150Mbps Wireless ADSL2/2+ Modem Router

AR-7284WnA / AR-7284WnB

User Manual

Version 1.0 / October, 2009

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. For more detailed information about this product, please refer to the User Manual on the CD-ROM. The software and specifications are subject to change without notice. Please visit our web site www.edimax.com for the update. All rights reserved including all brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders .

Notice according to GNU/GPL-Version 2

Contents

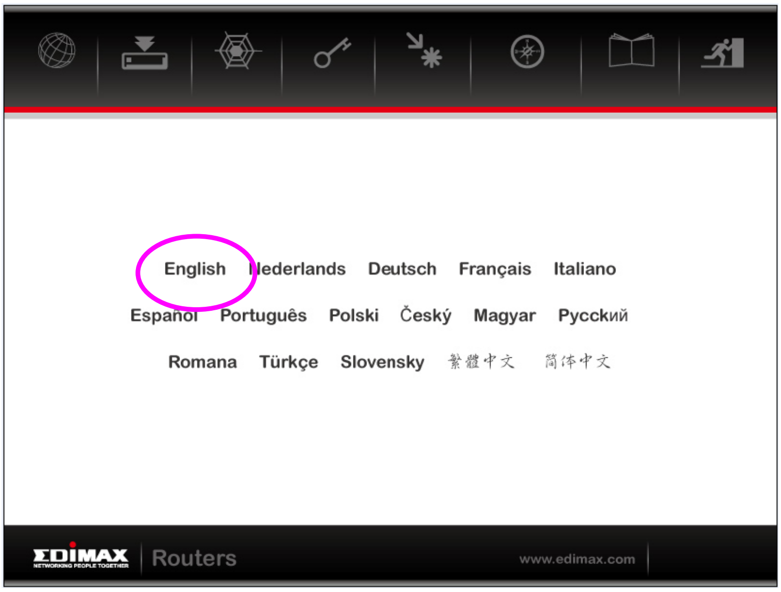
1 Introduction

The AR-7284WnA supports AnnexA mode. It provides four 10/100 base-T Ethernet ports for user. The device provides high-speed ADSL2+ broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps.

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

You can configure the router by running the Setup Wizard in the CD-ROM provided in the package. The wizard provides quick setup for Internet connection, Ethernet WAN Internet connection, SSID, wireless security, firmware upgrade and changing router's password. When you start the Setup Wizard, you will get the following Welcome screen. Please choose the language to start with and follow the easy steps in the Wizard. No instruction for the Setup Wizard is given here.

If you lost the CD-ROM or you prefer the traditional web setup, please follow the procedures in Manual to configure the router



1.1 Package List

- 1 x AR-7284WnA or AR-7284WnB
- 1 x external splitter
- 1 x power adapter
- 2 x telephone cables (RJ-11)
- 1 x Ethernet cable (RJ-45)
- 1 x Quick Installation Guide(QIG)
- 1 x CD (Multi-languages EZmax Wiard / QIG , USB driver & English Manual)

1.2 Safety Cautions

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

- Use volume labels to mark the type of power.
- Only use the power adapter packed within the device package.
- Pay attention to the power load of the electric outlet or power extension cord. An overloaded power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it as soon as possible.
- It’s necessary to prepare proper space for heat dissipation to avoid damage caused by overheating. The long and thin holes on the device are designed for heat dissipation and to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device in high temperature environment and avoid direct sunlight.
- Do not put this device in humid or watery environment. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do so, because any wrong connection may lead to electric or fire risk.
- Do not place this device on an unstable surface.

1.3 LEDs and Interfaces

Front Panel

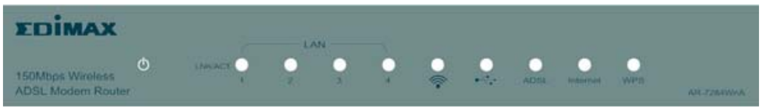


Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
⏻	Green	Off	The power is off.
		On	The power is on and the initialization is normal.
	Red	On	The device is initiating.
		Blinks	The firmware is upgrading.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blinks	Data is being transmitted through the LAN interface.
		On	The connection of LAN interface is normal.
📶	Green	Off	No WLAN connection.
		Blinks	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
⑂	Green	Off	No USB signal is detected.
		Blinks	Data is passing through USB port.
		On	The USB interface is ready.
ADSL	Green	Off	Initial self-test is failed.
		Blinks	The device is detecting DSL signal.
		On	The DSL line connection is established.
Internet	Green	Off	The device is running under Bridge

LED	Color	Status	Description
			mode, DSL connection is not present, or the power is off.
		On	Connected to network.
	Red	On	Network connection failed.
WPS	Green	On	The WPS indicator will light for 5 minutes after the WPS service is registered successfully.
		Blink Green	● The WPS indicator will light for 0.2s, and then off for 0.1s when the WPS button is pressed and the network card is ready for register. ● The WPS indicator will blink every 0.1s to indicate the WPS service fails to register. ● The WPS indicator lights for 5 times and off for 0.5s to indicate there are two or more wireless network cards register at the same time.
		Off	WPS service is not ready or WPS service has been setup successfully.

Rear Panel

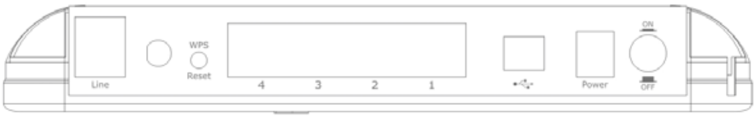


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
Line	RJ-11 interface that connects to the telephone set through the telephone cable.
WPS/Reset	● Press the button for 3 seconds to enable WPS. ● Press the button for 8 seconds to restore factory default configurations and reboot the device.
LAN1/2/3/4	Ethernet RJ-45 interface is connected to the Ethernet interfaces of computers or Ethernet devices.
⭠	USB device interface is connected to PC or other network devices.
Power	Power Jack that connects to power adapter. The power adapter output is: 12 V DC, 800 mA.
ON/OFF	Power switch.

1.4 System Requirements

Recommended system requirements are listed as follows:

- An 10 baseT/100BaseT Ethernet interface on your PC
- A hub or switch (connected to multiple PCs through one of Ethernet interfaces on this device)
- Operating system: Windows 98SE, Windows 2000, Windows ME, or Windows XP

- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.5 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- Zero installation PPP bridge mode (ZIPB)
- 1483B, 1483R, and MER access
- Multiple PVCs (up to eight), PVCs are independent
- Single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding PVC ports
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade via Web, TFTP and FTP
- Reset to the factory default setting
- DNS relay
- Virtual server
- DMZ
- Web user interface
- System status display
- PPP session PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Remote management
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP

2 Hardware Installation

2.1 Connecting the ADSL Router

Step 1 Connect the ‘Line’ port of the device and the ‘Modem’ port of the ADSL 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 the phone port on the wall (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connectto a telephone set.

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

Note:

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

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

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

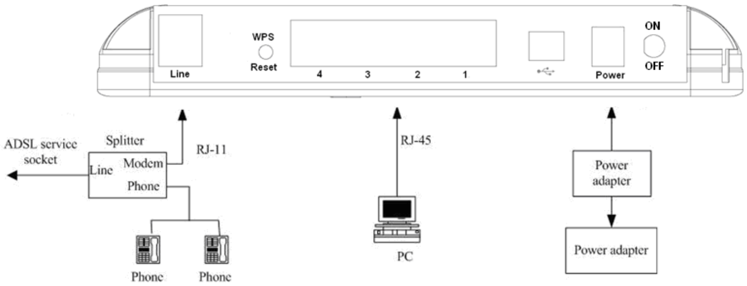


Figure 3 Connection diagram (without telephone sets before the splitter)

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

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

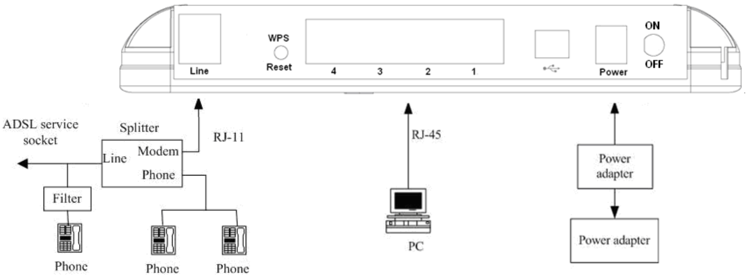


Figure 4 Connection diagram (with a telephone set before the splitter)

Connection 1 is recommended.

Note:

When connection type 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 before the splitter may cause connection problem 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 one microfilter.

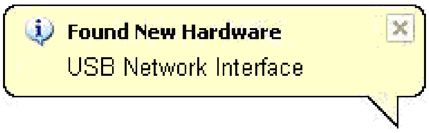
2.2 USB Installation

To connect the DSL gateway to the USB port of the PC, follow the instructions listed as follow:

Step 1 Connect one end of the USB cable to the USB port of the DSL gateway. As the cable has two different connectors and each connector is keyed, you may need to try both connectors and different orientations.

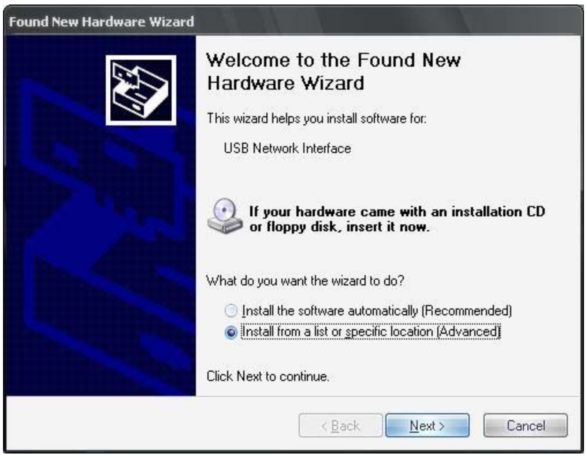
Step 2 Connect the other end of the USB cable into the USB port of the PC.

Step 3 For USB installation on Windows XP, once the PC powers up, a message appears in the system tray indicating that new hardware is found.



Found New Hardware
USB Network Interface

Step 4 The **Found New Hardware Wizard** dialog box appears. Select **Install the software automatically (Recommended)** and insert the Manual and Driver CD-ROM. Click **Next**. The system searches CD-ROM for the best USB driver.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

USB Network Interface

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

○ Install the software automatically (Recommended)

● Install from a list or specific location (Advanced)

Click Next to continue.

Step 5 The dialog will instruct you to choose driver from specific location.

3 About the Web Configurator

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

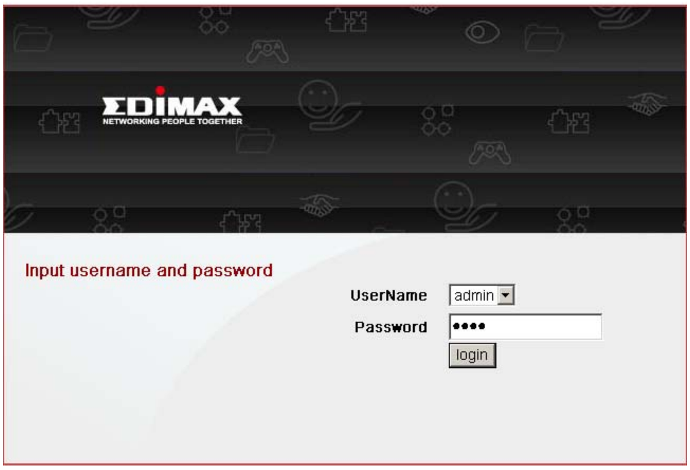
3.1 Access the Device

Follow the following instructions to access the device for the first time.

Step 1 Open the Internet Explorer (IE) browser and enter http://192.168.2.1.

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

- The user name and password of the super user are **admin** and **1234**.
- The user name and password of the normal user are **user** and **user.**

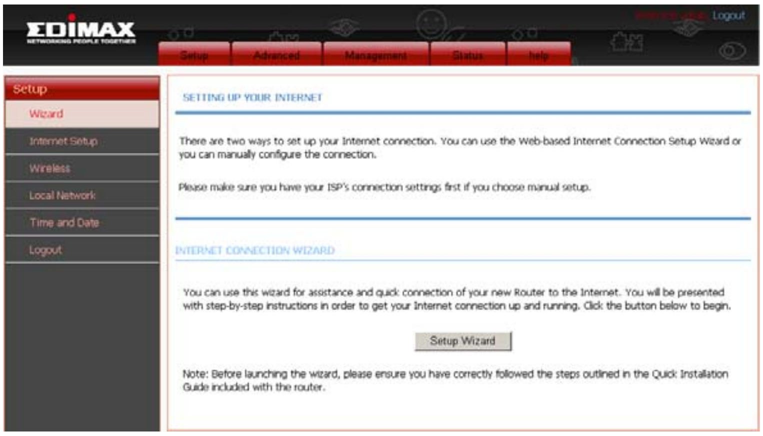


Input username and password

UserName admin

Password ••••

If you successfully logged in as the super user, the web page as 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.

Setup Wizard

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

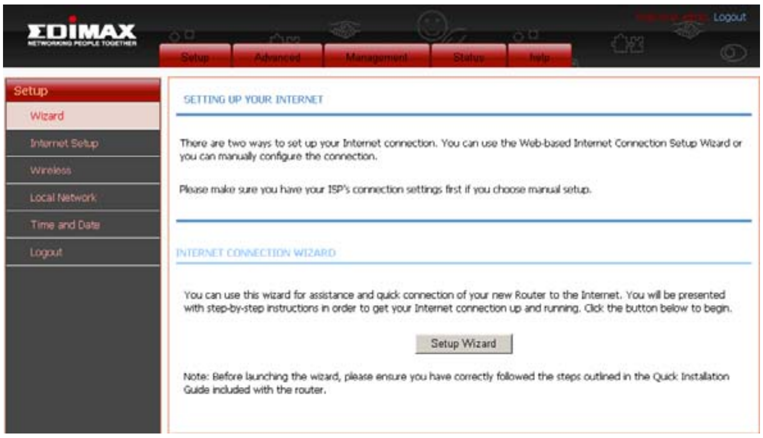
3.2 Setup

3.2.1 Wizard

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

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

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



SETTING UP YOUR INTERNET

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

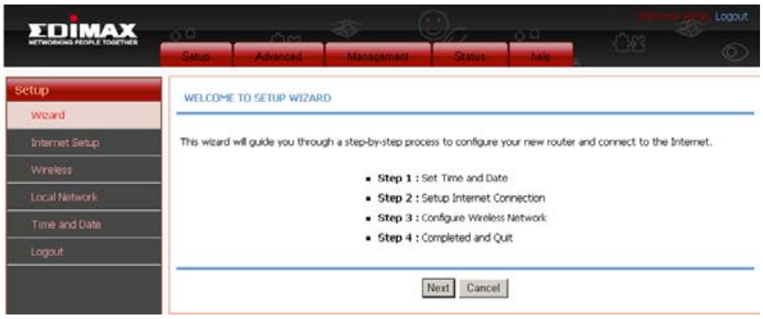
Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

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

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

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



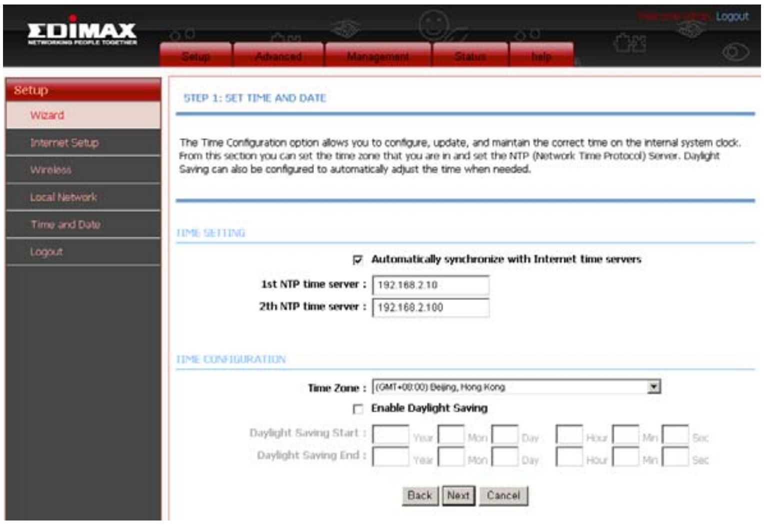
WELCOME TO SETUP WIZARD

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

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

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

Step 4 Set the time and date.



STEP 1: SET TIME AND DATE

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

TIME SETTING

☑ Automatically synchronize with Internet time servers

1st NTP time server : 192.168.2.10

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Time Zone : (GMT+08:00) Beijing, Hong Kong

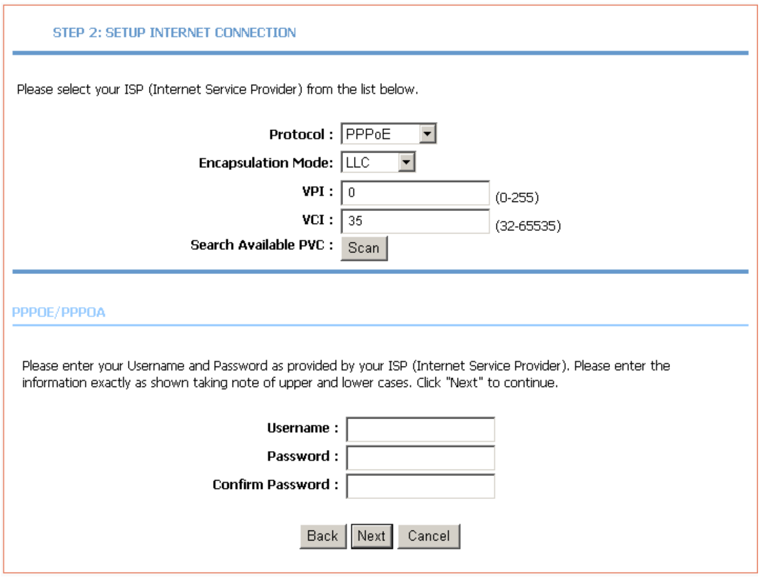
☐ Enable Daylight Saving

Daylight Saving Start : Year Mon Day Hour Min Sec

Daylight Saving End : Year Mon Day Hour Min Sec

Step 5 Configure the Internet connection.

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



STEP 2: SETUP INTERNET CONNECTION

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

Protocol : PPPoE

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC :

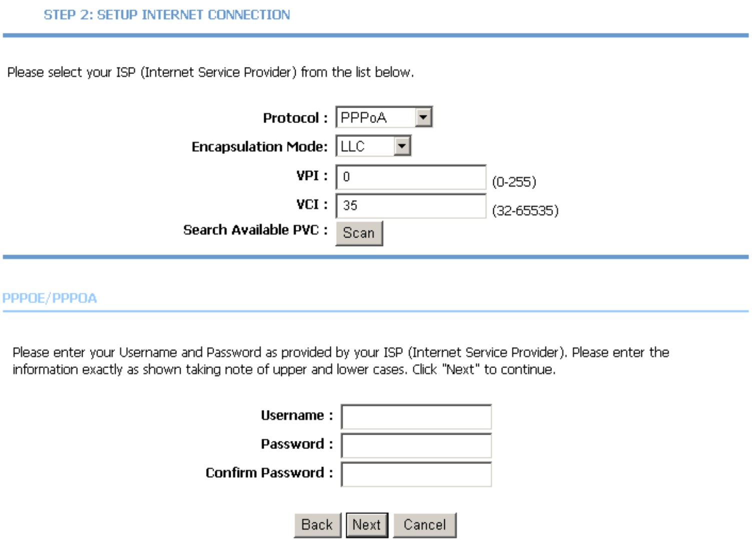
PPPOE/PPPOA

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 :



STEP 2: SETUP INTERNET CONNECTION

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

Protocol : PPPoA

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC :

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.

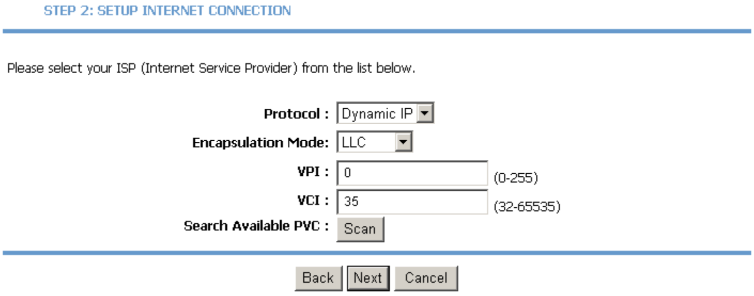
Username :

Password :

Confirm Password :

Set the user name and password here,which is 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

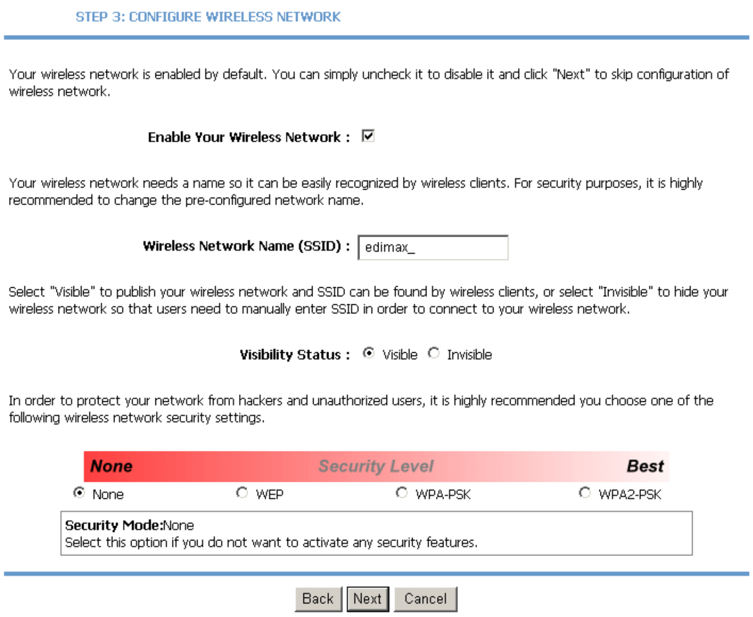
Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC :

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) : edimax_

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

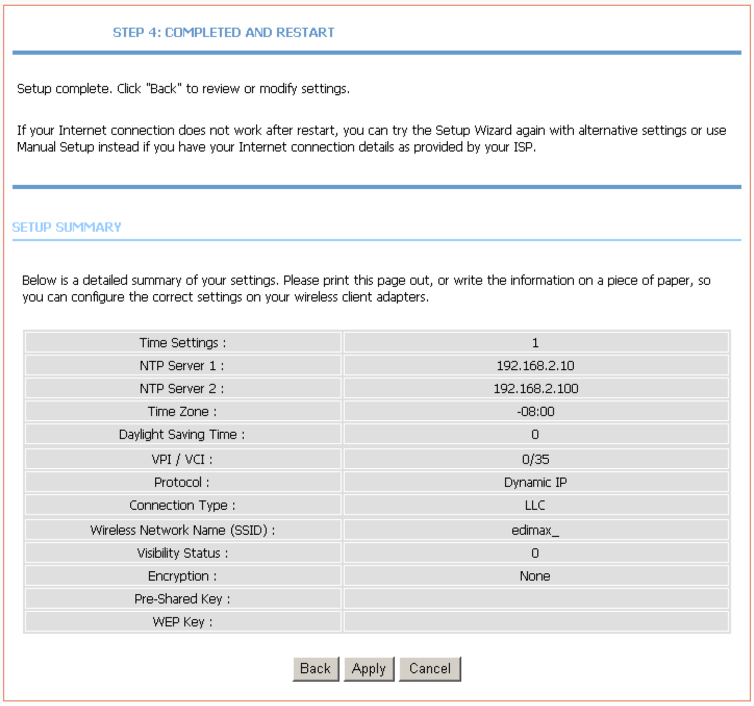
Visibility Status : ● Visible ○ Invisible

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

● None ○ WEP ○ WPA-PSK ○ WPA2-PSK

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

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



STEP 4: COMPLETED AND RESTART

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

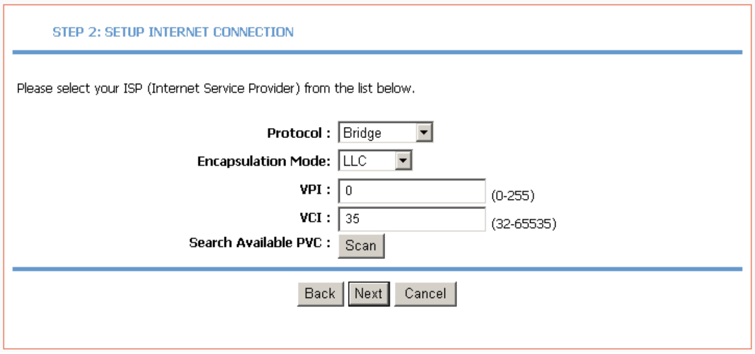
If your Internet connection does not work after restart, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

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

Time Settings :	1
NTP Server 1 :	192.168.2.10
NTP Server 2 :	192.168.2.100
Time Zone :	-08:00
Daylight Saving Time :	0
VPI / VCI :	0/35
Protocol :	Dynamic IP
Connection Type :	LLC
Wireless Network Name (SSID) :	edimax_
Visibility Status :	0
Encryption :	None
Pre-Shared Key :	
WEP Key :	

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

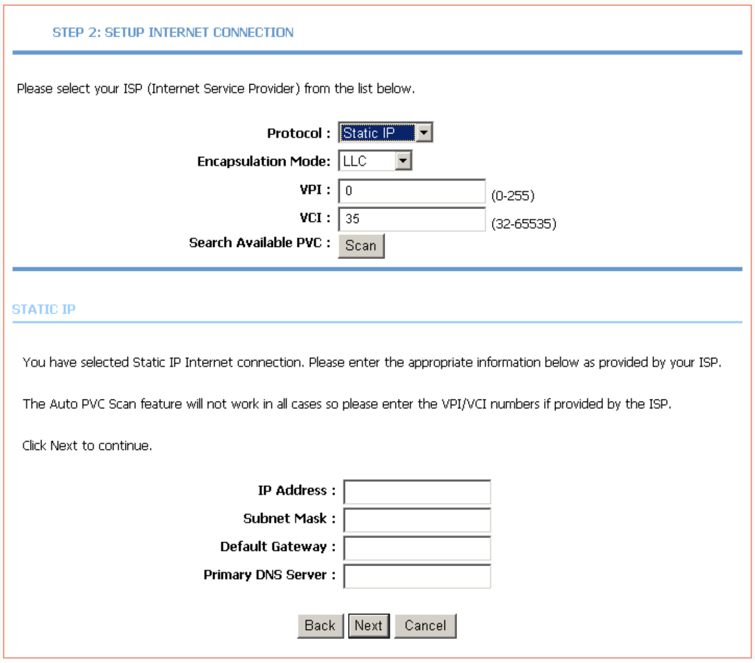
Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Scan

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 : 0 (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.

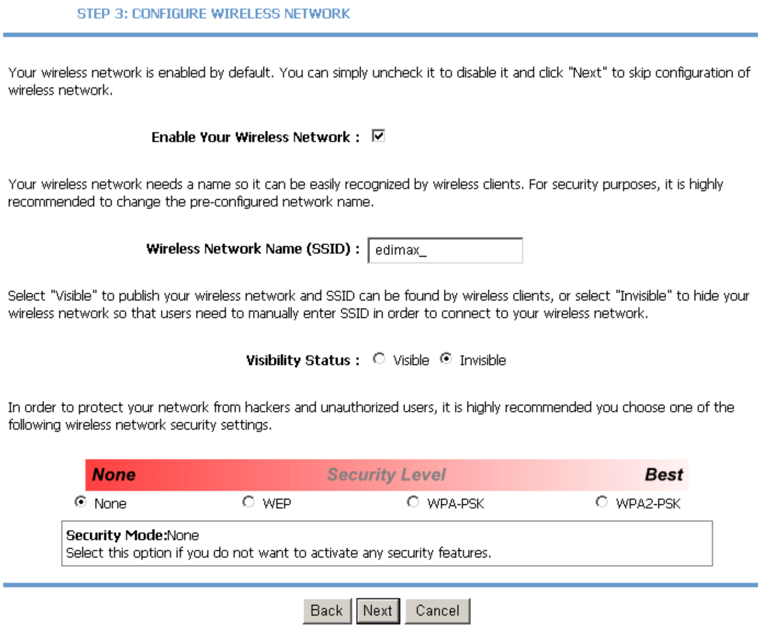
IP Address :

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 page appears.



STEP 3: CONFIGURE WIRELESS NETWORK

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

Enable Your Wireless Network : ☑

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

Wireless Network Name (SSID) : edimax_

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

Visibility Status : ○ Visible ● Invisible

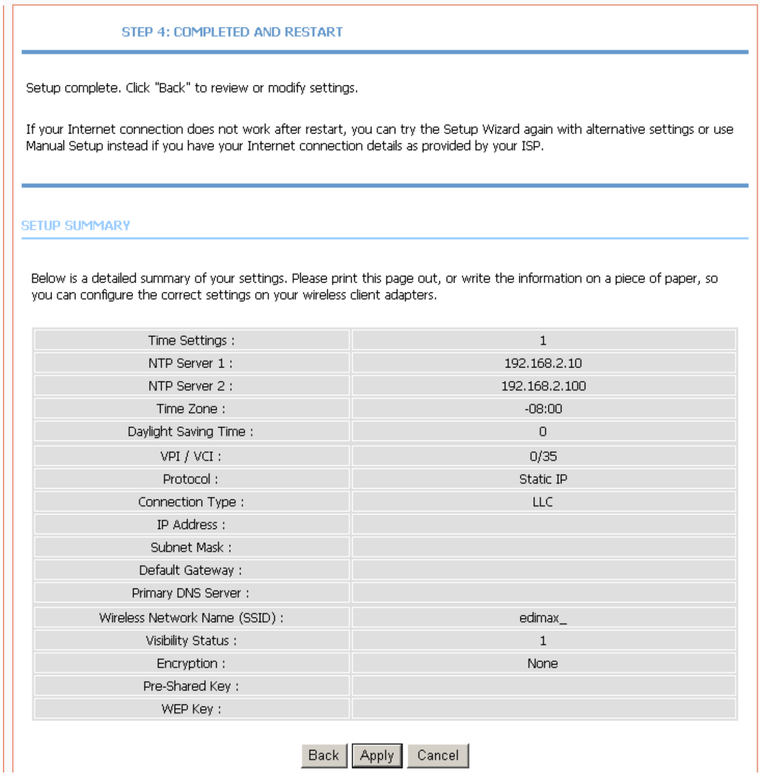
In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

● None ○ WEP ○ WPA-PSK ○ WPA2-PSK

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

Figure 5

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 after restart, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

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

Time Settings :	1
NTP Server 1 :	192.168.2.10
NTP Server 2 :	192.168.2.100
Time Zone :	-08:00
Daylight Saving Time :	0
VPI / VCI :	0/35
Protocol :	Static IP
Connection Type :	LLC
IP Address :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	
Wireless Network Name (SSID) :	edimax_
Visibility Status :	1
Encryption :	None
Pre-Shared Key :	
WEP Key :	

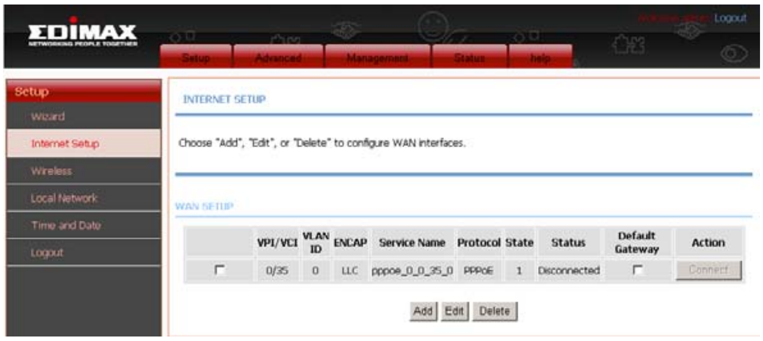
Step 7 When the settings are complete, click **Apply** to apply the settings.

Note:

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

3.2.2 Internet Setup

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



INTERNET SETUP

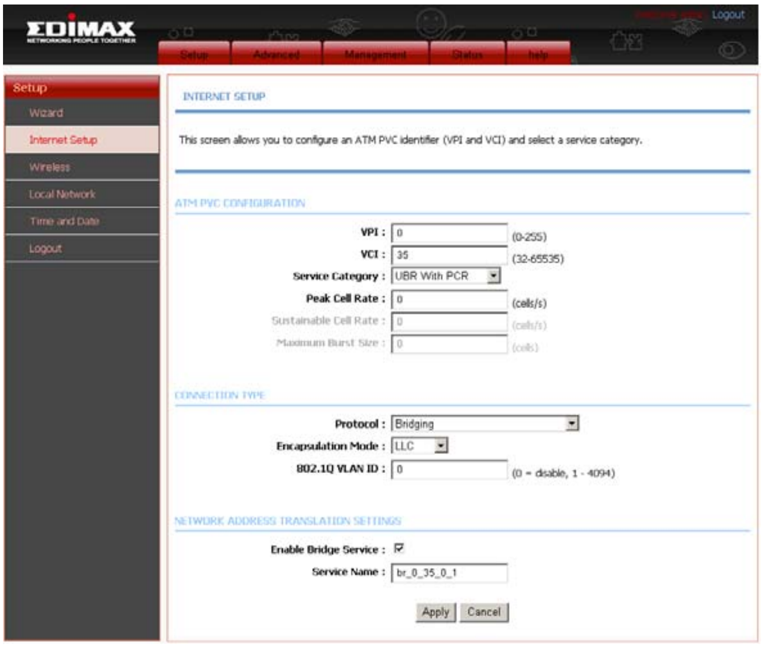
Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
□	0/35	0	LLC	pppoe_0_0_35_0	PPPoE	1	Disconnected	□	Connect

Add Edit Delete

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



INTERNET SETUP

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

ATM PVC CONFIGURATION

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

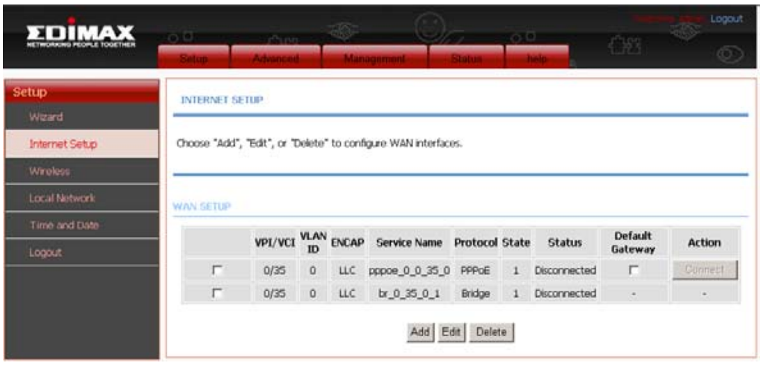
CONNECTION TYPE

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

NETWORK ADDRESS TRANSLATION SETTINGS

Enable Bridge Service : ☑
Service Name : br_0_35_0_1

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



INTERNET SETUP

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

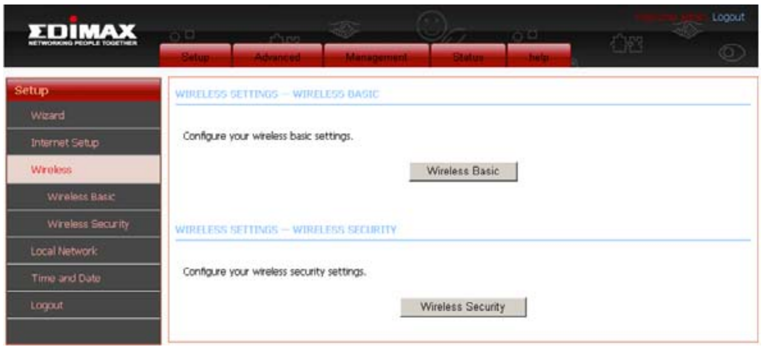
WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
□	0/35	0	LLC	pppoe_0_0_35_0	PPPoE	1	Disconnected	□	Connect
□	0/35	0	LLC	br_0_35_0_1	Bridge	1	Disconnected	-	-

3.2.3 Wireless Setup

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

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



WIRELESS SETTINGS -- WIRELESS BASIC

Configure your wireless basic settings.

Wireless Basic

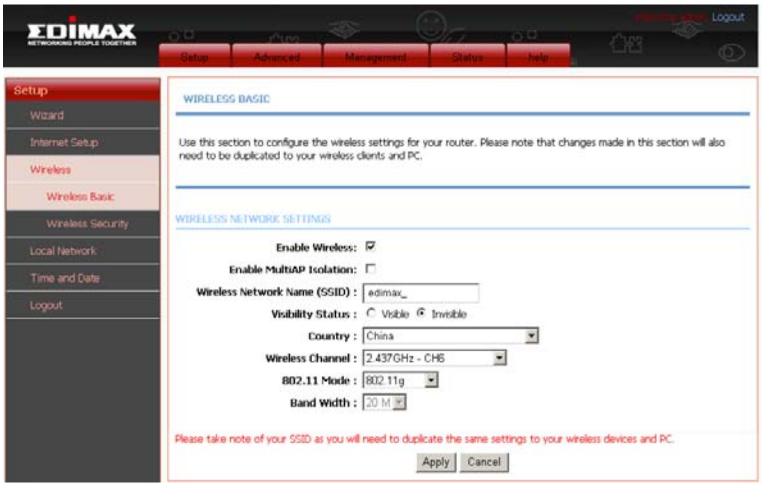
WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

Wireless Security

3.2.3.1 Wireless Basics

In the **Wireless Setup** page, click **Wireless Basics**. The page shown in the following figure appears. In this page, you can configure the parameters that wireless LAN clients can used to connect to this 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) : edimax_

Visibility Status : ○ Visible ● Invisible

Country : China

Wireless Channel : 2.437GHz - CH6

802.11 Mode : 802.11g

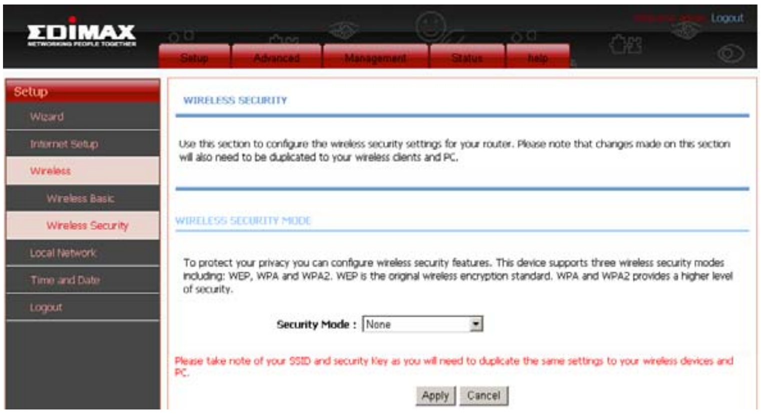
Band Width : 20 M

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

Click **Apply** to save the settings.

3.2.3.2 Wireless Security

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



WIRELESS SECURITY

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

WIRELESS SECURITY MODE

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

Security Mode : None

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

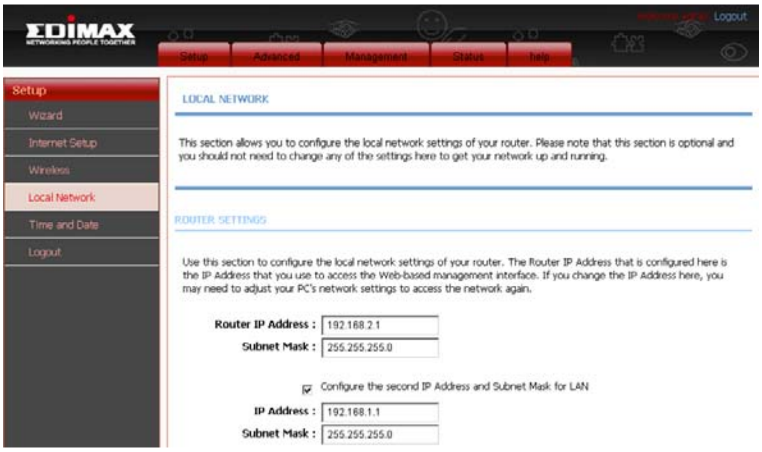
Click **Apply** to save the settings.

3.2.4 Local Network

You can configure the LAN IP address according to actual requirements. 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 as DHCP server on your LAN, the DHCP IP address pool 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

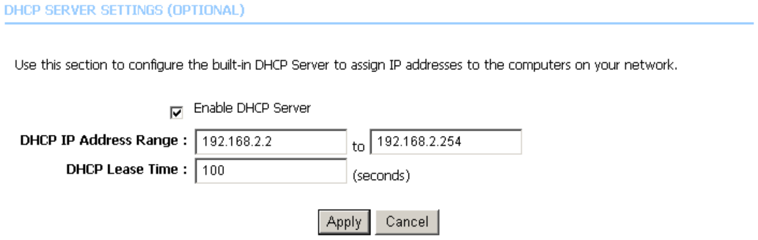
Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network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

Router IP Address : 192.168.2.1
Subnet Mask : 255.255.255.0

☑ Configure the second IP Address and Subnet Mask for LAN

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service will assign IP address to client computer connected to LAN interface. When the device acts as DHCP server, it will become the gateway of all computers on intranet. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP. The IP address pool can contain up to 253 IP addresses.



DHCP SERVER SETTINGS (OPTIONAL)

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

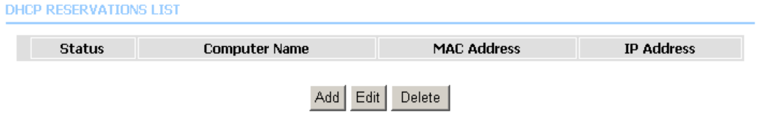
☑ Enable DHCP Server

DHCP IP Address Range : 192.168.2.2 to 192.168.2.254

DHCP Lease Time : 100 (seconds)

Click **Apply** to save the settings.

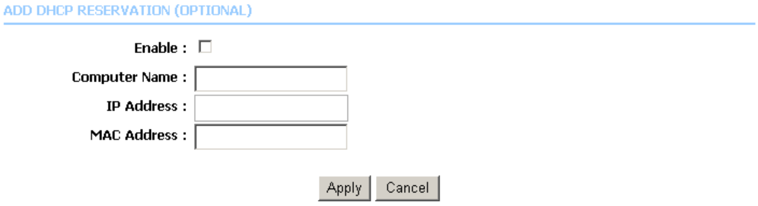
In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.



DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address

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



ADD DHCP RESERVATION (OPTIONAL)

Enable : □

Computer Name :

IP Address :

MAC Address :

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

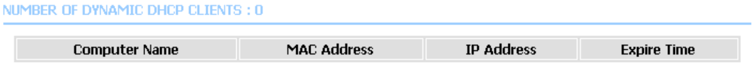
The **Computer Name** helps you to recognize the PC with the MAC address. For example: Father’s Laptop.

Click **Apply** to save the settings.

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

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

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

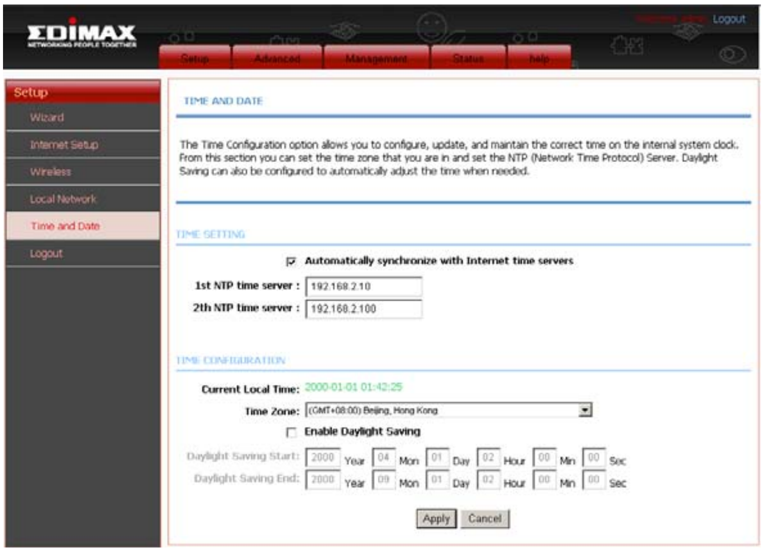


NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time

3.2.5 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 : 192.168.2.10

2th NTP time server : 192.168.2.100

TIME CONFIGURATION

Current Local Time: 2000-01-01 01:42:25

Time Zone: (GMT+08:00) Beijing, Hong Kong

☐ Enable Daylight Saving

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

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

In the **Time and Date** page, you can setup the time of the internal system clock. You can also set the time zone of the area of residence and the network time protocol (NTP) server. You can also configure daylight saving setting by selecting **Automatically synchronize with Internet time servers**.

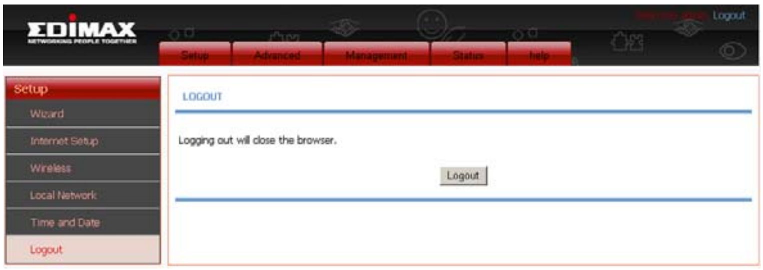
Select the specific time server and the time zone from the corresponding item in drop-down lists.

Select **Enable Daylight Saving** if necessary.

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 from web configuration menu.



LOGOUT

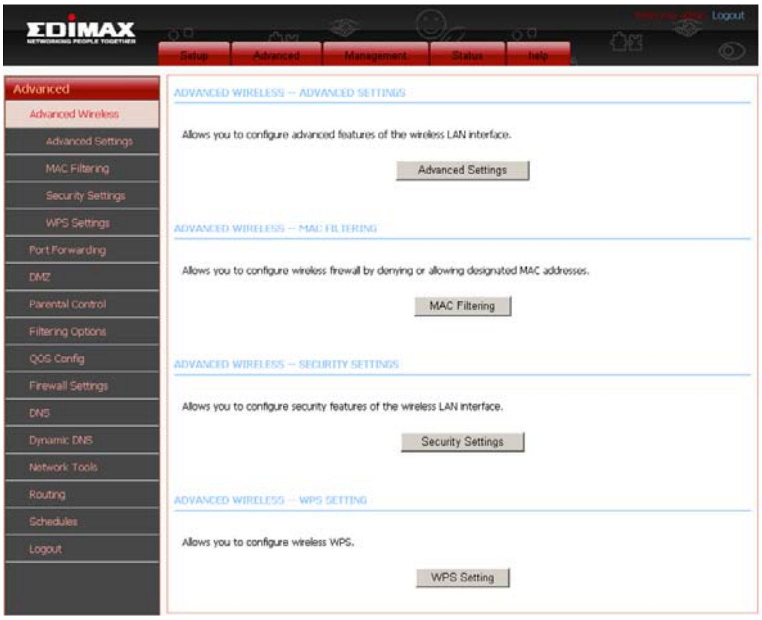
Logging out will close the browser.

3.3 Advanced

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

3.3.1 Advanced Wireless Settings

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



ADVANCED WIRELESS -- ADVANCED SETTINGS

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

ADVANCED WIRELESS -- MAC FILTERING

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

ADVANCED WIRELESS -- SECURITY SETTINGS

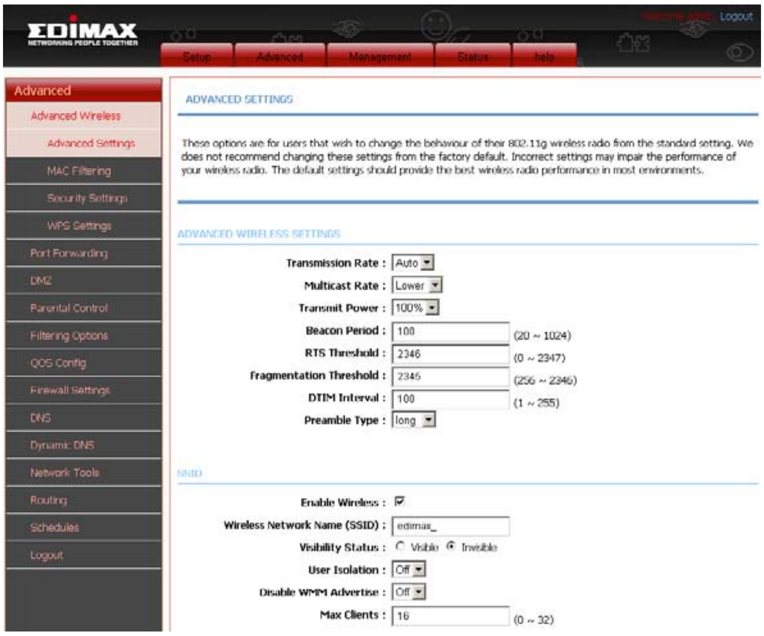
Allows you to configure security features of the wireless LAN interface.

ADVANCED WIRELESS -- WPS SETTING

Allows you to configure wireless WPS.

3.3.1.1 Advanced Settings

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



ADVANCED SETTINGS

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

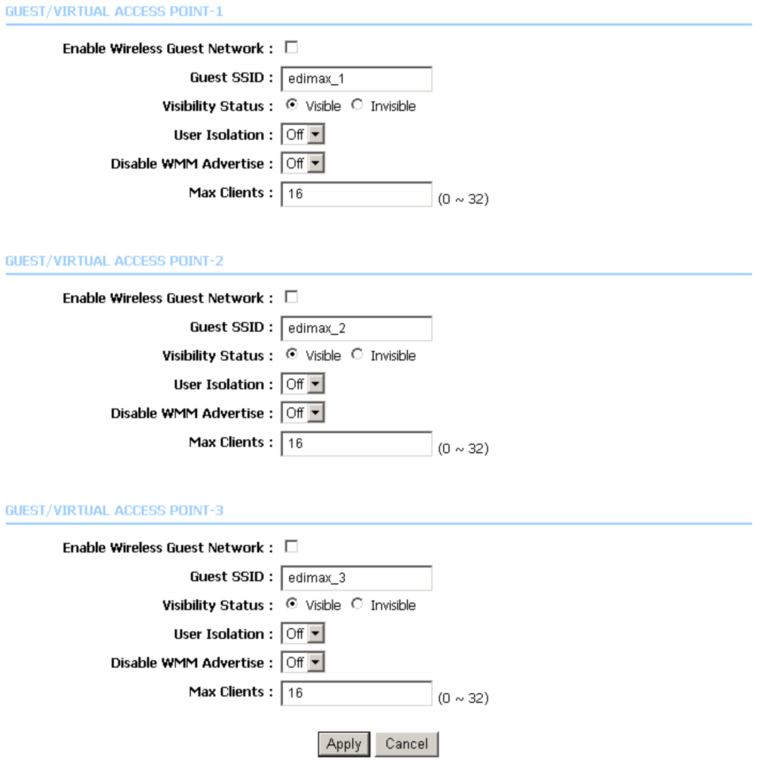
ADVANCED WIRELESS SETTINGS

Transmission Rate :	Auto	
Multicast Rate :	Lower	
Transmit Power :	100%	
Beacon Period :	100	(20 ~ 1024)
RTS Threshold :	2346	(0 ~ 2347)
Fragmentation Threshold :	2345	(256 ~ 2346)
DTIM Interval :	100	(1 ~ 255)
Preamble Type :	long	

SSID

Enable Wireless :	☑	
Wireless Network Name (SSID) :	edimax_	
Visibility Status :	○ Visible ● Invisible	
User Isolation :	Off	
Disable WMM Advertise :	Off	
Max Clients :	16	(0 ~ 32)

These settings are only for 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.



GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □

Guest SSID : edimax_1

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

Disable WMM Advertise : Off

Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □

Guest SSID : edimax_2

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

Disable WMM Advertise : Off

Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : □

Guest SSID : edimax_3

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

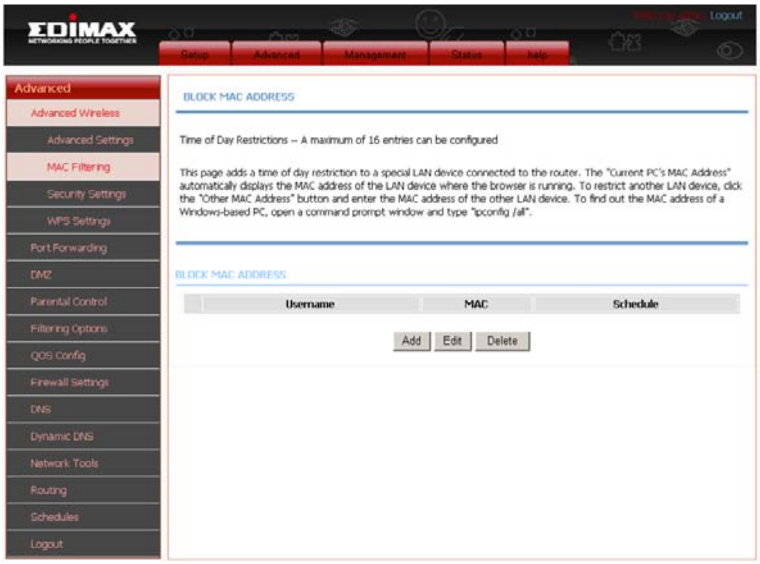
Disable WMM Advertise : Off

Max Clients : 16 (0 ~ 32)

Click **Apply** to save the settings.

3.3.1.2 MAC Filtering

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



BLOCK MAC ADDRESS

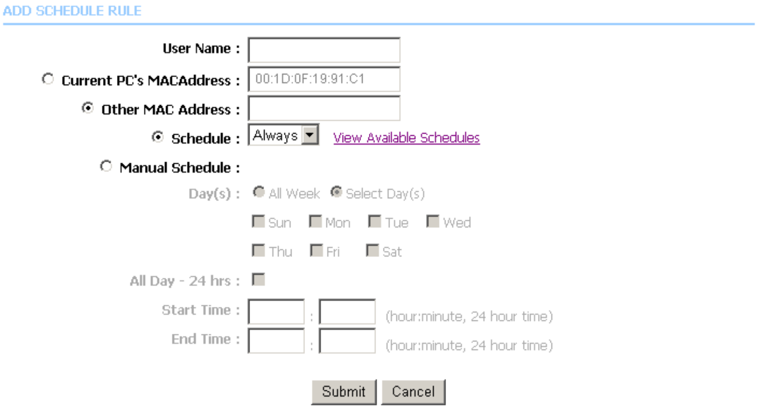
Time of Day Restrictions -- A maximum of 16 entries can be configured

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

BLOCK MAC ADDRESS

	Username	MAC	Schedule

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



ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:1D:0F:19:91:C1

● 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 : □

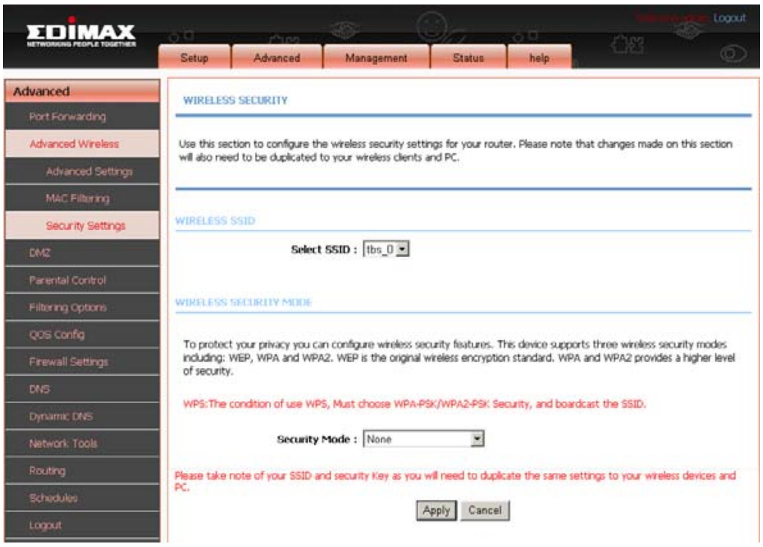
Start Time : : (hour:minute, 24 hour time)

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

Click **Apply** to save the settings.

3.3.1.3 Security Settings

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



WIRELESS SECURITY

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

WIRELESS SSID

Select SSID : tbs_0

WIRELESS SECURITY MODE

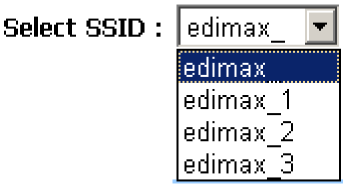
To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

WPS:The condition of use WPS, Must choose WPA-PSK/WPA2-PSK Security, and boardcast the SSID.

Security Mode : None

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

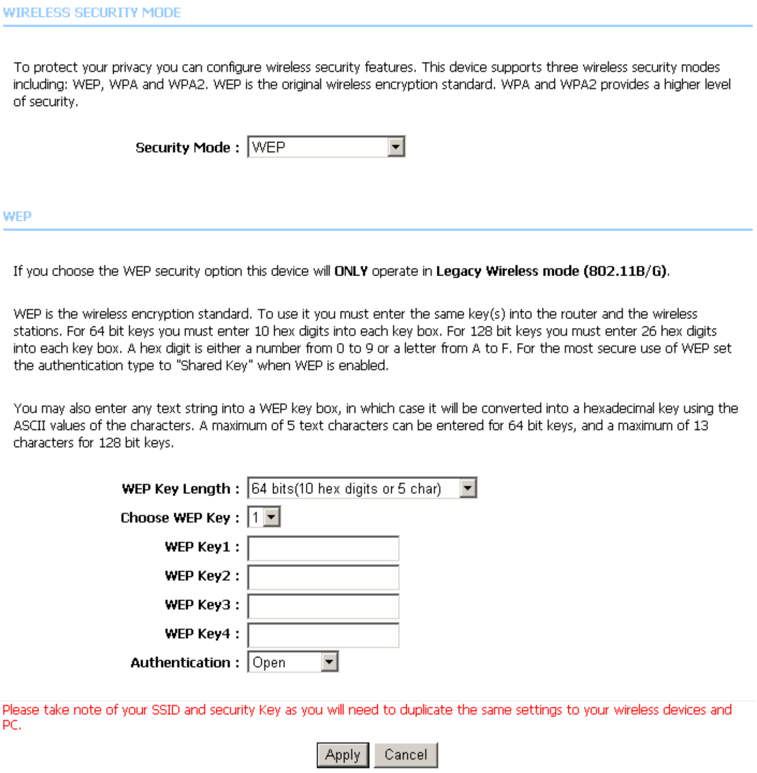
Select the SSID that you want to configure from the drop-down list.



Select SSID : edimax_

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.



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)**.

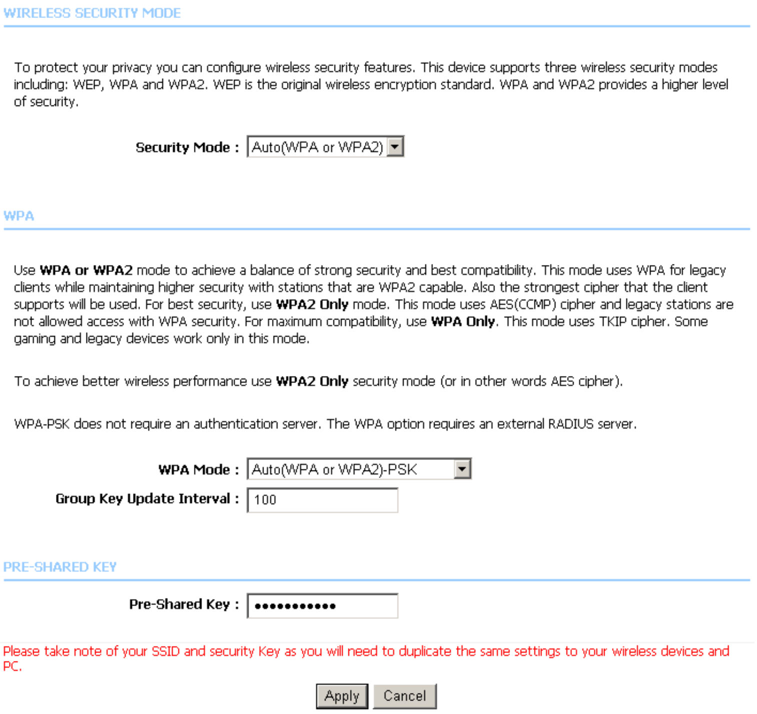
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a 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.

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


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

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

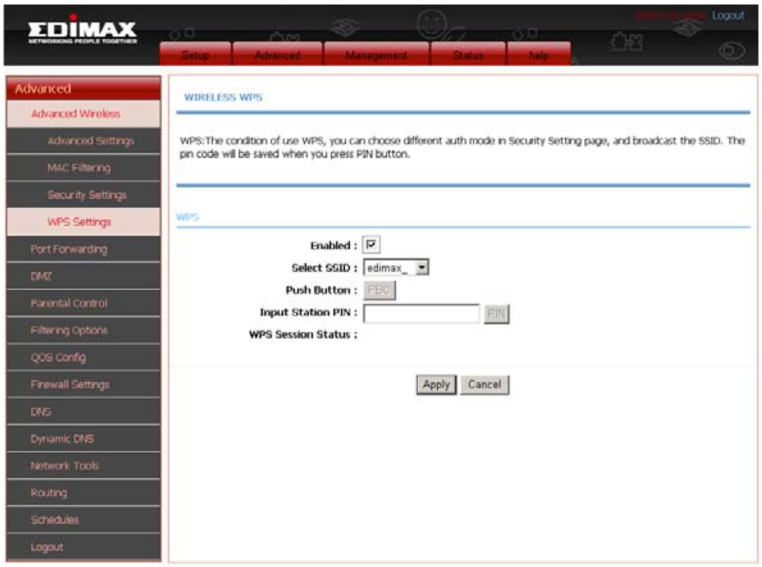
Pre-Shared Key : ●●●●●●●●●●●

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

Click **Apply** to save the settings.

3.3.1.4 WPS Settings

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



WIRELESS WPS

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

WPS

Enabled : ☑

Select SSID : edimax_

Push Button : PBC

Input Station PIN : PIN

WPS Session Status :

WPS Authentication: The WPS service is enabled by default.

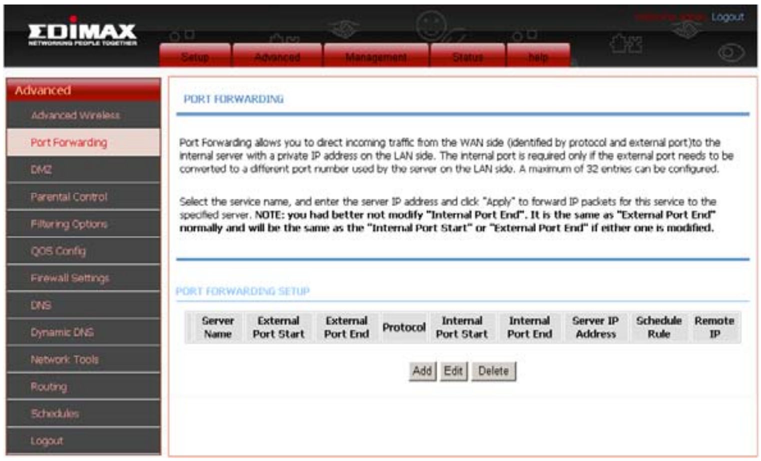
There are three setting methods you can use in the Wi-Fi Protected Setup. In order to use wps authentication, you can select one method from three methods.

- Press the WPS button on the rear panel for 3 seconds.
- In the **WPS Settings** page, click **PBC**. After setting, click **Apply** to make the setting effective.
- In the **WPS Settings** page, enter the **PIN** codes provided by station (STA), then click **PIN.** After settings, click **Apply** to take the settings effective.

3.3.2 Port Forwarding

This function is used to open ports on your device and redirect data from 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 specificed. 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

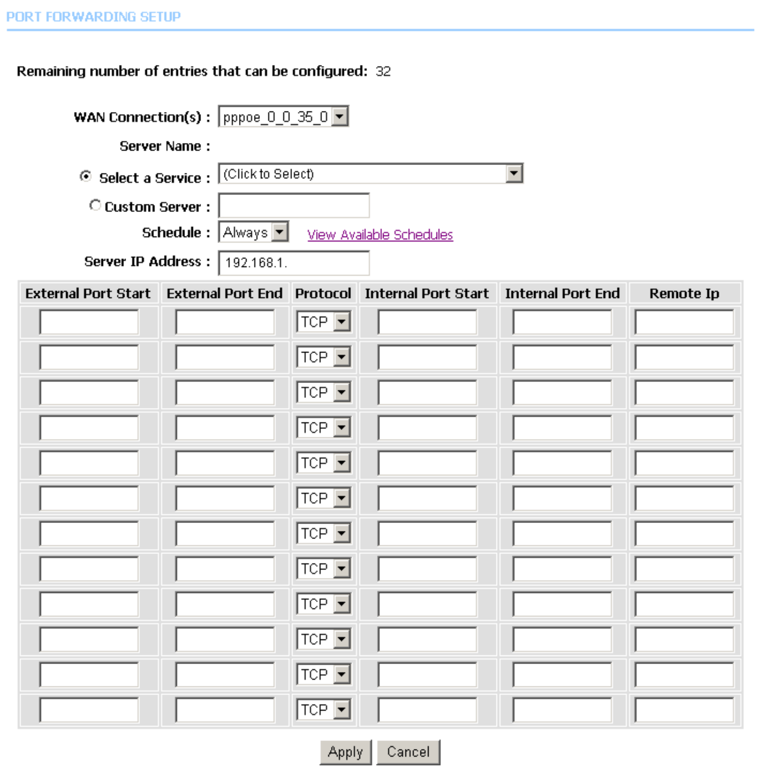
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server 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: you had better not modify "Internal Port End". It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

PORT FORWARDING SETUP

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

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



PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s) : pppoe_0_0_35_0

Server Name :

● Select a Service : (Click to Select)

○ Custom Server :

Schedule : Always

Server IP Address : 192.168.1.

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

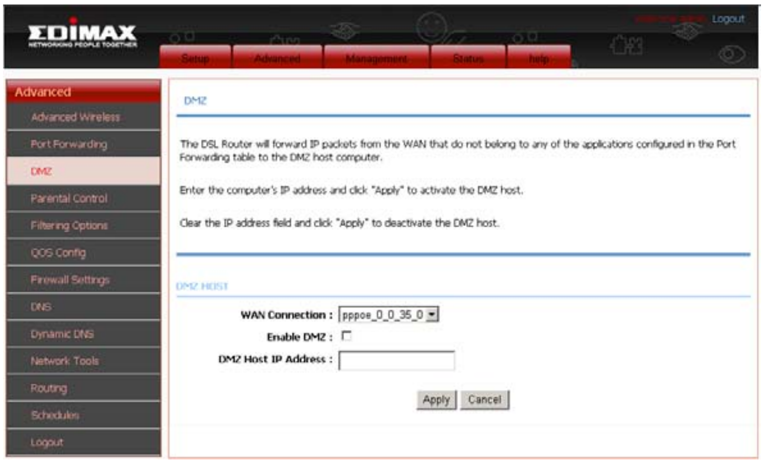
The **TCP/UDP** means the protocol type of the opened ports.

Click **Apply** to save the settings.

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 : pppoe_0_0_35_0

Enable DMZ : □

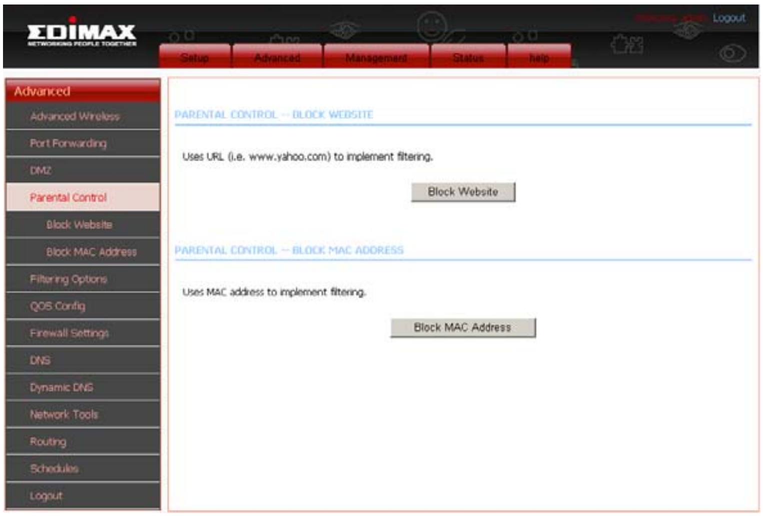
DMZ Host IP Address :

Apply Cancel

Click **Apply** to save the settings.

3.3.4 Parental Control

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



PARENTAL CONTROL -- BLOCK WEBSITE

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

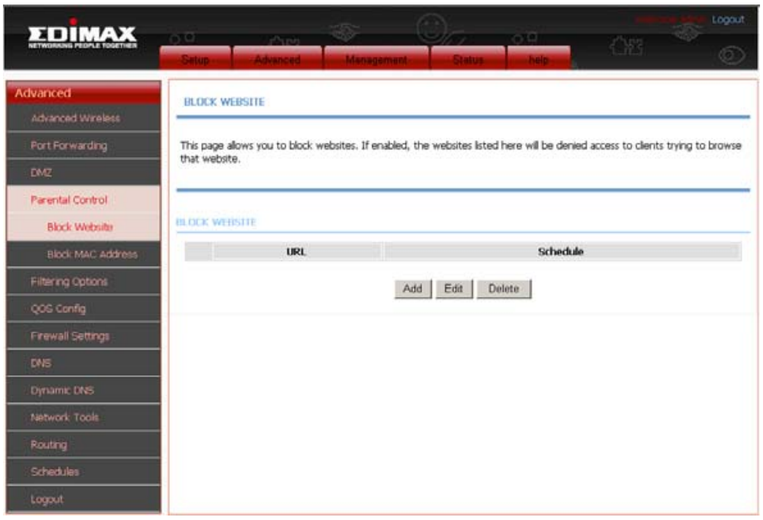
PARENTAL CONTROL -- BLOCK MAC ADDRESS

Uses MAC address to implement filtering.

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

3.3.4.1 Block Website

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



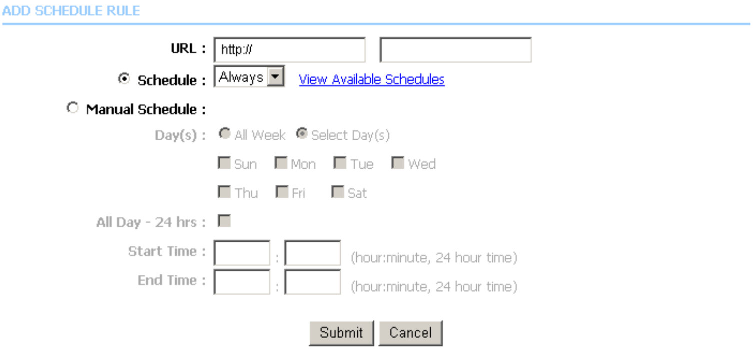
BLOCK WEBSITE

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

BLOCK WEBSITE

	URL	Schedule

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


ADD SCHEDULE RULE

URL : http://

● Schedule : Always

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

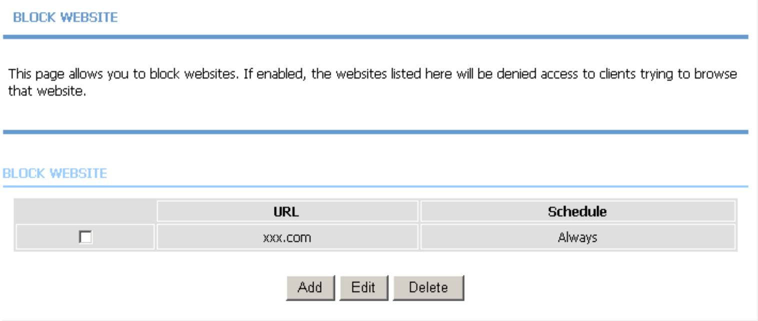
All Day - 24 hrs : □

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

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

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

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



BLOCK WEBSITE

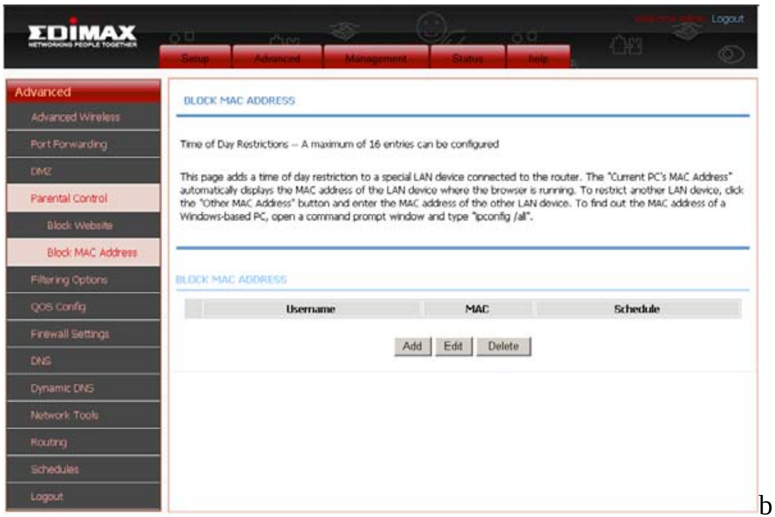
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule
□	xxx.com	Always

3.3.4.2 Block MAC Address

In the **Parental 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

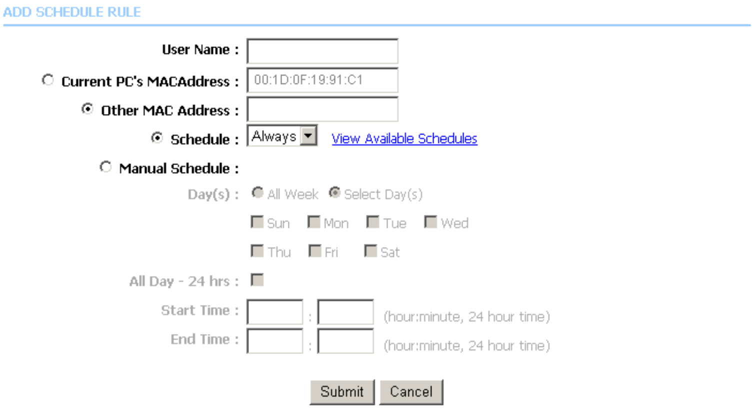
This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address 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".

BLOCK MAC ADDRESS

	Username	MAC	Schedule

b

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



ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:1D:0F:19:91:C1

● Other MAC Address :

● Schedule : Always ▾ View Available Schedules

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

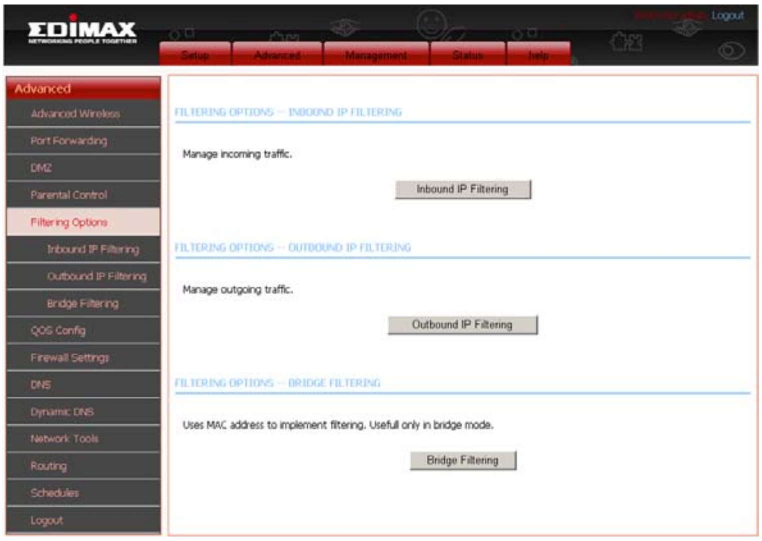
Start Time : : (hour:minute, 24 hour time)

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

Enter the user name and MAC address and select the corresponding time and days. Click **Submit** to add the MAC address to the **BLOCK MAC ADDRESS Table**.

3.3.5 Filtering Options

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



FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

FILTERING OPTIONS -- OUTBOUND IP FILTERING

Manage outgoing traffic.

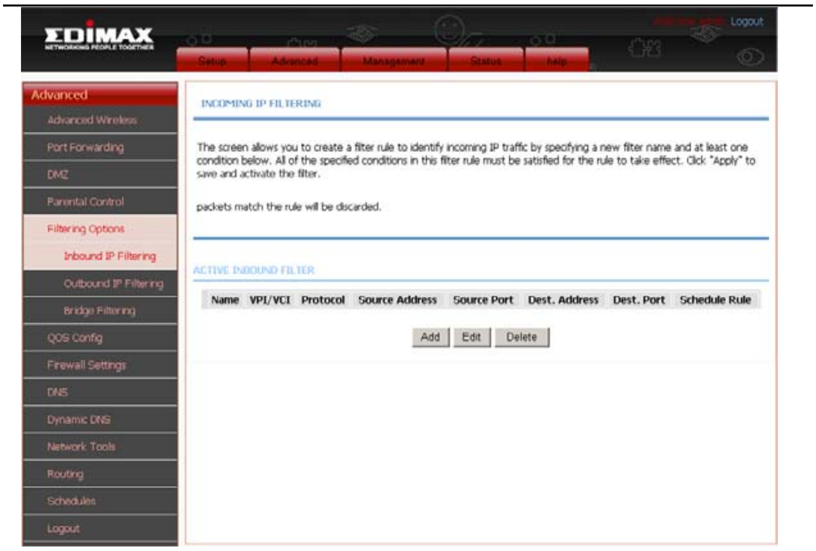
FILTERING OPTIONS -- BRIDGE FILTERING

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

3.3.5.1 Inbound IP Filtering

By default, all incoming IP traffic that does not originate from the internal network is blocked when the firewall is enabled. Normal outbound requests created by web browsing, email and other software you run, work as usual as the requests originated from your internal network. The inbound filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and you need to select at least one condition.

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



INCOMING IP FILTERING

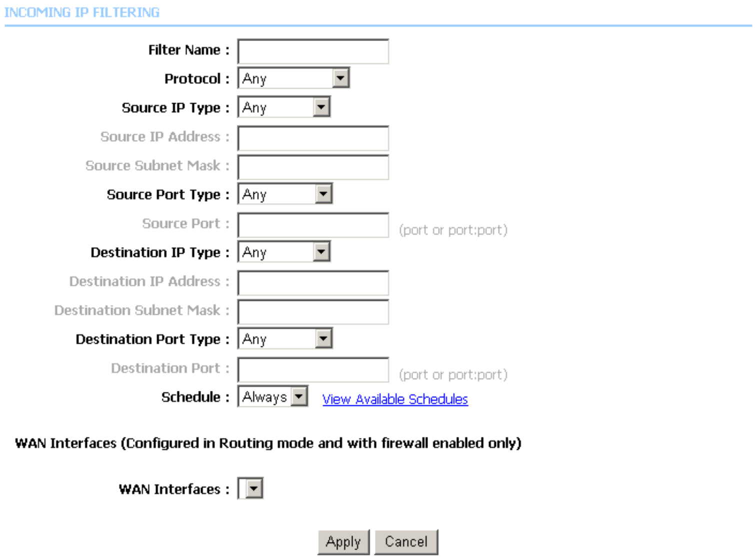
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

packets match the rule will be discarded.

ACTIVE INBOUND FILTER

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

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



INCOMING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : Always View Available Schedules

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

WAN Interfaces :

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

Note:

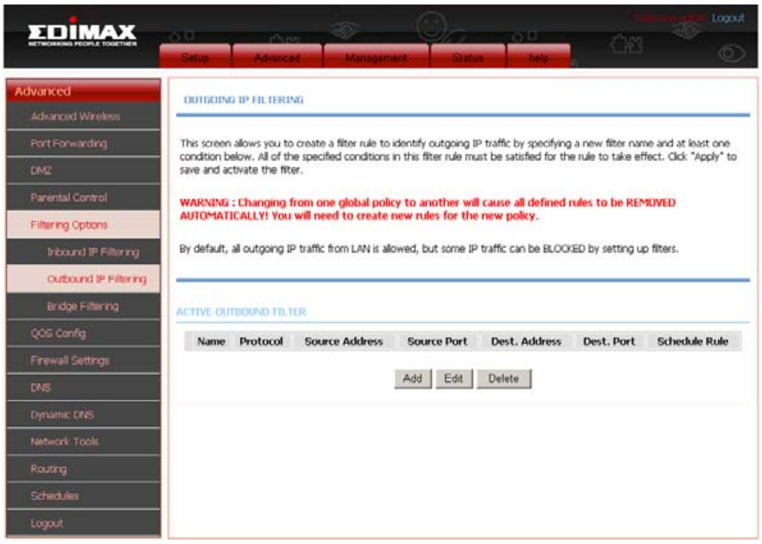
The settings only apply when the firewall is enabled.

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

3.3.5.2 Outbound IP Filtering

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

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



OUTGOING IP FILTERING

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

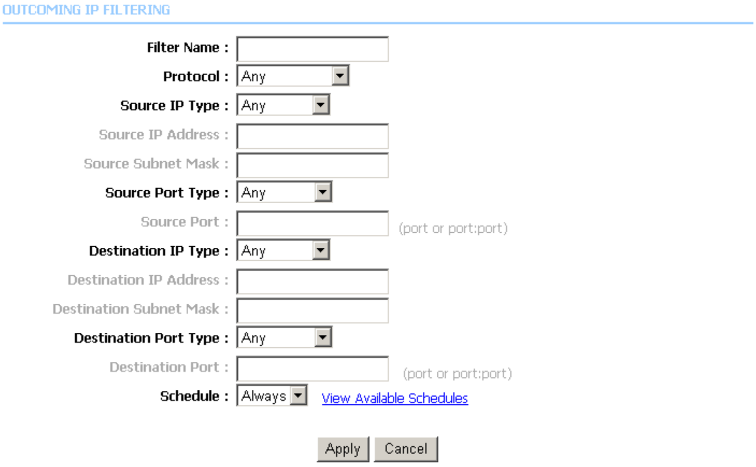
WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

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

ACTIVE OUTBOUND FILTER

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

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



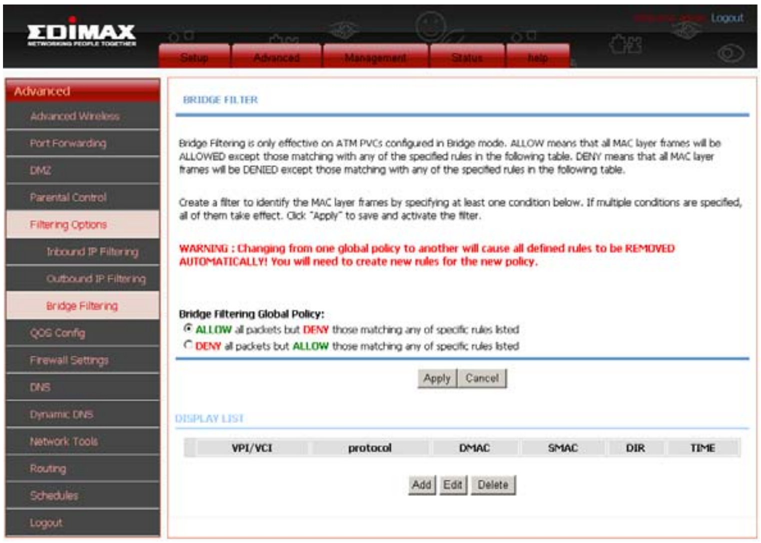
OUTCOMING IP FILTERING

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

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

3.3.5.3 Bridge Filtering

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



BRIDGE FILTER

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

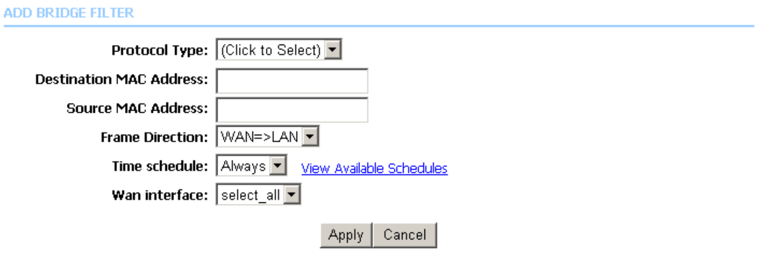
Apply | Cancel

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME

Add | Edit | Delete

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

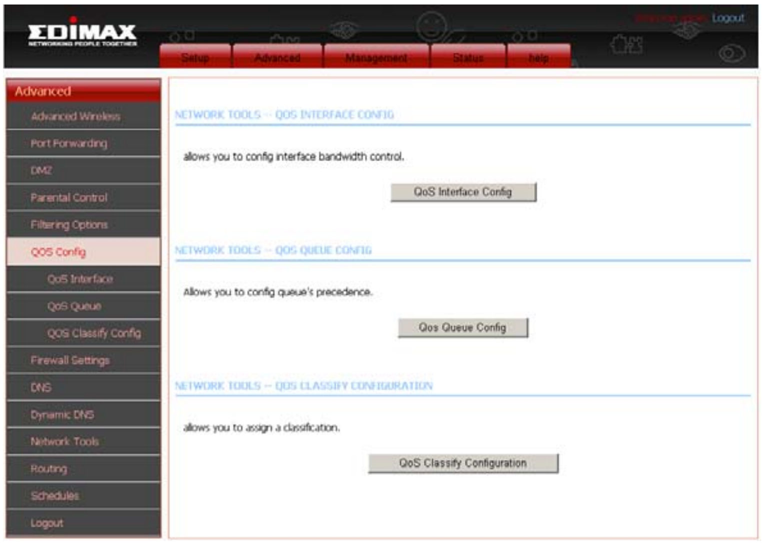
Time schedule: Always View Available Schedules

Wan interface: select_all

Click **Apply** to save the settings.

3.3.6 QoS Configuration

Choose **ADVANCED** > **QOS Config**. The QoS Configuration page shown in the following figure appears.



NETWORK TOOLS -- QOS INTERFACE CONFIG

allows you to config interface bandwidth control.

NETWORK TOOLS -- QOS QUEUE CONFIG

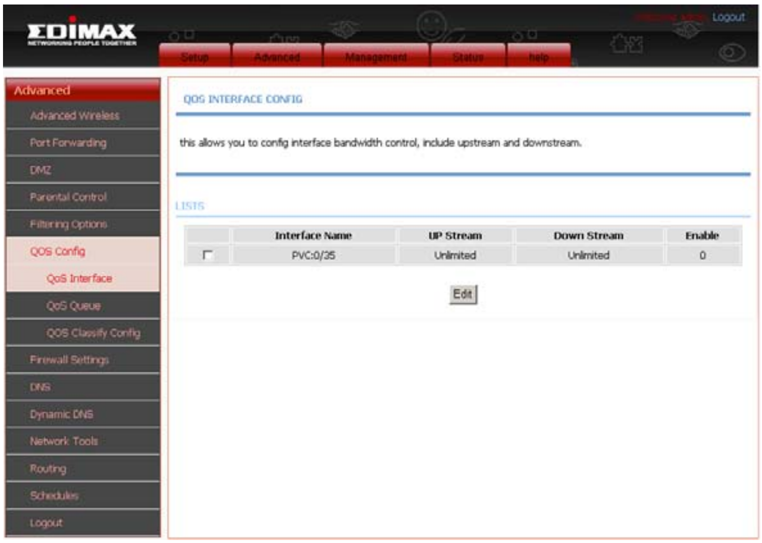
Allows you to config queue's precedence.

NETWORK TOOLS -- QOS CLASSIFY CONFIGURATION

allows you to assign a classfication.

3.3.6.1 QoS Interface

In the QoS Configuration page, click **QoS Interface Config**. The page shown in the following figure appears. In this page, you can configure bandwidth control.



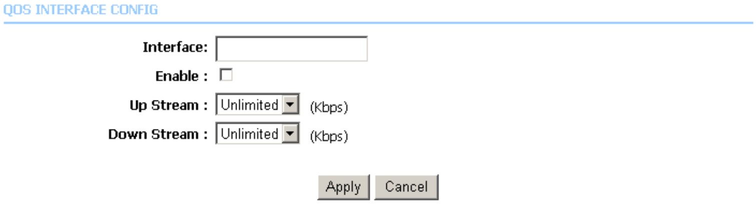
QOS INTERFACE CONFIG

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

LISTS

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

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



QOS INTERFACE CONFIG

Interface:

Enable : □

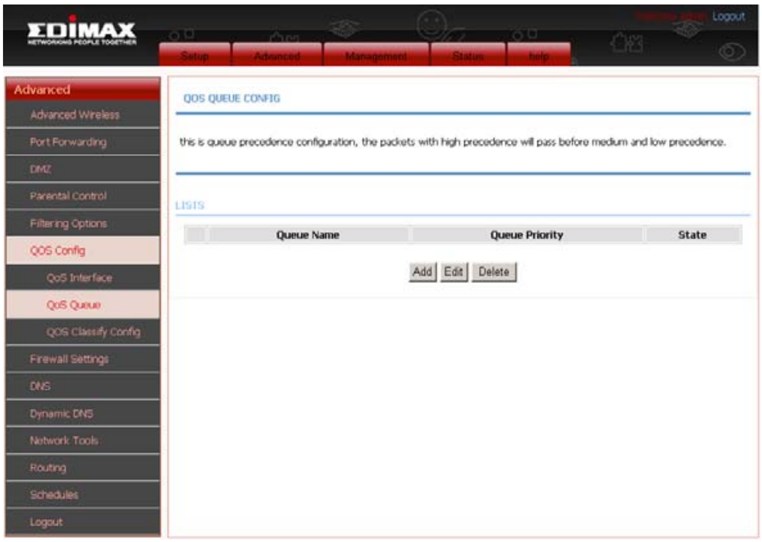
Up Stream : Unlimited (Kbps)

Down Stream : Unlimited (Kbps)

After configuration, click **Apply** to make configurations take effect.

3.3.6.2 QoS Queue Configuration

In the QoS Configuration page, click **QoS Queue Config**. The page shown in the following figure appears. In this page, you can configure the priority of queue.



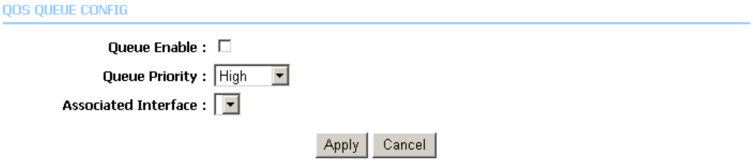
QOS QUEUE CONFIG

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

LISTS

	Queue Name	Queue Priority	State

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


QOS QUEUE CONFIG

Queue Enable : ☐

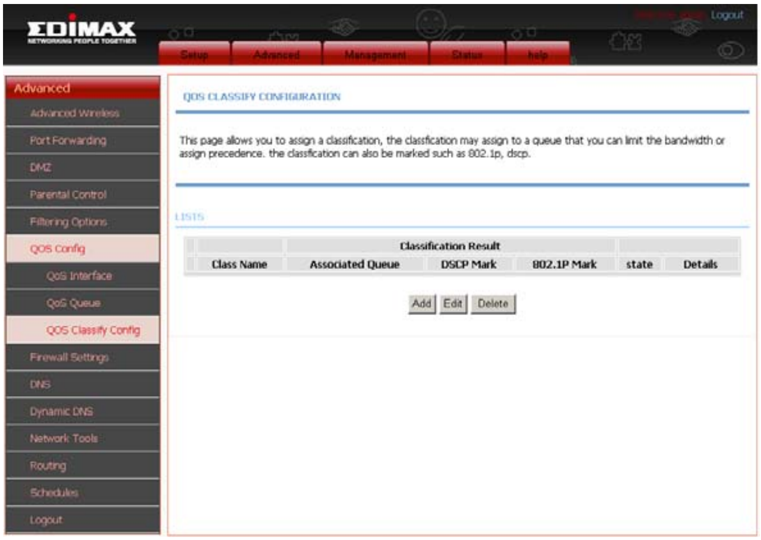
Queue Priority : High

Associated Interface :

After configuration, click **Apply** to take the configurations effect.

3.3.6.3 QoS Classify Configuration

In the QoS Configuration page, click **QoS Classify Configuration**. The page shown in the following figure appears. In this page, you can assign a QoS classification.



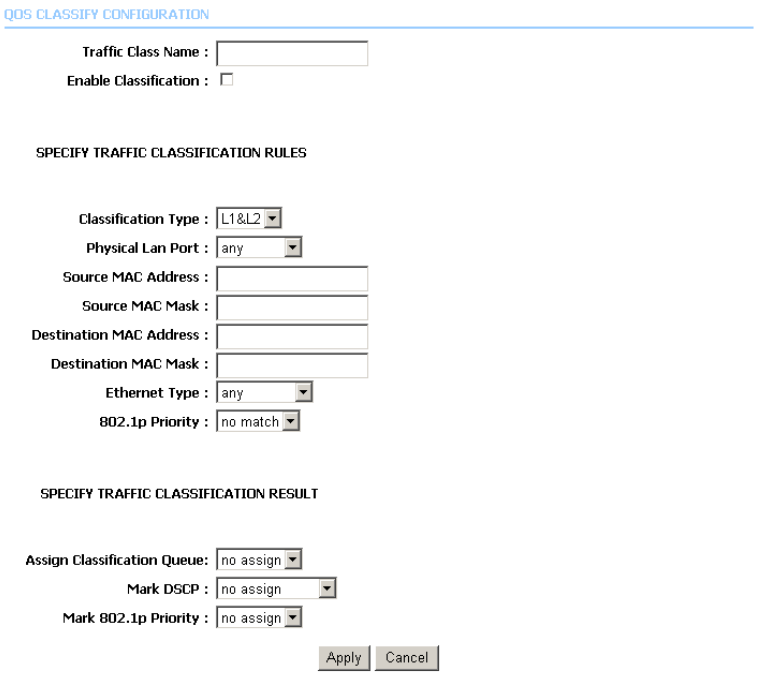
QOS CLASSIFY CONFIGURATION

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

LISTS

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

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



QOS CLASSIFY CONFIGURATION

Traffic Class Name :	
Enable Classification :	□

SPECIFY TRAFFIC CLASSIFICATION RULES

Classification Type :	L1&L2
Physical Lan Port :	any
Source MAC Address :	
Source MAC Mask :	
Destination MAC Address :	
Destination MAC Mask :	
Ethernet Type :	any
802.1p Priority :	no match

SPECIFY TRAFFIC CLASSIFICATION RESULT

Assign Classification Queue:	no assign
Mark DSCP :	no assign
Mark 802.1p Priority :	no assign

After configuration is done, click **Apply** to make the configuration take effect.

3.3.7 Firewall Settings

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

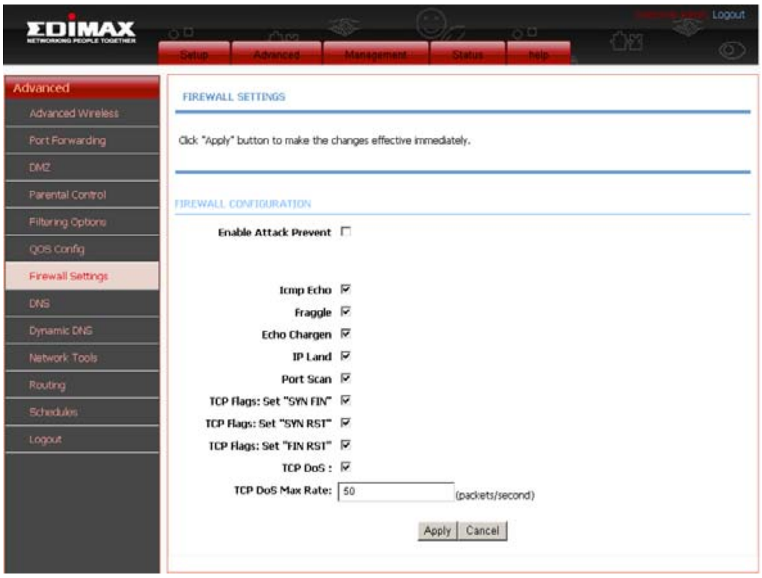
- The attackers attempt to flood a network, thereby preventing legitimate network traffic
- The attackers attempt to disrupt connections between two machines, thereby preventing access to a service
- The attackers attempt to prevent a particular individual

from accessing a service

- The attackers attempt to disrupt service to a specific system or person.

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)

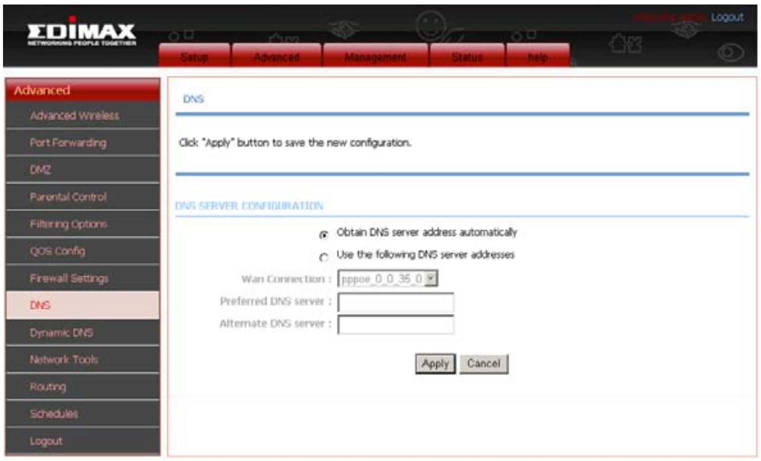
Click **Apply** to save the settings.

3.3.8 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 folllowing figure appears.



DNS

Click "Apply" button to save the new configuration.

DNS SERVER CONFIGURATION

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Wan Connection : pppoe_0_0_35_0

Preferred DNS server :

Alternate DNS server :

DNS SERVER CONFIGURATION

If you are using the device as DHCP server on the LAN, or if you are using DNS servers provided by your ISP, select **Obtain DNS server address automatically**.

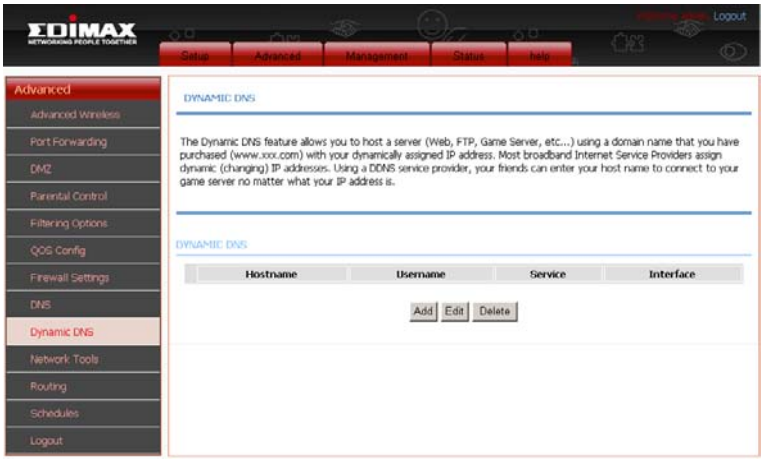
If you have DNS IP addresses provided by your ISP, enter these IP addresses in the preferred DNS server and the alternate DNS server field.

Click **Apply** to save the settings.

3.3.9 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 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 page appears.



DYNAMIC DNS

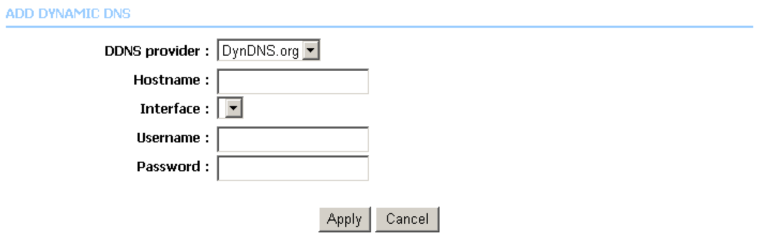
The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your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

DYNAMIC DNS

	Hostname	Username	Service	Interface

Add Edit Delete

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



ADD DYNAMIC DNS

DDNS provider : DynDNS.org

Hostname :

Interface :

Username :

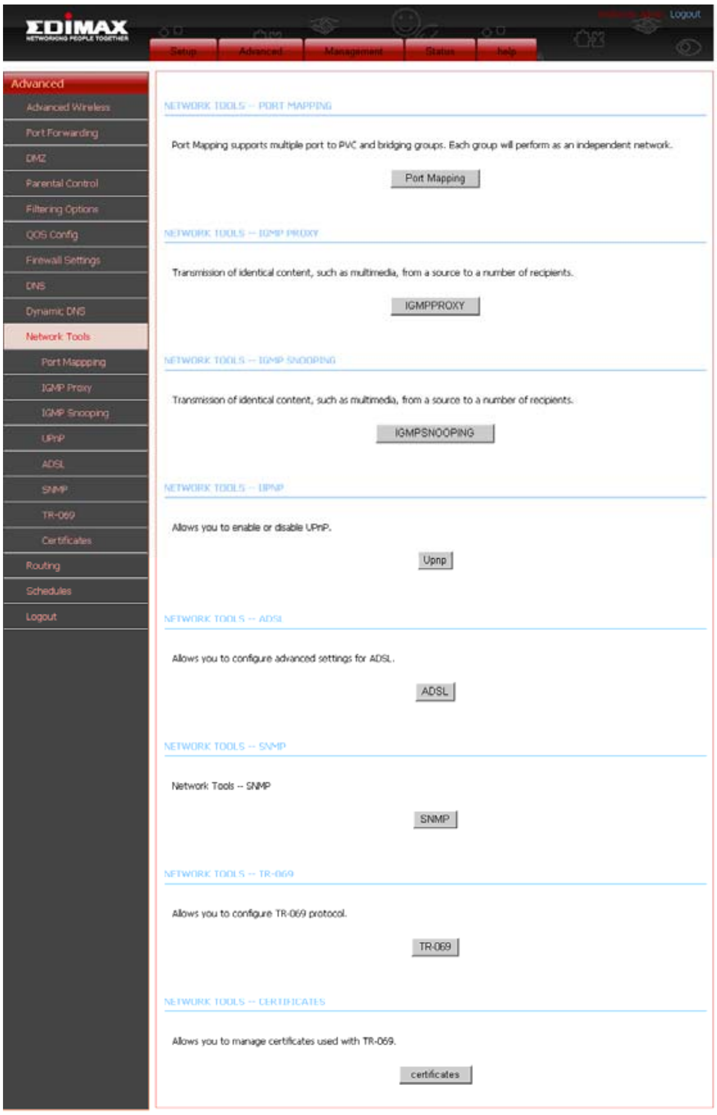
Password :

- **DDNS provider**: Select one of the DDNS service provider from the down-list. Available service providers 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.

3.3.10Network Tools

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



NETWORK TOOLS -- PORT MAPPING

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

NETWORK TOOLS -- IGMP PROXY

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

NETWORK TOOLS -- IGMP SNOOPING

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

NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.

NETWORK TOOLS -- ADSL

Allows you to configure advanced settings for ADSL.

NETWORK TOOLS -- SNMP

Network Tools -- SNMP

NETWORK TOOLS -- TR-069

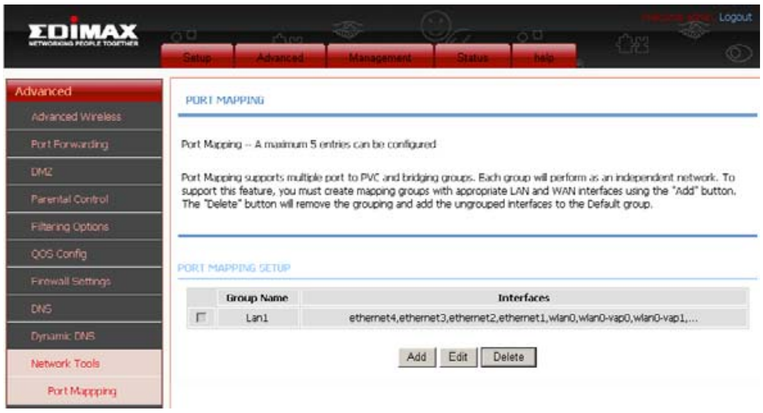
Allows you to configure TR-069 protocol.

NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

3.3.10.1 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

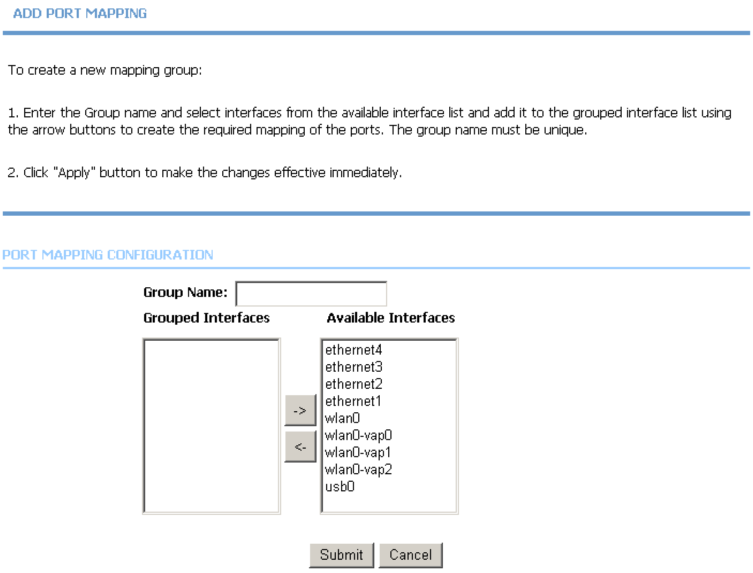
Port Mapping -- A maximum 5 entries can be configured

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	ethernet4,ethernet3,ethernet2,ethernet1,wlan0,wlan0-vap0,wlan0-vap1,...

Click **Add** to add a new 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:

The procedure for creating a mapping group is listed as follows:

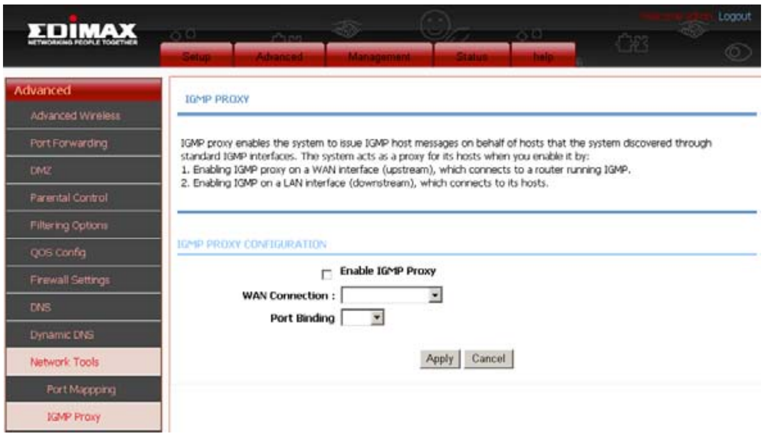
Step 1 Enter the group name.

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 **Submit** to save the settings.

3.3.10.2 IGMP Proxy

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



IGMP PROXY

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

IGMP PROXY CONFIGURATION

□ Enable IGMP Proxy

WAN Connection :

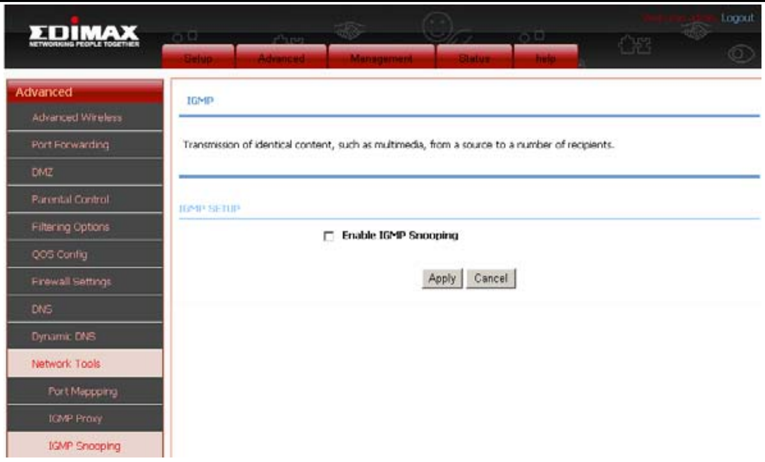
Port Binding

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.

Click **Apply** to save the settings.

3.3.10.3 IGMP Snooping

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



IGMP

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

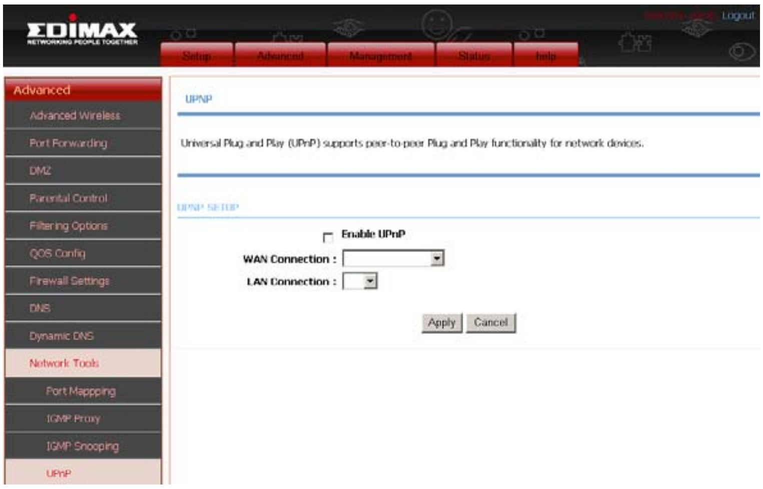
IGMP SETUP

□ Enable IGMP Snooping

After configuration, click **Apply** to save the settings.

3.3.10.4 UPnP

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



UPNP

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

UPNP SETUP

□ Enable UPnP

WAN Connection :

LAN Connection :

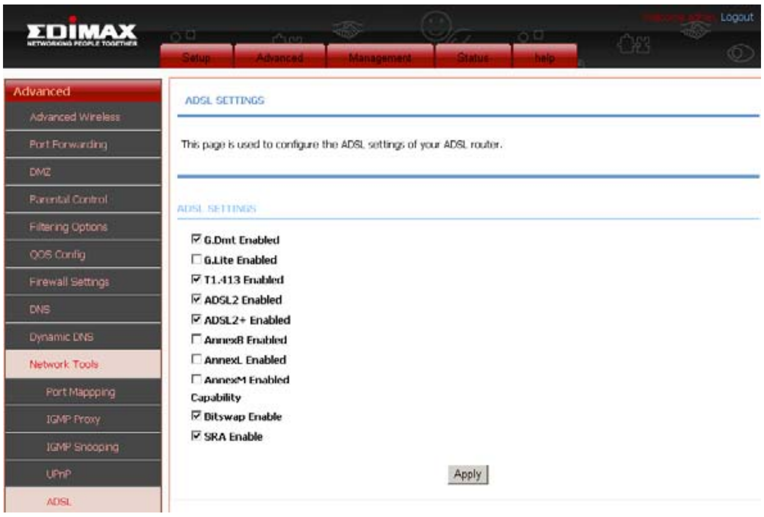
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio / video 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 will not respond malicious Internet requests.

Click **Apply** to save the settings.

3.3.10.5 ADSL Settings

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



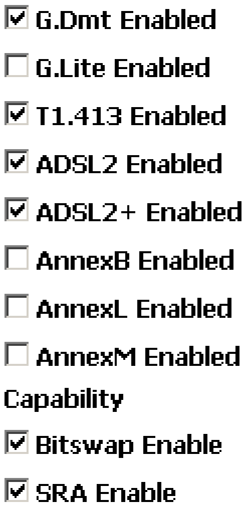
ADSL SETTINGS

This page is used to configure the ADSL settings of your ADSL router.

ADSL SETTINGS

☑ G.Dmt Enabled
☐ G.Lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ ADSL2+ Enabled
☐ AnnexB Enabled
☐ AnnexL Enabled
☐ AnnexM Enabled
Capability
☑ Bitswap Enable
☑ SRA Enable

In this page, you can select the DSL modulation. Normally, you can keep factory default setting.



☑ G.Dmt Enabled

☐ G.Lite Enabled

☑ T1.413 Enabled

☑ ADSL2 Enabled

☑ ADSL2+ Enabled

☐ AnnexB Enabled

☐ AnnexL Enabled

☐ AnnexM Enabled

Capability

☑ Bitswap Enable

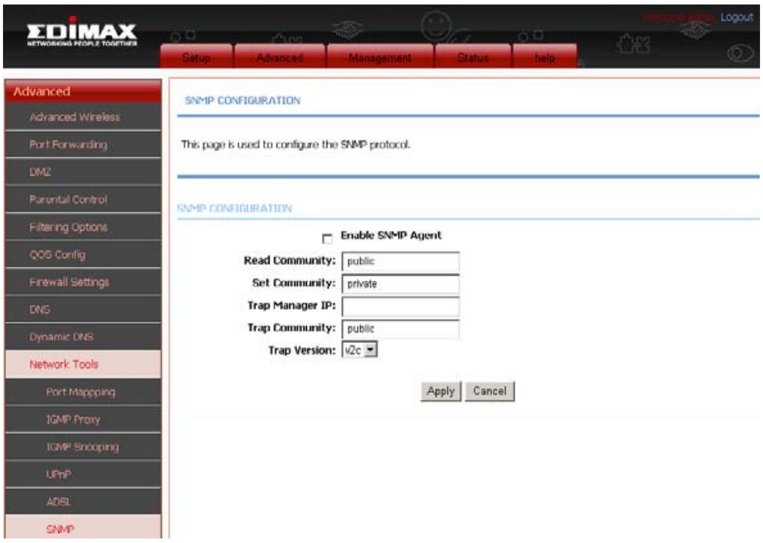
☑ SRA Enable

The AR-7284WnA supports AnnexA mode, so the AnnexB is not enabled.

Click **Apply** to save the settings.

3.3.10.6 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

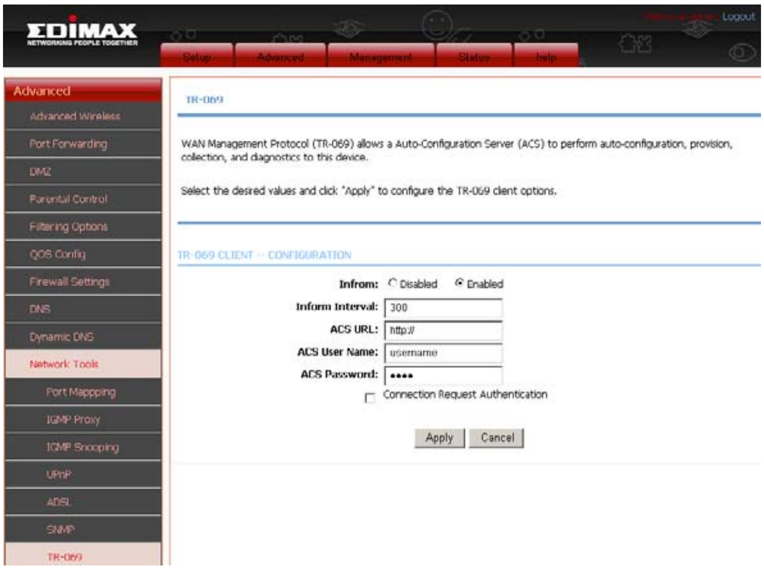
Trap Version: v2c

- **Read Community**: The network administrator must use this password to read the information of this device.
- **Set Community**: The network administrator must use this password to configure the information of this device.
- **Trap Manager IP**: The trap information is sent to this host.

Click **Apply** to save the settings.

3.3.10.7 TR069

Choose **ADVANCED** > **Network Tools** and click **TR-069**. The page shown in the following figure appears. In this page, you can configure the TR069 CPE.



TR-069

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

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

TR-069 CLIENT -- CONFIGURATION

Infrom: ○ Disabled ● Enabled

Inform Interval: 300

ACS URL: http://

ACS User Name: username

ACS Password: ••••

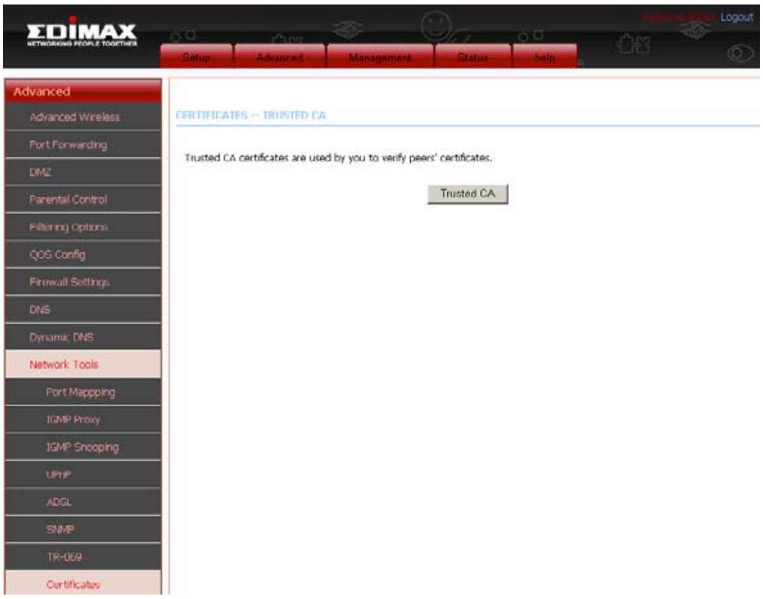
□ Connection Request Authentication

Apply Cancel

Click **Apply** to save settings.

3.3.10.8 Certificates

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

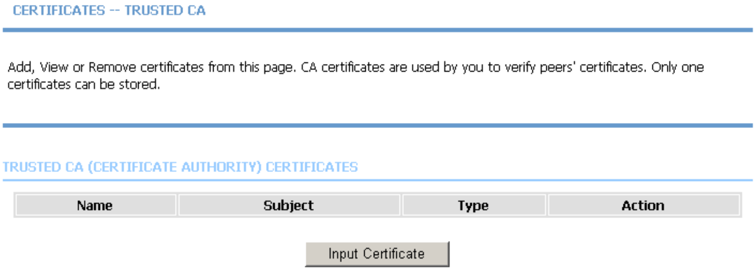


CERTIFICATES -- TRUSTED CA

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

Trusted CA

In the **Certificates** page, click **Trusted CA**. The page shown in the following figure appears.



CERTIFICATES -- TRUSTED CA

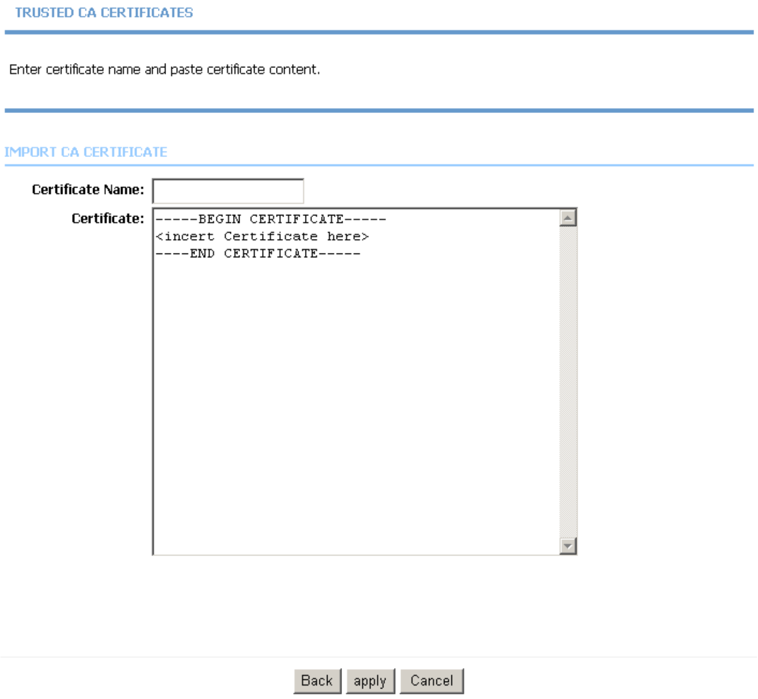
Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificates can be stored.

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action

Input Certificate

Click **Input Certificate**, the page shown in the following figure appears.



TRUSTED CA CERTIFICATES

Enter certificate name and paste certificate content.

IMPORT CA CERTIFICATE

Certificate Name:

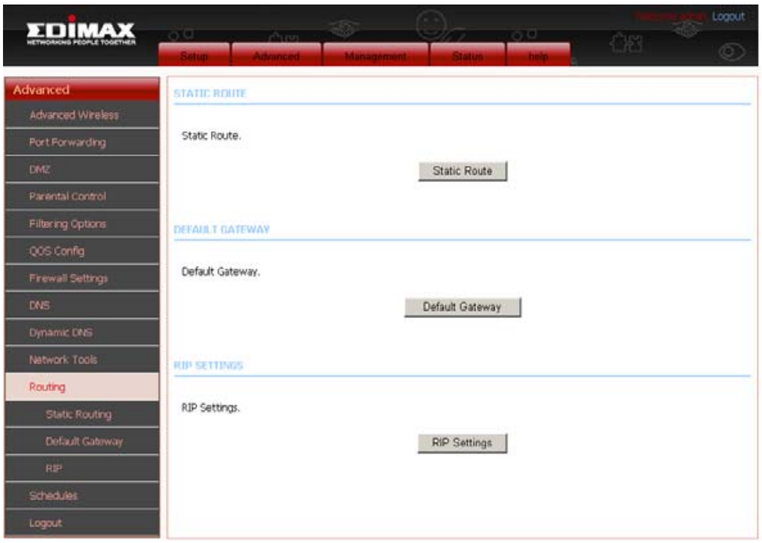
Certificate:

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

Click **Apply** to save the settings.

3.3.11Routing

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



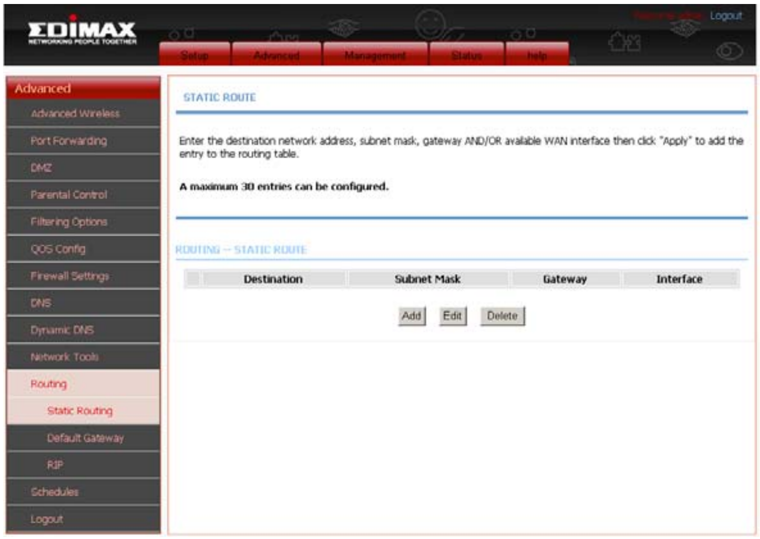
Static Route.

Default Gateway.

RIP Settings.

3.3.11.1 Static Route

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



STATIC ROUTE

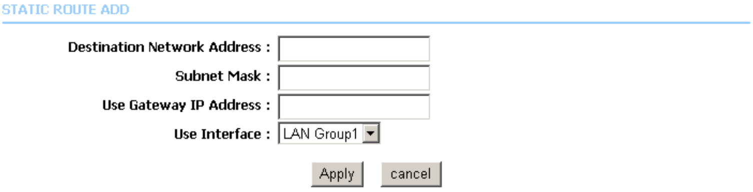
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

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



STATIC ROUTE ADD

Destination Network Address :	
Subnet Mask :	
Use Gateway IP Address :	
Use Interface :	LAN Group1

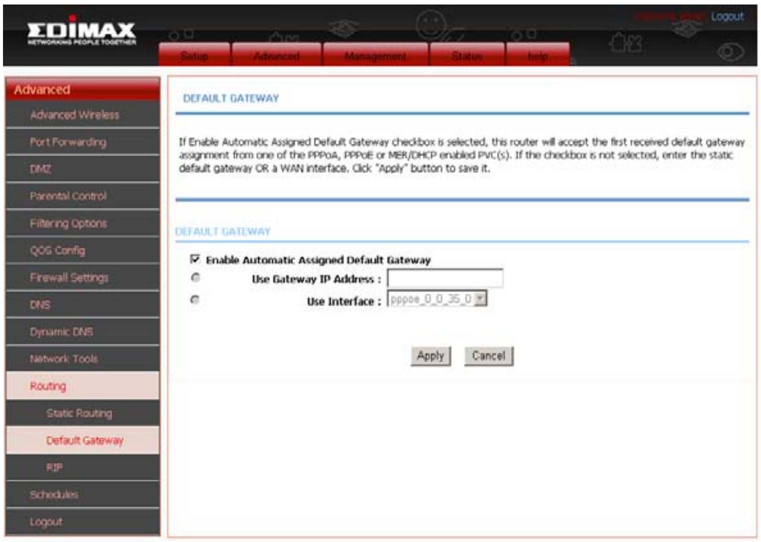
- **Destination Network Address**: The destination network address.
- **Subnet Mask**: The subnet mask of the destination network.
- **Use Gateway IP Address**: The gateway IP address of the destination network.
- **User Interface**: The interface name of the router output port.

You can only choose **Use Gateway IP Address** or **User Interface**.

Click **Apply** to save the settings.

3.3.11.2 Default Gateway

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



DEFAULT GATEWAY

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

DEFAULT GATEWAY

☑ Enable Automatic Assigned Default Gateway

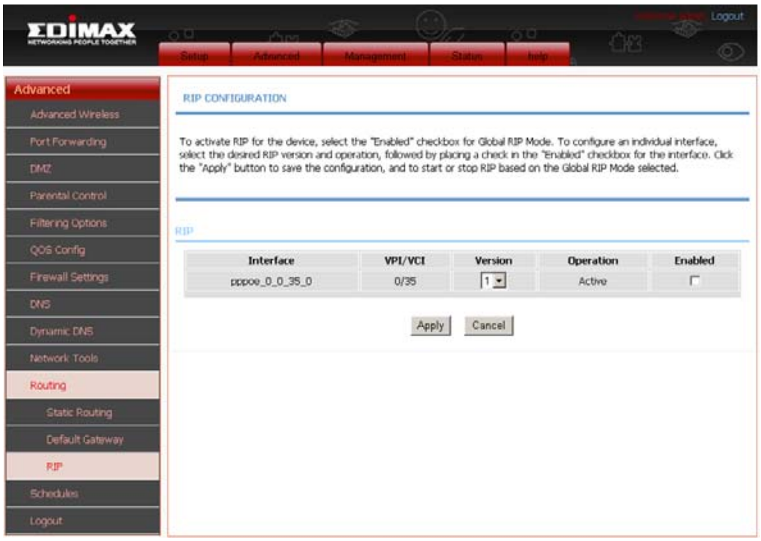
○ Use Gateway IP Address :

○ Use Interface : pppoe_0_0_35_0

Click **Apply** to save the settings.

3.3.11.3 RIP Settings

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



RIP CONFIGURATION

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

RIP

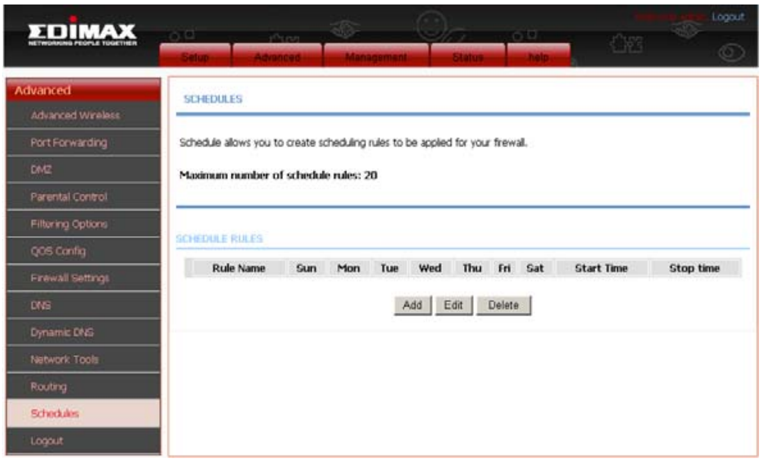
Interface	VPI/VCI	Version	Operation	Enabled
pppoe_0_0_35_0	0/35	1	Active	□

Apply Cancel

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.

3.3.12 Schedules

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



SCHEDULES

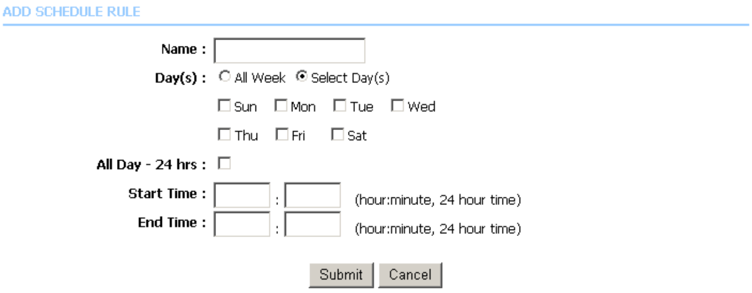
Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

SCHEDULE RULES

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

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



ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

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

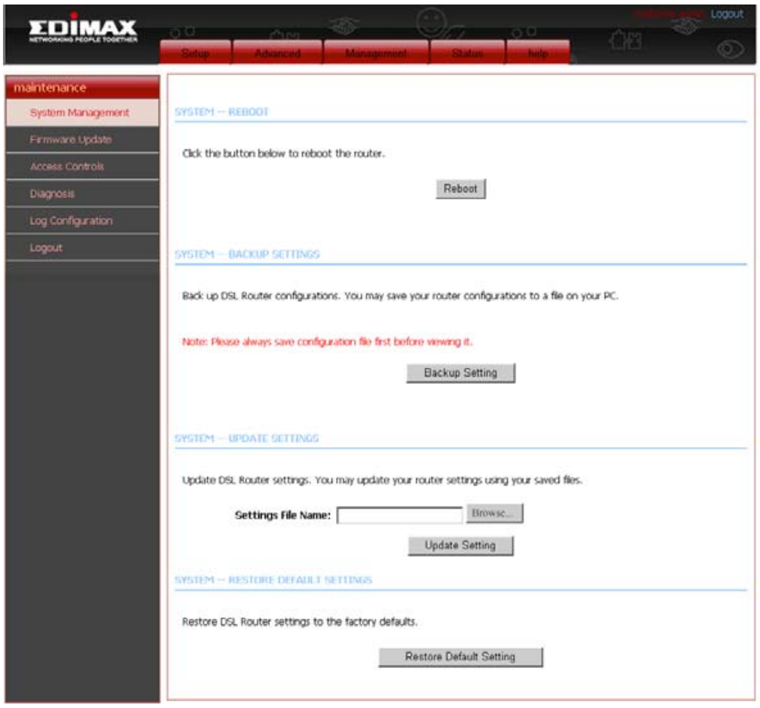
End Time : : (hour:minute, 24 hour time)

Click **Submit** to save settings.

3.4 Management

3.4.1 System

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



SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- BACKUP SETTINGS

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

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

SYSTEM -- UPDATE SETTINGS

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

Settings File Name:

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

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

The buttons in this page are described as follows:

Reboot: Reboot the device.

Backup Setting: Save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.

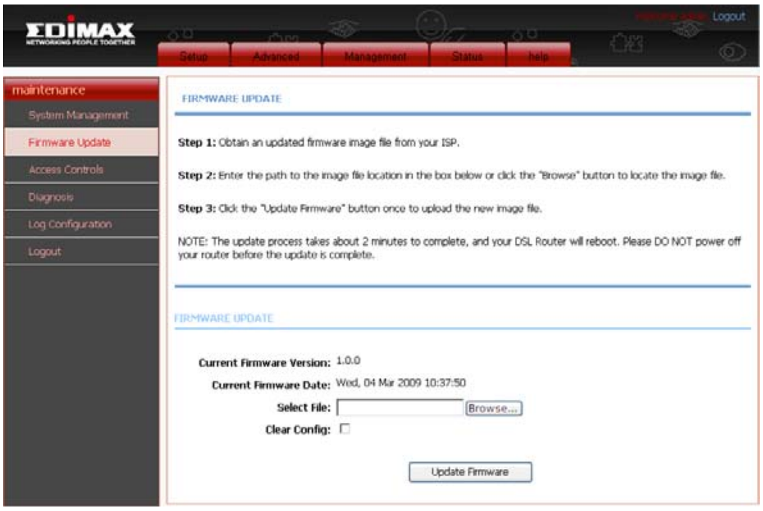
Update Setting: Click **Browse** to select the configuration file of device and click **Update Settings** to begin restoring the device configuration..

Restore Default Setting: Reset the device to default settings.

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

3.4.2 Firmware Update

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



FIRMWARE UPDATE

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

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

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

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

FIRMWARE UPDATE

Current Firmware Version: 1.0.0
Current Firmware Date: Wed, 04 Mar 2009 10:37:50
Select File: Browse...
Clear Config: □

Update Firmware

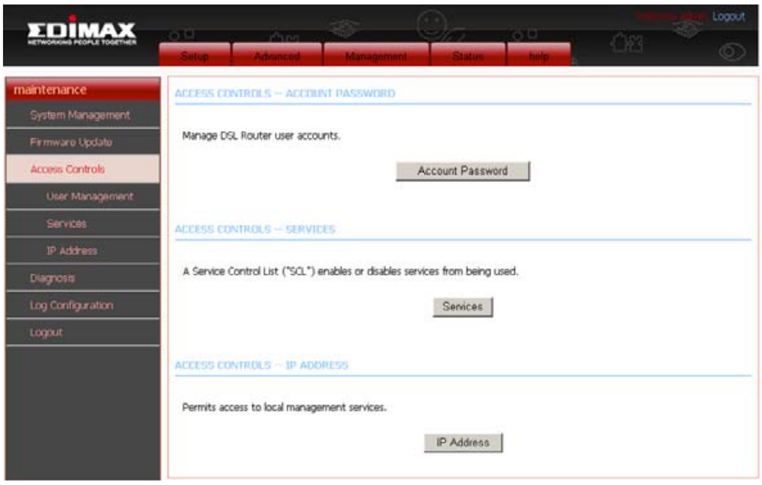
The procedure for updating the firmware is as follows:

Step 1 Click **Browse…**to search the file.

Step 2 Click **Update Firmware** to copy the file.
The device loads the file and reboots automatically.
Notice*: Do not turn off your device or press the reset button while this procedure is in progress.*

3.4.3 Access Controls

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



ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

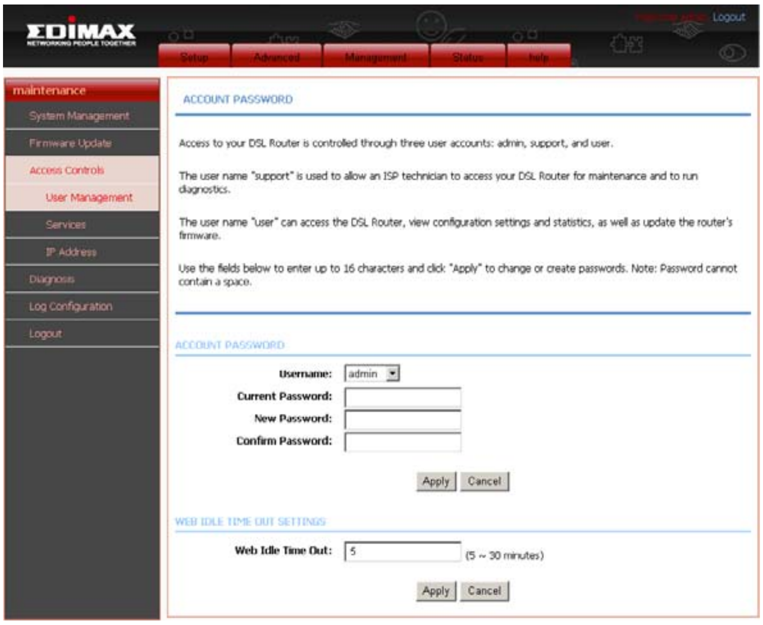
A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROLS -- IP ADDRESS

Permits access to local management services.

3.4.3.1 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.

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
Current Password:
New Password:
Confirm Password:

WEB IDLE TIME OUT SETTINGS

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

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

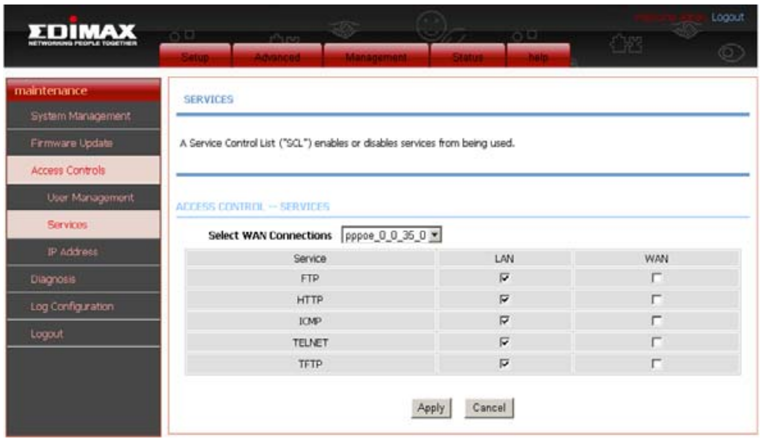
Select the **Username** from the drop-down list. You can select **admin**, **support**, or **user**.

Enter the current password, and input new password in both ‘New Password’ and ‘Confirm Password’ field to change the password.

Click **Apply** to save the settings.

3.4.3.2 Services

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



SERVICES

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

ACCESS CONTROL -- SERVICES

Select WAN Connections: pppoe_0_0_35_0

Service	LAN	WAN
FTP	☑	☐
HTTP	☑	☐
ICMP	☑	☐
TELNET	☑	☐
TFTP	☑	☐

Apply Cancel

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

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

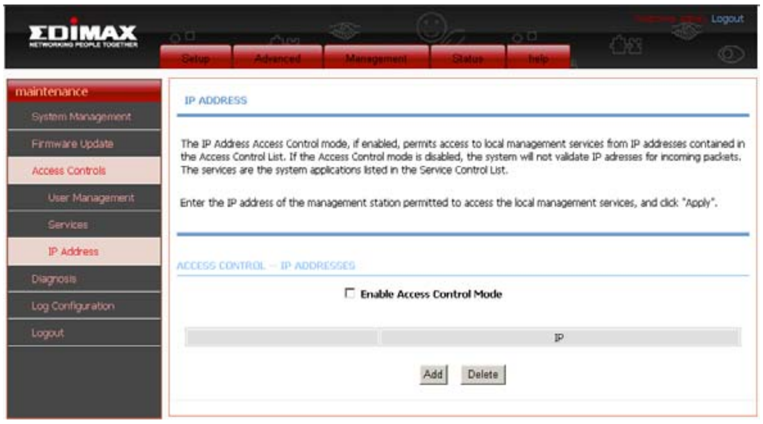
Click **Apply** to apply the settings.

Note:

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

3.4.3.3 IP Address

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



IP ADDRESS

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

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

ACCESS CONTROL -- IP ADDRESSES

□ Enable Access Control Mode

	IP

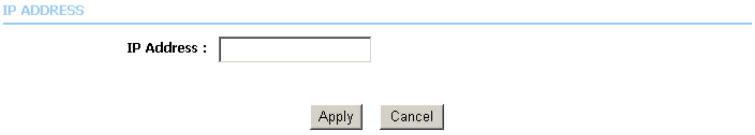
In this page, you can configure the IP address used with access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

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

Note:

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

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



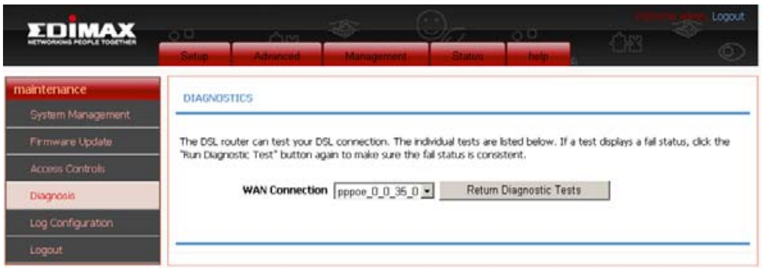
IP ADDRESS

IP Address :

Click **Apply** to apply the settings.

3.4.4 Diagnostics

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



DIAGNOSTICS

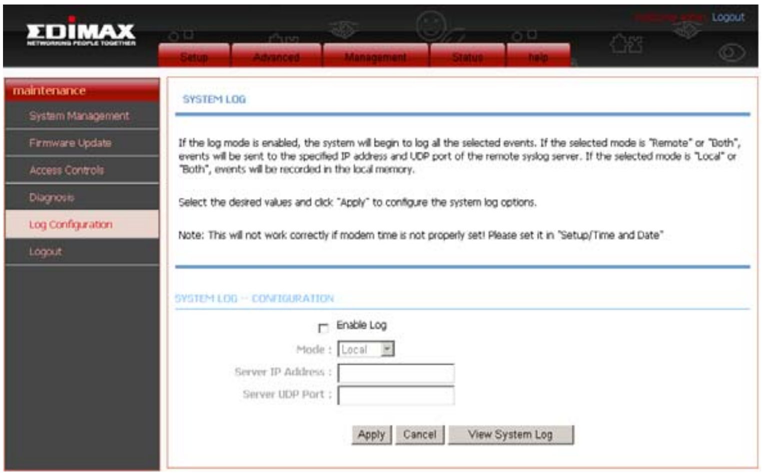
The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection pppoe_0_0_35_0

Click **Run Diagnostics Test** to run diagnostics.

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 :

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 syslog server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.

The procedure for logging the events is as follows:

Step 1 Select **Enable Log.**

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.

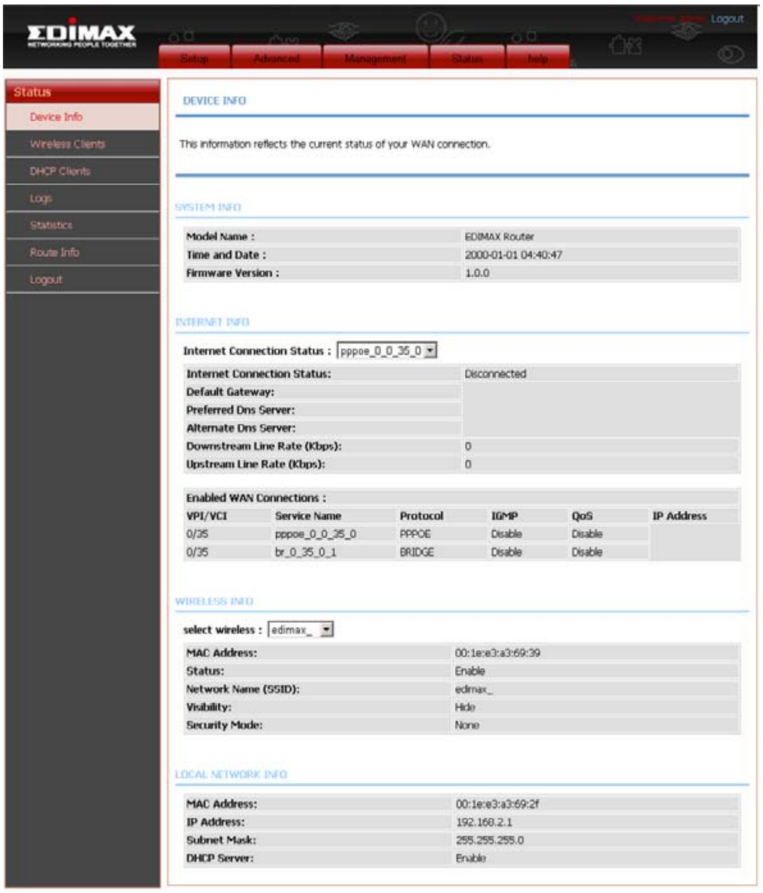
Step 5 Click **View System Log** to view the detail information of system log.

3.5 Status

You can view the system information and monitor device performance.

3.5.1 Device Info

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



DEVICE INFO

This information reflects the current status of your WAN connection.

SYSTEM INFO

Model Name :	EDIMAX Router
Time and Date :	2000-01-01 04:40:47
Firmware Version :	1.0.0

INTERNET INFO

Internet Connection Status : pppoe_0_0_35_0

Internet Connection Status:	Disconnected
Default Gateway:	
Preferred Dns Server:	
Alternate Dns Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
0/35	pppoe_0_0_35_0	PPPOE	Disable	Disable	
0/35	br_0_35_0_1	BRIDGE	Disable	Disable	

WIRELESS INFO

select wireless : edimax_

MAC Address:	00:1e:e3:a3:69:39
Status:	Enable
Network Name (SSID):	edimax_
Visibility:	Hide
Security Mode:	None

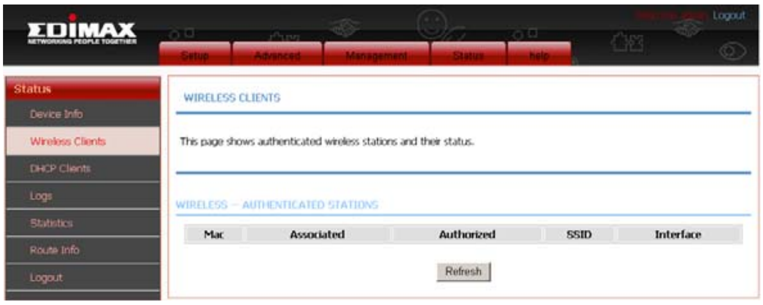
LOCAL NETWORK INFO

MAC Address:	00:1e:e3:a3:69:2f
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

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

3.5.2 Wireless Clients

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



WIRELESS CLIENTS

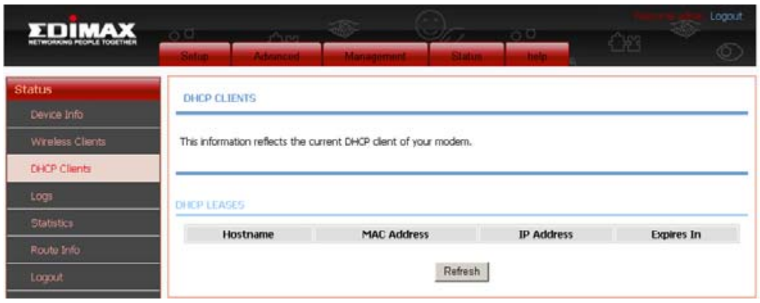
This page shows authenticated wireless stations and their status.

WIRELESS -- AUTHENTICATED STATIONS

Mac	Associated	Authorized	SSID	Interface

3.5.3 DHCP Clients

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



DHCP CLIENTS

This information reflects the current DHCP client of your modem.

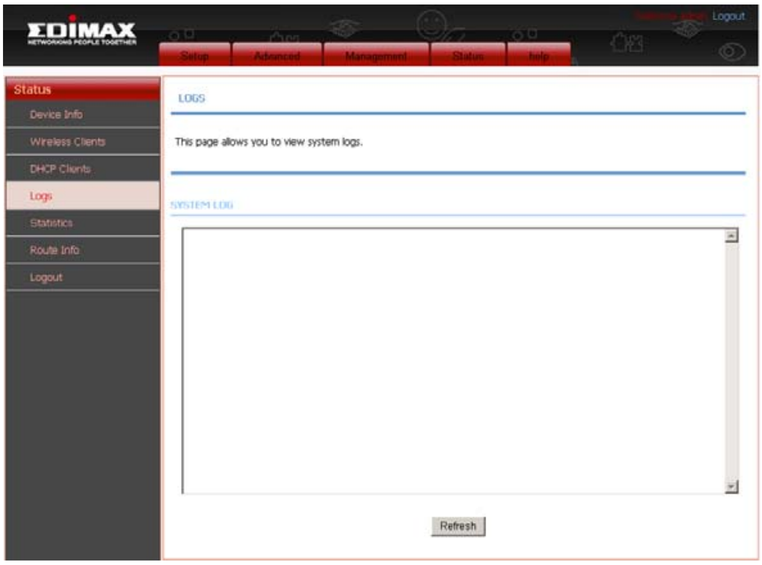
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

This page displays all client devices that obtain IP address from the device. You can view the host name, IP address, MAC address and expire time.

3.5.4 Logs

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

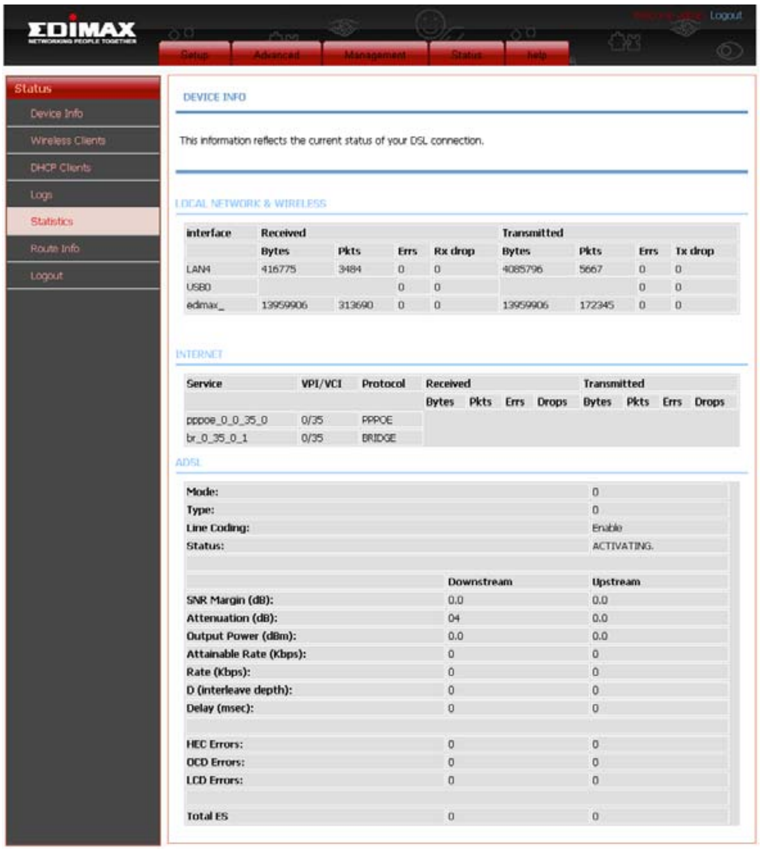


This page allows you to view system logs.

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

3.5.5 Statistics

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



DEVICE INFO

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN4	416775	3484	0	0	4085796	5667	0	0
USB0			0	0			0	0
edimax_	13959906	313690	0	0	13959906	172345	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoe_0_0_35_0	0/35	PPPOE								
br_0_35_0_1	0/35	BRIDGE								

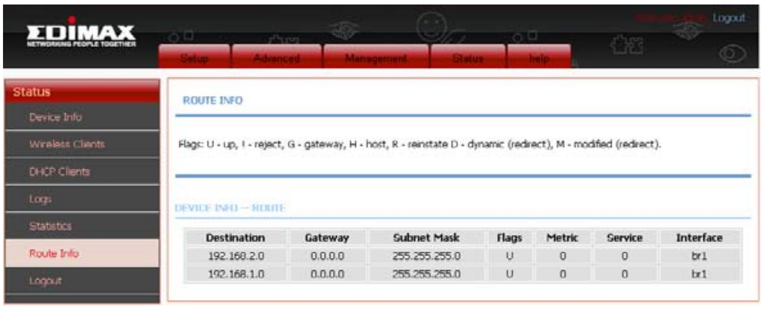
ADSL

Mode:		0
Type:		0
Line Coding:		Enable
Status:		ACTIVATING.
	Downstream	Upstream
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	04	0.0
Output Power (dBm):	0.0	0.0
Attainable Rate (Kbps):	0	0
Rate (Kbps):	0	0
D (interleave depth):	0	0
Delay (msec):	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total ES	0	0

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

3.5.6 Route Info

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



ROUTE INFO

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

DEVICE INFO -- ROUTE

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

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

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution

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

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

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in

EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries not intended for use

None

A declaration of conformity is available on www.edimax.com

N20379 AЯ46