8f:55:1b
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

3.5.2 Wireless Clients

Choose **STATUS** > **Wireless Clients**. The page shown in the following page appears. The page displays authenticated wireless stations and their statuses.



WIRELESS CLIENTS

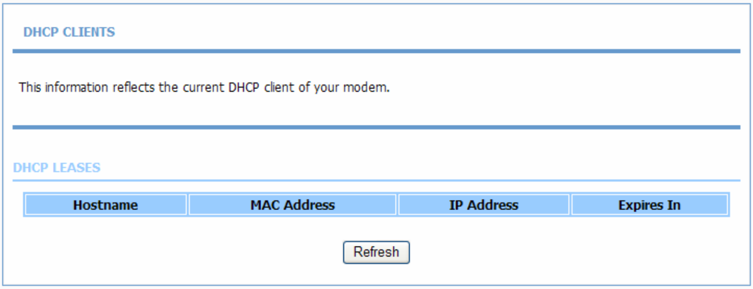
This page shows authenticated wireless stations and their status.

WIRELESS -- AUTHENTICATED STATIONS

Mac	Associated	Authorized	SSID	Interface

3.5.3 DHCP Clients

Choose **STATUS** > **DHCP Clients**. The page shown in the following page appears.



DHCP CLIENTS

This information reflects the current DHCP client of your modem.

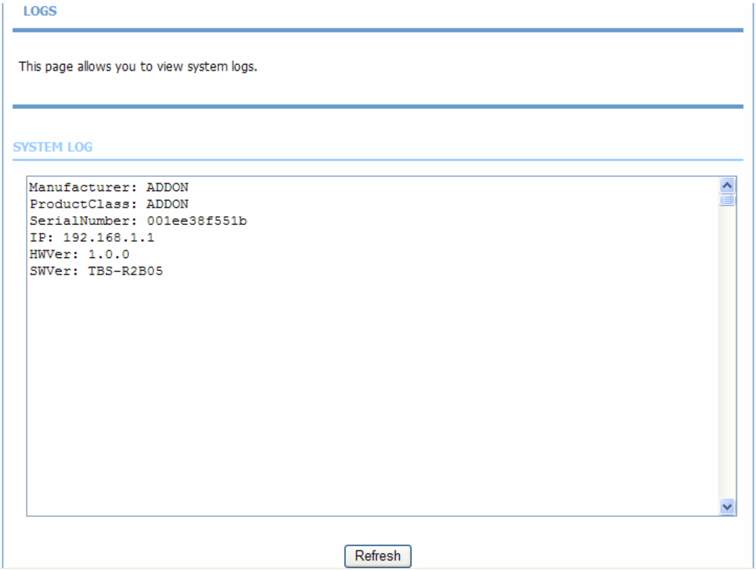
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).

3.5.4 Logs

Choose **STATUS** > **Logs**. The page shown in the following figure appears.



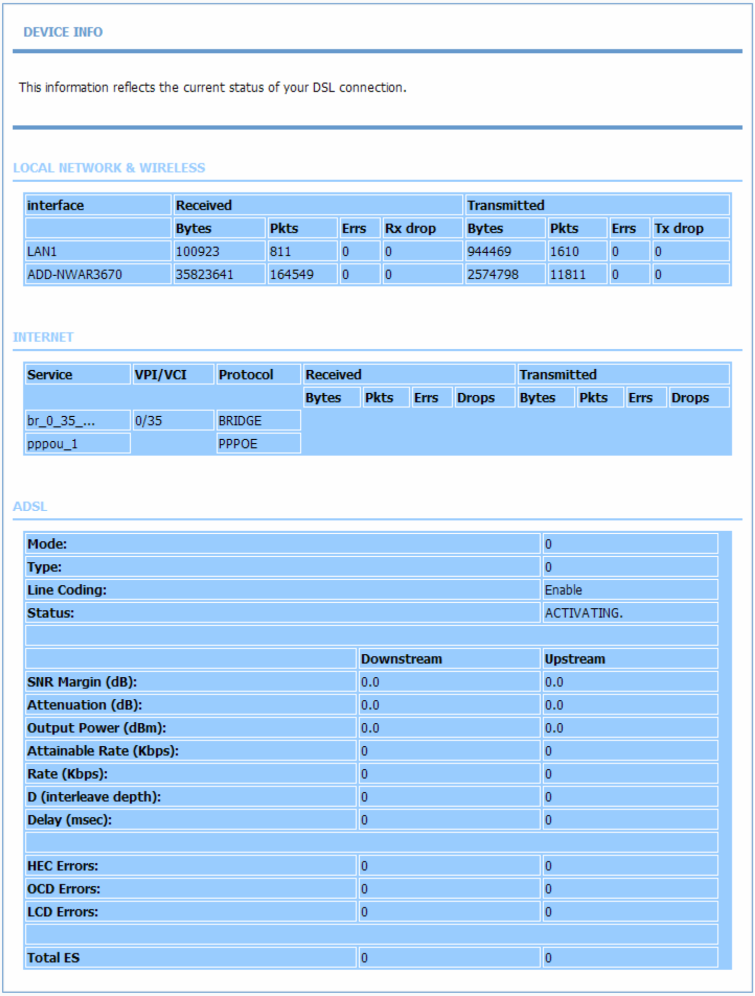
This page allows you to view system logs.

```
Manufacturer: ADDON
ProductClass: ADDON
SerialNumber: 001ee38f551b
IP: 192.168.1.1
HWVer: 1.0.0
SWVer: TBS-R2B05
```

This page lists the system log. Click **Refresh** to refresh the system log shown in the table.

3.5.5 Statistics

Choose **STATUS** > **Statistics**. The page shown in the following figure appears.



DEVICE INFO

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	100923	811	0	0	944469	1610	0	0
ADD-NWAR3670	35823641	164549	0	0	2574798	11811	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
br_0_35_...	0/35	BRIDGE								
pppou_1		PPPOE								

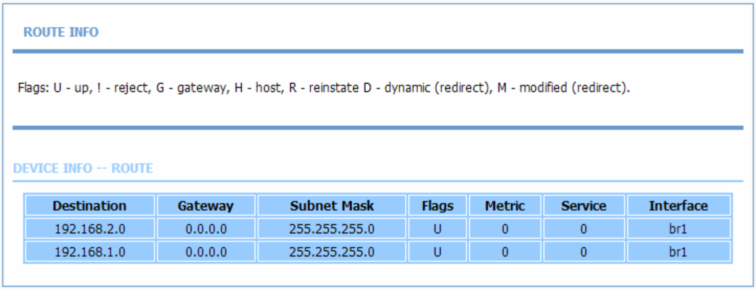
ADSL

Mode:		0
Type:		0
Line Coding:		Enable
Status:		ACTIVATING.
	Downstream	Upstream
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	0.0	0.0
Output Power (dBm):	0.0	0.0
Attainable Rate (Kbps):	0	0
Rate (Kbps):	0	0
D (interleave depth):	0	0
Delay (msec):	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total ES	0	0

This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.

3.5.6 Route Info

Choose **STATUS** > **Route Info**. The page shown in the following figure appears.



ROUTE INFO

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

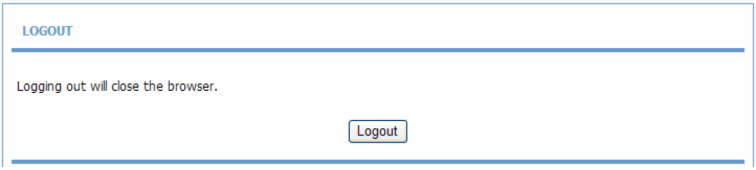
DEVICE INFO -- ROUTE

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	br1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br1

The table shows a list of destination routes commonly accessed by the network.

3.5.7 Logout

Choose **STATUS** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



LOGOUT

Logging out will close the browser.