BHS-RTA
ADVANCED USER’s MANUAL

Observa Telecom

OBJETIVOS Y SERVICIOS DE VALOR AÑADIDO S.L.

CONTENTS TABLE

1.- Introduction

The device supports multiple line modes. With 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 like net bars and office users. It provides high performance access to the Internet with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps. It supports 3G WAN, 3G backup, and Samba for USB storage.
The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security. The WLAN of the device supports 2T2R.

1.1.- Safety Precautions

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

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. 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 heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.2.- LEDs and Interfaces

Front Panel

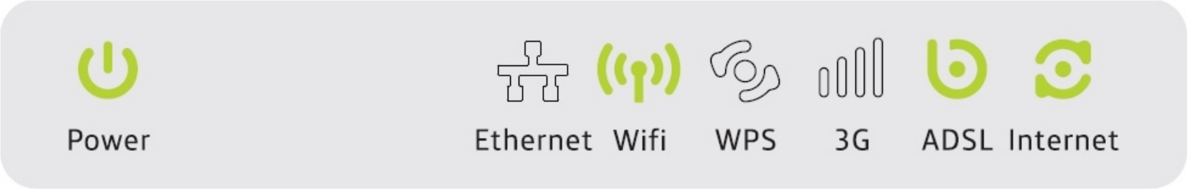


Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
Power	Red/Green	Off	Router powered off
		Blinking Green	Router on Self Testing startup
		Blinking 2Hz/Solid Red	Failure on power-on self-test
		Solid Green	Router powered on correctly.
Ethernet	Green	On	Ethernet connection is available.
		Blinking ON	There's one or more Ethernet connections with traffic
		Off	Ethernet connection is unavailable.
Wifi	Green	On	Wi-Fi connection is available.
		Off	Wi-Fi connection is unavailable.
		Blinking Green	Negotiation or traffic on line.

LED	Color	Status	Description
WPS	Red/Green	Solid Green	WPS active
		Blinking 2Hz Green	WPS negotiation open
		Solid Red (20 seconds)	Problems on WPS registration
3G	Red/Green	Blinking Green	Negotiation
		Solid Green	Up
		Quick Blinking Green	Tx/Rx traffic on line
		Solid Red	Authentication failed
		Off	Traffic through broadband interface
ADSL	Green	Off	Router powered off
		Blinking 2Hz	No line detected
		Blinking 4Hz	Line training
		Solid	Line up
Internet	Red/Green	Blinking Green	PPP/DHCP negotiation
		Solid Green	PPP/DHCP up
		Quick Blinking Green	Tx/Rx traffice on line
		Solid Red	Authentication failed

Rear Panel

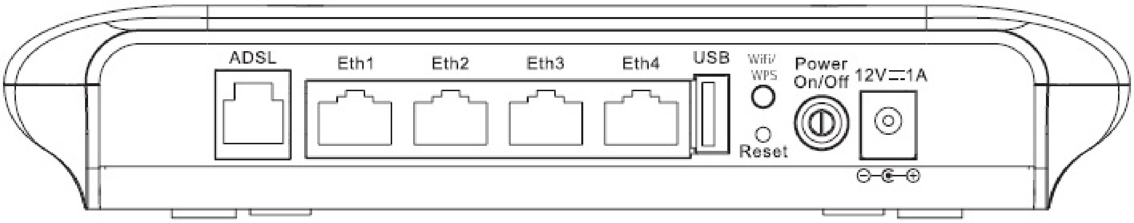


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
ADSL	RJ-11 interface connecting to a telephone set through a telephone cable
Eth1/2/3/4	Ethernet RJ-45 interfaces connecting to the Ethernet interfaces of computers or Ethernet devices
USB	Connecting to a 3G data card or other USB storage device
WLAN/WPS	● Press the button for less than 1 second to enable WLAN function. ● Press the button for more than 10 seconds to enable WPS function.
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for more than 5 seconds and then release.
Power On/Off	Push to power on/off the device.
12V⎓1A	Interface connecting to the power adapter. The power adapter output is: 12V DC, 800mA

1.3.- System Requirements

- A 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 Vista, Windows 7, 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

1.4.- 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
- Samba
- 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

2.- Hardware Installation

Step 1 Connect the **ADSL** 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: Connect to a telephone set.

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

Note:
Use twisted-pair cables to connect the device to a Hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and 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.

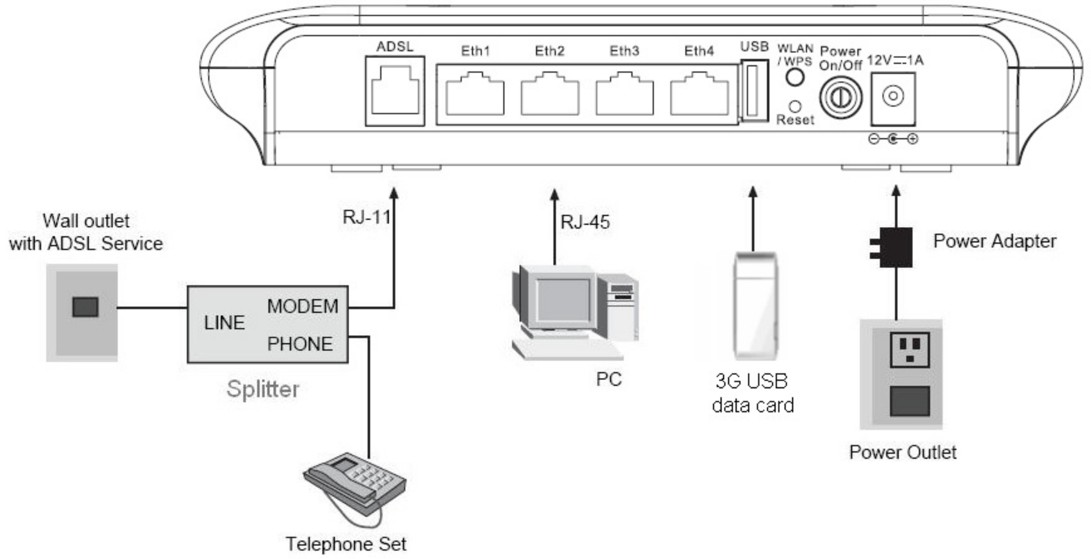


Figure 3 Connection diagram (without telephone sets before the splitter)

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.

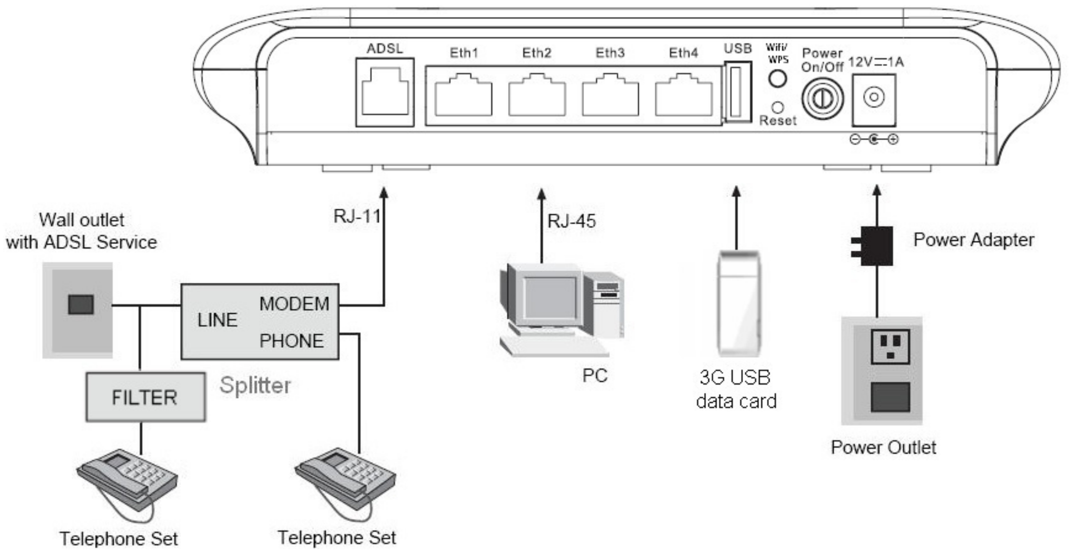


Figure 4 Connection diagram (with a telephone set before the splitter)

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.

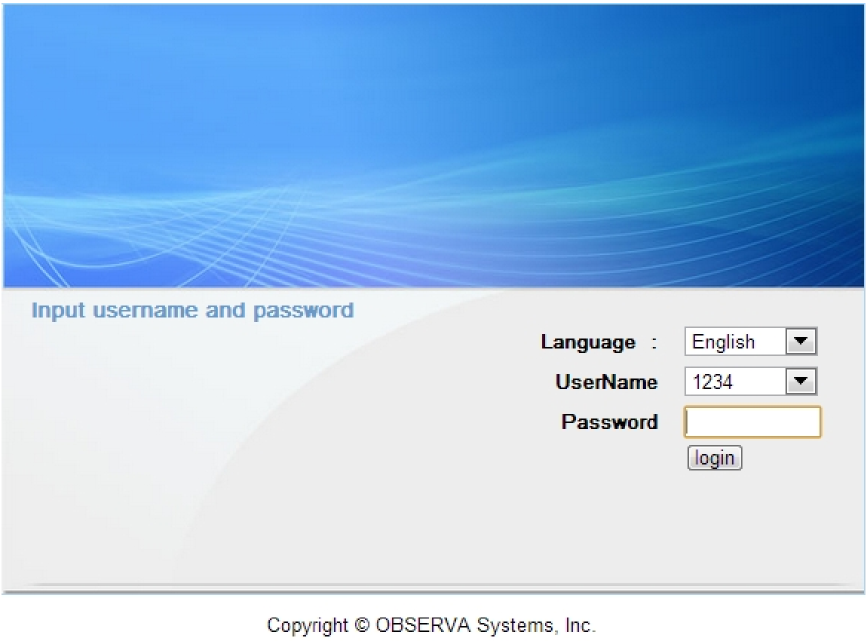
3.- Web Configuration

3.1.- Accesing the Device

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

Open the Internet Explorer (IE) browser and enter **http://192.168.1.1:8000**.

The **Login page** is shown as below. Choose the username **1234**, input the password **1234** and click **login**.



Input username and password

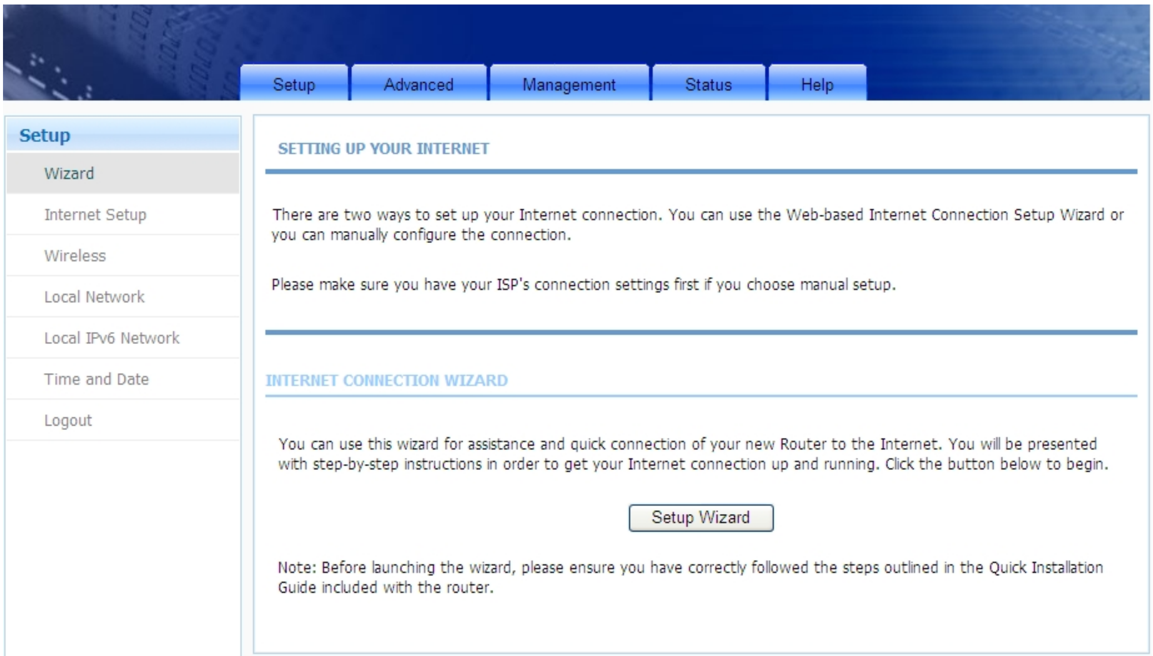
Language : English

UserName 1234

Password

Copyright © OBSERVA Systems, Inc.

If you log in 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

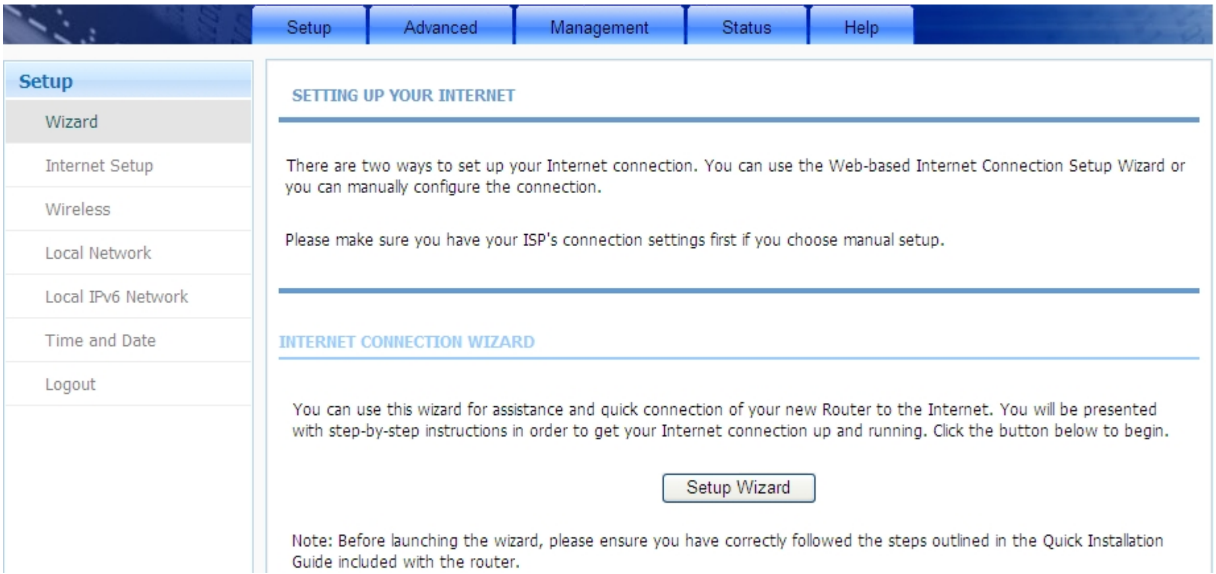
In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Internet Setup**, **Wireless**, **Local Network**, **Time and Date** and **Logout**.

3.2.1 Wizard

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

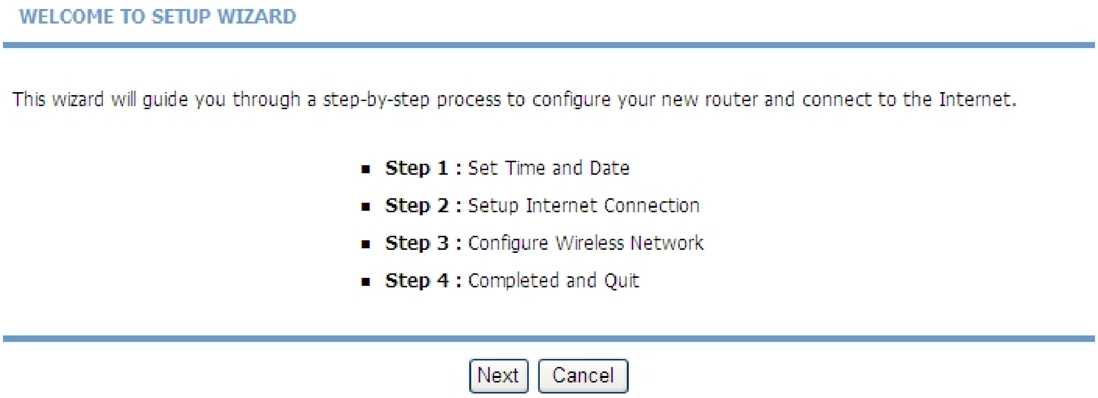
Please make sure you have your ISP's connection settings first if you choose manual setup.

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.



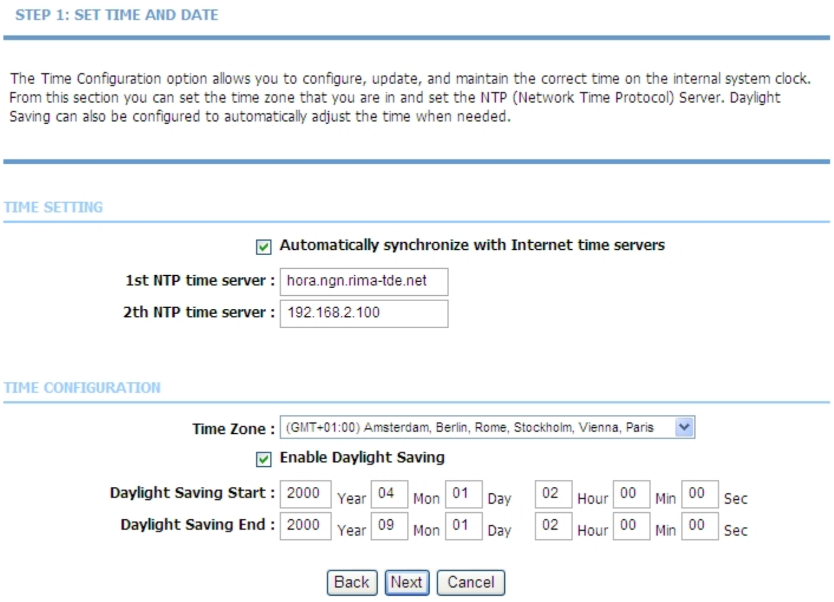
WELCOME TO SETUP WIZARD

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 : hora.ngn.rima-tde.net

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Time Zone : (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris

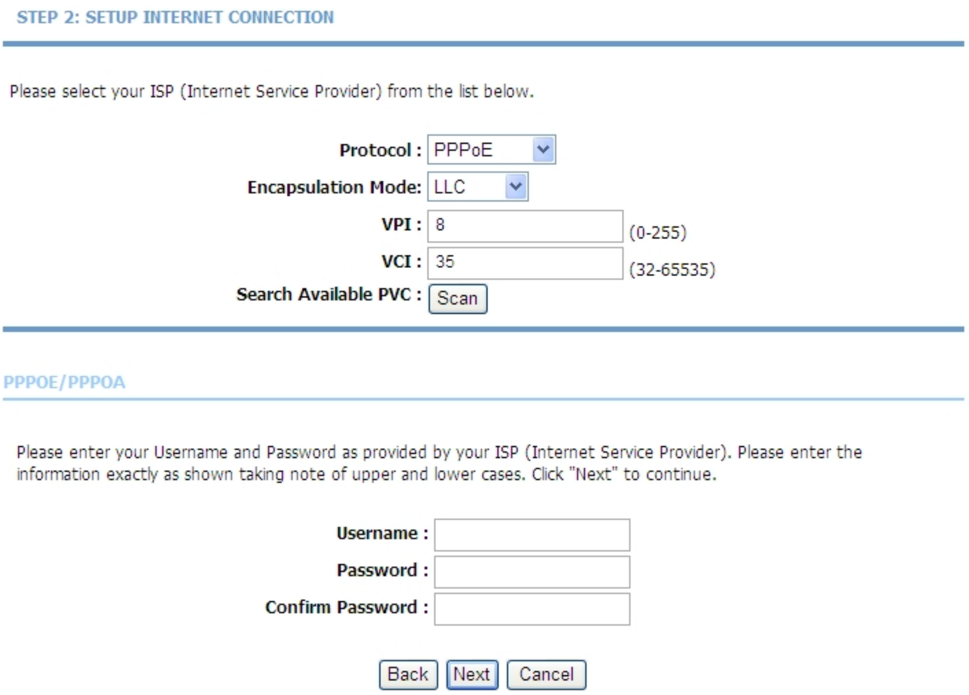
☑ Enable Daylight Saving

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

Set the VPI and VCI. If the **Protocol** is **PPPoE** or **PPPoA,** the page shown in the two following figure appears.



STEP 2: SETUP INTERNET CONNECTION

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

Protocol : PPPoE

Encapsulation Mode: LLC

VPI : 8 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Scan

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.

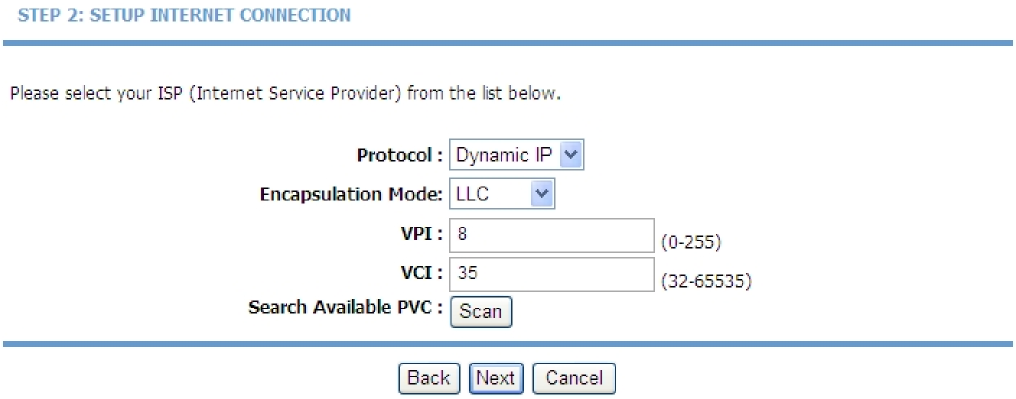
Username :

Password :

Confirm Password :

In this page, enter the user name and password as provided by your ISP.

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

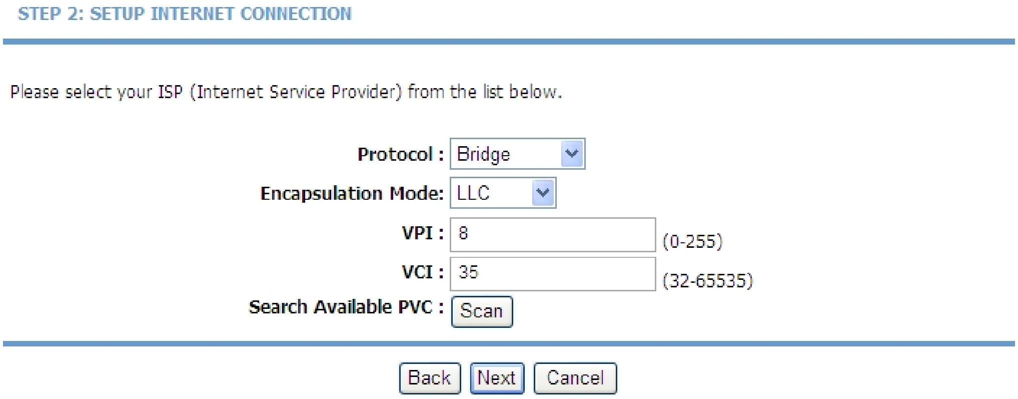


STEP 2: SETUP INTERNET CONNECTION

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

Protocol : Dynamic IP
Encapsulation Mode: LLC
VPI : 8 (0-255)
VCI : 35 (32-65535)
Search Available PVC :

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

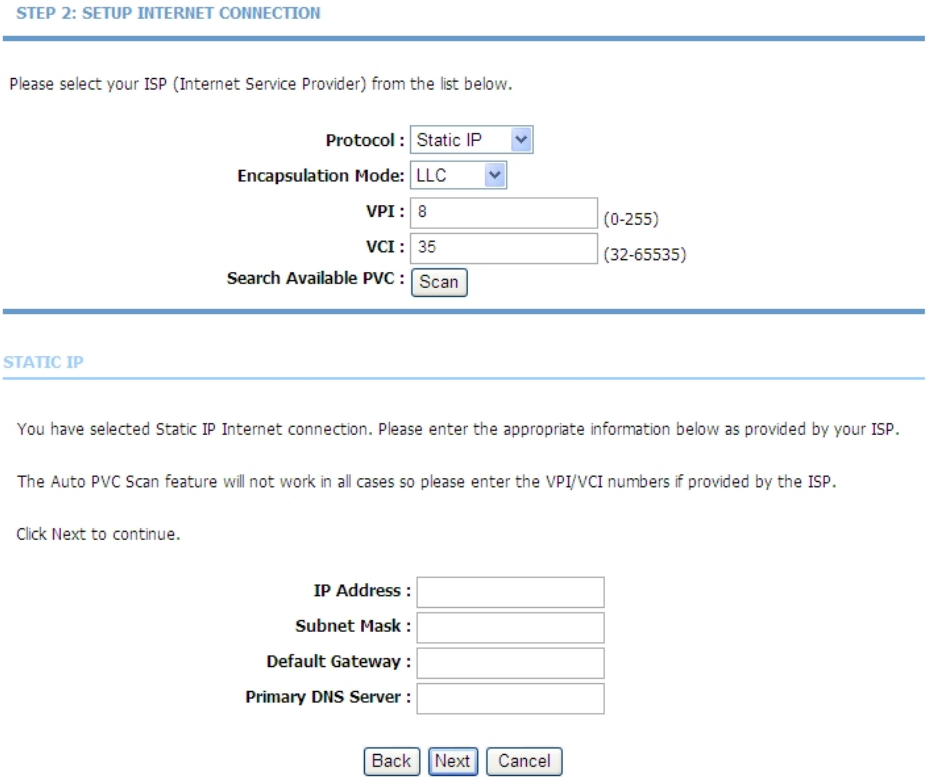


STEP 2: SETUP INTERNET CONNECTION

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

Protocol : Bridge
Encapsulation Mode: LLC
VPI : 8 (0-255)
VCI : 35 (32-65535)
Search Available PVC :

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: LLC
VPI : 8 (0-255)
VCI : 35 (32-65535)
Search Available PVC :

STATIC IP

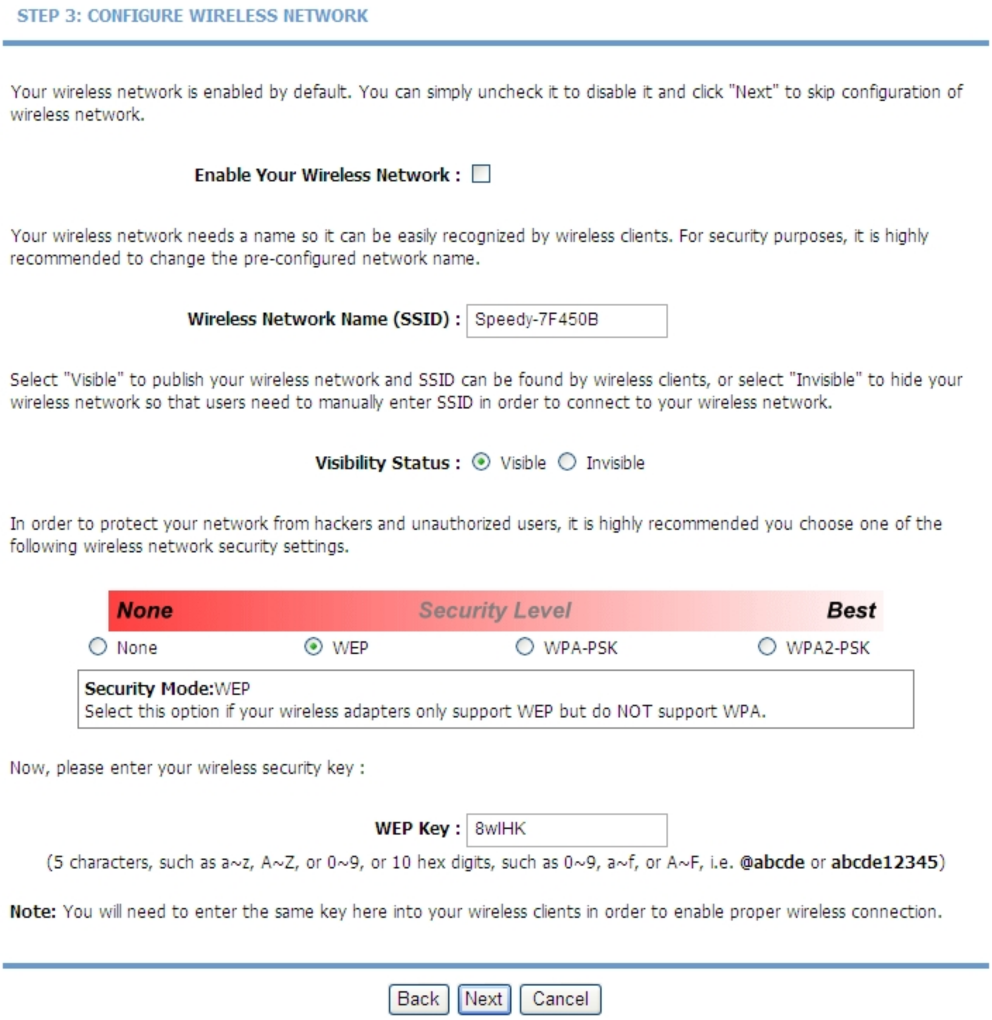
You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

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 figure 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) : Speedy-7F450B

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:WEP
Select this option if your wireless adapters only support WEP but do NOT support WPA.

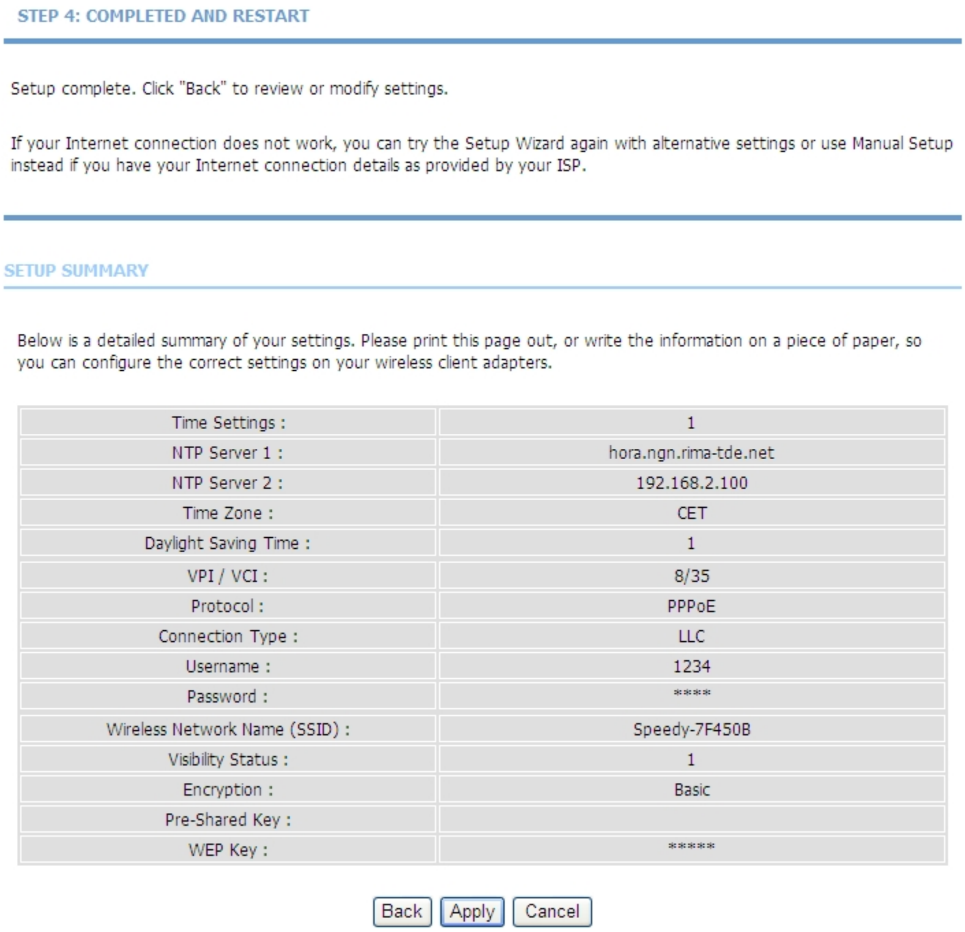
Now, please enter your wireless security key :

WEP Key : 8wIHK

(5 characters, such as a~z, A~Z, or 0~9, or 10 hex digits, such as 0~9, a~f, or A~F, i.e. **@abcde** or **abcde12345**)

Note: You will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

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.

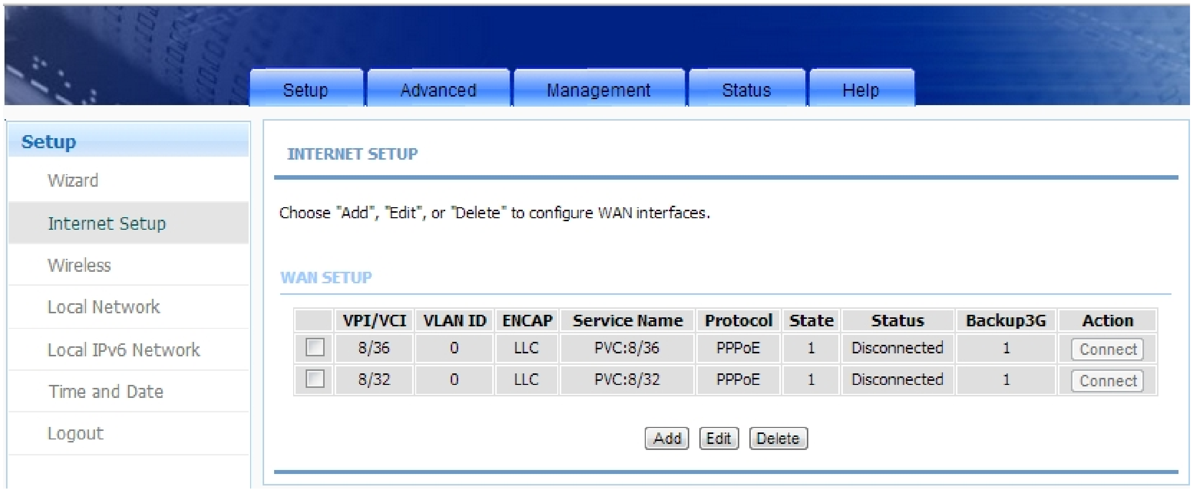
Time Settings :	1
NTP Server 1 :	hora.ngn.rima-tde.net
NTP Server 2 :	192.168.2.100
Time Zone :	CET
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
Username :	1234
Password :	****
Wireless Network Name (SSID) :	Speedy-7F450B
Visibility Status :	1
Encryption :	Basic
Pre-Shared Key :	
WEP Key :	*****

Step 7 Click **Apply** to save the settings.

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

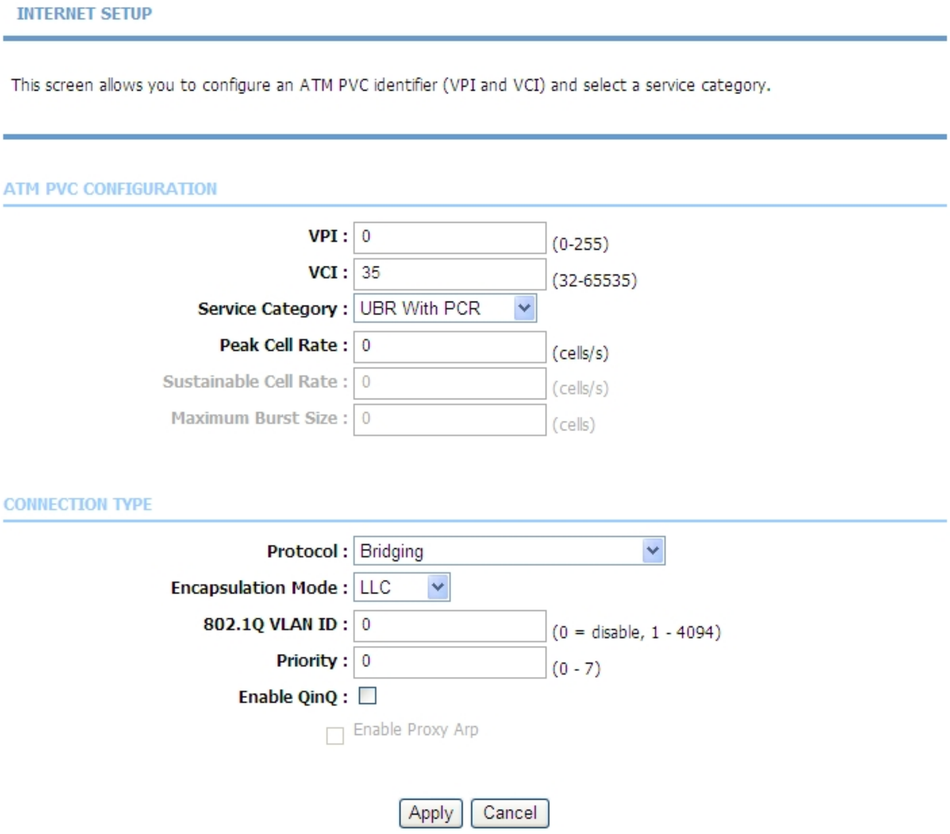
Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action
□	8/36	0	LLC	PVC:8/36	PPPoE	1	Disconnected	1	Connect
□	8/32	0	LLC	PVC:8/32	PPPoE	1	Disconnected	1	Connect

Figure 5

Click **Add** in **"INTERNET 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

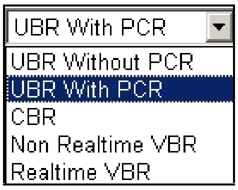
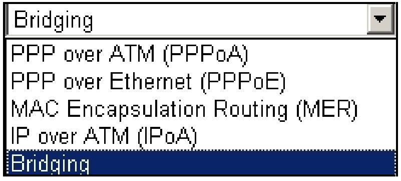
VPI :	0	(0-255)
VCI :	35	(32-65535)
Service Category :	UBR With PCR	
Peak Cell Rate :	0	(cells/s)
Sustainable Cell Rate :	0	(cells/s)
Maximum Burst Size :	0	(cells)

CONNECTION TYPE

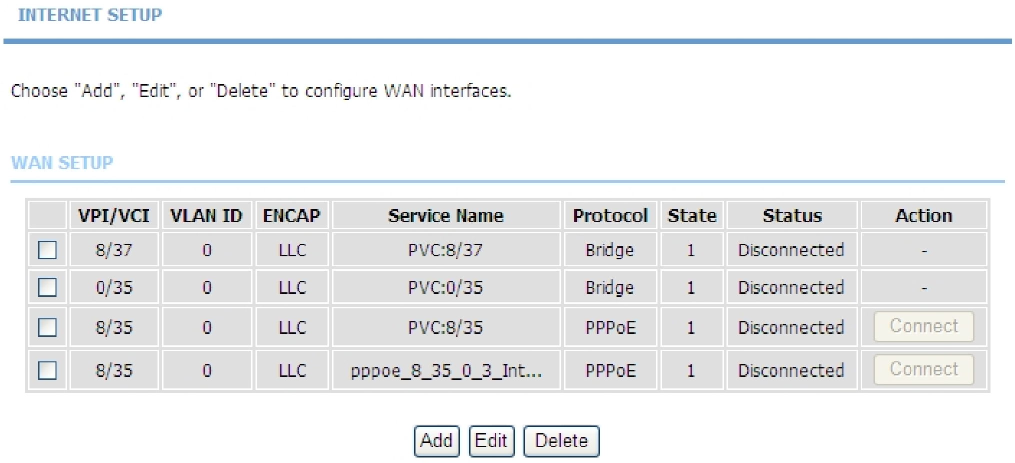
Protocol :	Bridging	
Encapsulation Mode :	LLC	
802.1Q VLAN ID :	0	(0 = disable, 1 - 4094)
Priority :	0	(0 - 7)
Enable QinQ :	□	

□ Enable Proxy Arp

The following table describes the parameters in this page.

Field	Description
PVC Settings	**VPI**: The virtual path between two points in an ATM network, and its valid value is from **0** to **255**. **VCI**: 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.  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

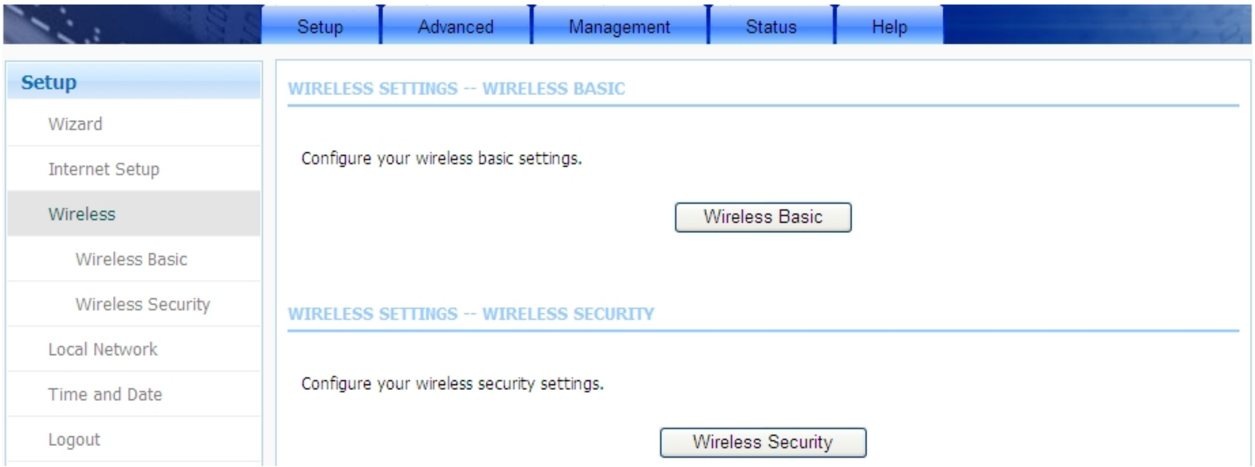
	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Action
□	8/37	0	LLC	PVC:8/37	Bridge	1	Disconnected	-
□	0/35	0	LLC	PVC:0/35	Bridge	1	Disconnected	-
□	8/35	0	LLC	PVC:8/35	PPPoE	1	Disconnected	Connect
□	8/35	0	LLC	pppoe_8_35_0_3_Int...	PPPoE	1	Disconnected	Connect

Figure 6

3.2.3 Wireless

This section describes the wireless LAN and basic configuration. A wireless LAN 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

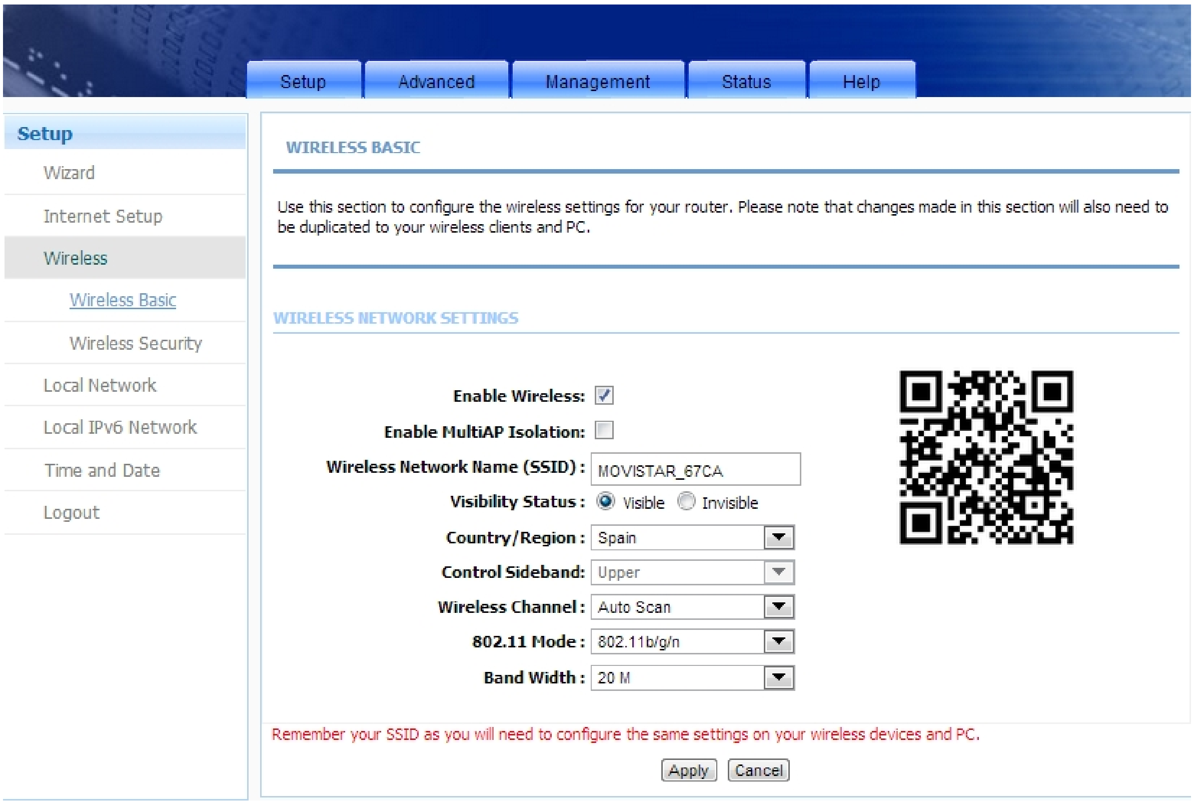
Configure your wireless basic settings.

WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

3.2.3.1 Wireless Basic

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) : MOVISTAR_67CA

Visibility Status : ● Visible ○ Invisible

Country/Region : Spain

Control Sideband: Upper

Wireless Channel : Auto Scan

802.11 Mode : 802.11b/g/n

Band Width : 20 M

Remember your SSID as you will need to configure the same settings on your wireless devices and PC.

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on or 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.
Control Sideband	Choose the channel selection mode as **Upper** or **Lower**.
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**, **802.11g**, **802.11n**, **802.11b/g**, **802.11n/g** and **802.11b/g/n**.
Band Width	Select the appropriate band of **20M**, **40M** or **20M/40M** from the pull-down menu.

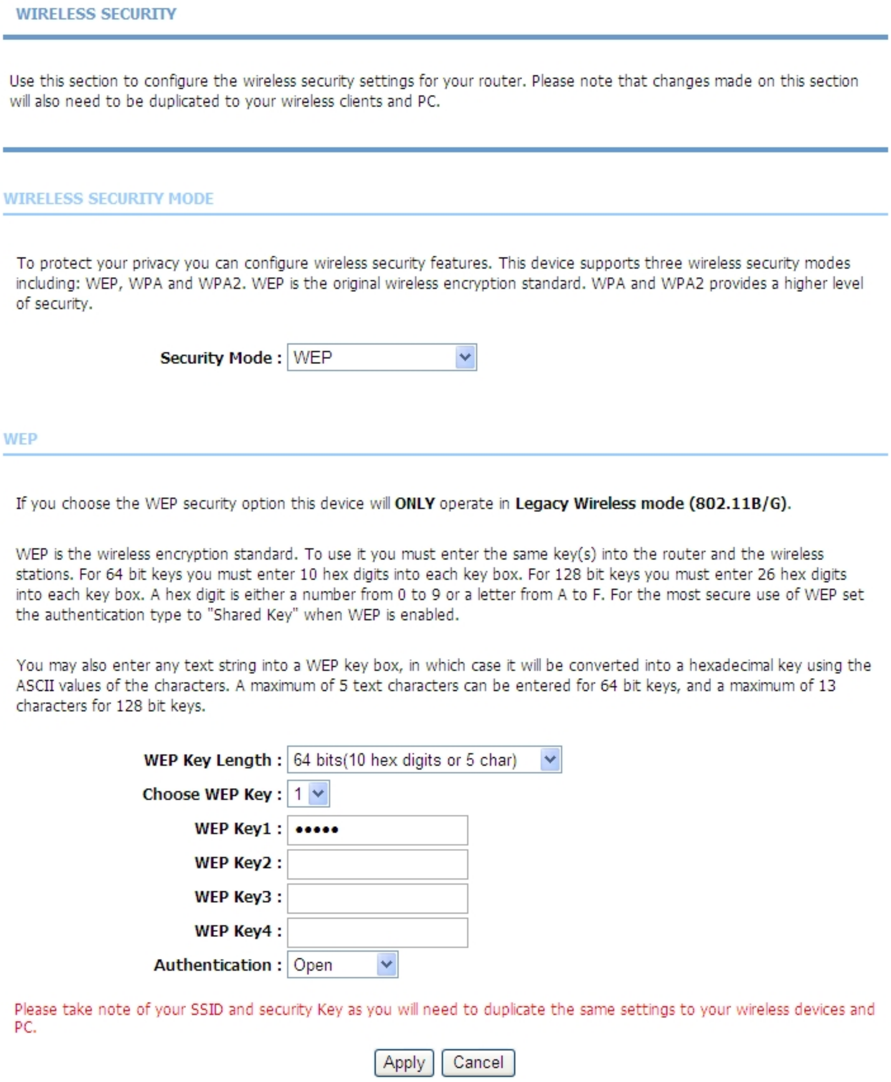
Click **Apply** to save the settings.

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.

Note:
Enable Wireless before configuring the wireless security settings in this page. Refer to 3.2.3.1 Wireless Basic.

When the Security Mode is set as **WEP**, 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 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 : WEP

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

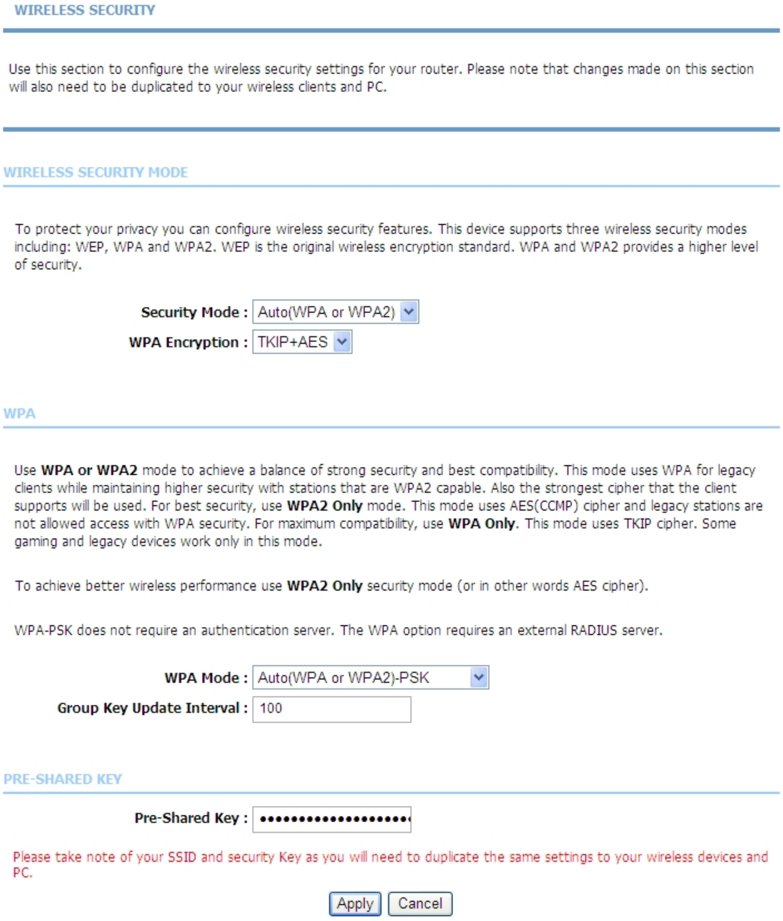
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

The following table describes the parameters of this page.

Field	Description
WEP Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Choose WEP Key	Choose the index of WEP Key. You can choose **Key 1**, **2**, **3** or **4**.
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is **8wlHK**.

Click **Apply** to save the settings.

When the Security Mode is set as **Auto (WPA or WPA2)**, **WPA2 only** or **WPA only**, 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 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 : Auto(WPA or WPA2)

WPA Encryption : TKIP+AES

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.

Figure 7

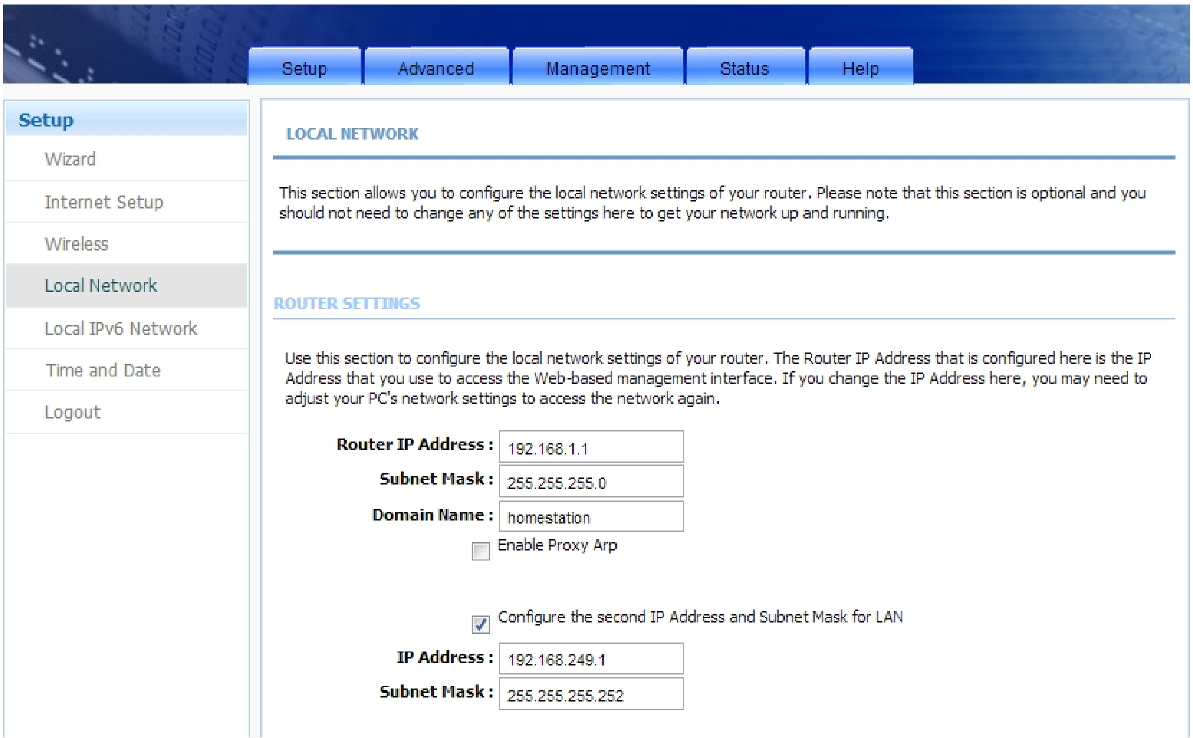
The following table describes the parameters in this page.

Field	Description
Security Mode	Configure the wireless encryption mode. You can choose **None**, **WEP**, **Auto(WPA or WPA2)**, **WPA 2 Only** or **WPA Only**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA Encryption	When WPA or WPA2 is selected, you can select WPA encryption as **AES** or **TKIP+AES**.
WPA Mode	● Select **PSK (Pre-Shared Key)**, enter the pre-shared key in the **Pre-Shared Key** field. ● Select **Enterprise (RADIUS)**, enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem. If the encrypton is set to **WEP**, the modem uses 802.1 X authentication, which is Radius authentication.

Field	Description
Group Key Update Interval	When WPA encryption is applied, messages sent are encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.

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

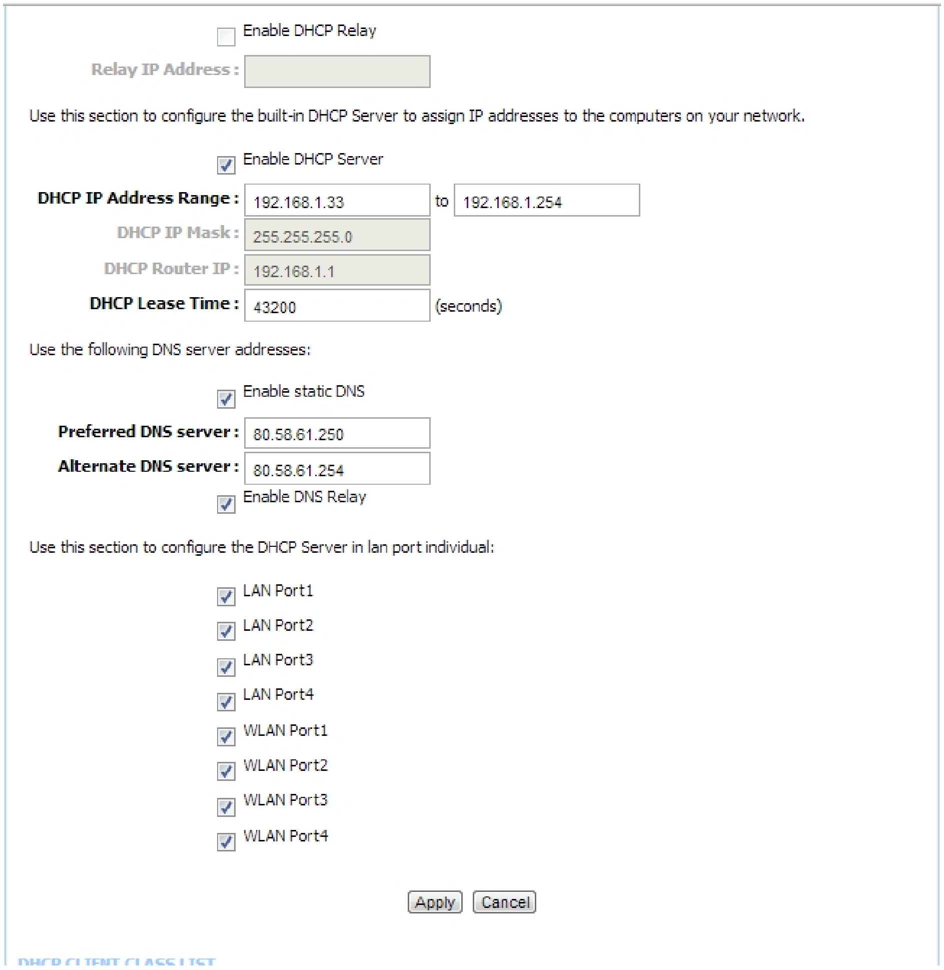
Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network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

Router IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Domain Name : homestation
☐ Enable Proxy Arp

☑ Configure the second IP Address and Subnet Mask for LAN
IP Address : 192.168.249.1
Subnet Mask : 255.255.255.252

Figure 8

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.



□ Enable DHCP Relay

Relay IP Address :

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 : 192.168.1.33 to 192.168.1.254

DHCP IP Mask : 255.255.255.0

DHCP Router IP : 192.168.1.1

DHCP Lease Time : 43200 (seconds)

Use the following DNS server addresses:

☑ Enable static DNS

Preferred DNS server : 80.58.61.250

Alternate DNS server : 80.58.61.254

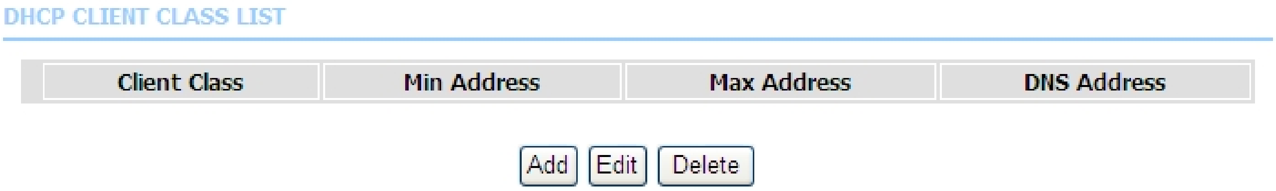
☑ Enable DNS Relay

Use this section to configure the DHCP Server in lan port individual:

☑ LAN Port1
☑ LAN Port2
☑ LAN Port3
☑ LAN Port4
☑ WLAN Port1
☑ WLAN Port2
☑ WLAN Port3
☑ WLAN Port4

Figure 9

Click **Apply** to save the settings.
The **DHCP Client Class List** section shown in the following figure appears.

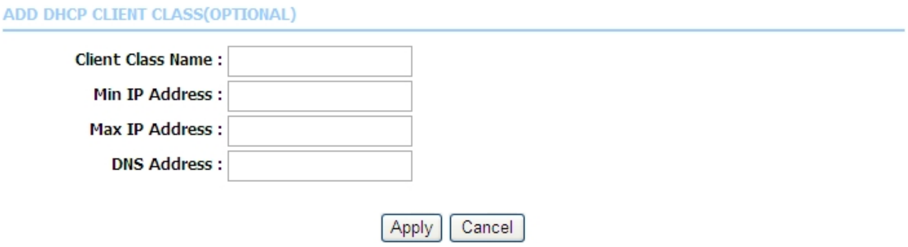


DHCP CLIENT CLASS LIST

Client Class	Min Address	Max Address	DNS Address

Figure 10

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



ADD DHCP CLIENT CLASS(OPTIONAL)

Client Class Name :

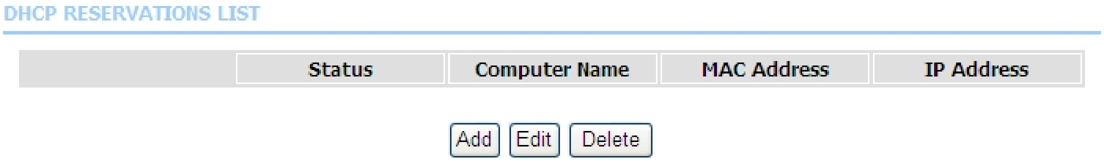
Min IP Address :

Max IP Address :

DNS Address :

Figure 11

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

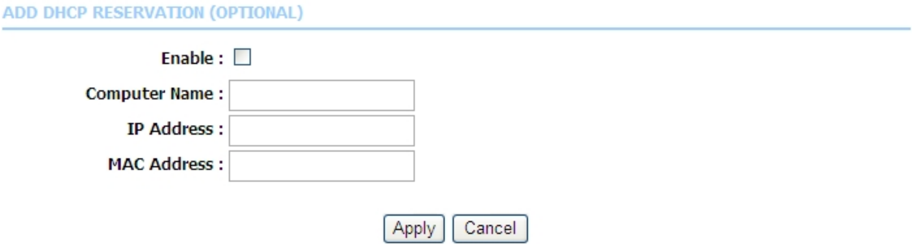


DHCP RESERVATIONS LIST

	Status	Computer Name	MAC Address	IP Address

Figure 12

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



ADD DHCP RESERVATION (OPTIONAL)

Enable : □

Computer Name :

IP Address :

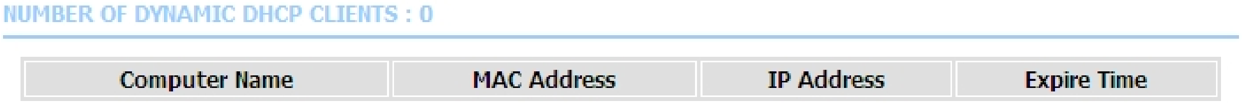
MAC Address :

Figure 13

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.

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).



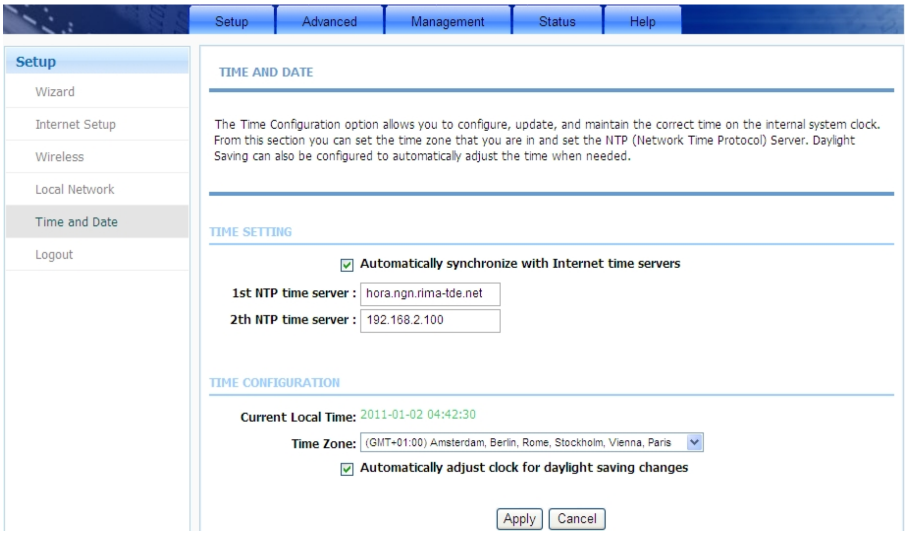
NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time

Figure 14

3.2.5 Time 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 : hora.ngn.rima-tde.net

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Current Local Time: 2011-01-02 04:42:30

Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris

☑ Automatically adjust clock for daylight saving changes

Figure 15

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**.

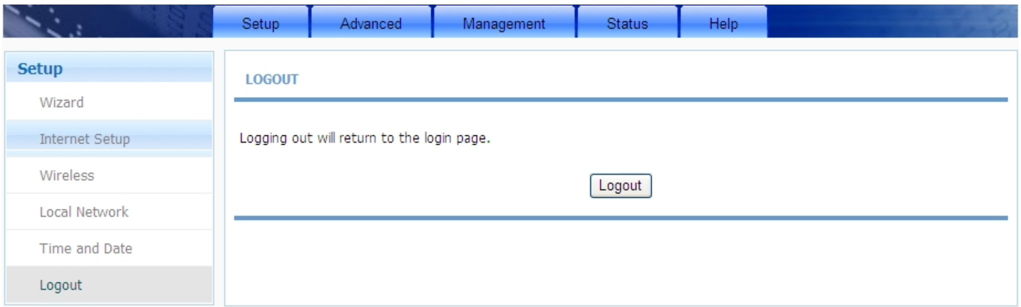
Select the specific time server and the time zone from the corresponding drop-down lists.

Select **Automatically adjust clock for daylight saving changes** 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.



Logging out will return to the login page.

Figure 16

3.3.- Advanced

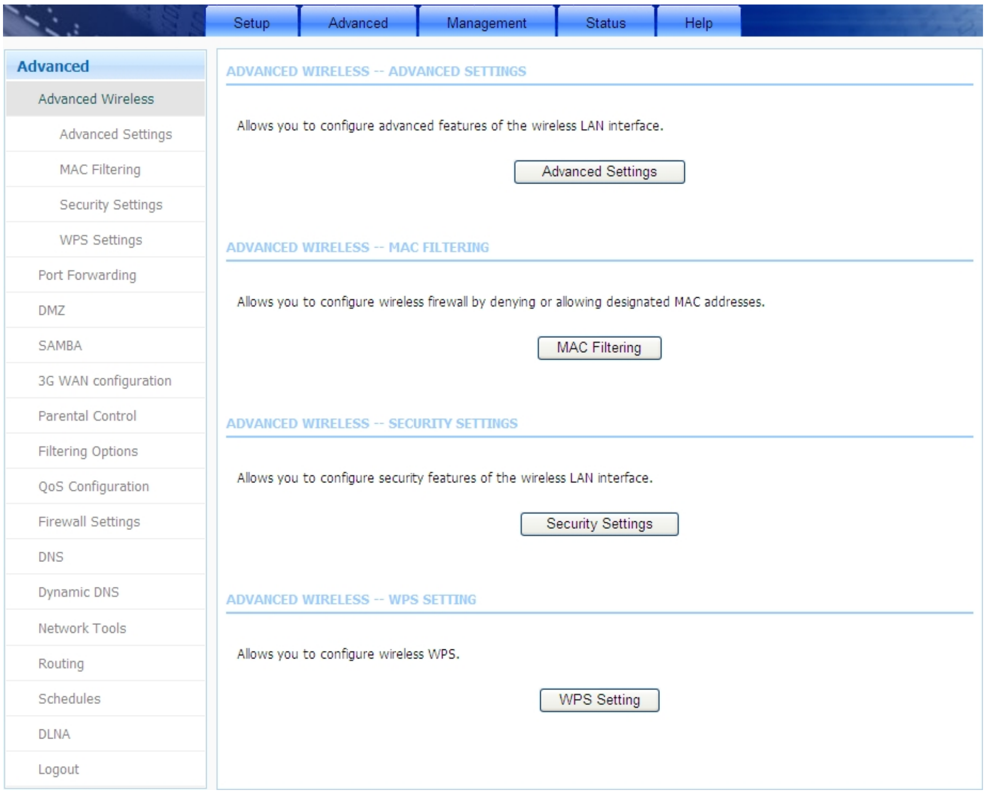
This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and troubleshoot.

In the main interface, click **Advanced** tab to enter the **Advanced** menu as shown in the following figure. The submenus are **Advanced Wireless**, **Port Fowarding**, **DMZ**, **SAMBA**, **3G Configuration**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Firewall Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, **Schedules**, **DLNA** and **Logout**.

3.3.1 Advanced Wireless

This function is used to modify the standard 802.11g wireless radio settings. It is suggested not to change the defaults, as incorrect settings may reduce 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.

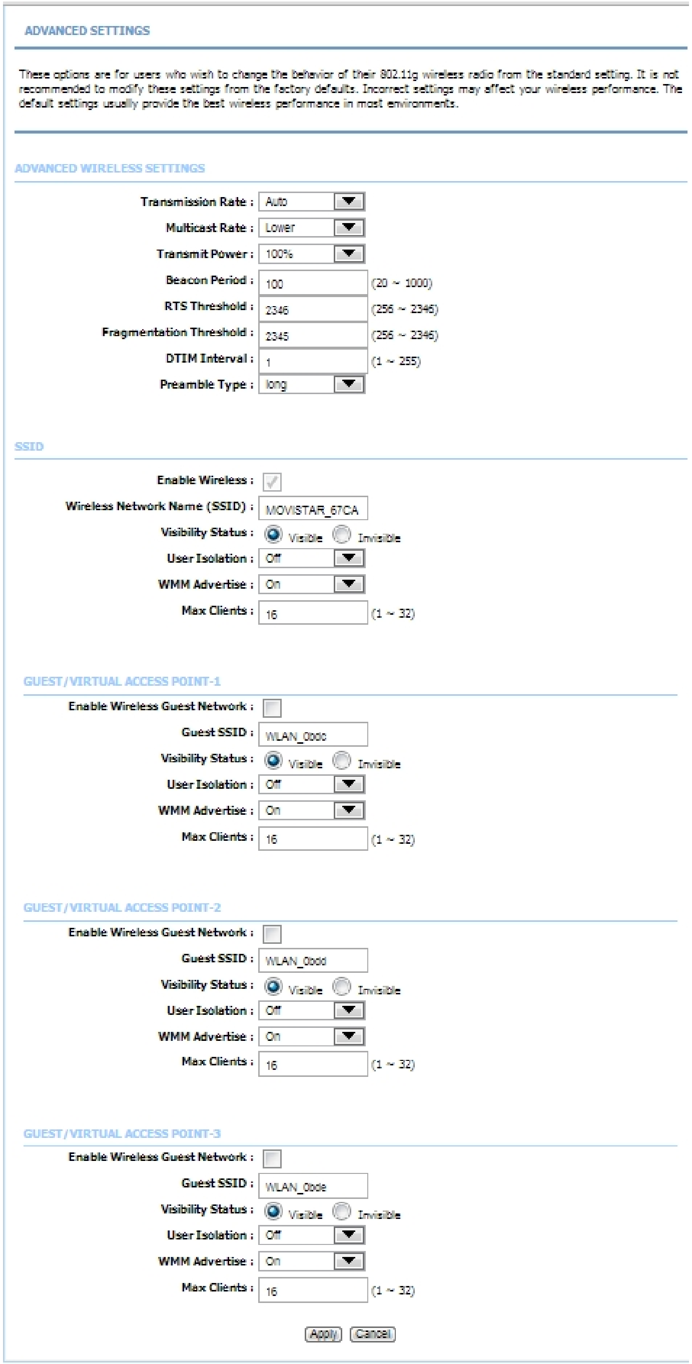
ADVANCED WIRELESS -- WPS SETTING

Allows you to configure wireless WPS.

Figure 17

3.3.1.1 Advanced Settings

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



ADVANCED SETTINGS

These options are for users who wish to change the behavior of their 802.11g wireless radio from the standard setting. It is not recommended to modify these settings from the factory defaults. Incorrect settings may affect your wireless performance. The default settings usually provide the best wireless 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 : 1 (1 ~ 255)
Preamble Type : long

SSID

Enable Wireless : ☑
Wireless Network Name (SSID) : MOVISTAR_67CA
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □
Guest SSID : WLAN_0bdc
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □
Guest SSID : WLAN_0bdd
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : □
Guest SSID : WLAN_0bde
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)

Figure 18

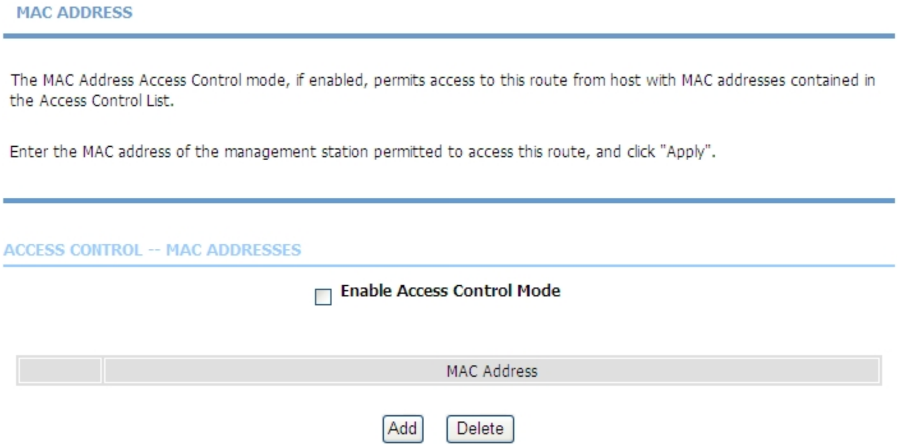
Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless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

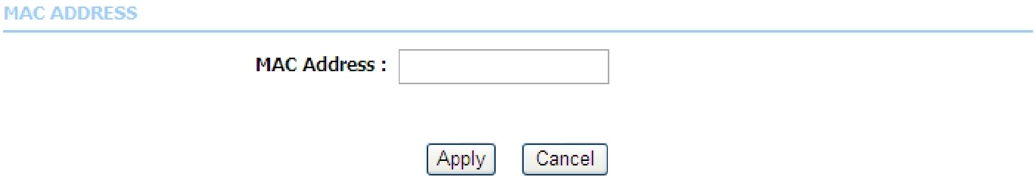
ACCESS CONTROL -- MAC ADDRESSES

□ Enable Access Control Mode

	MAC Address

Figure 19

Choose **Enable Access Control Mode**, and then click **Add** to add a MAC Address as shown in the following figure.



MAC ADDRESS

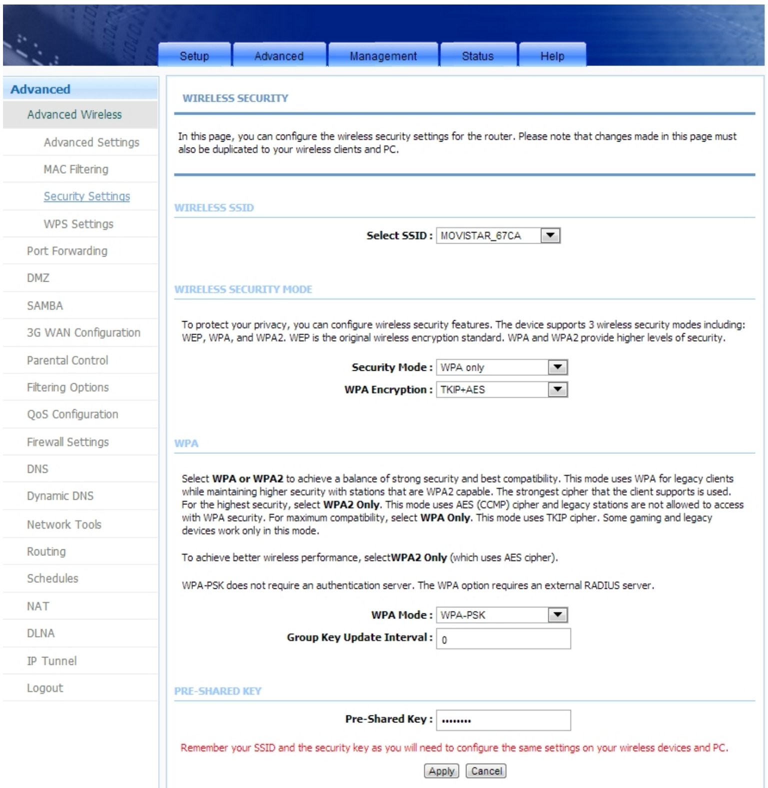
MAC Address :

Figure 20

Click Apply to finish.

3.3.1.3 Security Settings

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



WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SSID

Select SSID : MOVISTAR_67CA

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode : WPA only
WPA Encryption : TKIP+AES

WPA

Select **WPA or WPA2** 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. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select**WPA2 Only** (which uses 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 : 0

PRE-SHARED KEY

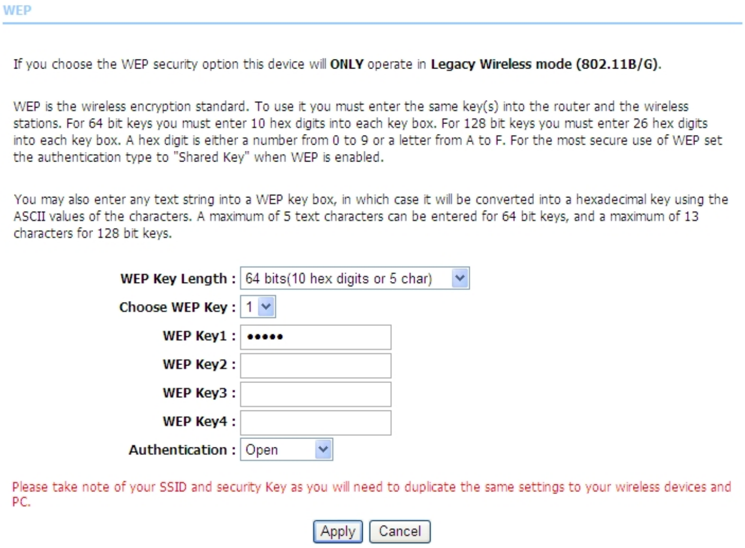
Pre-Shared Key : ••••••••

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Figure 21

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.

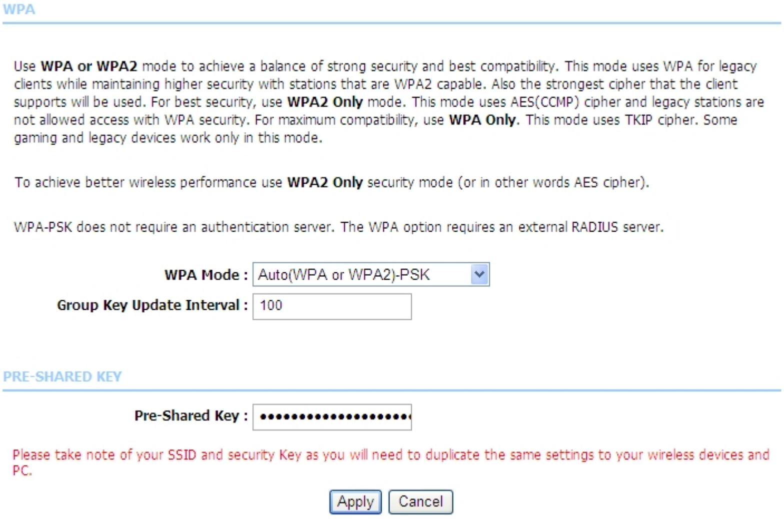
You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

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.

Figure 22

If you select **AUTO (WPA or WPA2)**, **WPA Only** or **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 : Auto(WPA or WPA2)-PSK
Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : •••••••••••••••••••

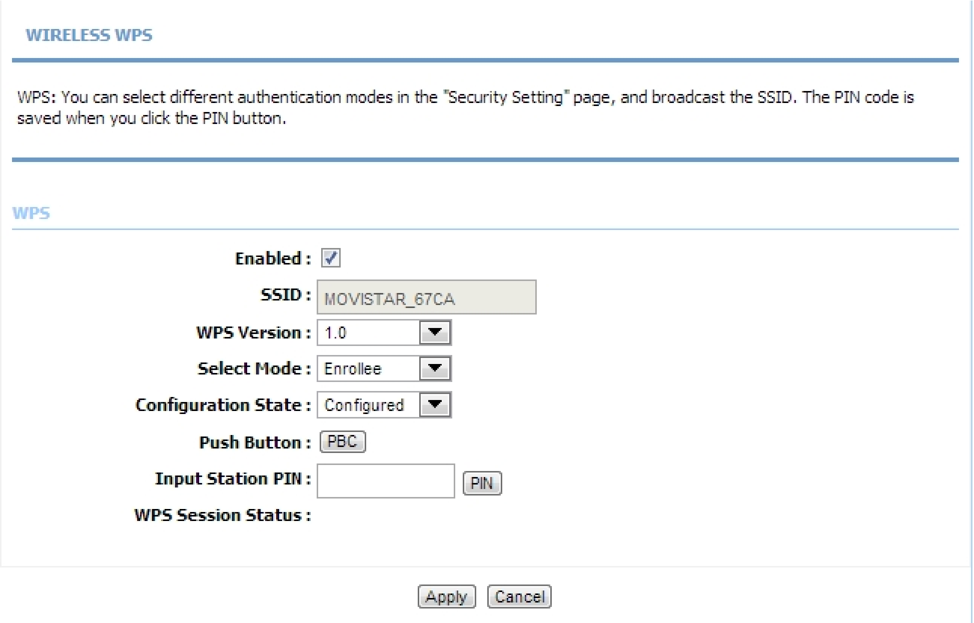
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Figure 23

Click **Apply** to save the settings. For detailed configuration, you may refer to 3.2.3.2 Wireless Security.

3.3.1.4 WPS Settings

Select **WPS Settings**.This page is used to config WPS settings.



WIRELESS WPS

WPS: You can select different authentication modes in the "Security Setting" page, and broadcast the SSID. The PIN code is saved when you click the PIN button.

WPS

Enabled : ☑
SSID : MOVISTAR_67CA
WPS Version : 1.0
Select Mode : Enrollee
Configuration State : Configured
Push Button : PBC
Input Station PIN :
WPS Session Status :

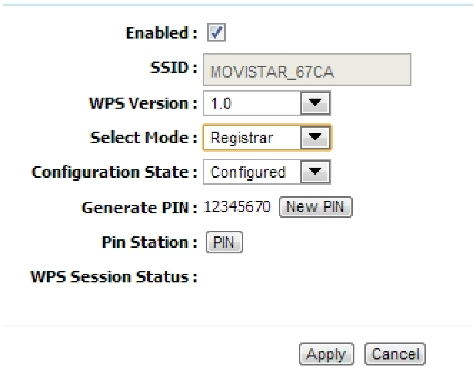
Figure 24

The following table describes the parameters of this page.

Field	Description
Enabled	Choose to enable WPS function to set the following parameters.
Select SSID	Select one SSID of the CPE.
Select Mode	Select the mode either **Registar** or **Enrollee**. When an AP or a station used Registar mode, the other should use Enrollee mode.
Configuration State	When **Configured** state is selected, wireless parameters (for

Field	Description
	example, the encryption password) are provided by the CPE in WPS negotiation. When **Unconfigured** state is selected, wireless parameters are provided by the connecting user end (for example, PC).
Push Button	Press the button, the CPE will connect the station automaticlly.
Input Station PIN	You need to enter a pin the station which mode is Enrollee Generate. Press the button to connect the other with the pin.

When **Registrar** mode is chosen, the following figure appears. In this condition, only PIN button can be used.



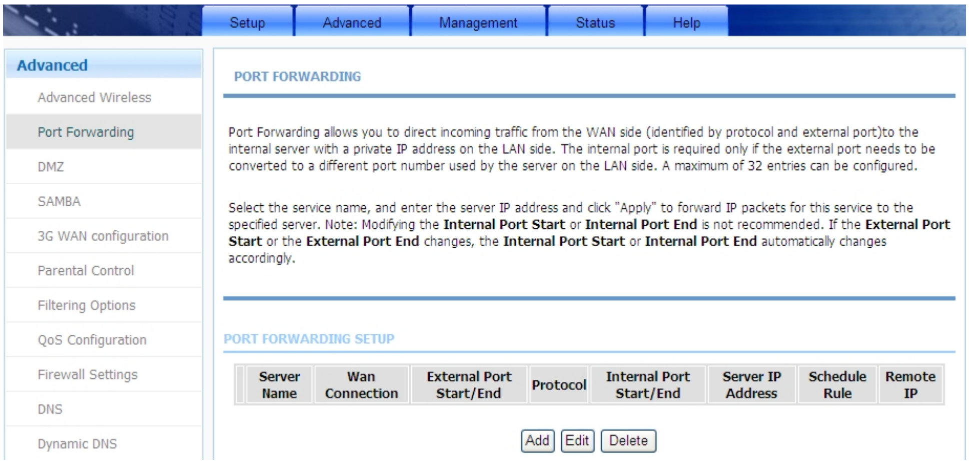
Enabled : ☑
SSID : MOVISTAR_67CA
WPS Version : 1.0
Select Mode : Registrar
Configuration State : Configured
Generate PIN : 12345670
Pin Station :
WPS Session Status :

The following table describes the parameters of this page.

Field	Description
Generate PIN	Press the button to generate a pin used by the AP and the station.
PIN Station	Press the button to connect the station with the pin.
WPS Session Status	Display the session status.

3.3.2 Port 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.

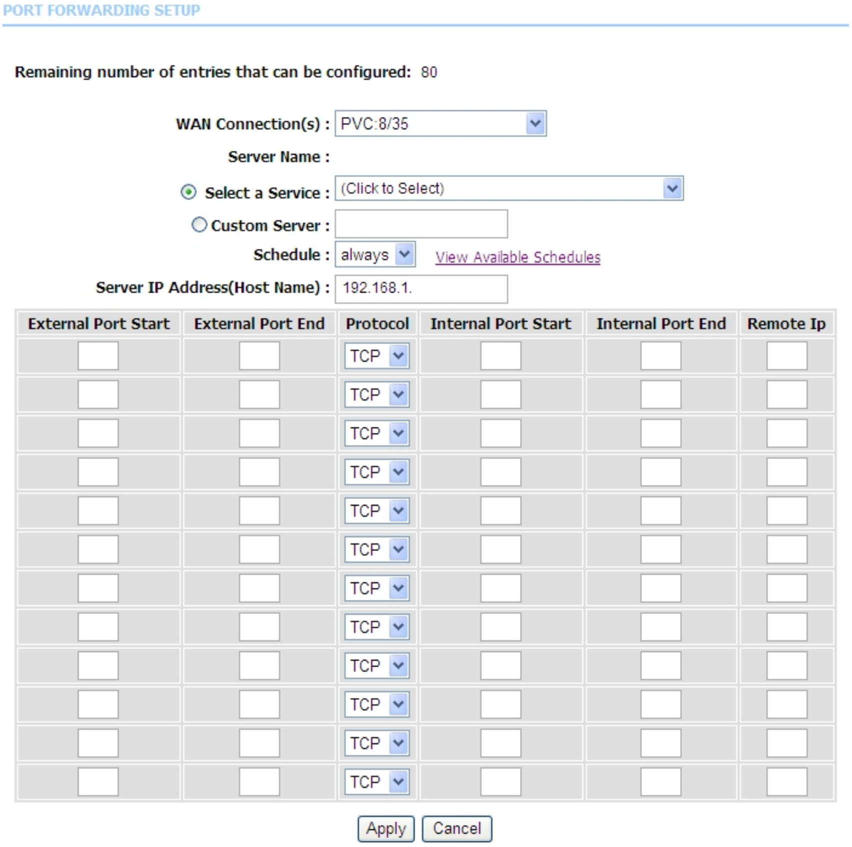
Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the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

Figure 25

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


PORT FORWARDING SETUP

Remaining number of entries that can be configured: 80

WAN Connection(s) : PVC:8/35

Server Name :

● Select a Service : (Click to Select)

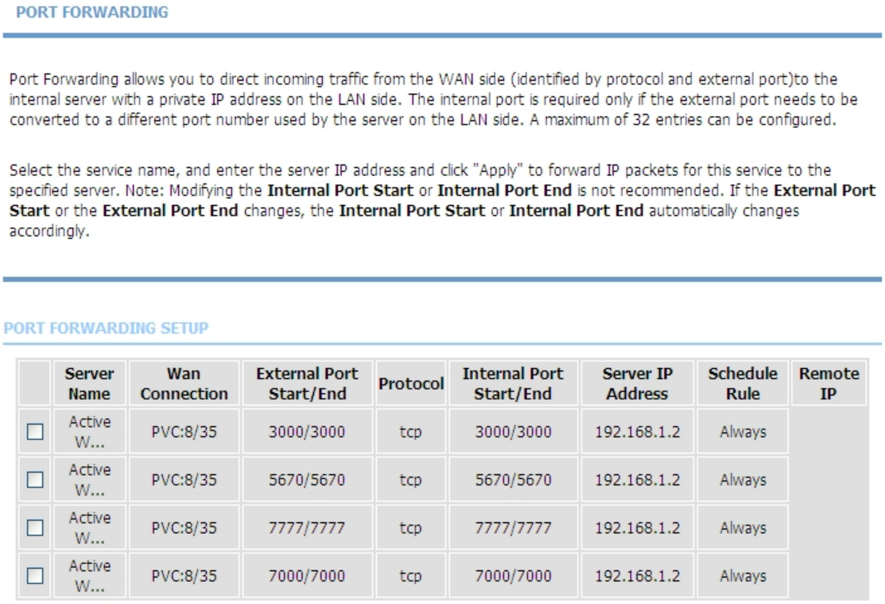
○ Custom Server :

Schedule : always View Available Schedules

Server IP Address(Host Name) : 192.168.1.

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

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.

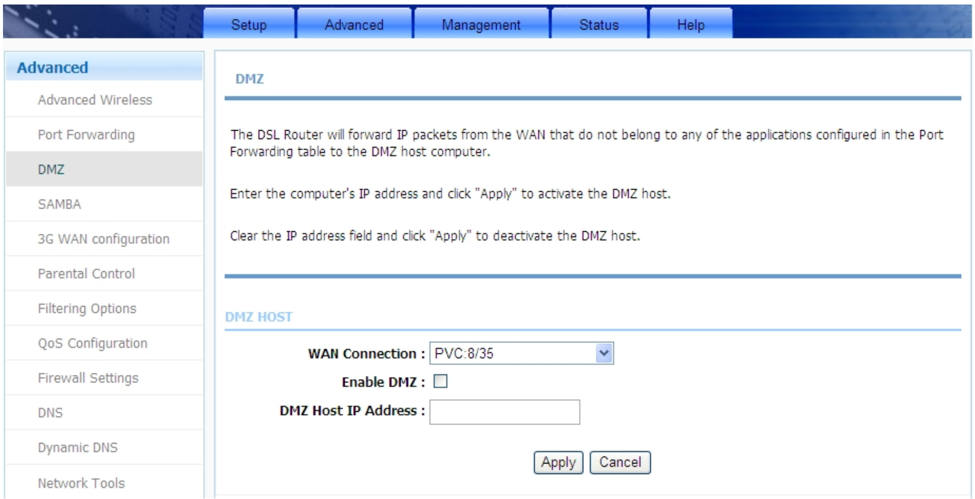
PORT FORWARDING SETUP

	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
□	Active W...	PVC:8/35	3000/3000	tcp	3000/3000	192.168.1.2	Always	
□	Active W...	PVC:8/35	5670/5670	tcp	5670/5670	192.168.1.2	Always	
□	Active W...	PVC:8/35	7777/7777	tcp	7777/7777	192.168.1.2	Always	
□	Active W...	PVC:8/35	7000/7000	tcp	7000/7000	192.168.1.2	Always	

Figure 26

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 : PVC:8/35

Enable DMZ : □

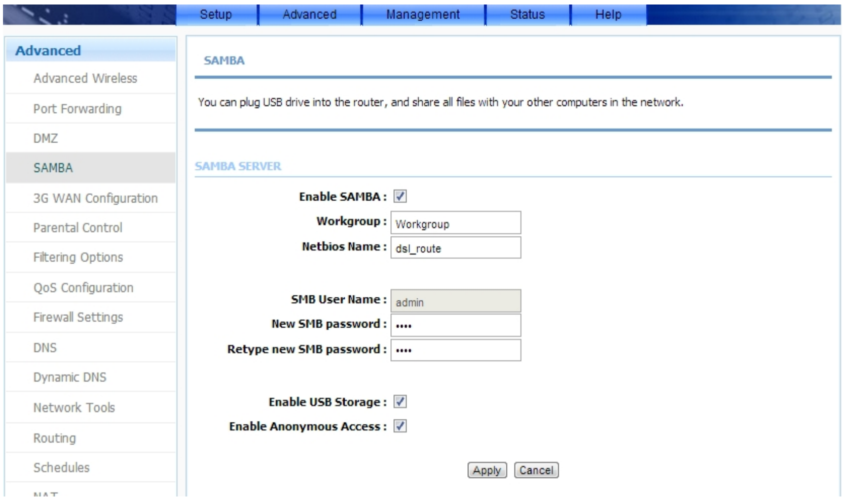
DMZ Host IP Address :

Figure 27

Click **Apply** to save the settings.

3.3.4 SAMBA (Servidor de Ficheros)

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



You can plug USB drive into the router, and share all files with your other computers in the network.

Enable SAMBA : ☑
Workgroup : Workgroup
Netbios Name : dsl_route

SMB User Name : admin
New SMB password : ••••
Retype new SMB password : ••••

Enable USB Storage : ☑
Enable Anonymous Access : ☑

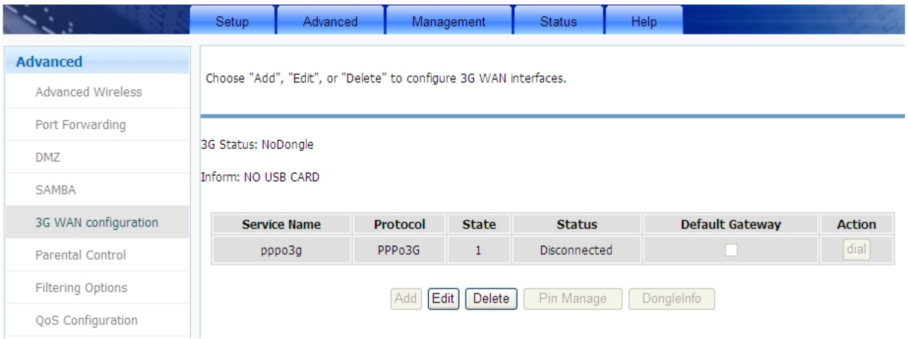
Figure 28

The following table describes the parameters of this page.

Field	Description
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 WAN Configuration

Choose **Advanced** > **3G WAN Configuration**. The page shown in the following figure appears.



Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

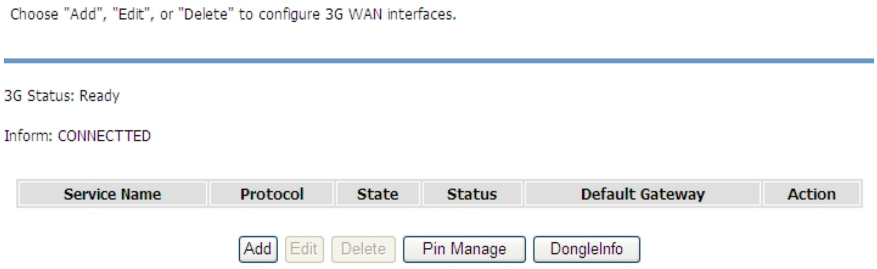
3G Status: NoDongle

Inform: NO USB CARD

Service Name	Protocol	State	Status	Default Gateway	Action
pppo3g	PPPo3G	1	Disconnected	□	dial

Figure 29

If you want to access the Internet through 3G connection, a 3G USB data card is required. Connect the 3G data card to the USB interface of the Router and the following will appear.



Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

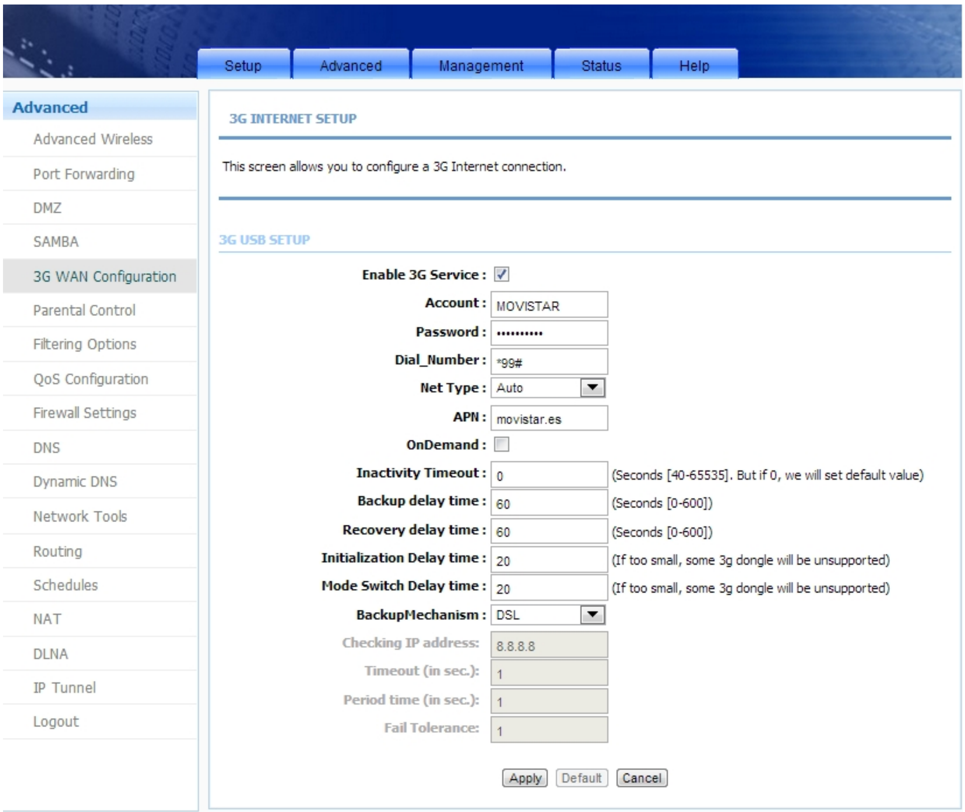
3G Status: Ready

Inform: CONNECTTED

Service Name	Protocol	State	Status	Default Gateway	Action

Figure 30

Click **Add** to display the following figure. In this page, you can configure 3G Internet connection.



3G INTERNET SETUP

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

3G USB SETUP

Enable 3G Service :	☑	
Account :	MOVISTAR	
Password :	••••••••••	
Dial_Number :	*99#	
Net Type :	Auto	
APN :	movistar.es	
OnDemand :	□	
Inactivity Timeout :	0	(Seconds [40-65535]. But if 0, we will set default value)
Backup delay time :	60	(Seconds [0-600])
Recovery delay time :	60	(Seconds [0-600])
Initialization Delay time :	20	(If too small, some 3g dongle will be unsupported)
Mode Switch Delay time :	20	(If too small, some 3g dongle will be unsupported)
BackupMechanism :	DSL	
Checking IP address:	8.8.8.8	
Timeout (in sec.):	1	
Period time (in sec.):	1	
Fail Tolerance:	1	

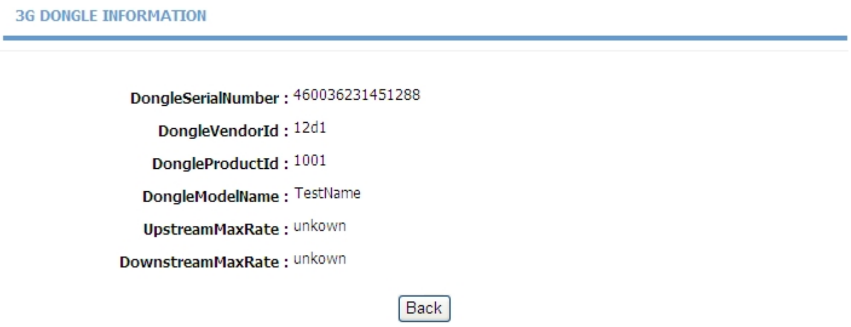
Figure 31

The following table describes the parameters of this page.

Field	Description
Enable 3G Service	You may choose to enable or disable 3G service.
Account	Enter the account.
Password	Enter the password.
Dial_Number	Enter the dial number.
APN	Enter the access point.
OnDemand	You may choose to dial on demand.
Inactivity Timeout	Set the period without flow before disconnecting 3G connection. When 0 is set, 3G connection will always be connected regardless of flow.
Backup delay time	Set the period before starting 3G dial after ADSL disconnection.
Initialization Delay time	Set the initialization time of 3G USB data card.
Mode Switch Delay time	Set the time for the 3G USB data card to switch from a storage device to a communication device.

Field	Description
Backup Mechanism	When DSL is selected, 3G dial starts after DSL disconnection. Usually DSL is selected. When IPCHECK is selected, 3G dial starts when DSL connection is established and the address set in Checking IP address can not be pinged.
Checking IP address	It is an address for 3G detection. After DSL dialup, if this address cannot be pinged, 3G dial will be started.
Timeout (in sec.)	Set the ping timeout.
Period time (in sec.)	Set the interval between two times of ping.
Fail Tolerance	Set the allowed times of ping failure.

You may click **DongleInfo** to view 3G network card information as shown in the following figure.

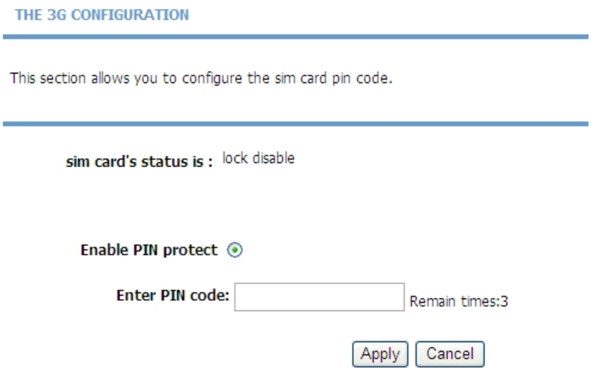


3G DONGLE INFORMATION

DongleSerialNumber : 460036231451288
DongleVendorId : 12d1
DongleProductId : 1001
DongleModelName : TestName
UpstreamMaxRate : unkown
DownstreamMaxRate : unkown

Figure 32

Click **Pin Manage** to enable the 3G PIN code as shown in the following figure.



THE 3G CONFIGURATION

This section allows you to configure the sim card pin code.

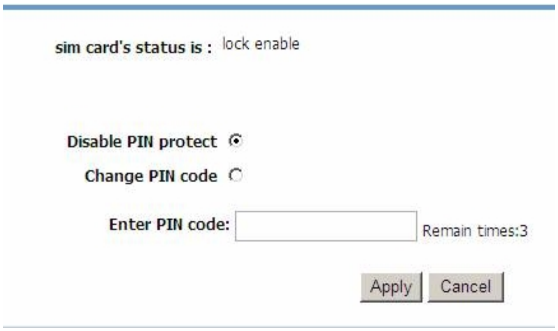
sim card's status is : lock disable

Enable PIN protect ●

Enter PIN code: Remain times:3

Figure 33

Enter the applied PIN code in the **Enter PIN code** field, and then click **Apply** to finish.
You can disable the 3G PIN code as shown in the following figure.

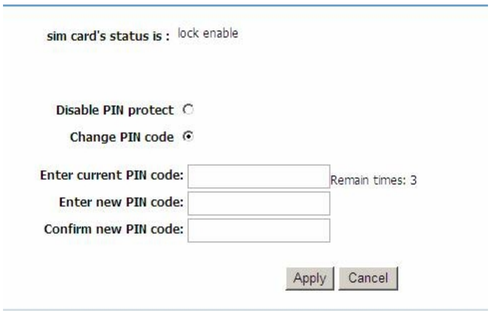


sim card's status is : lock enable

Disable PIN protect ●
Change PIN code ○

Enter PIN code: Remain times:3

Select **Disable PIN protect**, and then click **Apply** to finish.
You can Change the PIN code as shown in the following figure.



sim card's status is : lock enable

Disable PIN protect ○
Change PIN code ●

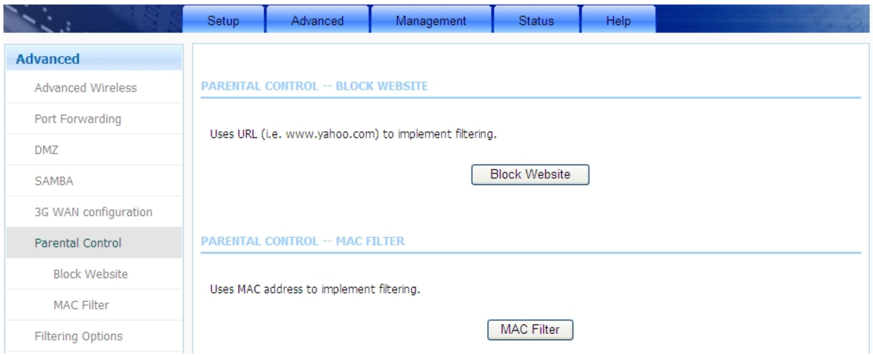
Enter current PIN code: ______ Remain times: 3
Enter new PIN code: ______
Confirm new PIN code: ______

Enter current PIN code and a new one for twice, and then click **Apply** to finish.

Note:
If a wrong PIN code is input continuously for three times, the PUK code will be required to unlock the PIN code.

3.3.6 Parental 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

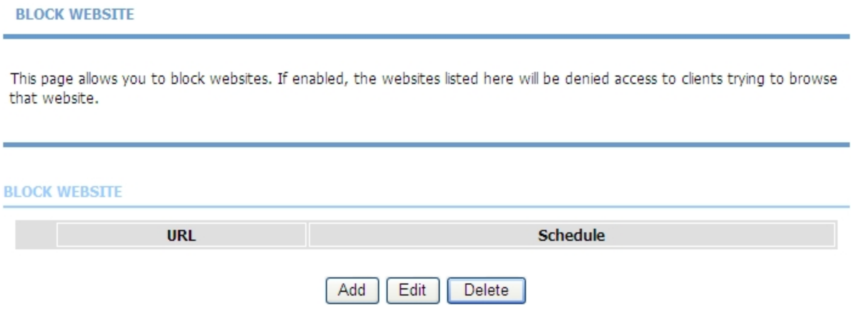
Uses MAC address to implement filtering.

Figure 34

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

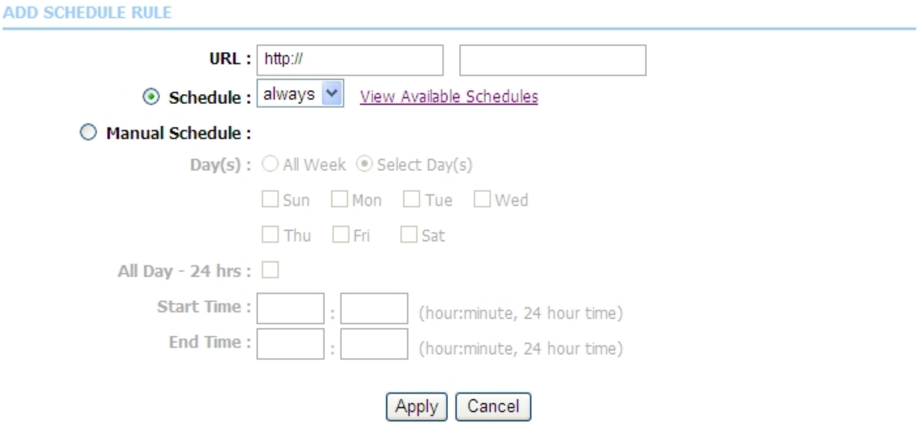
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule

Figure 35

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



ADD SCHEDULE RULE

URL : http://

● 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 : □

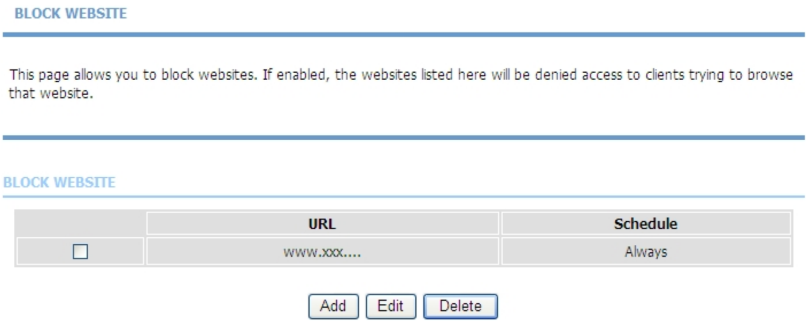
Start Time : __ : __ (hour:minute, 24 hour time)

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

Figure 36

Enter the website in the **URL** field. Select the **Schedule** from the 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.

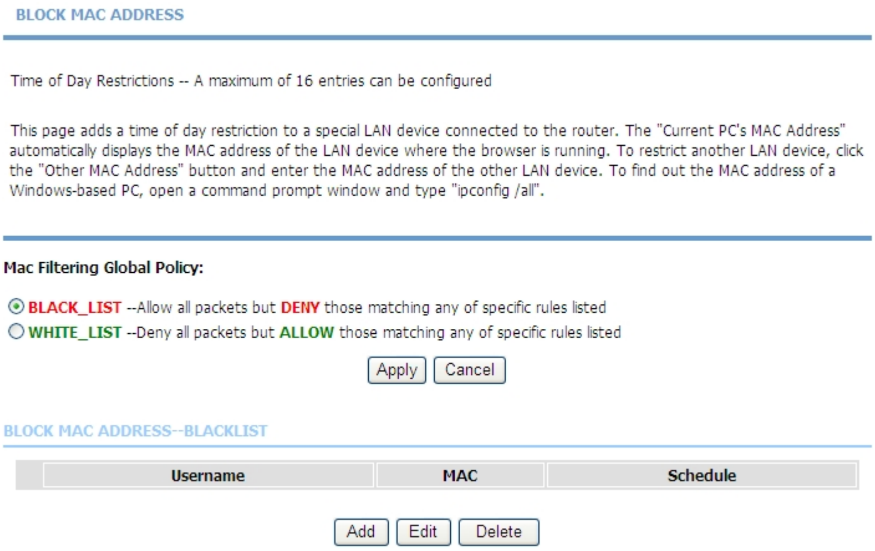
BLOCK WEBSITE

	URL	Schedule
□	www.xxx....	Always

Figure 37

3.3.6.2 Block MAC Filter

In the **Parent Control** page, click **Block MAC Address**. 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".

Mac Filtering Global Policy:

● BLACK_LIST --Allow all packets but DENY those matching any of specific rules listed

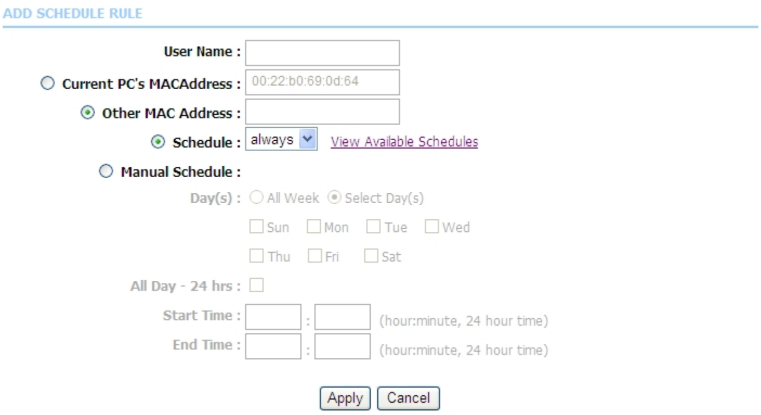
○ WHITE_LIST --Deny all packets but ALLOW those matching any of specific rules listed

BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule

Figure 38

Choose **BLACK_LIST** or **WHITE_LIST**, and then click **Add**. The page shown in the following figure appears.



ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:22:b0:69:0d:64

● Other MAC Address :

● Schedule : always

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

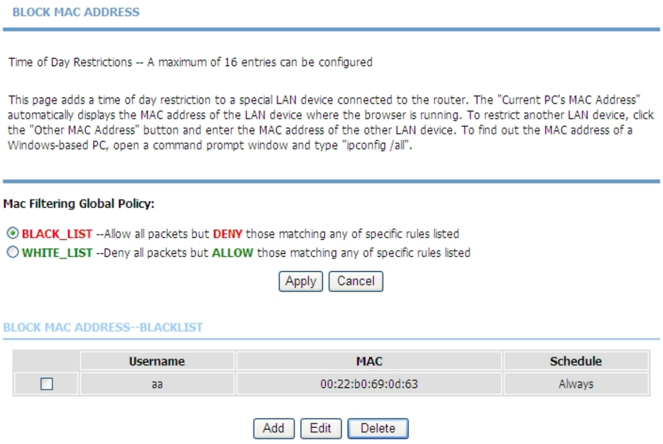
All Day - 24 hrs : □

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

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

Figure 39

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".

Mac Filtering Global Policy:

● BLACK_LIST --Allow all packets but DENY those matching any of specific rules listed
○ WHITE_LIST --Deny all packets but ALLOW those matching any of specific rules listed

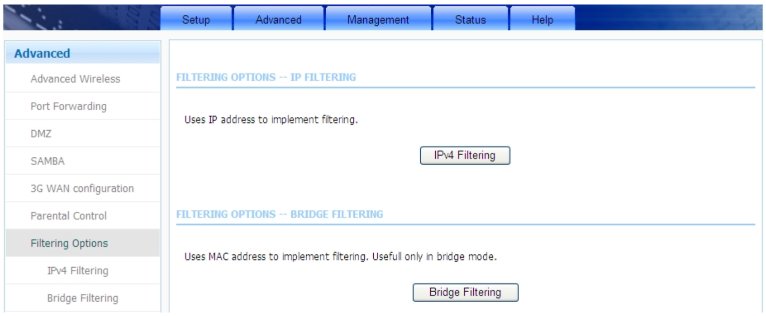
BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule
□	aa	00:22:b0:69:0d:63	Always

Figure 40

3.3.7 Filtering Options

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



FILTERING OPTIONS -- IP FILTERING

Uses IP address to implement filtering.

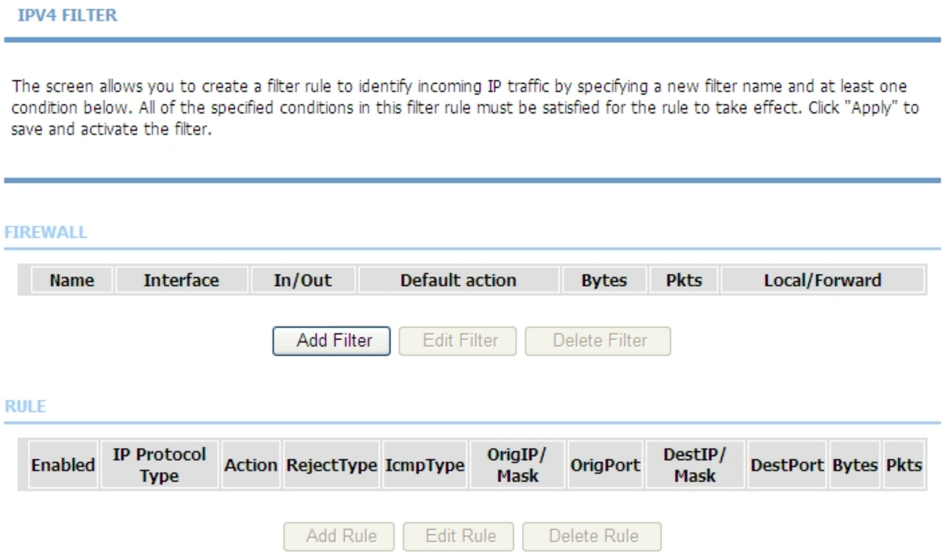
FILTERING OPTIONS -- BRIDGE FILTERING

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

Figure 41

3.3.7.1 IPv4 Filtering

In the **Filtering Options** page, click **IPv4 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv4 firewall function.



IPV4 FILTER

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one 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.

FIREWALL

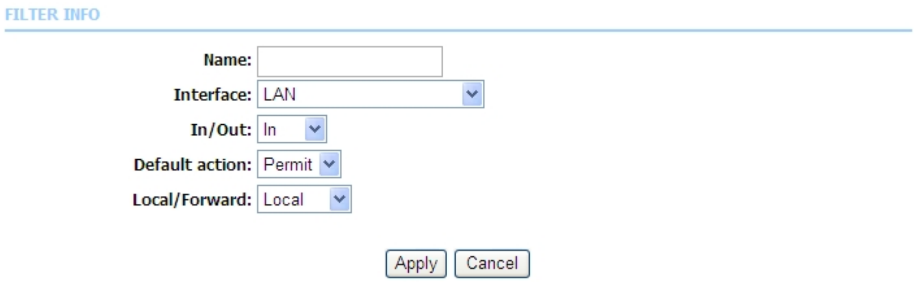
Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward

RULE

Enabled	IP Protocol Type	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts

Figure 42

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



FILTER INFO

Name:
Interface: LAN
In/Out: In
Default action: Permit
Local/Forward: Local

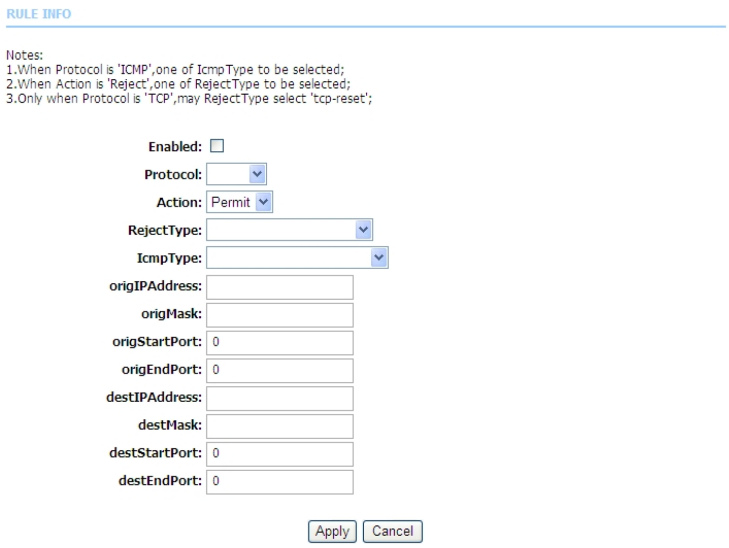
Figure 43

Enter the **Filter Name** and specify at least one of the following criteria: Interface, In/Out, Default action and Local/Forward.

Click **Apply** to save the settings.

Note:
The settings are applicable only when the firewall is enabled.

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



RULE INFO

Notes:
1.When Protocol is 'ICMP',one of IcmpType to be selected;
2.When Action is 'Reject',one of RejectType to be selected;
3.Only when Protocol is 'TCP',may RejectType select 'tcp-reset';

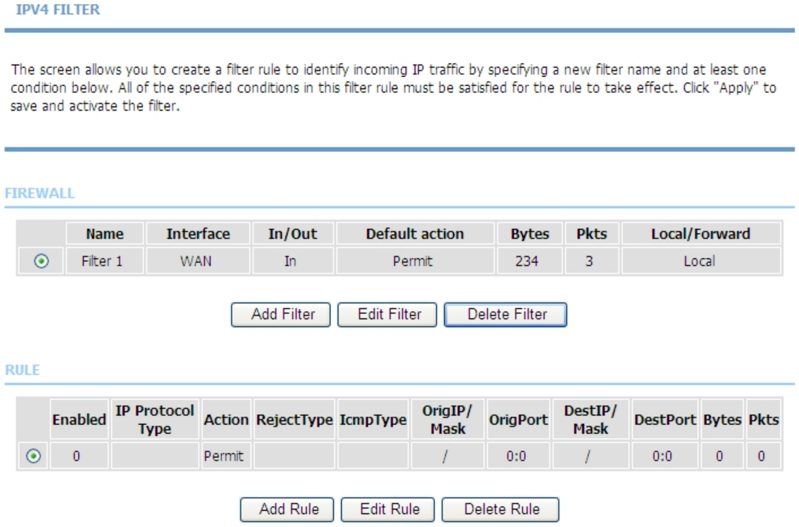
Enabled:	□
Protocol:	
Action:	Permit
RejectType:	
IcmpType:	
origIPAddress:	
origMask:	
origStartPort:	0
origEndPort:	0
destIPAddress:	
destMask:	
destStartPort:	0
destEndPort:	0

Figure 44

The following table describes the parameters of this page.

Field	Description
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose **TCP**, **UDP** or **ICMP**.
Action	The action when the rule is matched. **Permit** means allowing the message to pass, **Drop** means discarding messages without a reply, and **Reject** means discarding messages with a reply.
Reject Type	The type of message sent in a Reject action.
Icmp Type	Type of ICMP messages
origIPAddress	Original IP address
origMask	Original address mask
origStart/End Port	Original start/ end port, which is the original port range
destIPAddress	Destination address
destMask	Destination address mask
dest Start/End Port	Destination start/ end port, which is the original port range

After setting the parameters, click **Apply**. The page shown in the following figure appears.



IPV4 FILTER

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one 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.

FIREWALL

	Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward
●	Filter 1	WAN	In	Permit	234	3	Local

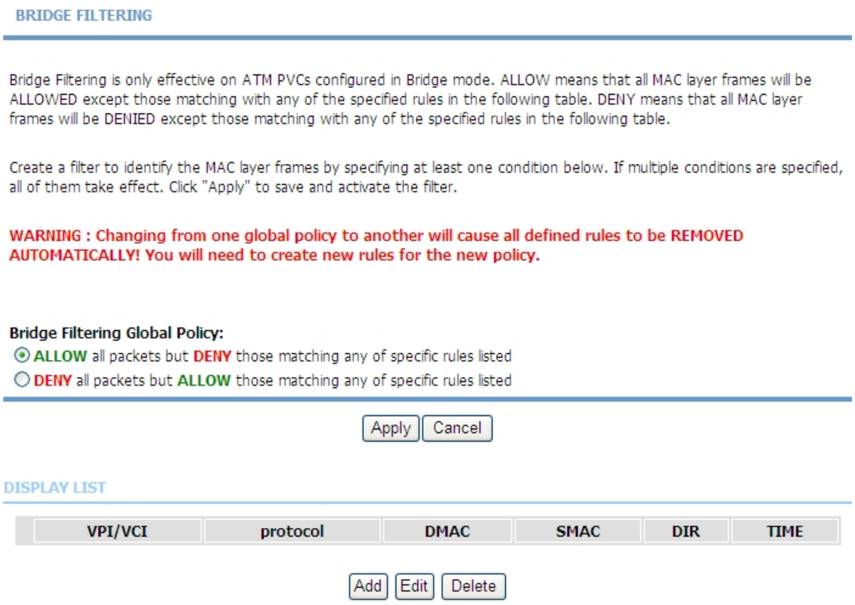
RULE

	Enabled	IP Protocol Type	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts
●	0		Permit			/	0:0	/	0:0	0	0

Figure 45

3.3.7.2 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

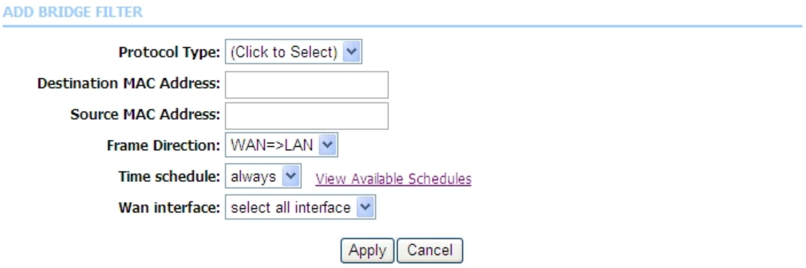
○ DENY all packets but ALLOW those matching any of specific rules listed

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME

Figure 46

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

Figure 47

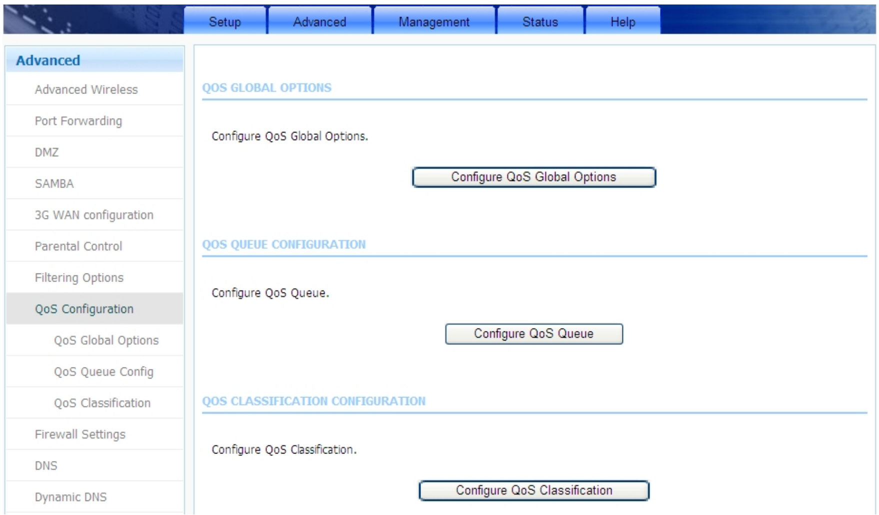
The following table describes the parameters of this page.

Field	Description
Protocol Type	Choose a third-layer protocol type for bridge filtering from the drop-down list. You may choose **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX, NetBEUI** or **IGMP**.
Destination MAC Address	The MAC address of sendee of the message
Source MAC Address	The MAC address of sender of the message
Frame Direction	Choose the sending direction as **WAN to LAN** or **LAN to WAN**.
Time schedule	Choose the filtering strategy as **always** or **never**.
Wan interface	Set an effective interface for the bridge filtering rule.

Click **Apply** to save the settings.

3.3.8 QoS Configuration

Choose **Advanced** > **QoS Configuration**. The **QoS Configuration** page shown in the following figure appears.



Configure QoS Global Options.

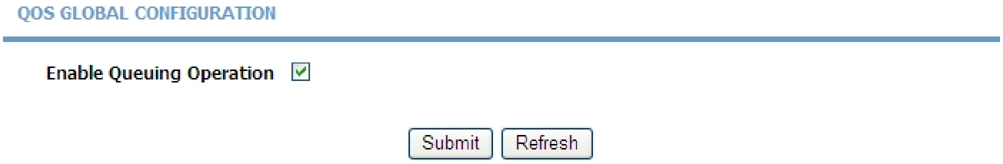
Configure QoS Queue.

Configure QoS Classification.

Figure 48

3.3.8.1 QoS Global Options

In the **QoS Configuration** page, click **QoS Global Options**. The page shown in the following figure appears.You can tick in the checkbox and then click **Submit** to enable queuing operation.

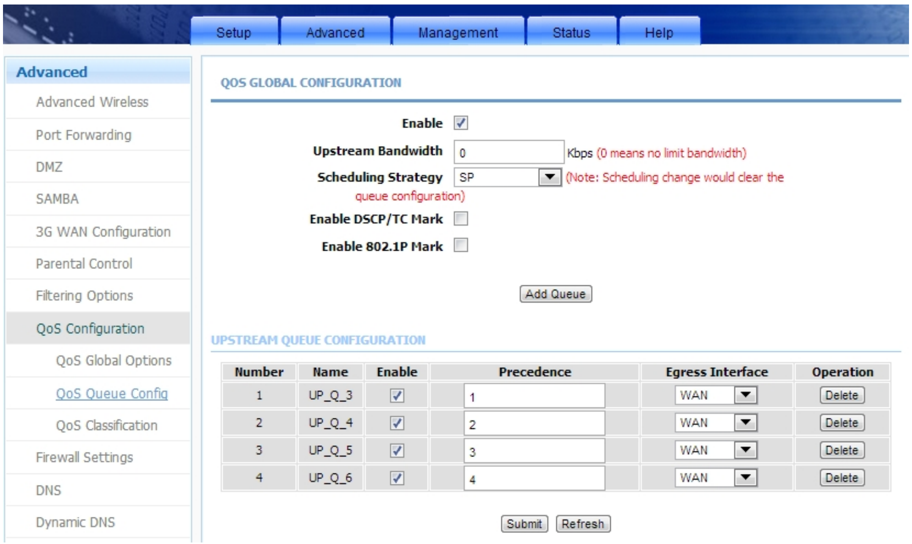


Enable Queuing Operation ☑

Figure 49

3.3.8.2 QoS Queue Config

In the **QoS Configuration** page, click **QoS Queue Config**. The page shown in the following figure appears. In this page, you can set QoS flow control.



Enable ☑
Upstream Bandwidth 0 Kbps (0 means no limit bandwidth)
Scheduling Strategy SP (Note: Scheduling change would clear the queue configuration)
Enable DSCP/TC Mark □
Enable 802.1P Mark □

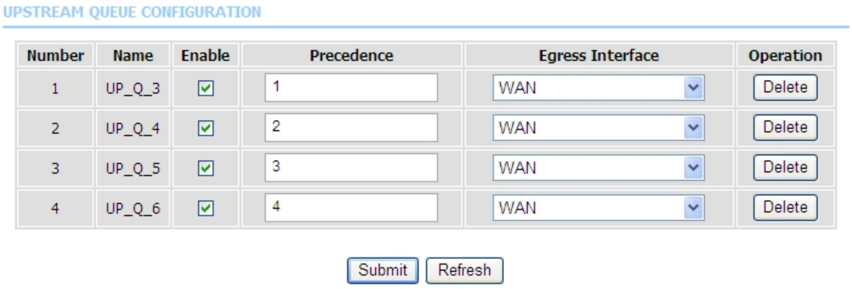
Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	☑	1	WAN	Delete
2	UP_Q_4	☑	2	WAN	Delete
3	UP_Q_5	☑	3	WAN	Delete
4	UP_Q_6	☑	4	WAN	Delete

Figure 50

The following table describes the parameters of this page.

Field	Description
Direction	Choose **Upstream** queue or **Downstream** queue.
Enable	Tick in the box to enable queue.
Upstream Bandwidth	Total bandwith for upstream flow
Scheduling Strategy	Scheduling algorithm of QoS queue
Enable DSCP/TC Mark	You may tick in the box to permit DSCP/TC Mark.
Enable 802.1P Mark	You may tick in the box to permit 802.1P Mark.

After setting the parameters, click **Add Queue** to add a queue.
In the above page, when **Upstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.

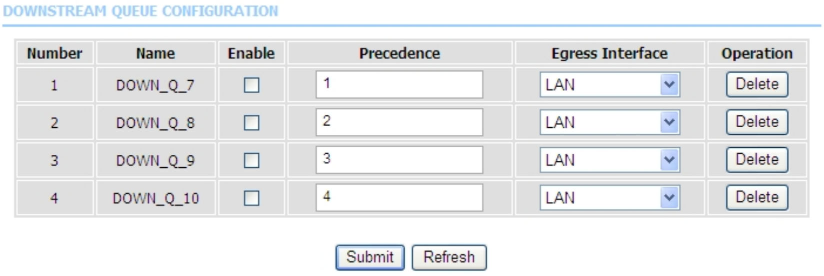


UPSTREAM QUEUE CONFIGURATION

Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	☑	1	WAN	Delete
2	UP_Q_4	☑	2	WAN	Delete
3	UP_Q_5	☑	3	WAN	Delete
4	UP_Q_6	☑	4	WAN	Delete

Figure 51

When **Downstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.



DOWNSTREAM QUEUE CONFIGURATION

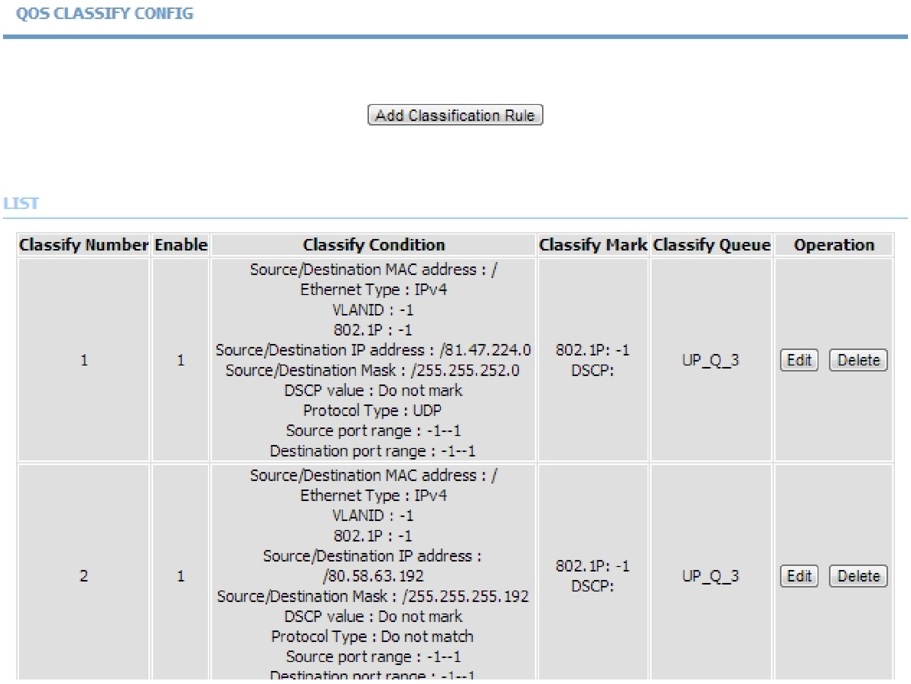
Number	Name	Enable	Precedence	Egress Interface	Operation
1	DOWN_Q_7	□	1	LAN	Delete
2	DOWN_Q_8	□	2	LAN	Delete
3	DOWN_Q_9	□	3	LAN	Delete
4	DOWN_Q_10	□	4	LAN	Delete

Figure 52

After modifying a queue, click **Submit** to enable the modification. Click **Refresh** to refresh the queue.

3.3.8.3 QoS Classification

In the **QoS Configuration** page, click **QoS Classification**. The page shown in the following figure appears.You can configure QoS queue rule.



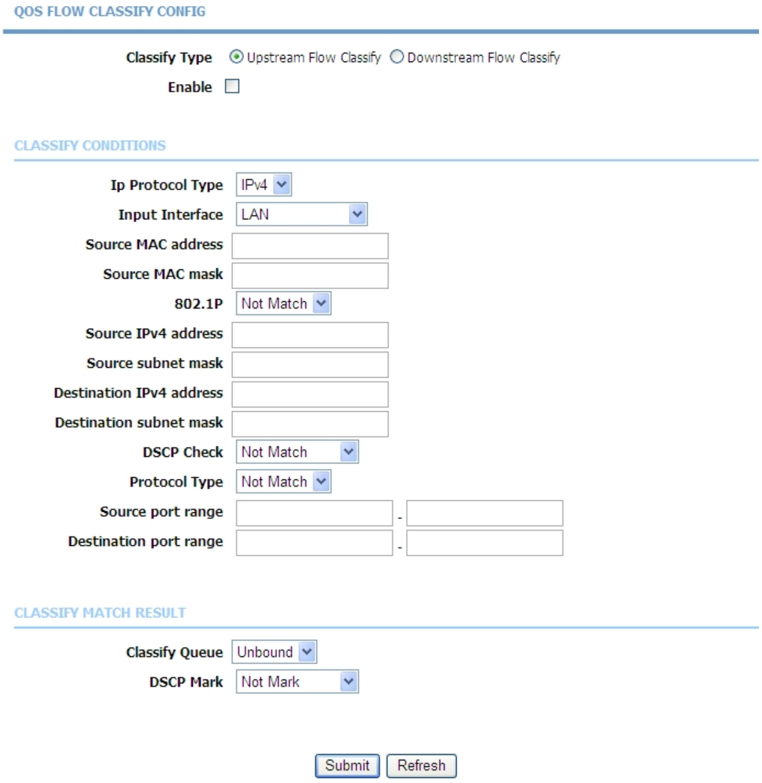
QOS CLASSIFY CONFIG

LIST

Classify Number	Enable	Classify Condition	Classify Mark	Classify Queue	Operation
1	1	Source/Destination MAC address : / Ethernet Type : IPv4 VLANID : -1 802.1P : -1 Source/Destination IP address : /81.47.224.0 Source/Destination Mask : /255.255.252.0 DSCP value : Do not mark Protocol Type : UDP Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	Edit Delete
2	1	Source/Destination MAC address : / Ethernet Type : IPv4 VLANID : -1 802.1P : -1 Source/Destination IP address : /80.58.63.192 Source/Destination Mask : /255.255.255.192 DSCP value : Do not mark Protocol Type : Do not match Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	Edit Delete

Figure 53

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



QOS FLOW CLASSIFY CONFIG

Classify Type	● Upstream Flow Classify ○ Downstream Flow Classify
Enable	□

CLASSIFY CONDITIONS

Ip Protocol Type	IPv4
Input Interface	LAN
Source MAC address	
Source MAC mask	
802.1P	Not Match
Source IPv4 address	
Source subnet mask	
Destination IPv4 address	
Destination subnet mask	
DSCP Check	Not Match
Protocol Type	Not Match
Source port range	-
Destination port range	-

CLASSIFY MATCH RESULT

Classify Queue	Unbound
DSCP Mark	Not Mark

Figure 54

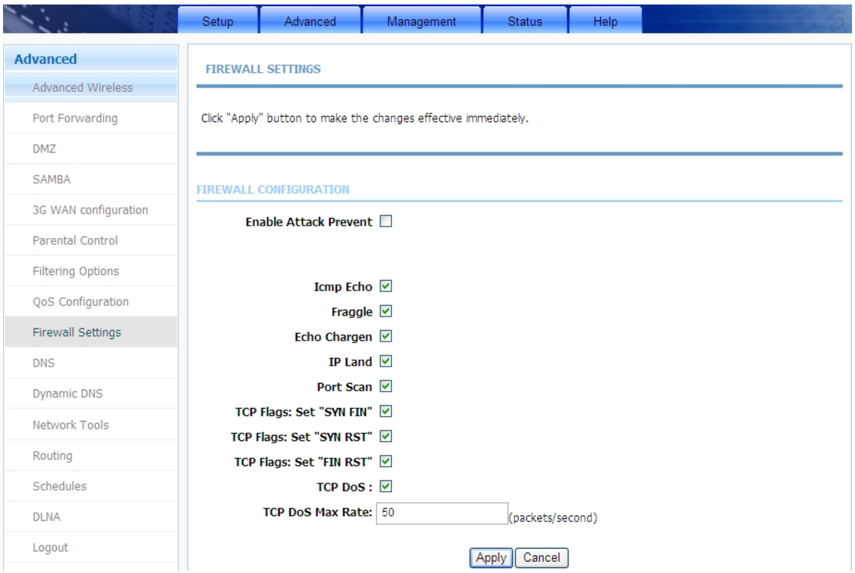
The following table describes the parameters of this page.

Field	Description
Classify Type	Set the QoS rule type as **Upstream** or **Downstream**.
Enable	Tick in the box to enable this QoS rule.
Ip Protocol Type	Select the protocol type **IPv4**.
Input Interface	Based on the Classify Type, choose a WAN/LAN interface.
802.1P	Choose a matched 802.1P VLAN priority.
DSCP Check	Choose a matched DSCP type.
Protocol Type	Choose a protocol type matching with the QoS rule.
Classify Queue	Choose a QoS queue for the rule.
DSCP Mark	Set a DSCP Mark for this QoS rule.

You may click **Edit** to modify the existing classification rule.

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 SETTINGS

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

FIREWALL CONFIGURATION

Enable Attack Prevent ☐

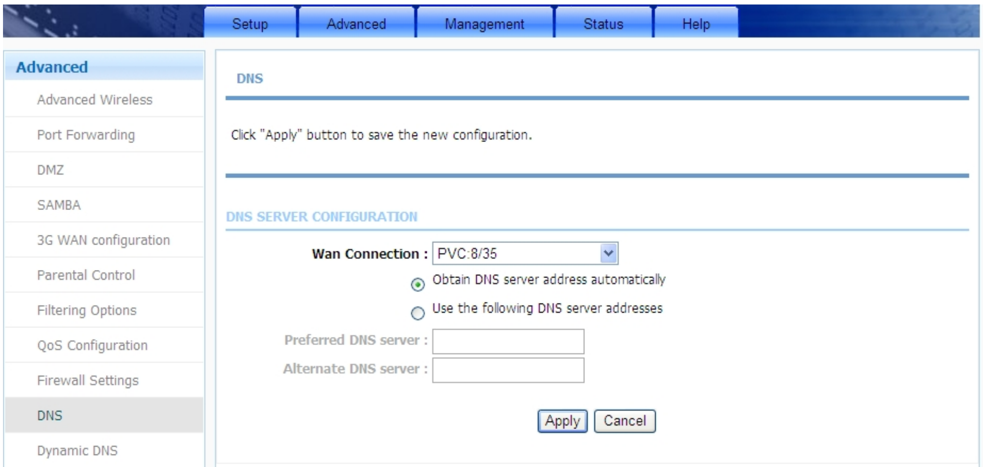
Icmp Echo ☑
Fraggle ☑
Echo Chargen ☑
IP Land ☑
Port Scan ☑
TCP Flags: Set "SYN FIN" ☑
TCP Flags: Set "SYN RST" ☑
TCP Flags: Set "FIN RST" ☑
TCP DoS : ☑
TCP DoS Max Rate: 50 (packets/second)

Figure 55

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 : PVC:8/35

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Preferred DNS server :

Alternate DNS server :

Apply Cancel

Figure 56

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

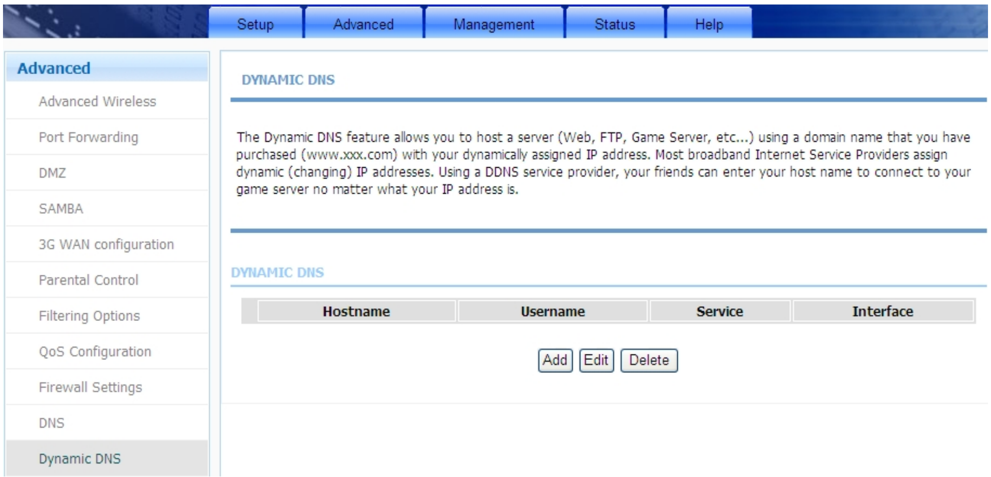
If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

Click **Apply** to save the settings.

3.3.11 Dynamic 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 (DyndDNS.org or dlinkddns.com).

Choose **Advanced** > **Dynamic DNS**. The page shown in the following figure 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.

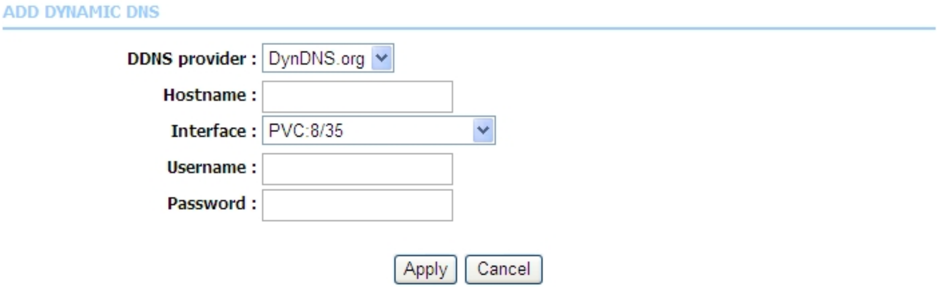
DYNAMIC DNS

Hostname	Username	Service	Interface

Add Edit Delete

Figure 57

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



ADD DYNAMIC DNS

DDNS provider : DynDNS.org
Hostname :
Interface : PVC:8/35
Username :
Password :

Figure 58

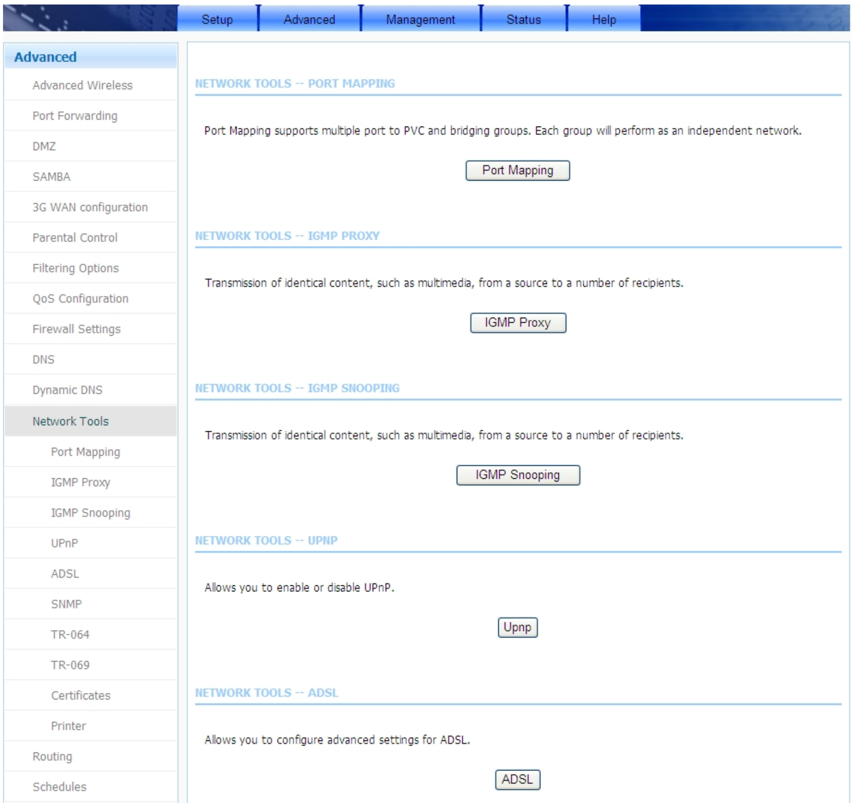
The following table describes the parameters of this page.

Field	Description
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

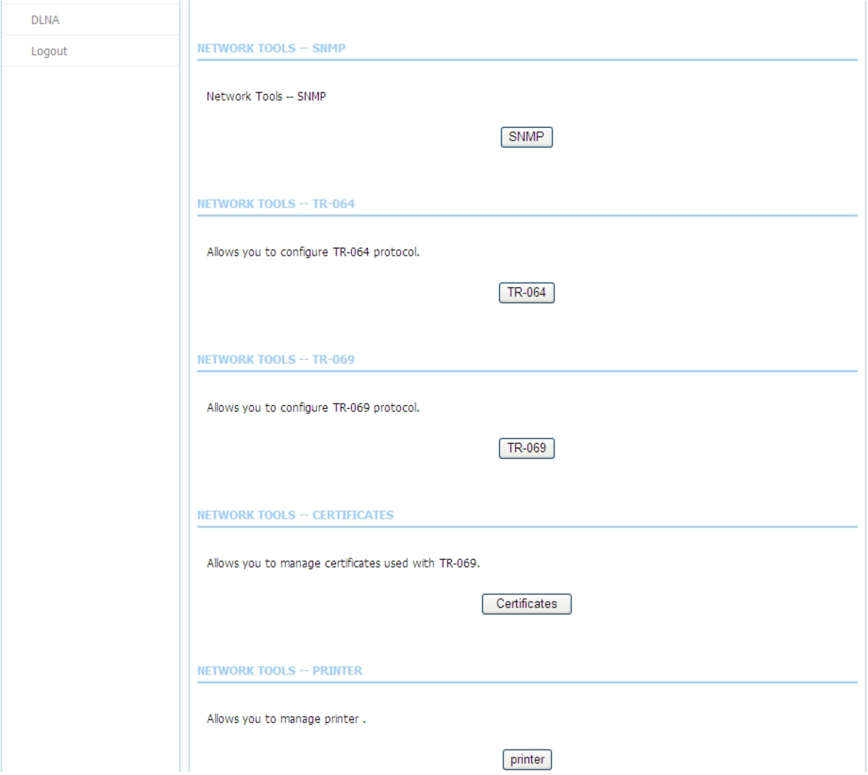
Transmission of identical content, such as multimedia, from a source to a number of recipients.

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-064

Allows you to configure TR-064 protocol.

NETWORK TOOLS -- TR-069

Allows you to configure TR-069 protocol.

NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

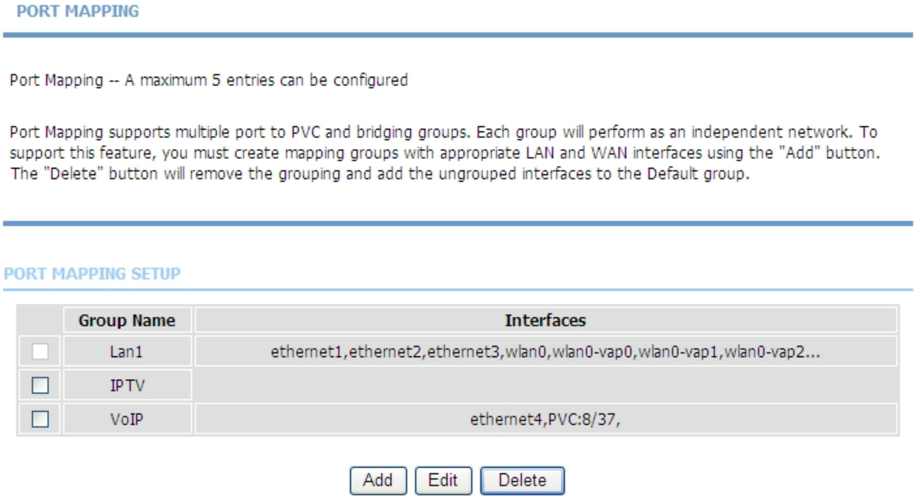
NETWORK TOOLS -- PRINTER

Allows you to manage printer .

Figure 59

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

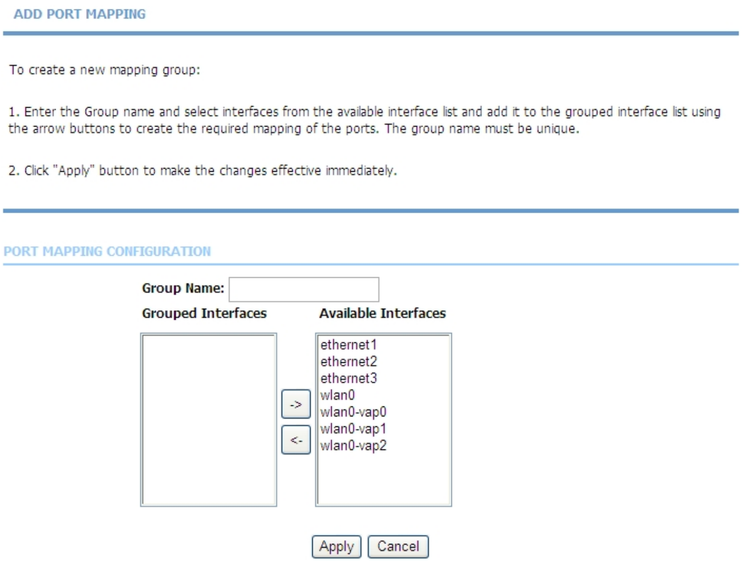
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

PORT MAPPING SETUP

	Group Name	Interfaces
□	Lan1	ethernet1,ethernet2,ethernet3,wlan0,wlan0-vap0,wlan0-vap1,wlan0-vap2...
□	IPTV	
□	VoIP	ethernet4,PVC:8/37,

Figure 60

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 wlan0 wlan0-vap0 wlan0-vap1 wlan0-vap2

Figure 61

The procedure for creating a mapping group is as follows:

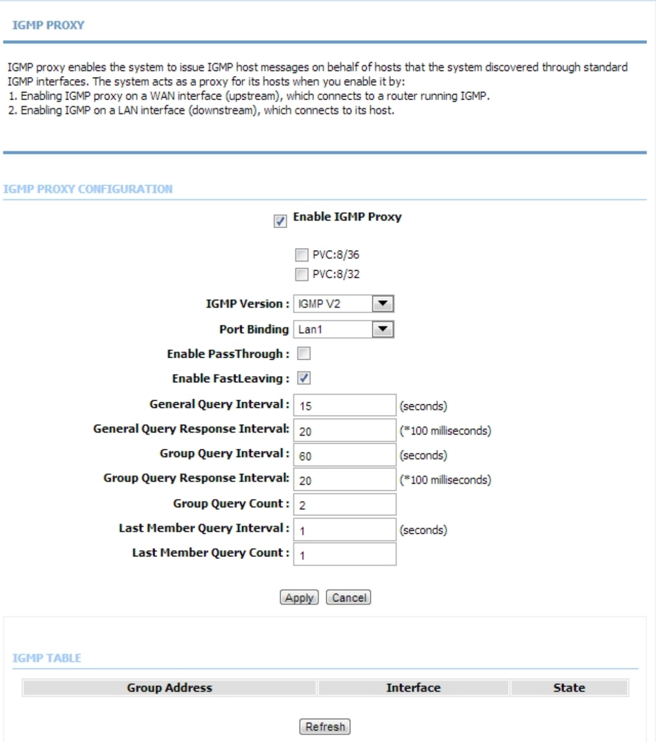
Step 1 Enter the group name.

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 host.

IGMP PROXY CONFIGURATION

☑ Enable IGMP Proxy

☐ PVC:8/36
☐ PVC:8/32

IGMP Version : IGMP V2
Port Binding Lan1
Enable PassThrough : ☐
Enable FastLeaving : ☑
General Query Interval : 15 (seconds)
General Query Response Interval: 20 (*100 milliseconds)
Group Query Interval : 60 (seconds)
Group Query Response Interval: 20 (*100 milliseconds)
Group Query Count : 2
Last Member Query Interval : 1 (seconds)
Last Member Query Count : 1

IGMP TABLE

Group Address	Interface	State

Figure 62

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.

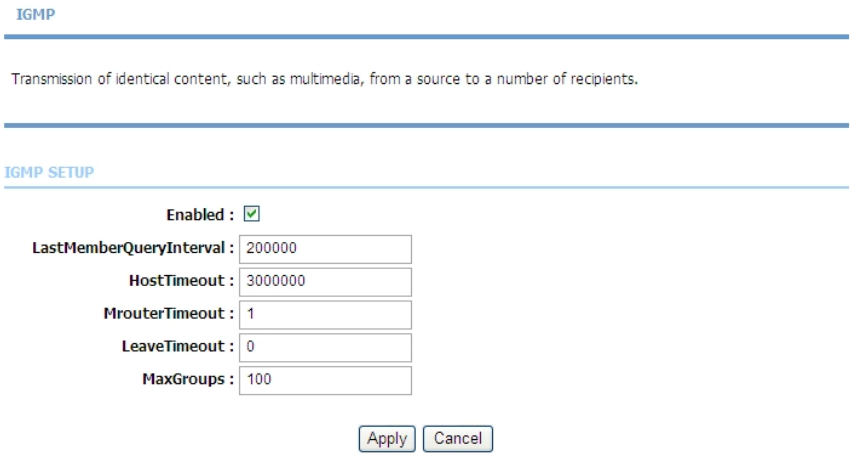
The following table describes the parameters of this page.

Field	Description
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

Choose **Advanced** > **Network Tools** and click **IGMP Snooping**. The page shown in the following figure appears. When IGMP Snooping is enabled, 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

Enabled : ☑

LastMemberQueryInterval : 200000

HostTimeout : 3000000

MrouterTimeout : 1

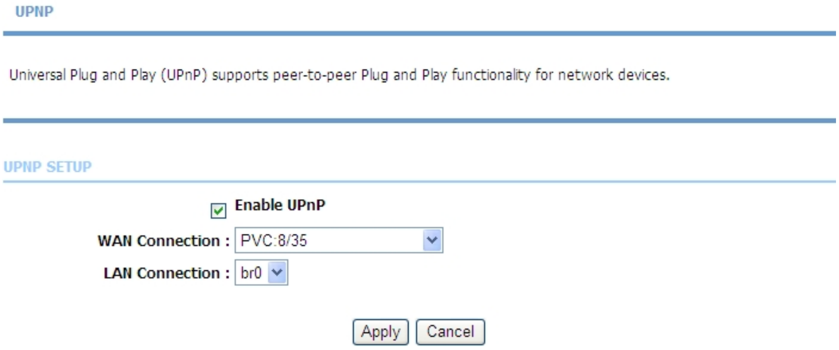
LeaveTimeout : 0

MaxGroups : 100

Figure 63

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 : PVC:8/35

LAN Connection : br0

Figure 64

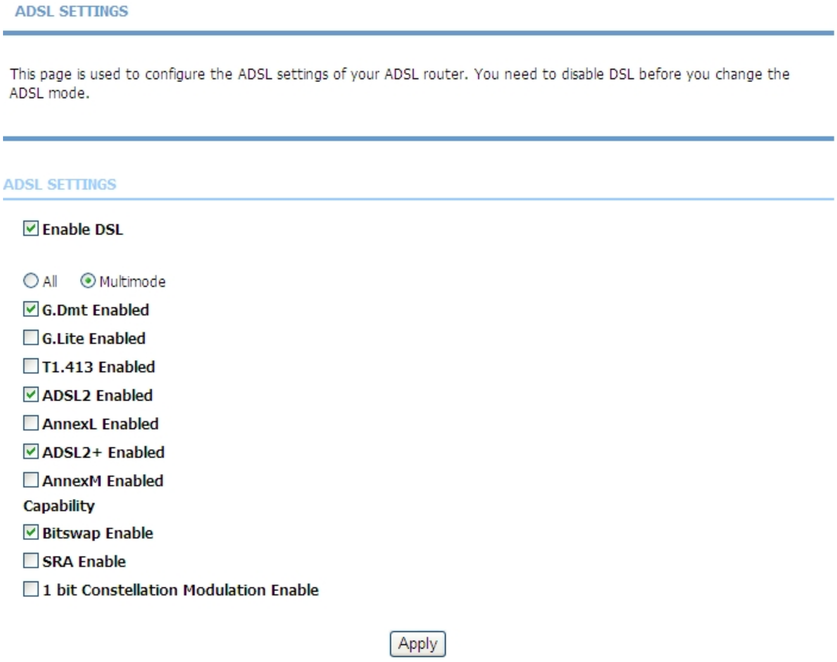
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

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

Choose **Advanced** > **Network Tools** and click **ADSL**. 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

○ All ● Multimode

☑ 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

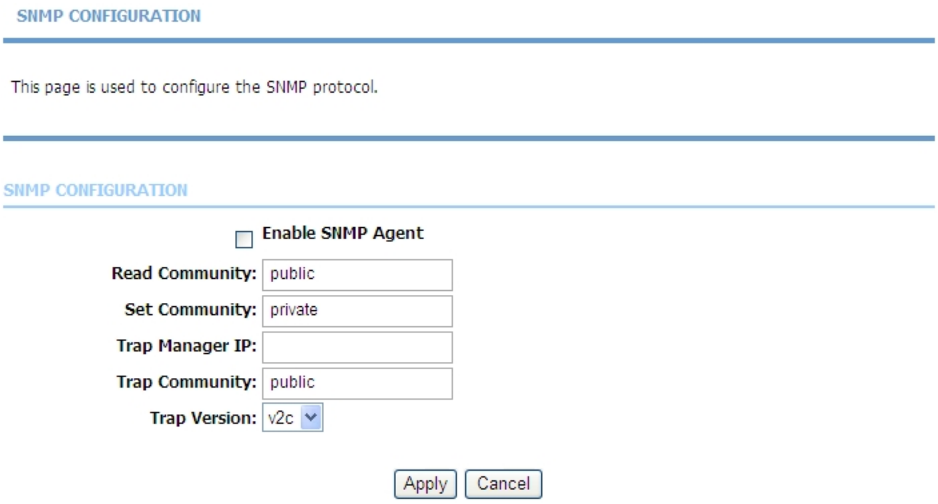
Figure 65

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

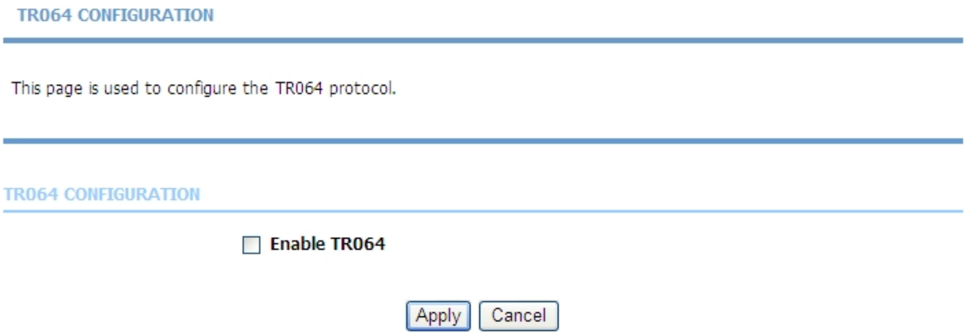
Trap Version: v2c

Figure 66

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.

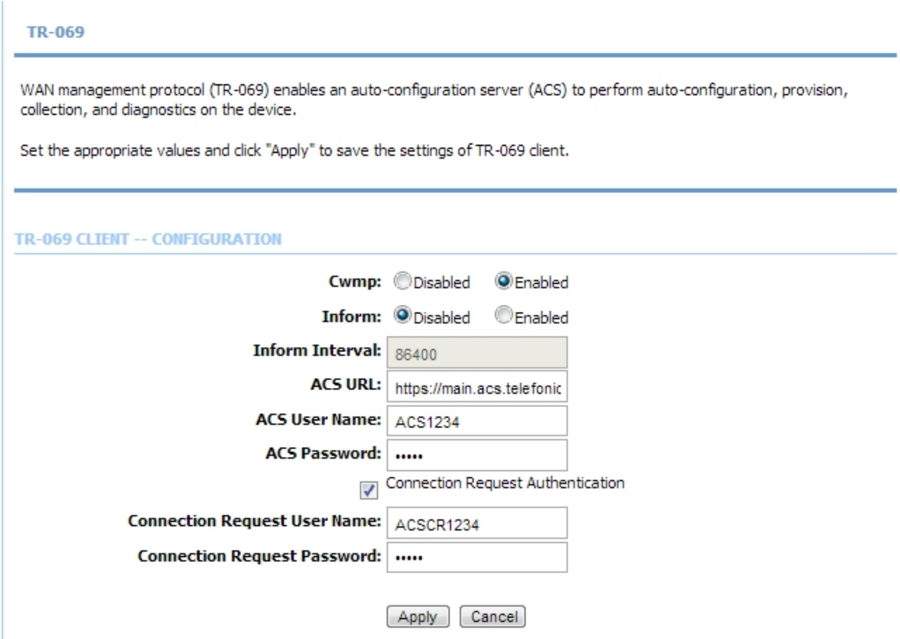
TR064 CONFIGURATION

□ Enable TR064

Figure 67

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) enables an auto-configuration server (ACS) to perform auto-configuration, provision, collection, and diagnostics on the device.

Set the appropriate values and click "Apply" to save the settings of TR-069 client.

TR-069 CLIENT -- CONFIGURATION

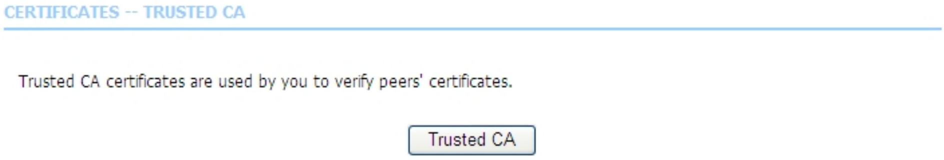
Cwmp: ○ Disabled ● Enabled
Inform: ● Disabled ○ Enabled
Inform Interval: 86400
ACS URL: https://main.acs.telefonic
ACS User Name: ACS1234
ACS Password: •••••
☑ Connection Request Authentication
Connection Request User Name: ACSCR1234
Connection Request Password: •••••

Figure 68

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.

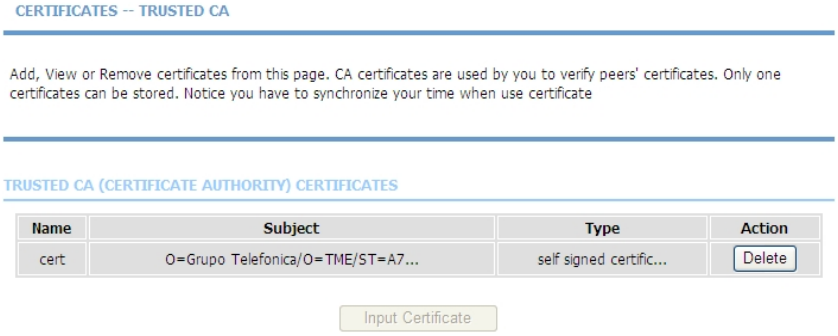


CERTIFICATES -- TRUSTED CA

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

Figure 69

Click **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

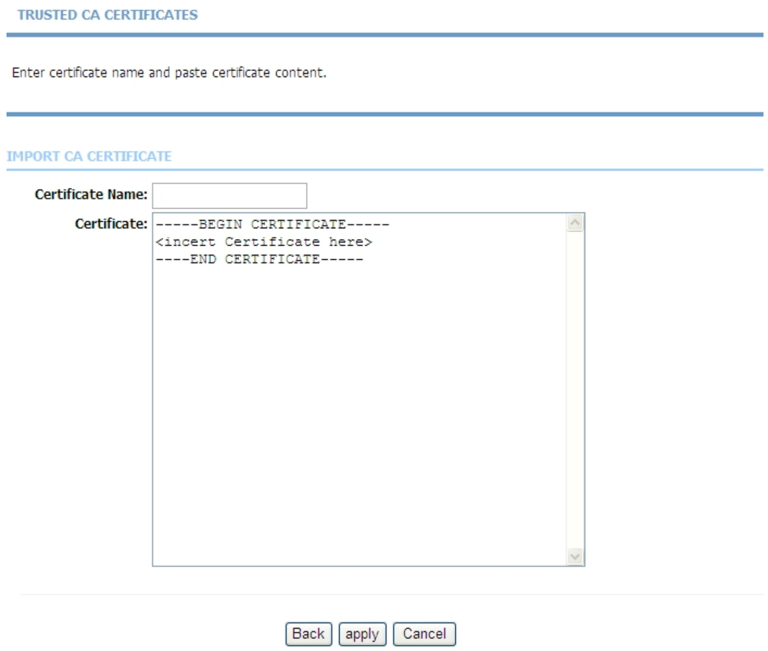
TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action
cert	O=Grupo Telefonica/O=TME/ST=A7...	self signed certific...	Delete

Figure 70

Click **Input Certificate** button to import a certification.

Note:
You can input a certificate after deleting the existing certificate.



TRUSTED CA CERTIFICATES

Enter certificate name and paste certificate content.

IMPORT CA CERTIFICATE

Certificate Name:

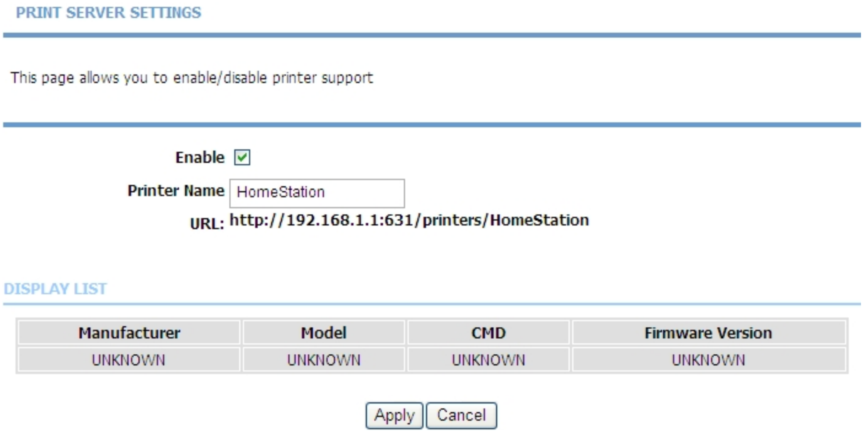
Certificate:

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

Figure 71

3.3.12.10 Printer

Choose **Advanced** > **Network Tools** and click **Printer**. The **Printer** page shown in the following figure appears. In this page, you can enable/disable printer support.



PRINT SERVER SETTINGS

This page allows you to enable/disable printer support

Enable ☑

Printer Name HomeStation

URL: http://192.168.1.1:631/printers/HomeStation

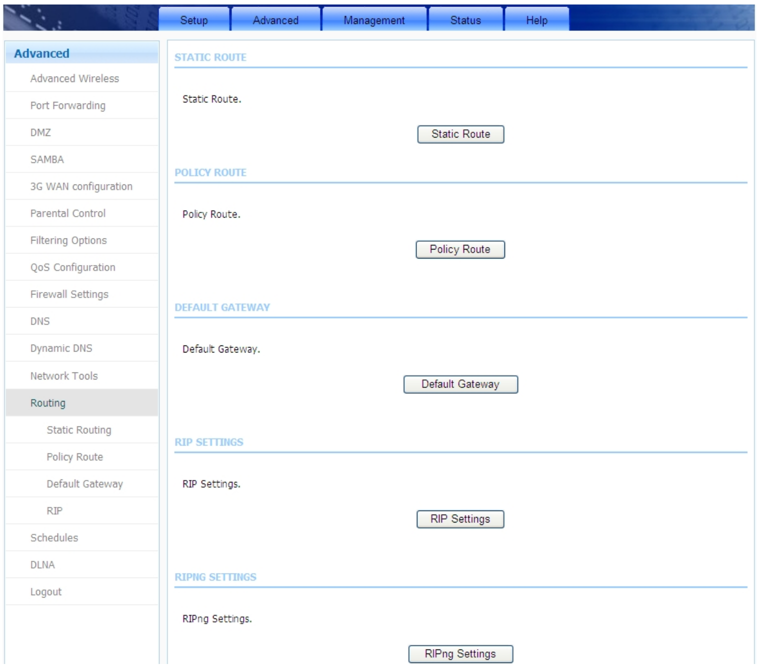
DISPLAY LIST

Manufacturer	Model	CMD	Firmware Version
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN

Figure 72

3.3.13 Routing

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



STATIC ROUTE

Static Route.

POLICY ROUTE

Policy Route.

DEFAULT GATEWAY

Default Gateway.

RIP SETTINGS

RIP Settings.

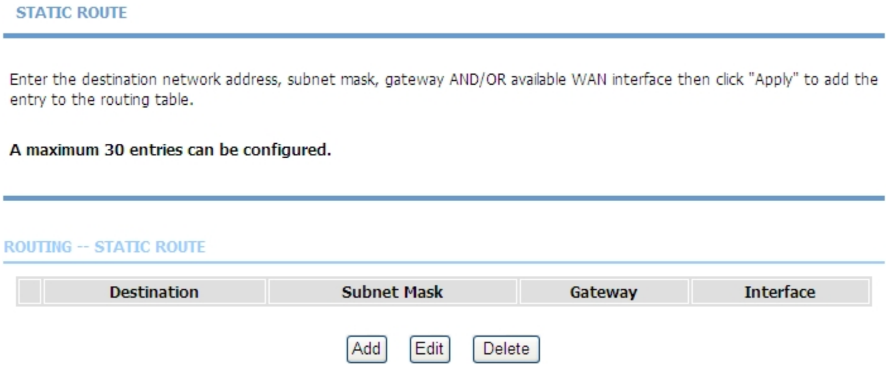
RIPNG SETTINGS

RIPng Settings.

Figure 73

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.

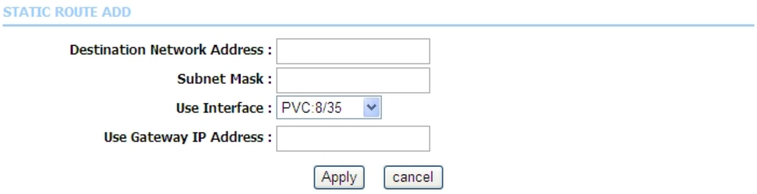
A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

Figure 74

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



STATIC ROUTE ADD

Destination Network Address :
Subnet Mask :
Use Interface : PVC:8/35
Use Gateway IP Address :

Figure 75

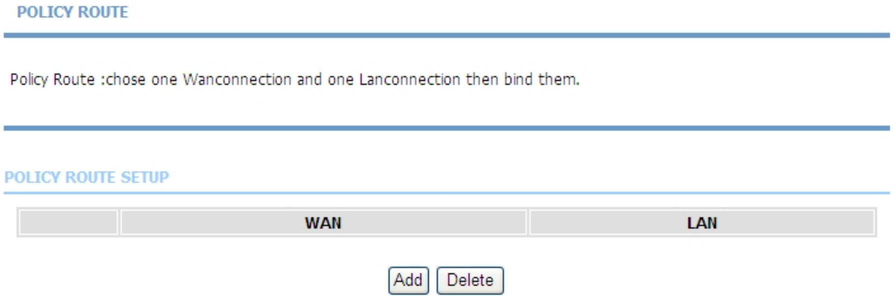
The following table describes the parameters of this page.

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

Click **Apply** to save the settings.

3.3.13.2 Policy Route

Choose **Advanced** > **Routing** and click **Policy Route**. The page shown in the following figure appears. The policy route binds one WAN connection and one LAN interface.



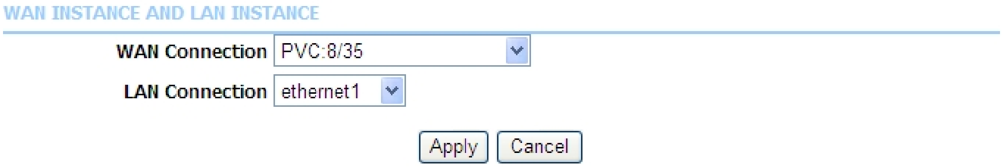
POLICY ROUTE

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

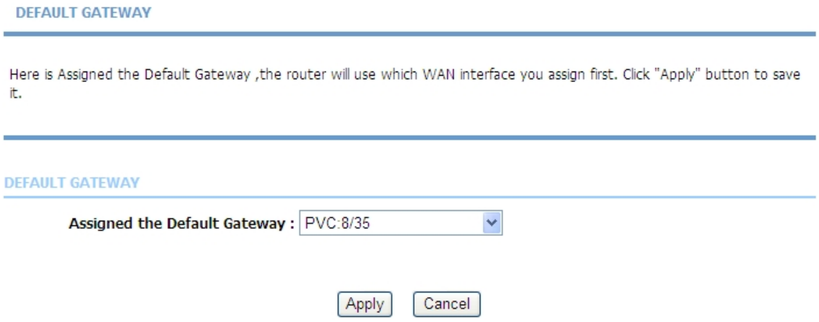
WAN Connection: PVC:8/35

LAN Connection: ethernet1

Figure 76

3.3.13.3 Default Gateway

Choose **Advanced** > **Routing** and click **Default Gateway**. The page shown in the following figure appears. You may assign a default gateway for the router to use first.



DEFAULT GATEWAY

Here is Assigned the Default Gateway ,the router will use which WAN interface you assign first. Click "Apply" button to save it.

DEFAULT GATEWAY

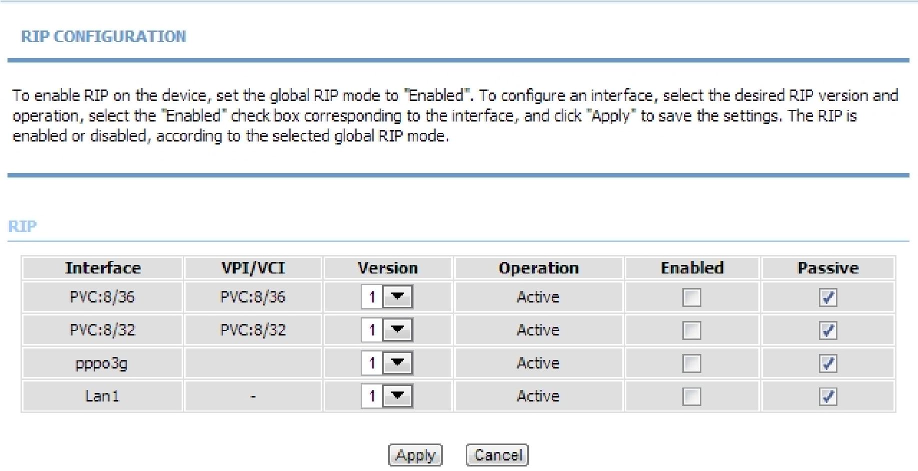
Assigned the Default Gateway : PVC:8/35

Figure 77

Click **Apply** to save the settings.

3.3.13.4 RIP

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 enable RIP on the device, set the global RIP mode to "Enabled". To configure an interface, select the desired RIP version and operation, select the "Enabled" check box corresponding to the interface, and click "Apply" to save the settings. The RIP is enabled or disabled, according to the selected global RIP mode.

RIP

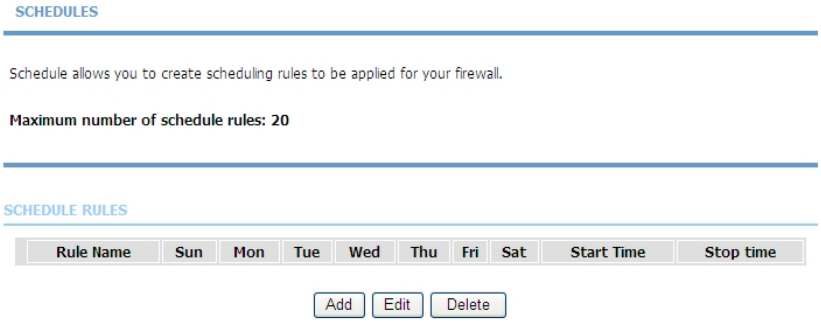
Interface	VPI/VCI	Version	Operation	Enabled	Passive
PVC:8/36	PVC:8/36	1	Active	□	☑
PVC:8/32	PVC:8/32	1	Active	□	☑
pppo3g		1	Active	□	☑
Lan1	-	1	Active	□	☑

Figure 78

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.

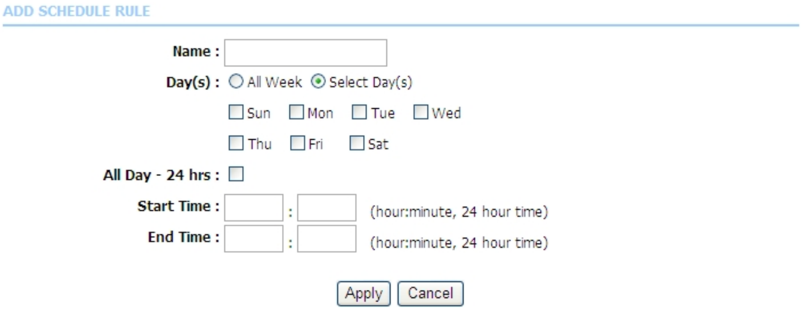
Maximum number of schedule rules: 20

SCHEDULE RULES

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

Figure 79

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



ADD SCHEDULE RULE

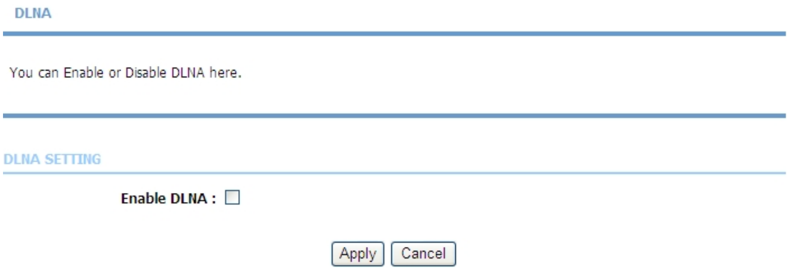
Name :
Day(s) : ○ All Week ● Select Day(s)
□ Sun □ Mon □ Tue □ Wed
□ Thu □ Fri □ Sat
All Day - 24 hrs : □
Start Time : : (hour:minute, 24 hour time)
End Time : : (hour:minute, 24 hour time)

Figure 80

Click **Apply** to save the settings.

3.3.15 DLNA

Choose **Advanced** > **DLNA**. The page shown in the following figure appears. In this page, you can choose to enable DLNA and click **Apply**.



DLNA

You can Enable or Disable DLNA here.

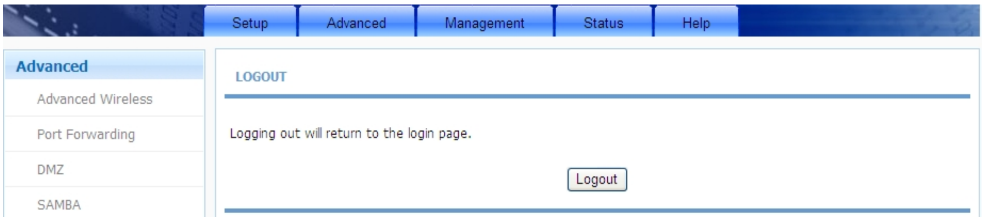
DLNA SETTING

Enable DLNA : □

Figure 81

3.3.16 Logout

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 return to the login page.

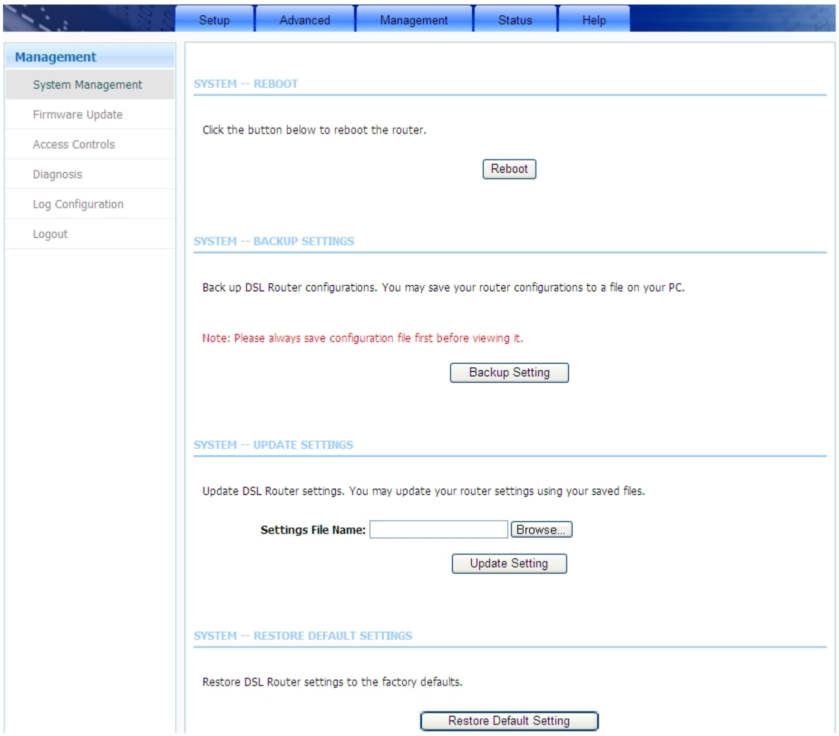
Figure 82

3.4.- Management

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure. The submenus are **System Managemen**t, **Firmware Update**, **Access Controls**, **Diagnosis**, **Log Configuration** and **Logout**.

3.4.1 System Management

Choose **Management** > **System Management**. The 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.

Figure 83

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

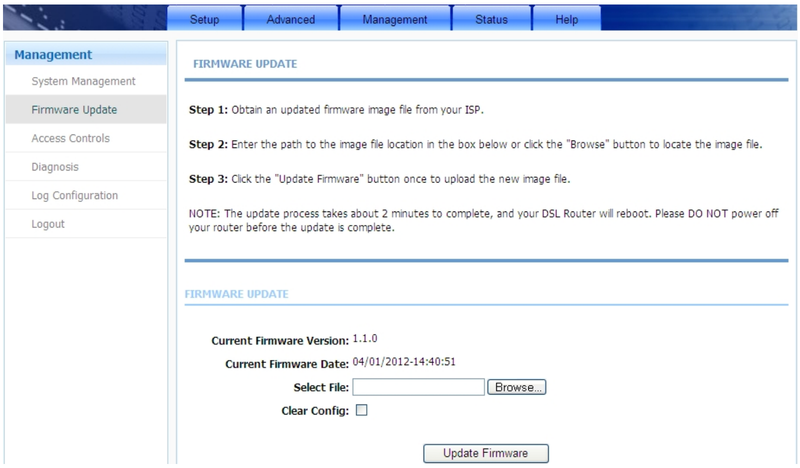
The buttons in this page are described as follows.

Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to 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 then click **Update Settings** to begin updating the device configuration.
Restore Default Setting	Click this button to reset the device to default settings.

Note:
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: 1.1.0
Current Firmware Date: 04/01/2012-14:40:51
Select File:
Clear Config: □

To update the firmware, take the following steps.

Step 1 Click **Browse...**to find the file.

Step 2 Select **Click Config**.

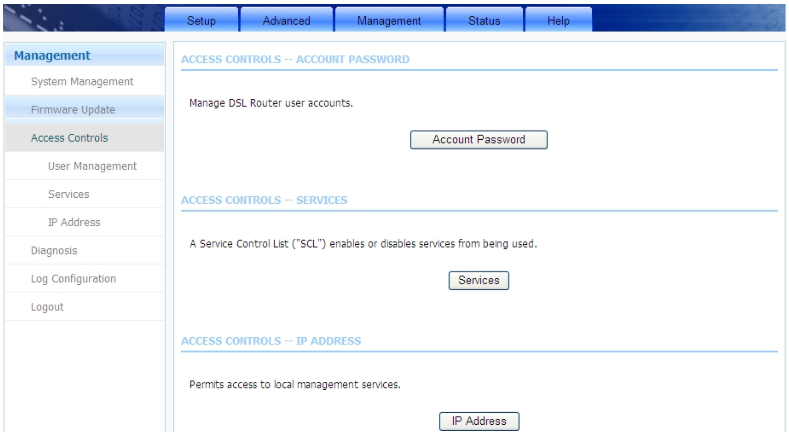
Step 3 Click **Update Firmware** to copy the file.

The device loads the file and reboots automatically.

Note:
Do not turn off your device or press the Reset button while an operation in this page 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 **User Management**, **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.

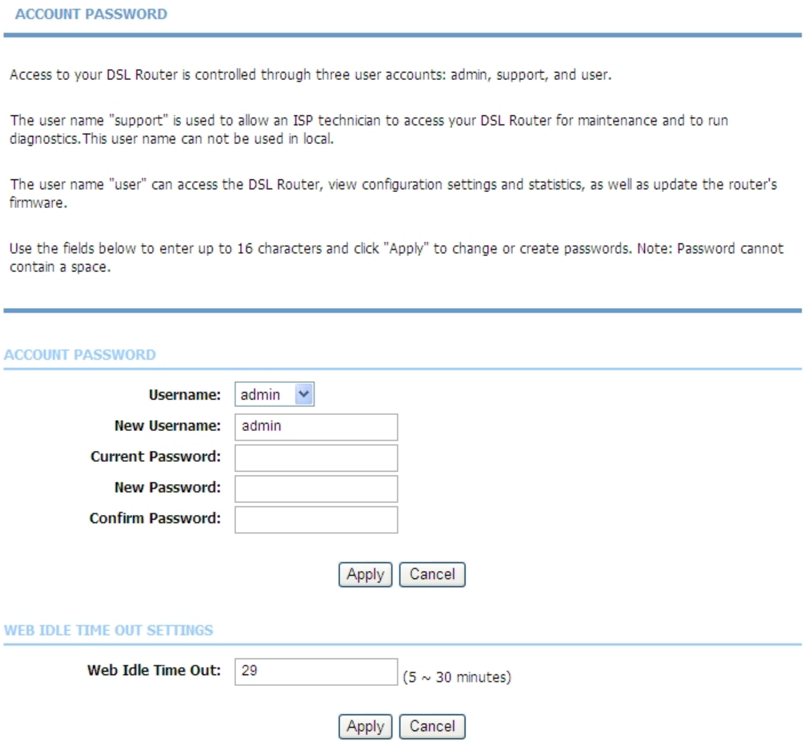
ACCESS CONTROLS -- IP ADDRESS

Permits access to local management services.

Figure 84

3.4.3.1 Account Password

In the **Access Controls** page, click **Account Password**. 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)

Figure 85

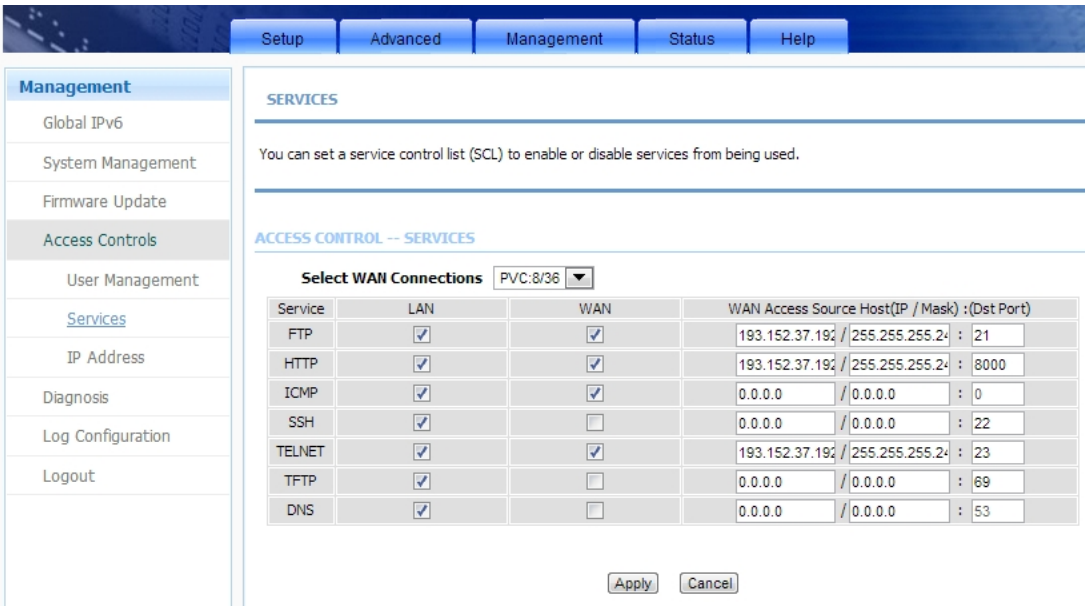
You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings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

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

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

You can set a service control list (SCL) to enable or disable services from being used.

ACCESS CONTROL -- SERVICES

Select WAN Connections PVC:8/36

Service	LAN	WAN	WAN Access Source Host(IP / Mask) :(Dst Port)
FTP	☑	☑	193.152.37.192 / 255.255.255.24 : 21
HTTP	☑	☑	193.152.37.192 / 255.255.255.24 : 8000
ICMP	☑	☑	0.0.0.0 / 0.0.0.0 : 0
SSH	☑	□	0.0.0.0 / 0.0.0.0 : 22
TELNET	☑	☑	193.152.37.192 / 255.255.255.24 : 23
TFTP	☑	□	0.0.0.0 / 0.0.0.0 : 69
DNS	☑	□	0.0.0.0 / 0.0.0.0 : 53

Figure 86

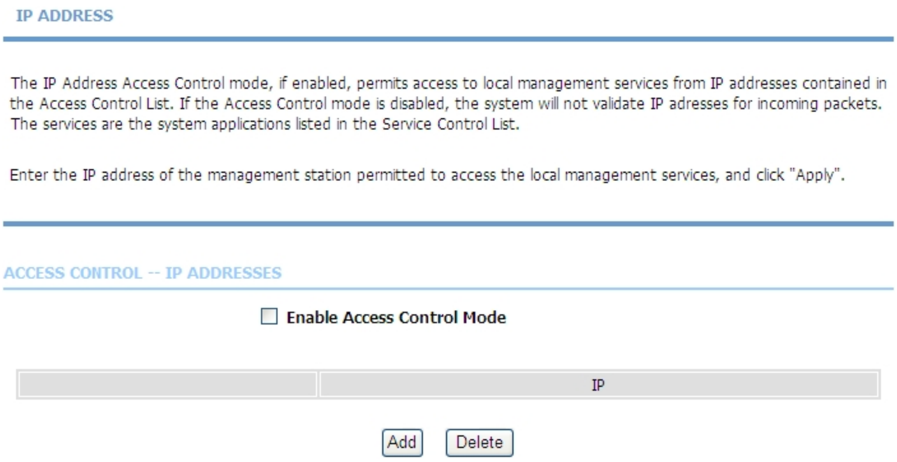
In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

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

Figure 87

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.

Tick **Enable Access Control Mode** to enable ACL.

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

To add an IP address to the IP list, cick **Add**. The page shown in the following figure appears.

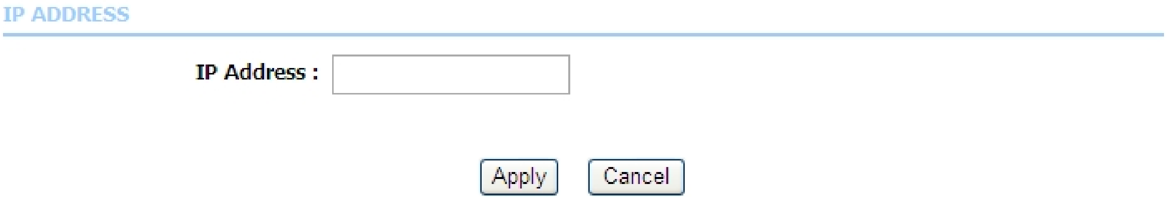
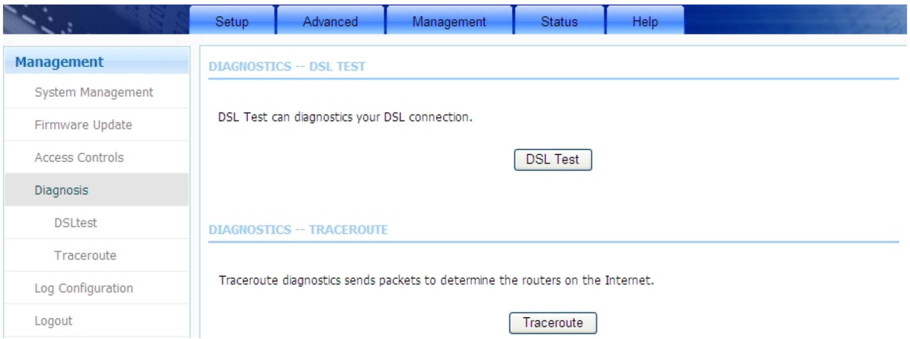


Figure 88

Click **Apply** to apply the settings.

3.4.4 Diagnosis

Choose **Management** > **Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test** and **Traceroute**.



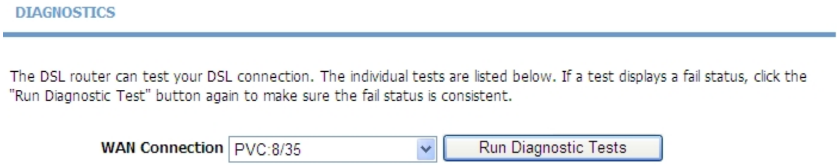
DSL Test can diagnostics your DSL connection.

Traceroute diagnostics sends packets to determine the routers on the Internet.

Figure 89

3.4.4.1 DSL Test

In the **Diagnosis** page, click **DSL Test**. The page shown in the following figure appears. In this page, you can test your DSL connection.

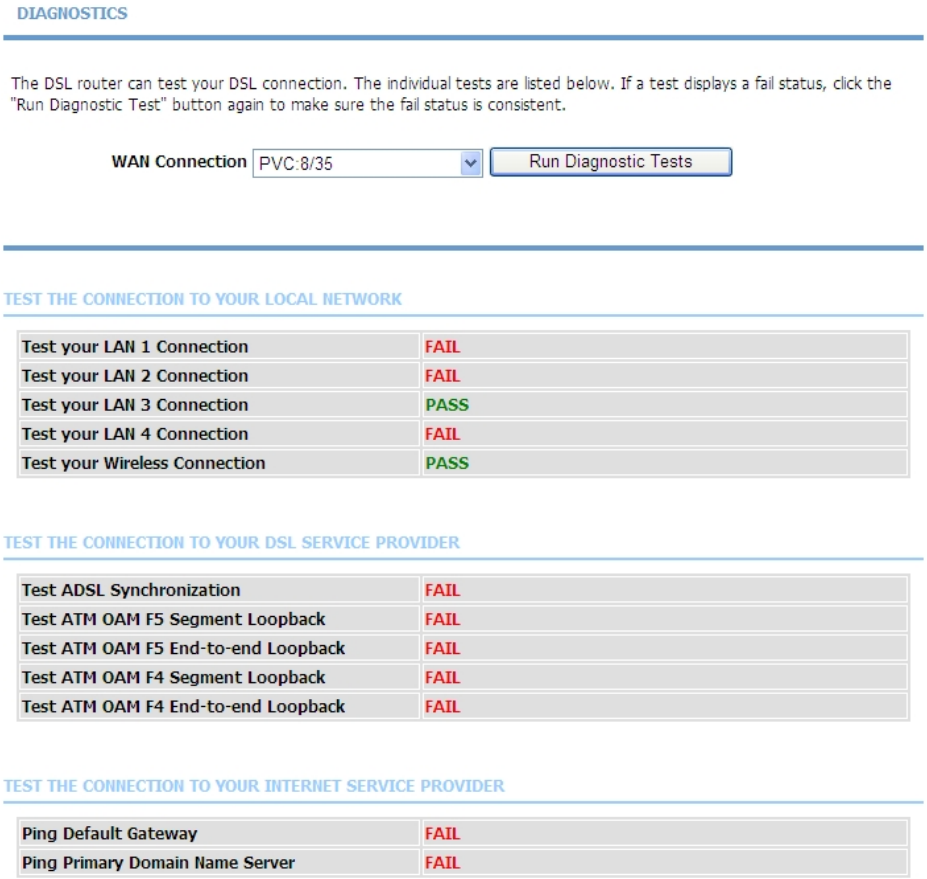


The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection PVC:8/35

Figure 90

Click **Run Diagnostic Tests**. After testing, 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: PVC:8/35

TEST THE CONNECTION TO YOUR LOCAL NETWORK

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

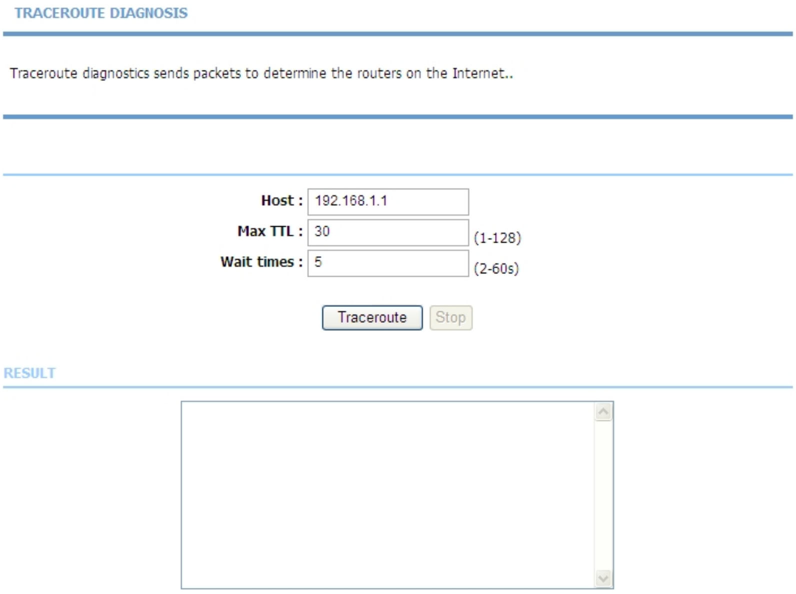
TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER

Ping Default Gateway	FAIL
Ping Primary Domain Name Server	FAIL

Figure 91

3.4.4.2 Traceroute

In the **Diagnosis** page, click **Traceroute**. The page shown in the following figure appears. In this page, you can determine the routers on the Internet by sending packets.



TRACEROUTE DIAGNOSIS

Traceroute diagnostics sends packets to determine the routers on the Internet..

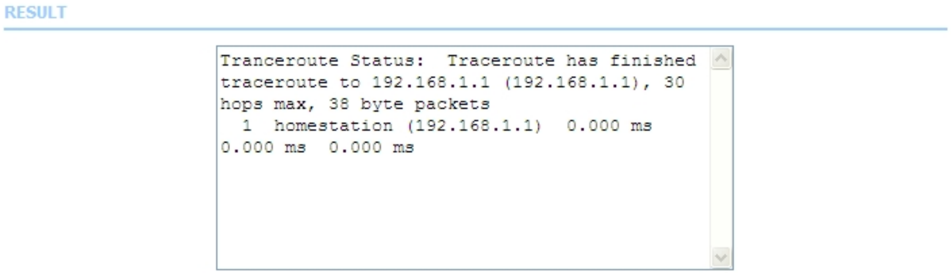
Host : 192.168.1.1

Max TTL : 30 (1-128)

Wait times : 5 (2-60s)

Figure 92

Click **Traceroute** to begin diagnosis. After finish, the page shown in the following figure appears.



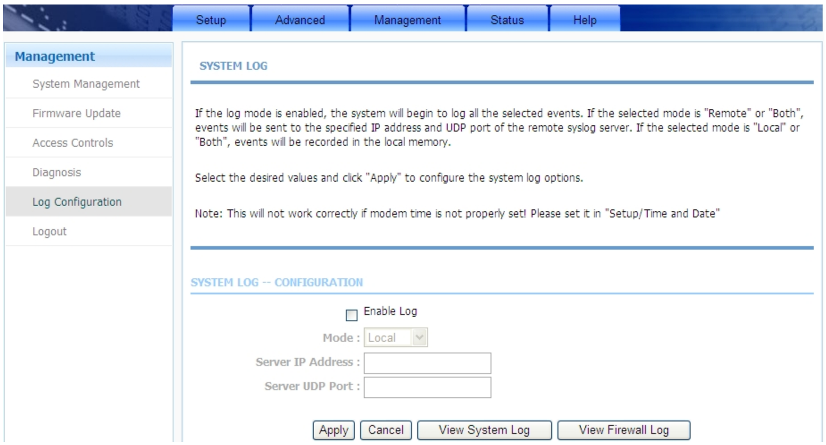
RESULT

```
Tranceroute Status:  Traceroute has finished
traceroute to 192.168.1.1 (192.168.1.1), 30
hops max, 38 byte packets
  1  homestation (192.168.1.1)  0.000 ms
0.000 ms  0.000 ms
```

Figure 93

3.4.5 Log Configuration

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 :

Figure 94

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.

To log the events, take the following steps.

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

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

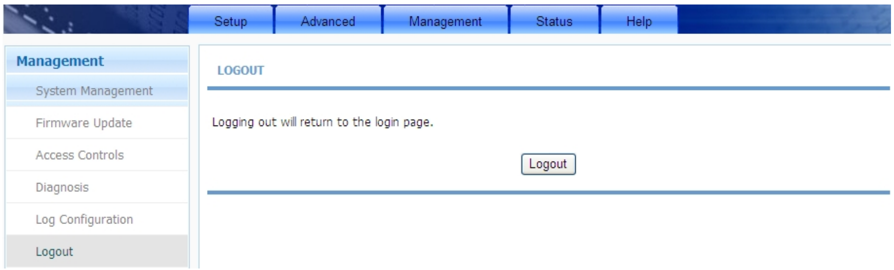
Step 3 Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

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 return to the login page.

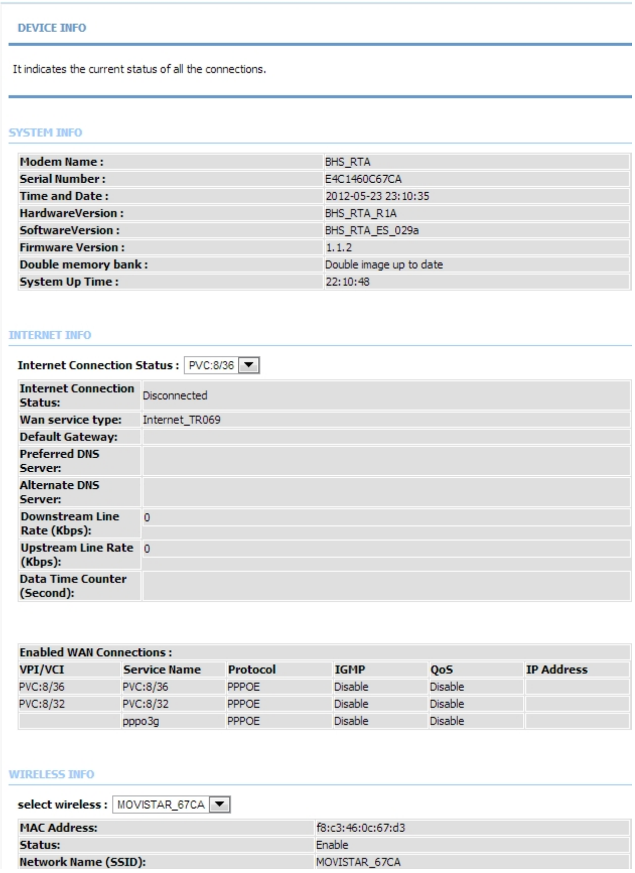
Figure 95

3.5.- Status

In the main interface, click **Status** tab to enter the **Status** menu as shown in the following figure. The submenus are **Device Info**, **Wireless Clients**, **DHCP clients**, **Logs**, **Statistics**, **Route Info** and **Logout**. 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

It indicates the current status of all the connections.

SYSTEM INFO

Modem Name :	BHS_RTA
Serial Number :	E4C1460C67CA
Time and Date :	2012-05-23 23:10:35
HardwareVersion :	BHS_RTA_R1A
SoftwareVersion :	BHS_RTA_ES_029a
Firmware Version :	1.1.2
Double memory bank :	Double image up to date
System Up Time :	22:10:48

INTERNET INFO

Internet Connection Status : PVC:8/36

Internet Connection Status:	Disconnected
Wan service type:	Internet_TR069
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0
Data Time Counter (Second):	

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
PVC:8/36	PVC:8/36	PPPOE	Disable	Disable	
PVC:8/32	PVC:8/32	PPPOE	Disable	Disable	
	pppo3g	PPPOE	Disable	Disable	

WIRELESS INFO

select wireless : MOVISTAR_67CA

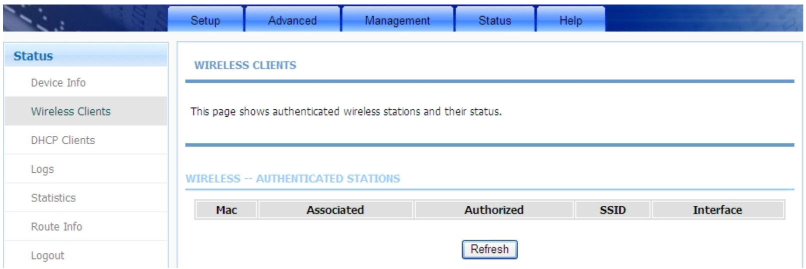
MAC Address:	f8:c3:46:0c:67:d3
Status:	Enable
Network Name (SSID):	MOVISTAR_67CA

Figure 96

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 figure appears. The page displays authenticated wireless stations and their statuses.



WIRELESS CLIENTS

This page shows authenticated wireless stations and their status.

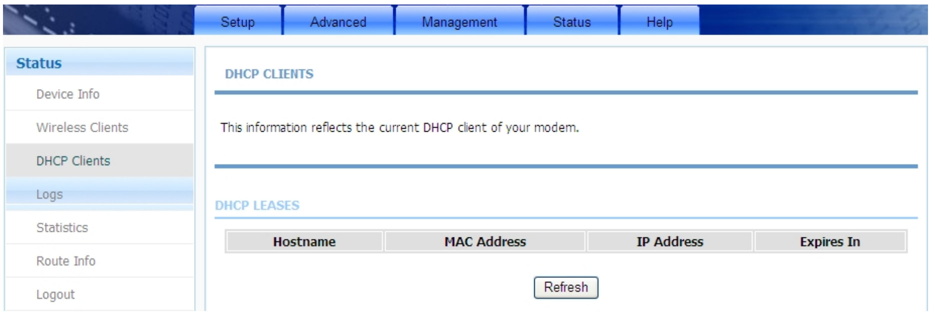
WIRELESS -- AUTHENTICATED STATIONS

Mac	Associated	Authorized	SSID	Interface

Figure 97

3.5.3 DHCP Clients

Choose **Status** > **DHCP Clients**. The page shown in the following figure appears. 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).



DHCP CLIENTS

This information reflects the current DHCP client of your modem.

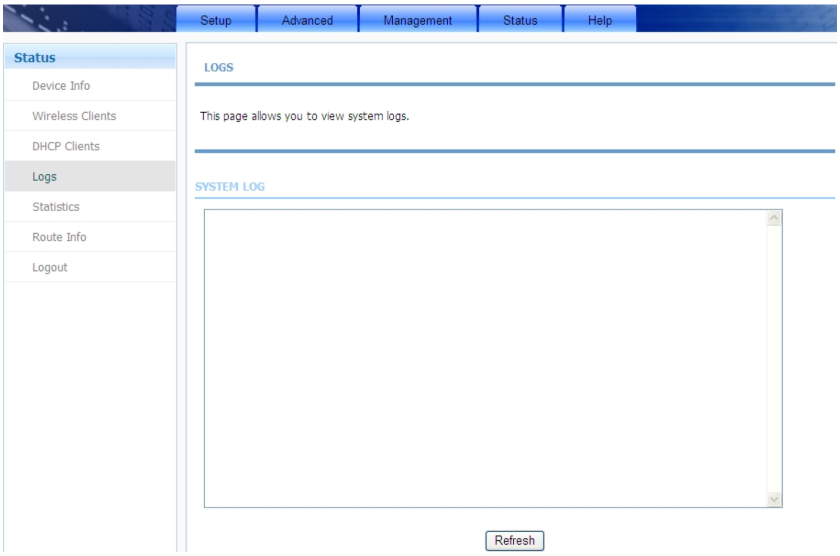
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

Figure 98

3.5.4 Logs

Choose **Status** > **Logs**. The page shown in the following figure appears. This page lists the system log. Click **Refresh** to refresh the system log shown in the table.



LOGS

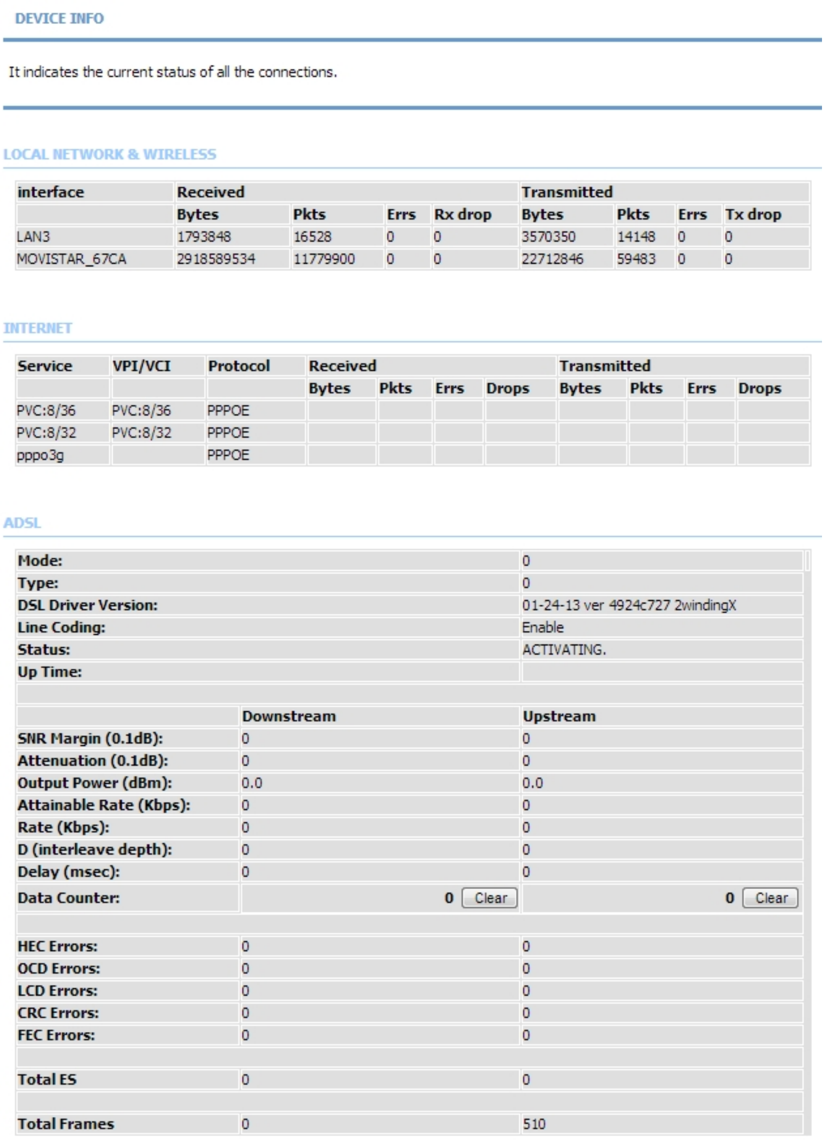
This page allows you to view system logs.

SYSTEM LOG

Figure 99

3.5.5 Statistics

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



DEVICE INFO

It indicates the current status of all the connections.

LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN3	1793848	16528	0	0	3570350	14148	0	0
MOVISTAR_67CA	2918589534	11779900	0	0	22712846	59483	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
PVC:8/36	PVC:8/36	PPPOE								
PVC:8/32	PVC:8/32	PPPOE								
pppo3g		PPPOE								

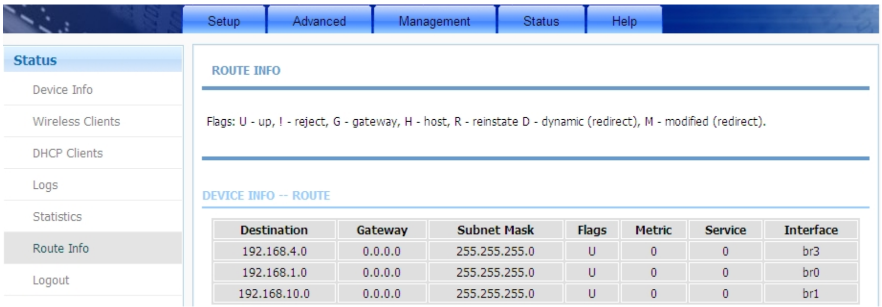
ADSL

Mode:		0
Type:		0
DSL Driver Version:		01-24-13 ver 4924c727 2windingX
Line Coding:		Enable
Status:		ACTIVATING.
Up Time:		
	Downstream	**Upstream**
SNR Margin (0.1dB):	0	0
Attenuation (0.1dB):	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
Data Counter:	**0** Clear	**0** Clear
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
CRC Errors:	0	0
FEC Errors:	0	0
Total ES	0	0
Total Frames	0	510

Figure 100

3.5.6 Route Info

Choose **Status** > **Route Info**. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.



ROUTE INFO

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

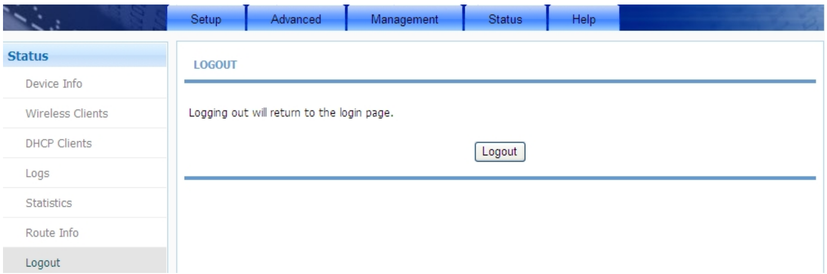
DEVICE INFO -- ROUTE

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.4.0	0.0.0.0	255.255.255.0	U	0	0	br3
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	br1

Figure 101

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.

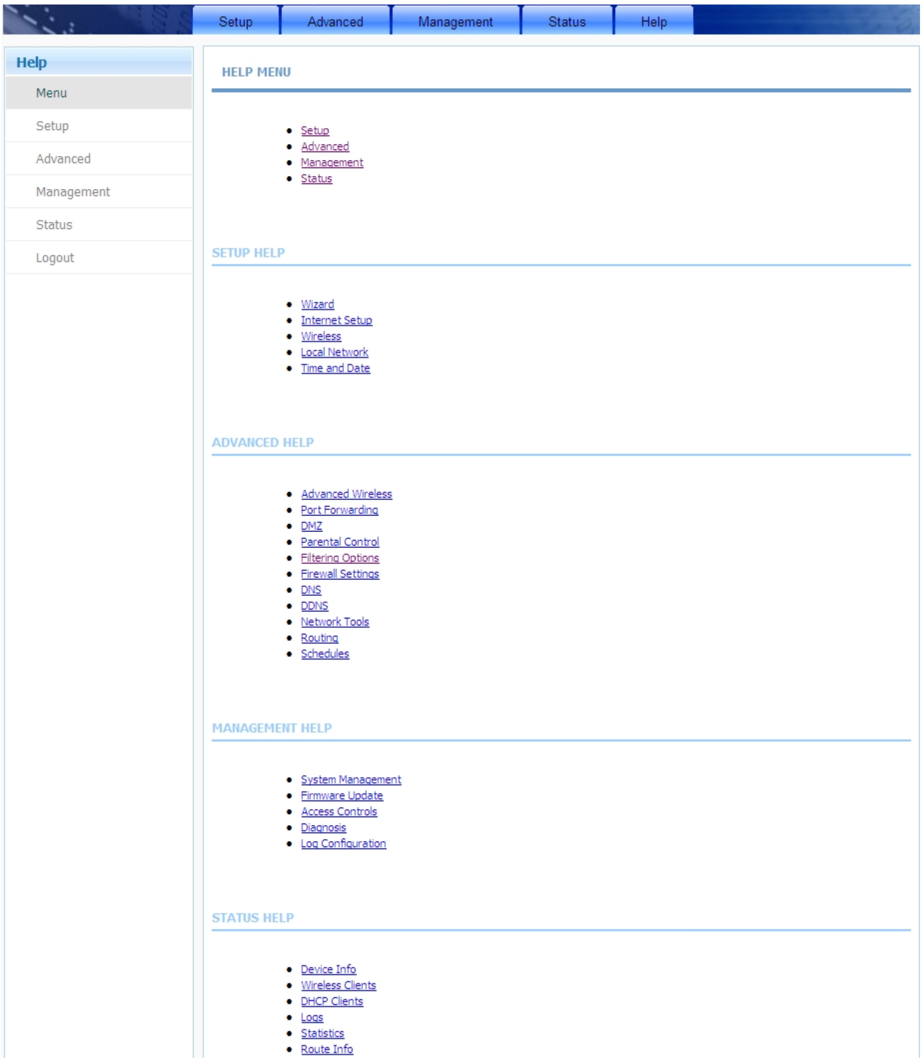


Logging out will return to the login page.

Figure 102

3.6.- Help

In the main interface, click **Help** tab to enter the **Help** menu as shown in the following figure. This section provides detailed configuration information for the device. Click a wanted link to view corresponding information.


Setup
Advanced
Management
Status
Help
Help
Menu
Setup
Advanced
Management
Status
Logout
HELP MENU
Setup
Advanced
Management
Status
SETUP HELP
Wizard
Internet Setup
Wireless
Local Network
Time and Date
ADVANCED HELP
Advanced Wireless
Port Forwarding
DMZ
Parental Control
Filtering Options
Firewall Settings
DNS
DDNS
Network Tools
Routing
Schedules
MANAGEMENT HELP
System Management
Firmware Update
Access Controls
Diagnosis
Log Configuration
STATUS HELP
Device Info
Wireless Clients
DHCP Clients
Logs
Statistics
Route Info