EDIMAX
NETWORKING PEOPLE TOGETHER

Wired / Wireless Broadband Router

3G-6200Wg

User Manual

Version 1.0 / 9, 2008

Linux Open Source Code

Certain Edimax products include software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Please see the **GNU** (www.gnu.org) and **LPGL** (www.gnu.org) Web sites to view the terms of each license.

The GPL Code and LGPL Code used in Edimax products are distributed without any warranty and are subject to the copyrights of their authors. For details, see the GPL Code and LGPL Code licenses. You can download the firmware-files at http://www.edimax.com under "Download" page.

※ 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's Manual on the CD-ROM.

※ Software and specifications subject to change without notice. Please visit our web site for the update.

※

Introduction

Thank you for purchasing Edimax 3G-6200Wg wireless 802.11b/g 3G broadband router! This high cost-efficiency router is the best choice for Mobile / Small office / Home office users, all computers and network devices can share a single wireless 3G modem or xDSL / cable** modem internet connection at high speed. Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced. When the number of your computers and network-enabled devices grow, you can also expand the number of network slot by simple attach a hub or switch, to extend the scope of your network!

You can configure the router by running the Setup Wizard in the CD-ROM provided in the package. The wizard provides quick setup for wireless 3G/3.5G 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 this Quick Installation Guide to configure the router

** Note : Only one Internet connection (wireless 3G or xDSL/Cable) can be used at the same time.

Features

- High Internet access throughput
- Allow multiple users to share a single Internet connection
- Supports up to 253 network client users
- Provides two USB port for connecting USB printer
- Internet Access via Cable or xDSL modem
- Access Servers on your LAN from the Public Network
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11g/b wireless LAN access point
- Support DHCP (Server/Client) for easy setup
- Support advance features such as: special applications, DMZ, virtual server, access control, firewall
- Allow you to monitor the router's status such as: DHCP Client Log, System Log, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management
- Remote Management allows configuration and upgrades from a remote site (over the Internet)

Minimum Requirements

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- Computer with a Web-Browser (Internet Explorer 5.0 or higher / Netscape Navigator 7.2 or higher)

Package Contents

- One Wireless broadband router
- One Quick Installation Guide
- One User Manual CD
- One Power Adapter
- Ethernet Cable
- Antenna
- Accessories

Note

The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the

Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by access time.

Back Panel

The diagram (fig1.0) below shows the broadband router's back panel. The router's back panel is divided into four sections, LAN, WAN, USB, and Reset:

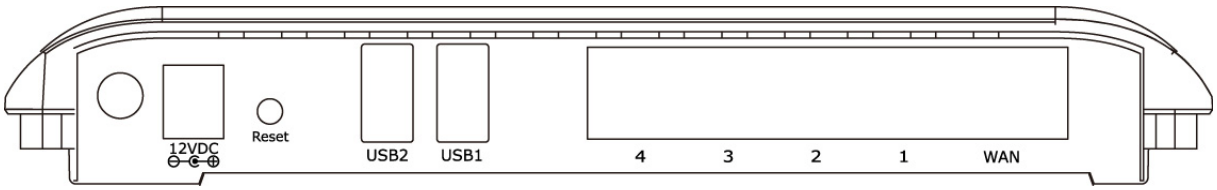


Figure 1.0

1) Local Area Network (LAN)
The Broadband router's 4 LAN ports are where you connect your LAN's PCs, hubs / switches etc.

2) Wide Area Network (WAN)
The WAN port connected to your xDSL or Cable modem which linked to the Internet.

3) USB
The USB ports allow you to share printer through them. Each port can support printer .

4) Reset button
When you experience some problem on using this router, or you forgot your password, you can press the reset button for **longer** than 10 seconds and the router will reset itself to the factory default settings (**warning**: your original configurations will be replaced with the factory default settings)

Front Panel

On the router's front panel there are LEDs, which shows the status of this router. Below is the list of each LED and its description.

Figure 1.1

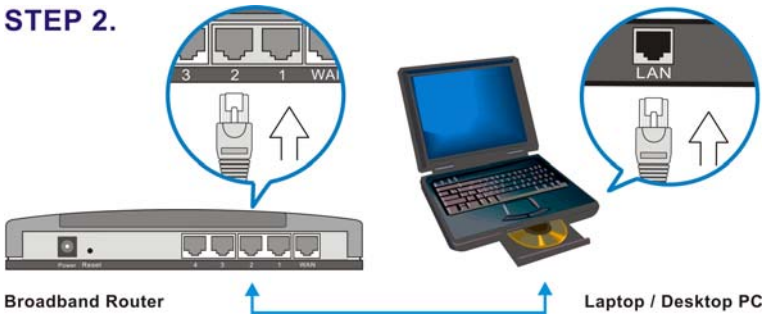
LED	Light Status	Description
PWR	ON	Router is powered on
WAN 10/100M	ON	WAN port is connected at 100Mbps
	Off	WAN port is connected at 10Mbps
WAN LNK/ACT	ON	WAN is connected
	Off	WAN is unconnected
	Flashing	WAN port is sending / receiving data
LAN 10/100M (Port 1-4)	ON	LAN port is connected at 100Mbps
	Off	LAN port is connected at 10Mbps
LAN LNK/ACT (Port 1-4)	ON	LAN port is connected
	Off	LAN port is unconnected
	Flashing	LAN port is sending / receiving data
USB	ON	USB device is connected
	Off	USB device is not connected
	Flashing	USB printer is printing USB modem card is sending / receiving data
WLAN	ON	Wireless LAN has been activated
	Off	Wireless LAN is disabled
	Flashing	Wireless LAN is sending / receiving data

Setup Diagram

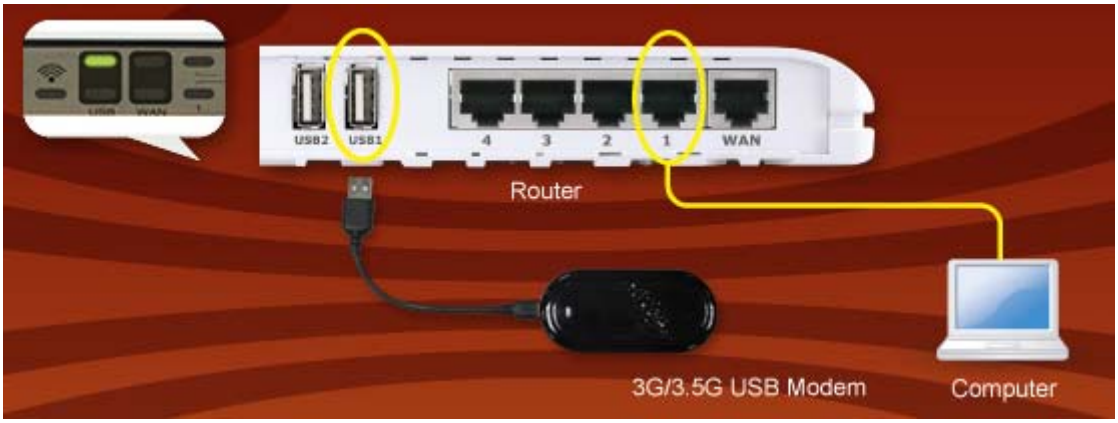
(A) 3G/3.5G Modem card installation:

If you have 3G/3.5G modem card and SIM card, please follow the following instructions to establish connection

1. Connect power adapter to 3G-6200Wg
2. Connect another Ethernet cable from the any LAN ports (1~4) on router to the Ethernet socket on the PC



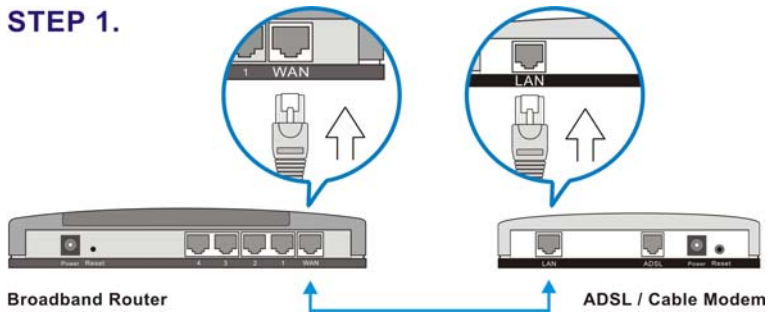
3. Insert SIM card into 3G/3.5G modem card, and connect the modem card with one of USB port of 3G-6200Wg. The corresponding USB LED indicator on 3G-6200Wg will light.



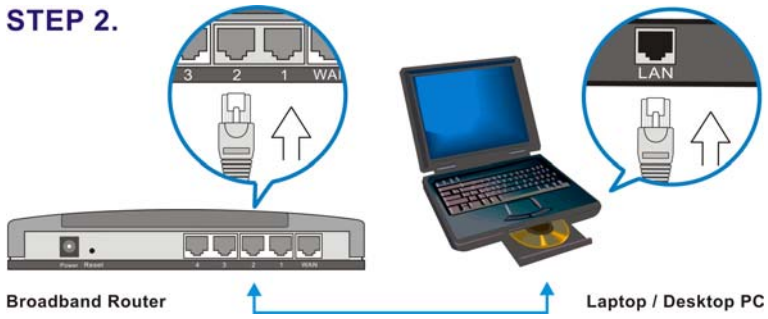
(B) Cabling installation:

If you can also access Internet by xDSL/Cable modem, please follow the following instructions:

1. Connect the Ethernet cable from the router's WAN port to the LAN port of the modem.



2. Connect another Ethernet cable from the any LAN ports (1~4) on router to the Ethernet socket on the PC.



3. Check to make sure the router's LINK LED is lit; to confirm the cable connections are made correctly.

Figure 1.2 below shows a typical setup for a Local Area Network (LAN).

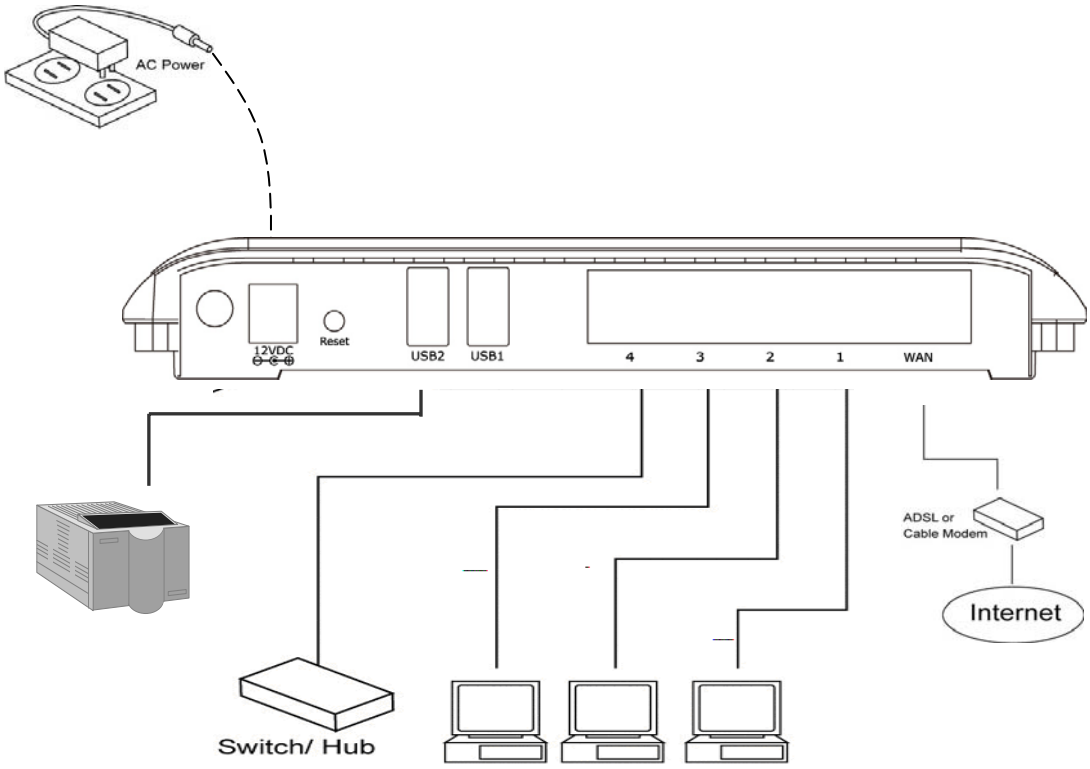


Figure 1.2

Getting started

This is a step-by-step instruction on how to start using the router and get connected to the Internet.

1) Setup your network as shown in the setup diagram above (fig 1.2).

2) You will need to set your LAN PC clients so that it can obtain an IP address automatically. All LAN clients require an IP address. Just like the mailing address in real world, it allows LAN clients to find one another. (If you already configured your PC to obtain an IP automatically, please jump to step 3, page 11)

Configure your PC to obtain an IP address automatically

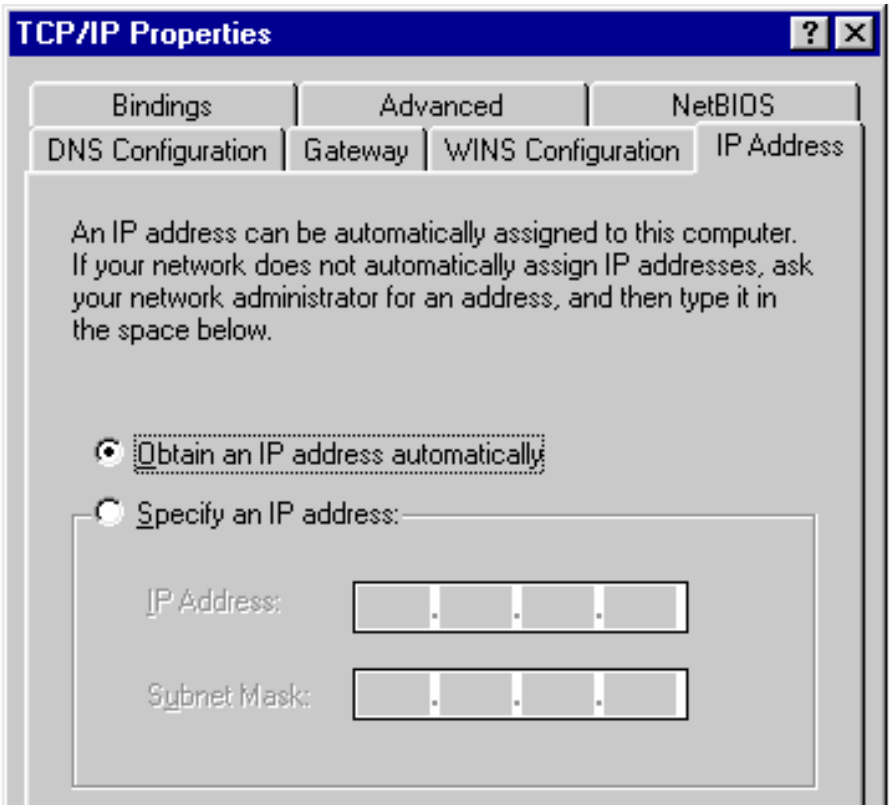
Broadband router's DHCP function is switched on by default; this means that you can obtain an IP address automatically once you've configured your PC to obtain an IP address automatically. This section will show you how to configure your PC's so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating systems. For other operating

systems (Macintosh, Sun, etc.), follow the manufacturer's instructions. The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for:

2a) **Windows 95/98/Me**
2b) **Windows XP**
2c) **Windows 2000,** and
2d) **Windows NT**.

2a) Windows 95/98/Me

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear.
3. Check your list of Network Components. If TCP/IP is not installed, click the *Add* button to install it; if TCP/IP is installed, jump to **step 6**.
4. In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.
5. In the *Select Network Protocol* dialog box, select *Microsoft* and *TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows installation CD to complete the installation.
6. After installing TCP/IP, go back to the Network dialog box. Select TCP/IP from the list of Network Components and then click the Properties button.
7. Check each of the tabs and verify the following settings:
   - **Bindings**: Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
   - **Gateway**: All fields are blank.
   - **DNS Configuration**: Select *Disable DNS.*
   - **WINS Configuration**: Select *Disable WINS Resolution.*
   - **IP Address**: Select *Obtain IP address automatically*.



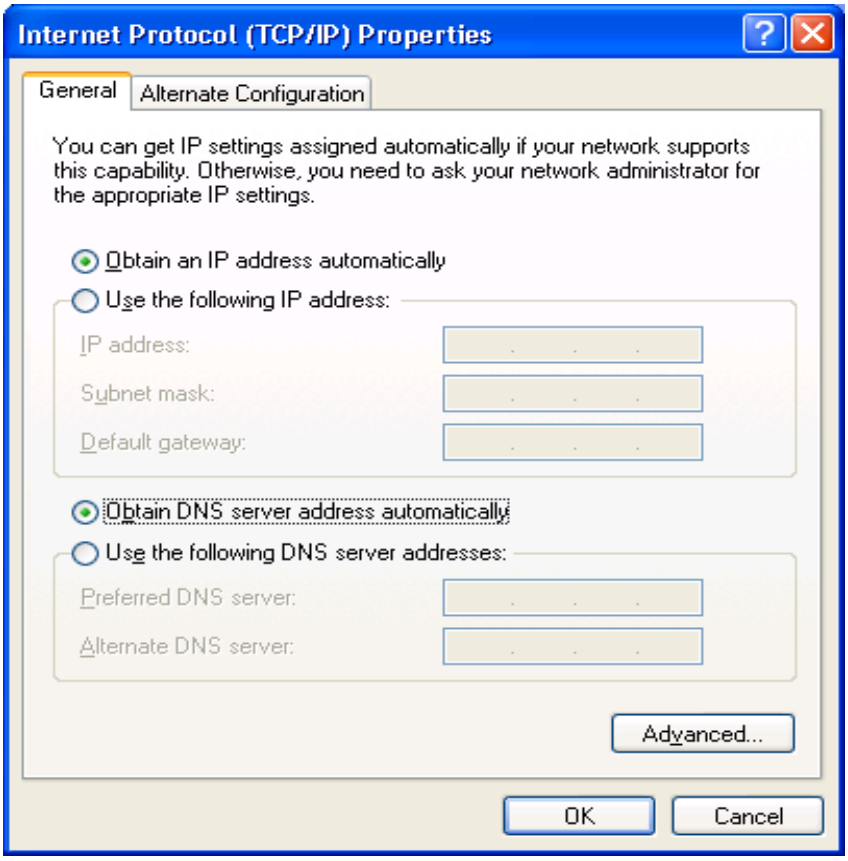
8. Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2b) Windows XP

1. Click the *Start* button and select *Settings*, then click *Network Connections.* The *Network Connections* window will appear.
2. Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
4. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



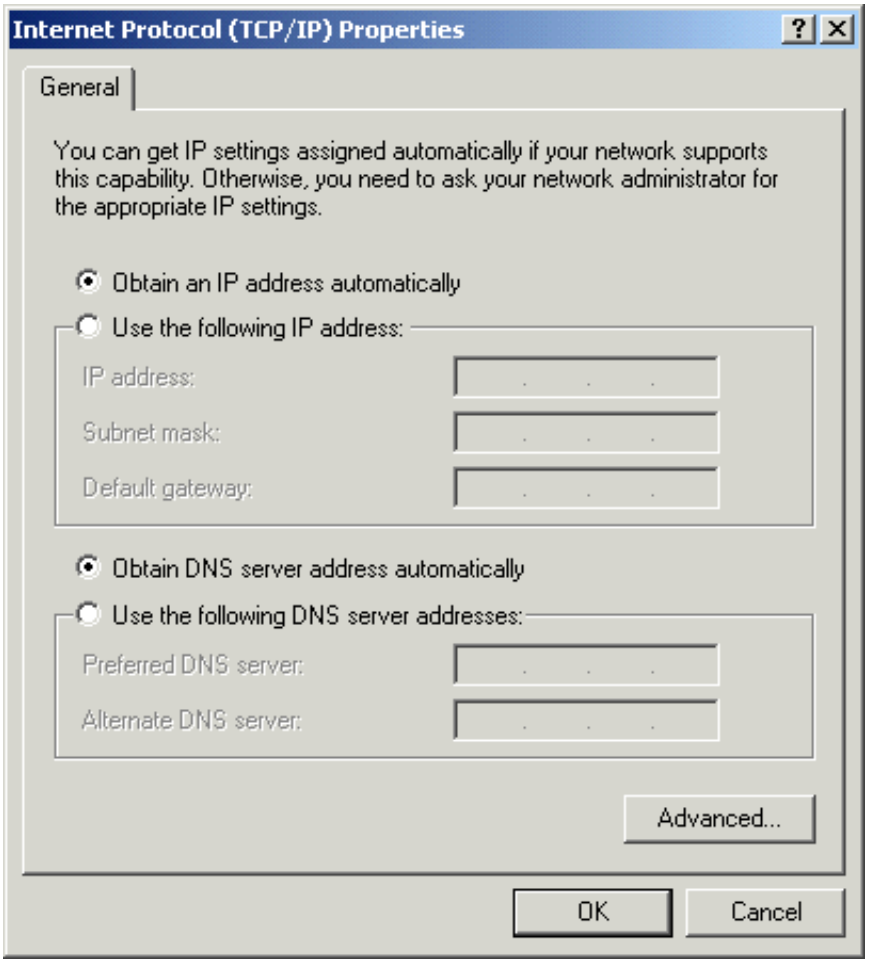
5. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2c) Windows 2000

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. In the *Local Area Connection* window, click the *Properties* button.
4. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
5. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



6. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

.

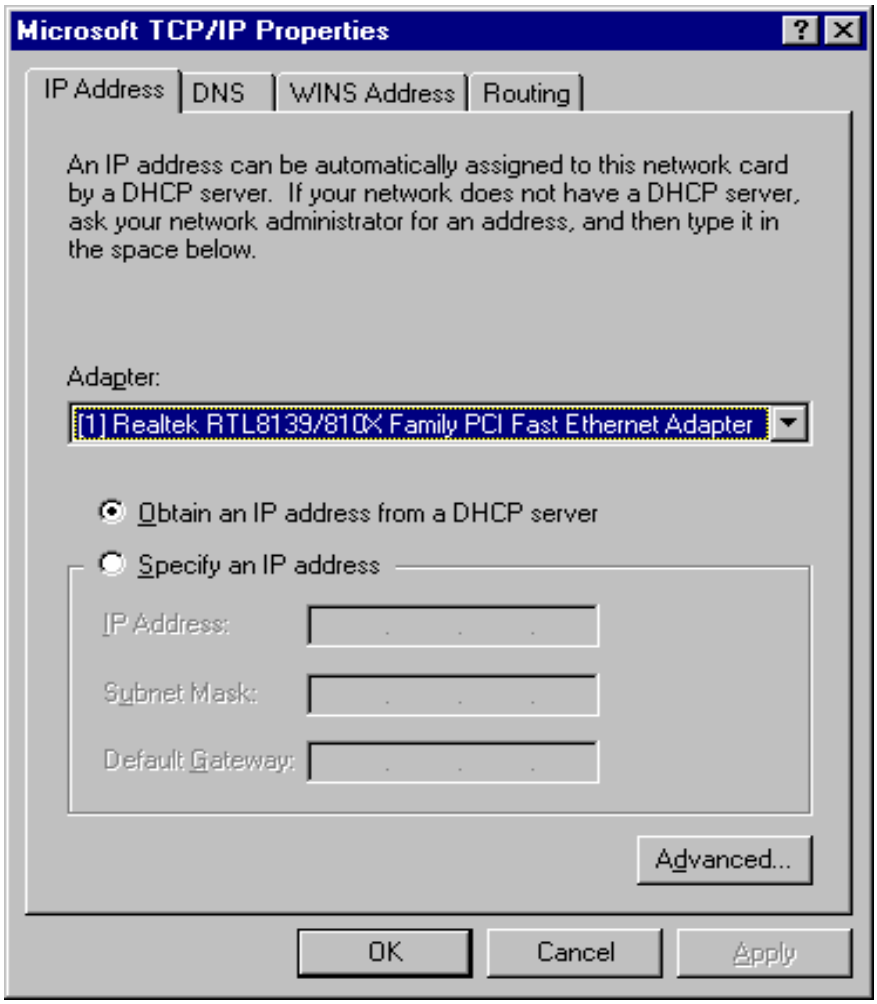
2d) Windows NT

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

2. Double-click *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.

3. Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 5**.

4. In the *Select Network Protocol* window, select the *TCP/IP Protocol* and click the *Ok* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
5. After you install TCP/IP, go back to the Network window. Select TCP/IP from the list of Network Protocols and then click the Properties button.
6. Check each of the tabs and verify the following settings:
   - **IP Address:** Select *Obtain an IP address from a DHCP server*.
   - **DNS:** Make all fields blank.
   - **WINS:** Make all fields blank.
   - **Routing:** Make all fields blank.



7. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

3) Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give each of your LAN clients an IP address. By default the Broadband Router's DHCP server is enabled so that you can obtain an IP address automatically. To see if you have obtained an IP address, see Appendix A.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off. (To disable the Broadband router's DHCP server see chapter 2 LAN Port)

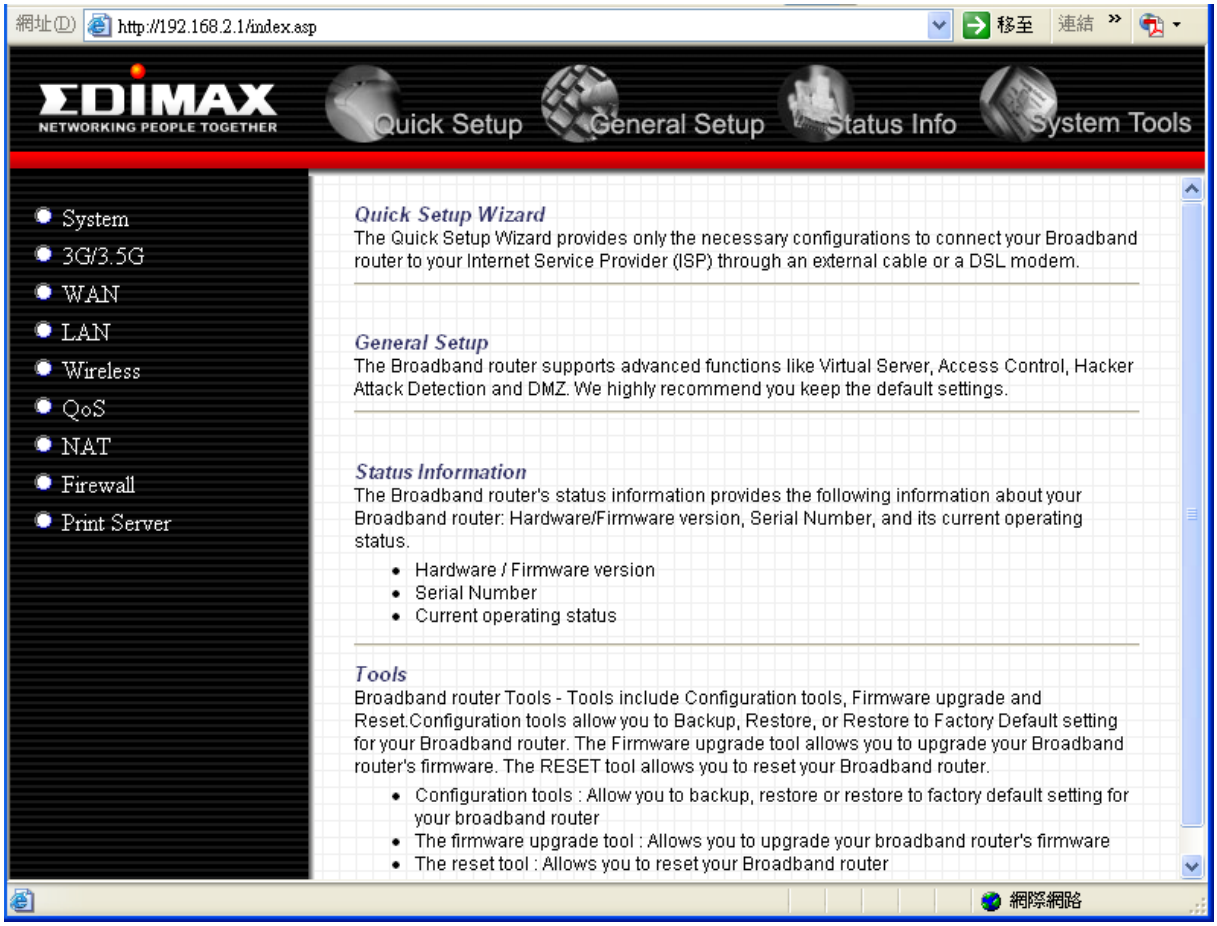
4) Once your PC has obtained an IP address from your router, enter the default IP address **192.168.2.1** (broadband router's IP address) into your PC's web browser and press <enter>

5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

Note: By default the user name is "**admin**" and the password is "**1234**". For security reasons it is recommended that you change the password as soon as possible (in General setup/system/password, see chapter 2)

6) The **HOME** page screen below will appear. The **Home** Page is divided into

four sections, **Quick Setup Wizard**, **General Setup**, **Status Info** and **System Tools.**



Quick Setup Wizard *(Chapter 1)*
Select your Internet connection type and setup the configurations needed to connect to your Internet Service Provider (ISP).

General Setup *(Chapter 2)*
This section contains configurations for the Broadband router's advanced functions such as: address mapping, virtual server, access control, hacker attack prevention, DMZ, special applications and other functions to meet your needs.

Status Info *(Chapter 3)*
In this section you can see the Broadband router's system information, Internet Connection, Device Status, System Log, Security Log and DHCP client information.

Tools *(Chapter 4)*

This section contains the broadband router’s tool sets - tools include configuration, firmware upgrade and Reset. Configuration tools allow you to backup (save), restore, or restore to factory default configuration for your Broadband router. The firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

7) Click on **Quick Setup Wizard** (see chapter 1) to start configuring settings required by your ISP so that you can start accessing the Internet. The other sections (General Setup, Status Information and Tools) do not need to be configured unless you wish to implement/monitor more advanced features/information.
Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter.

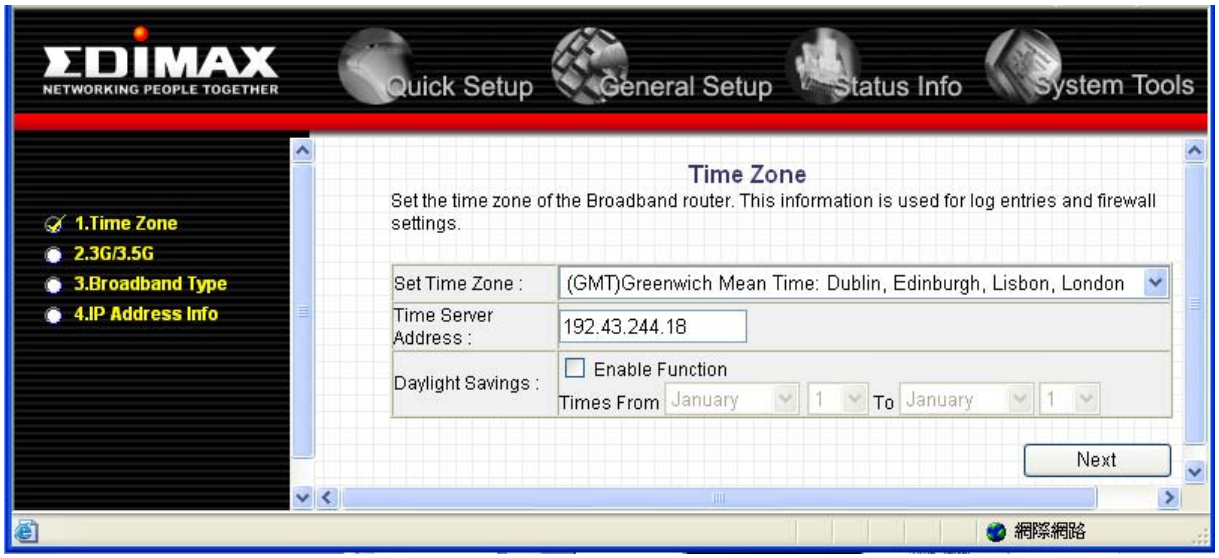
Chapter 1

Quick Setup

The Quick Setup section is designed to get you using the broadband router as quickly as possible. In the Quick Setup you are required to fill in only the information necessary to access the Internet. Once you click on the **Quick Setup Wizard** in the HOME page, you should see the screen below.

Step 1) Time Zone

The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as log entries and firewall settings.



Parameter	Description
Set Time Zone	Select the time zone of the country you are living. The router will set its time based on your selection
Time Server Address	You can manually assign time server address if the default time server dose not work
Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below)
Times From	Select the period in which you wish to start using daylight saving
Times to	Select the period in which you wish to stop using daylight saving

Click on **NEXT** to proceed to the next page (step 2): Broadband Type.

Step 2) 3G/3.5G Internet Configuration

3G-6200Wg supports most of 3G/3.5G modem cards, just connect the modem card to the USB port of 3G-6200Wg and 3G-6200Wg will recognize it automatically, no additional setup procedure required. However, some of modem cards require PIN code or account / password (you have to use 3G-6200Wg's web interface to input these information), and some modem cards requires you to connect the modem card with your PC and install driver / utility before you connect it with 3G-6200Wg (all PCs which need to access Internet by 3G-6200Wg requires to perform this procedure once). If you still not able to connect to Internet, please use wired Internet connection to access our website :http://www.edimax.com/ ,download latest version of firmware and upgrade 3G-6200Wg's firmware. If you still not be able to get connected by your 3G/3.5G modem card, please contact your dealer of purchase and provide the model name of the 3G/3.5G modem card you have, we'll try our best to help you to solve the problem.

Only one Internet connection (wireless / wired) can be used at the same time. Wireless connection (3G/3.5G) will be selected first, and use wired Internet connection as backup. Therefore, please DO NOT connect your 3G/3.5G modem card with 3G-6200Wg, or your telecomm service provider may charge you with high communication fee. For example, if you connect 3G/3.5G modem card with 3G-6200Wg when you're using wired Internet connection, wired connection will be dropped and use 3G/3.5G wireless connection instead. If 3G/3.5G wireless signal reception is poor and the connection can not be restored within 60 seconds, 3G-6200Wg will use wired Internet connection again, and will not switch back to wireless Internet connection (This only happens with wired Internet connection is available. If wired connection is unavailable, 3G-6200Wg will try to establish 3G/3.5G wireless connection again and again). If you want to use 3G/3.5G wireless connection again, you need to remove 3G/3.5G modem card from 3G-6200Wg and reconnect it back after 5 seconds.

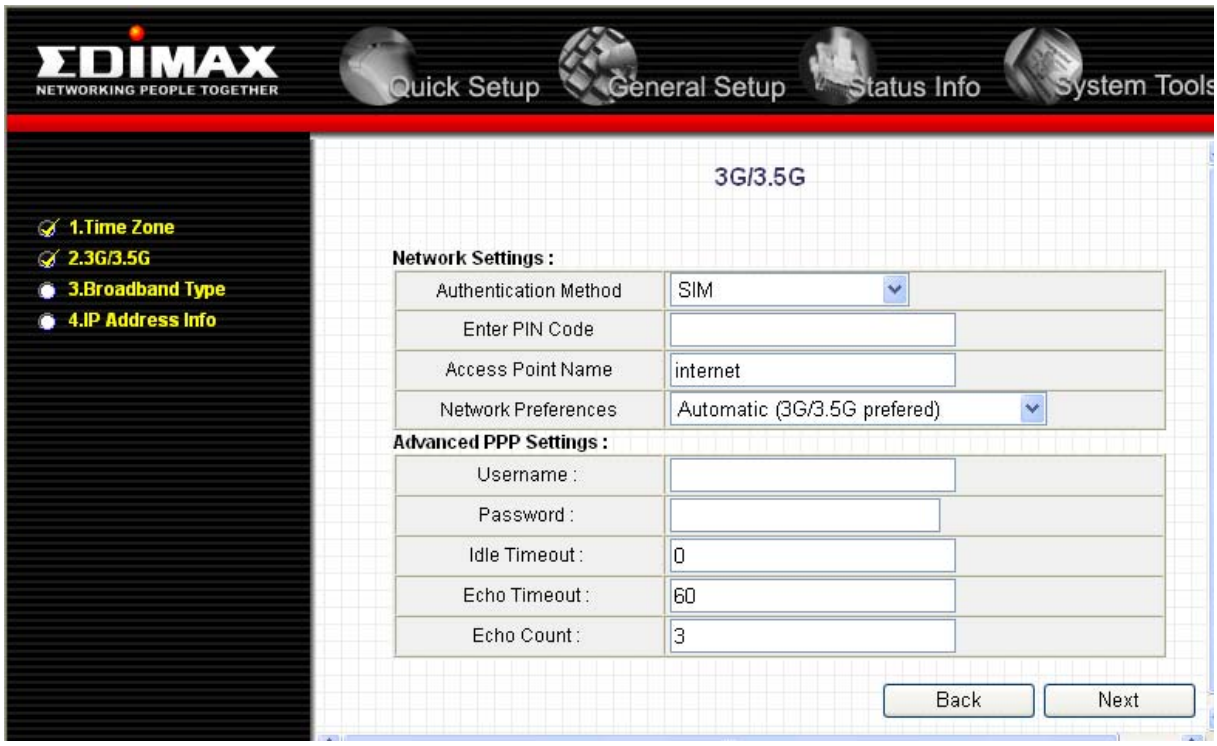
(A) Plug and play, no setup procedure required.

Connect the USB 3G/3.5G modem card with 3G-6200Wg and make sure the corresponding USB LED indicator of 3G-6200Wg lights up, then you can use the web browser to access Internet.

(B) PIN code or user name / password required:

Please check the authentication method you want to use. Most of telecomm service providers require you to input PIN Code, please check 'SIM' and input the PIN code provided by telecomm service provider. Most of options listed here are optional and you don't have to provide those information if telecomm service provider doesn't provide you with those information.
If telecomm provider provides you with username / password, please check /User

Name / Password box and input the user name / password provided by telecomm service provider, then click ‘APPLY’ button. Wait for 1 minute (for 3G-6200Wg to reboot), then you can access Internet.



(C) Driver / Utility required on PC side

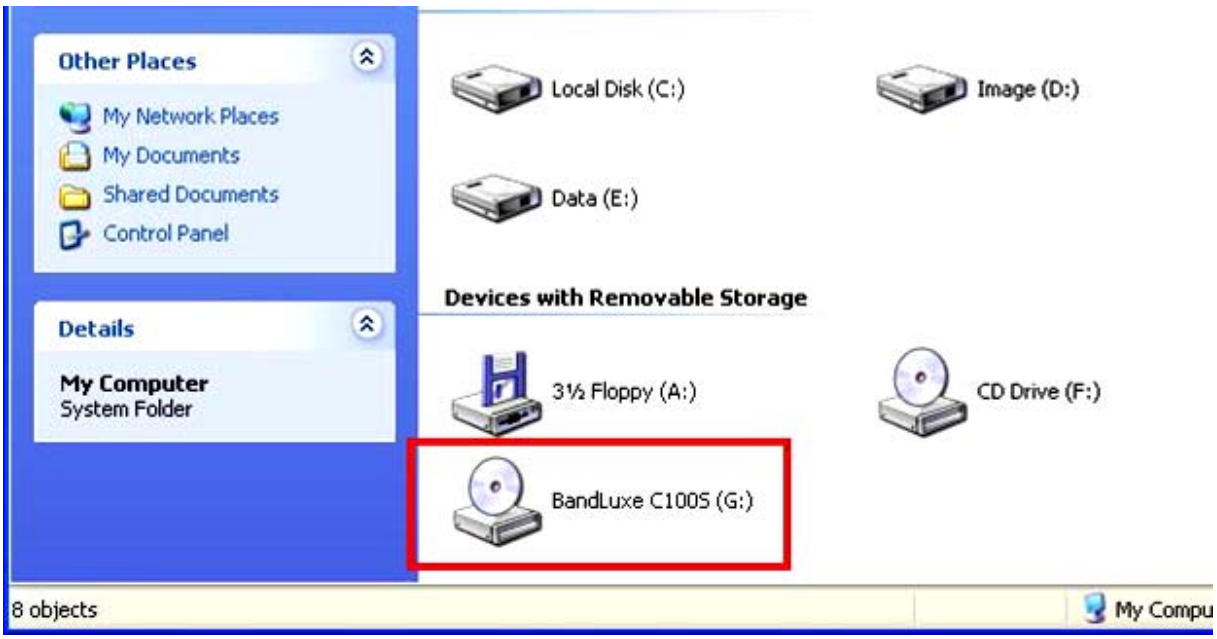
Some 3G/3.5G modem card does not work with instructions (A) or (B) listed above (ex. BandLuxe C100S). You need to install 3G/3.5G modem card driver / utility on every PC which needs to access Internet first. After driver / utility installation is complete, every PC will be able to access Internet via 3G/6200Wg.

1. Plug in the BandLuxe C100S modem card to the USB port of your computer.

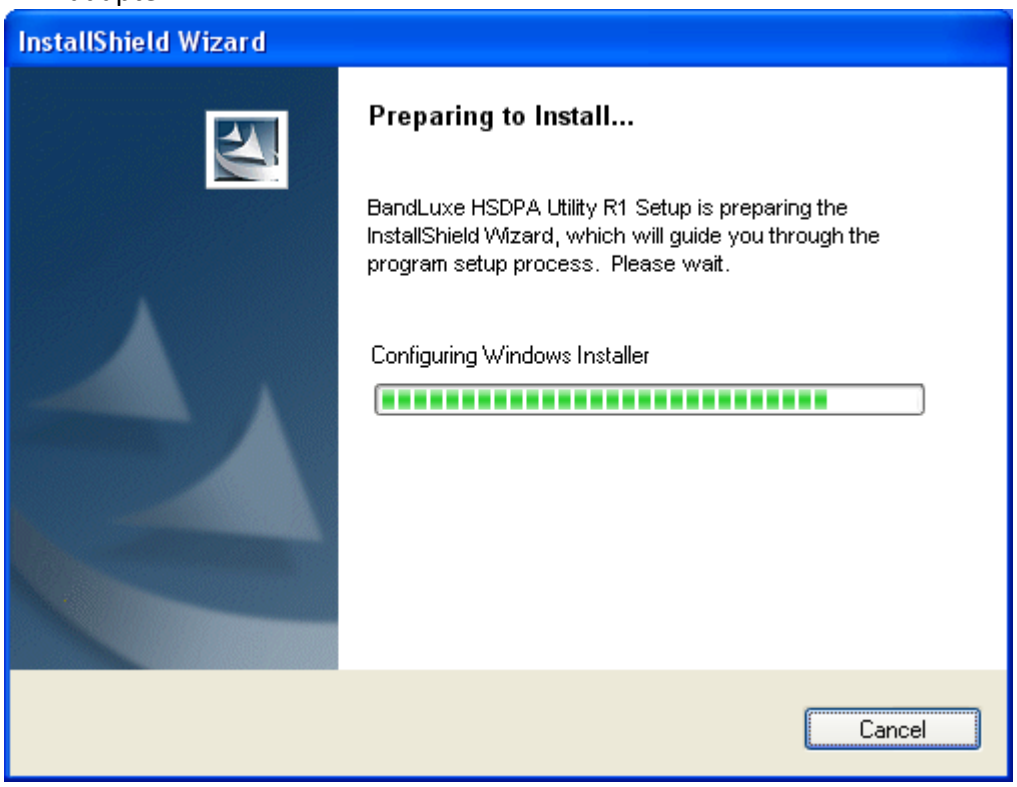
2. The system will detect the hardware of C100S USB adapter and also the storage inside the adapter.

3. Please click “Cancel” to ignore the message of the found new hardware wizard.

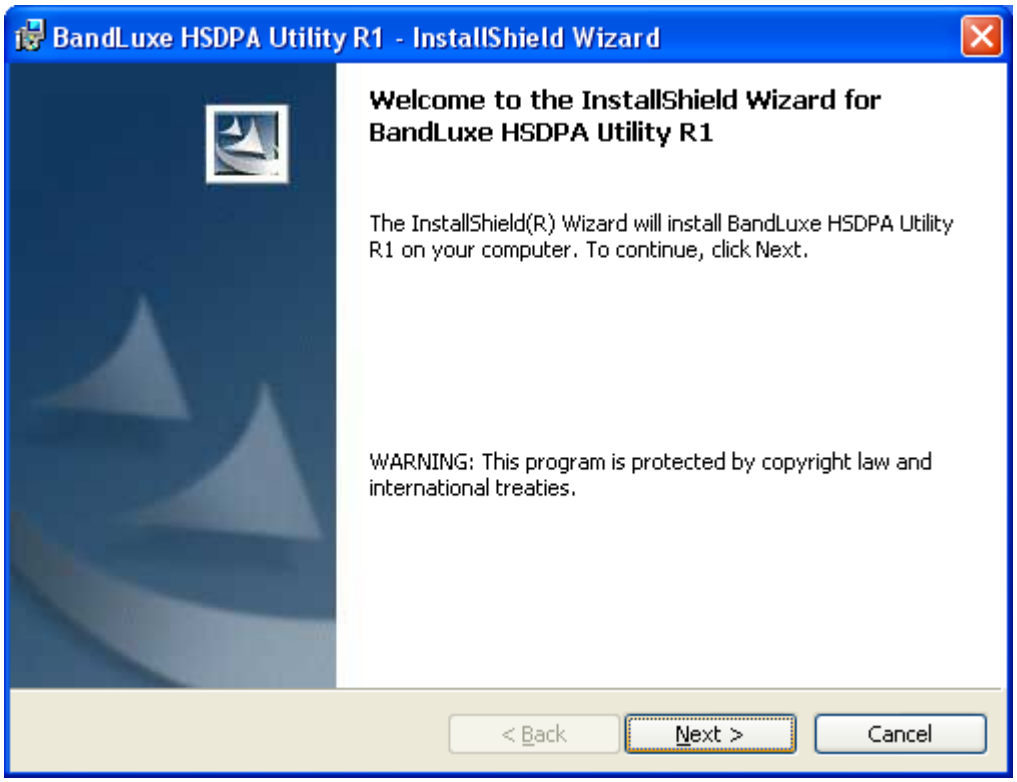
4. Please go to “My computer”, you will see the BandLuxe C100S. Double click the device.



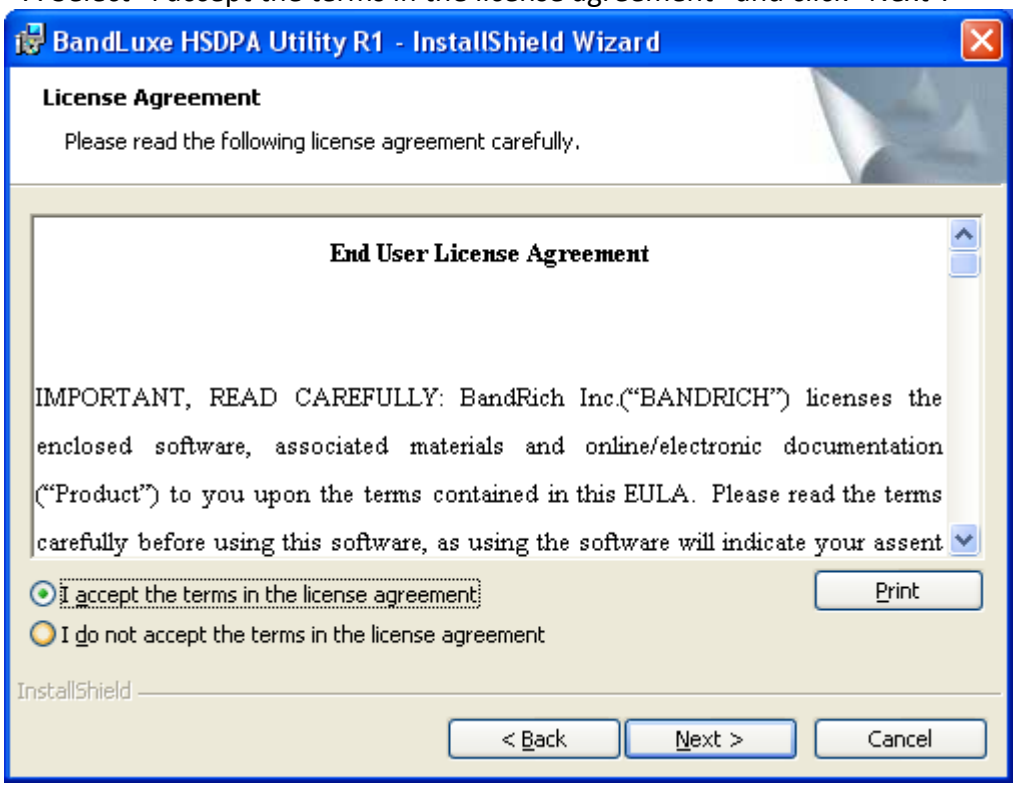
5. The program inside the adapter will prepare to install the driver and utility of the adapter.



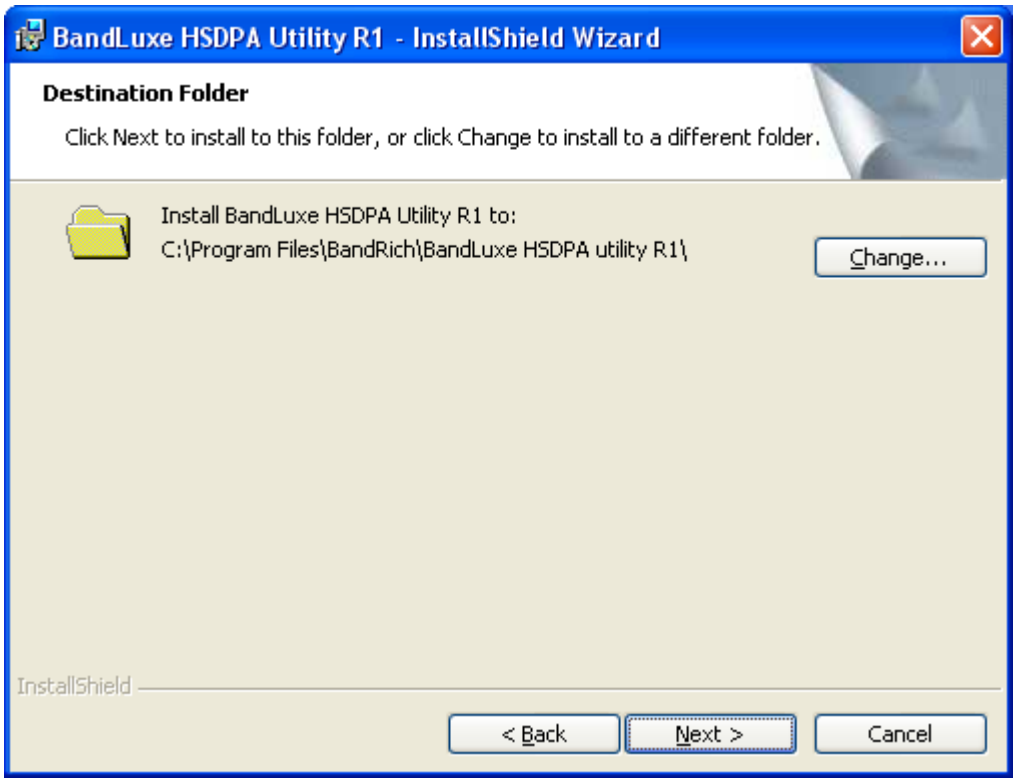
6. Click “Next”.



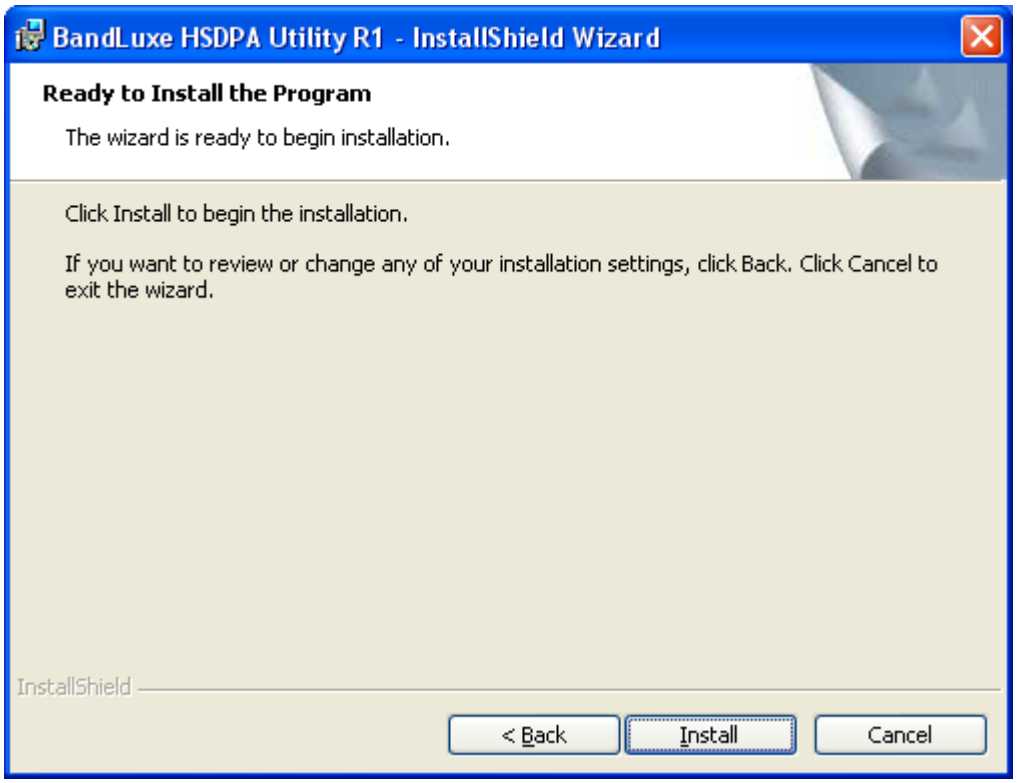
7. Select “I accept the terms in the license agreement” and click “Next”.



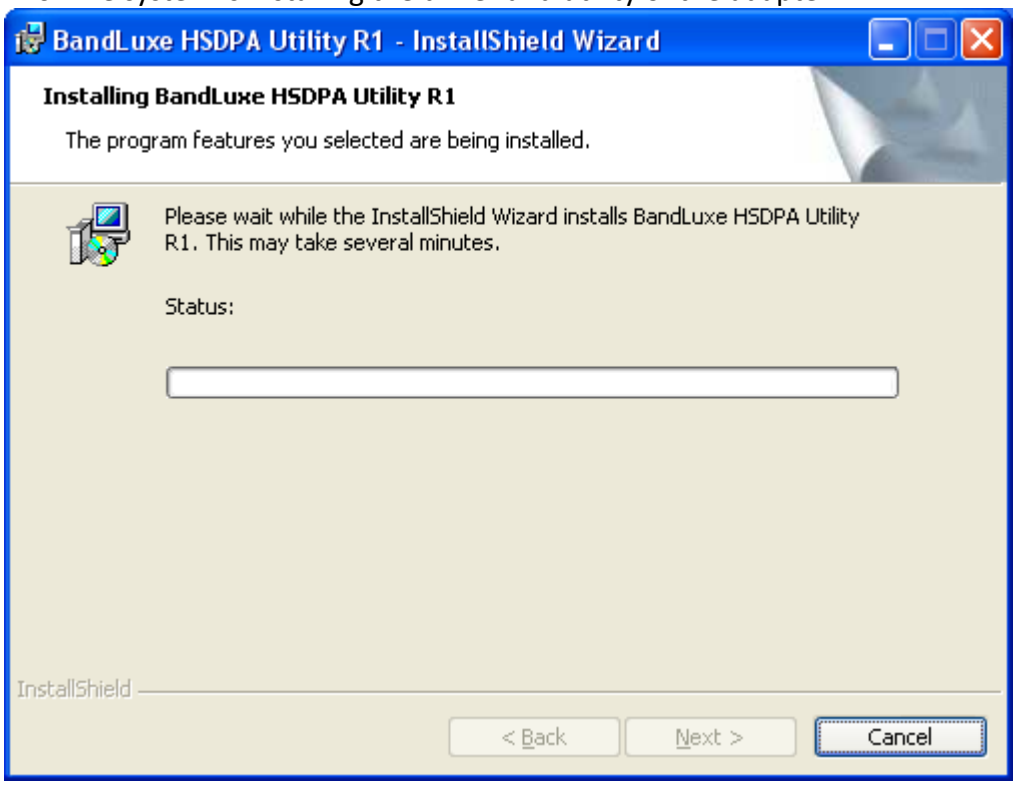
8. If you want to change the destination folder, please click “Change”. Click “Next” to continue.



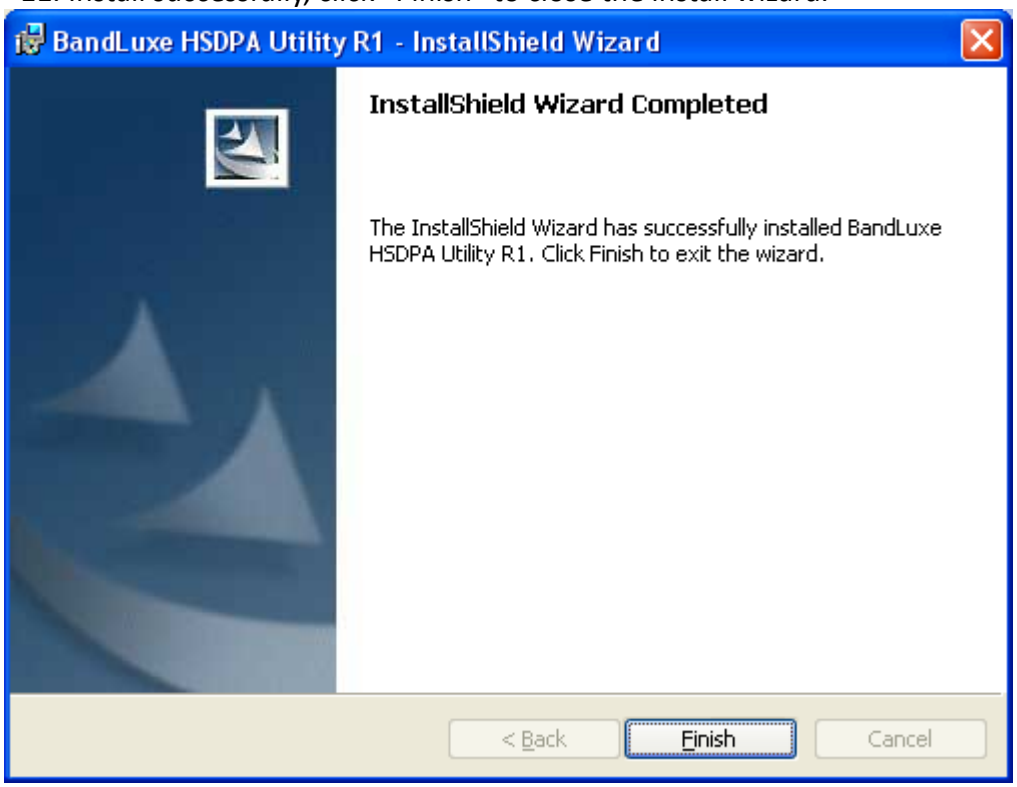
9. Click “install”.



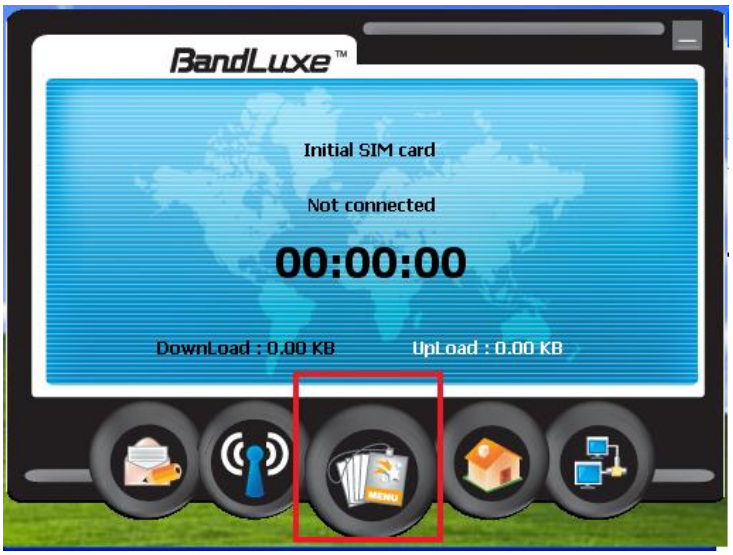
10. The system is installing the driver and utility of the adapter.



11. Install successfully, click “Finish” to close the install wizard.



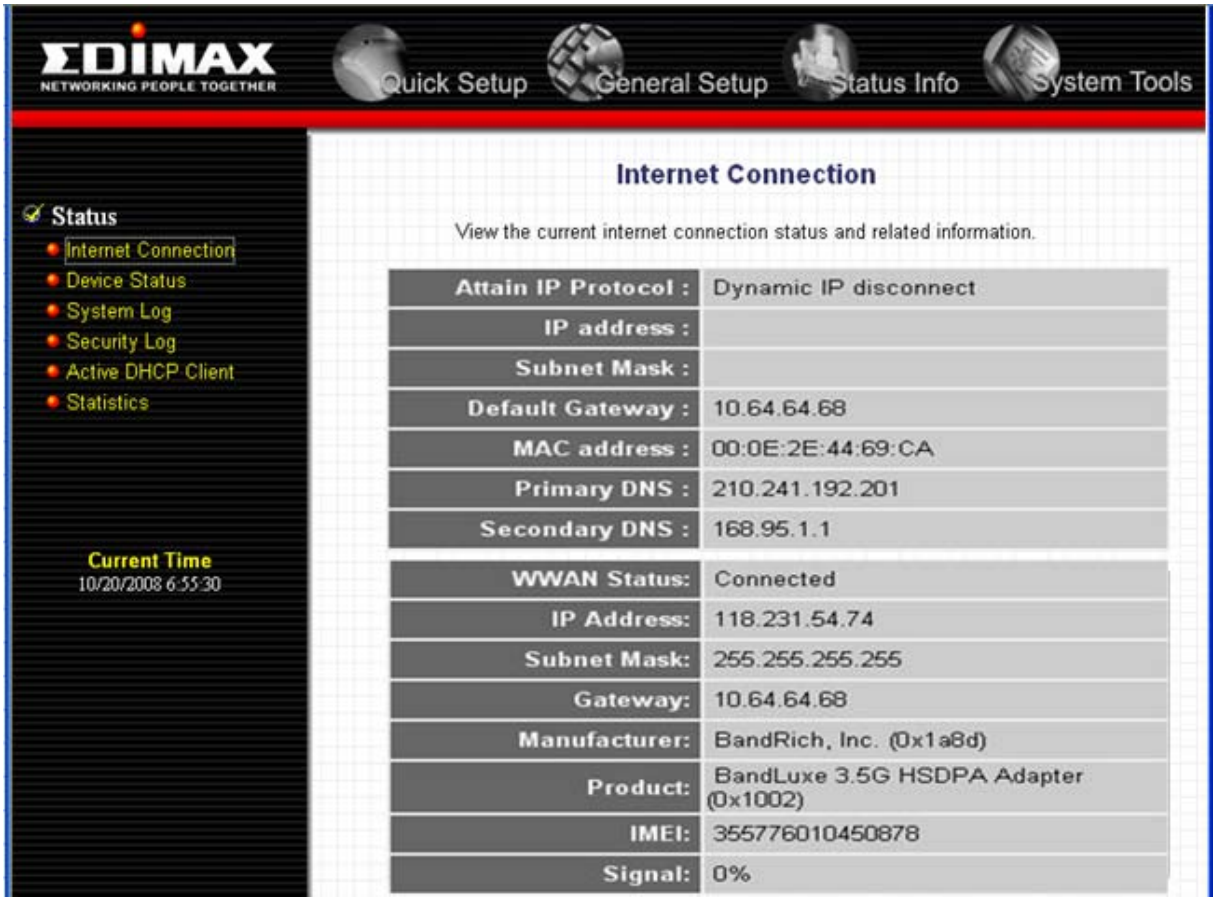
12. The utility of C100S will start up automaticity.
    Please select the “MENU”



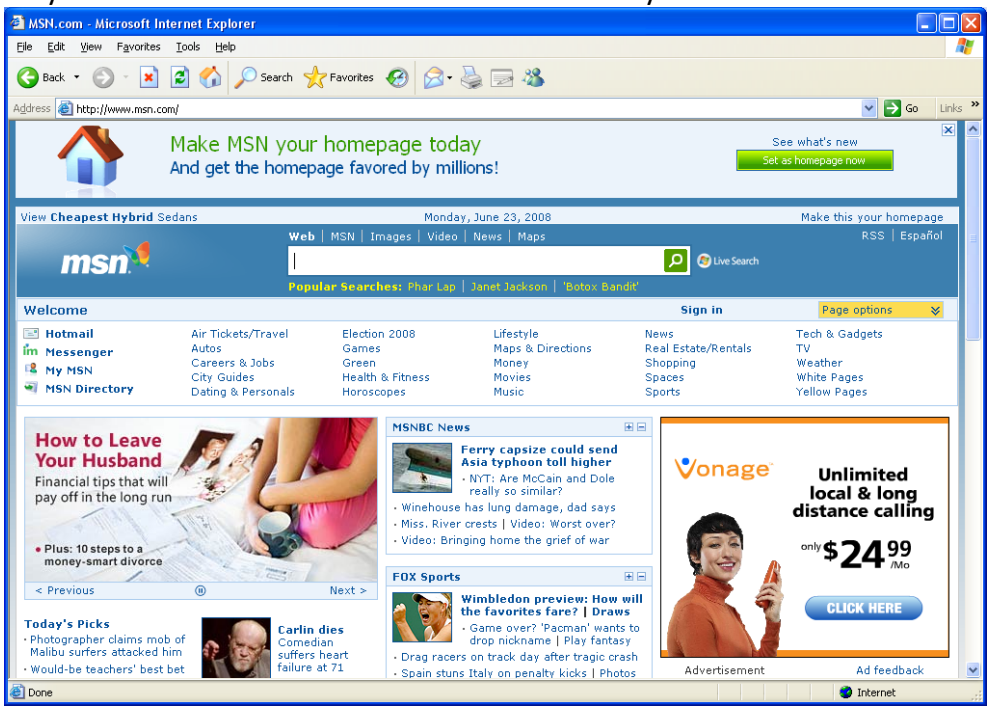
13. Click “Setting”.

14. Select the “Auto connect on startup”.

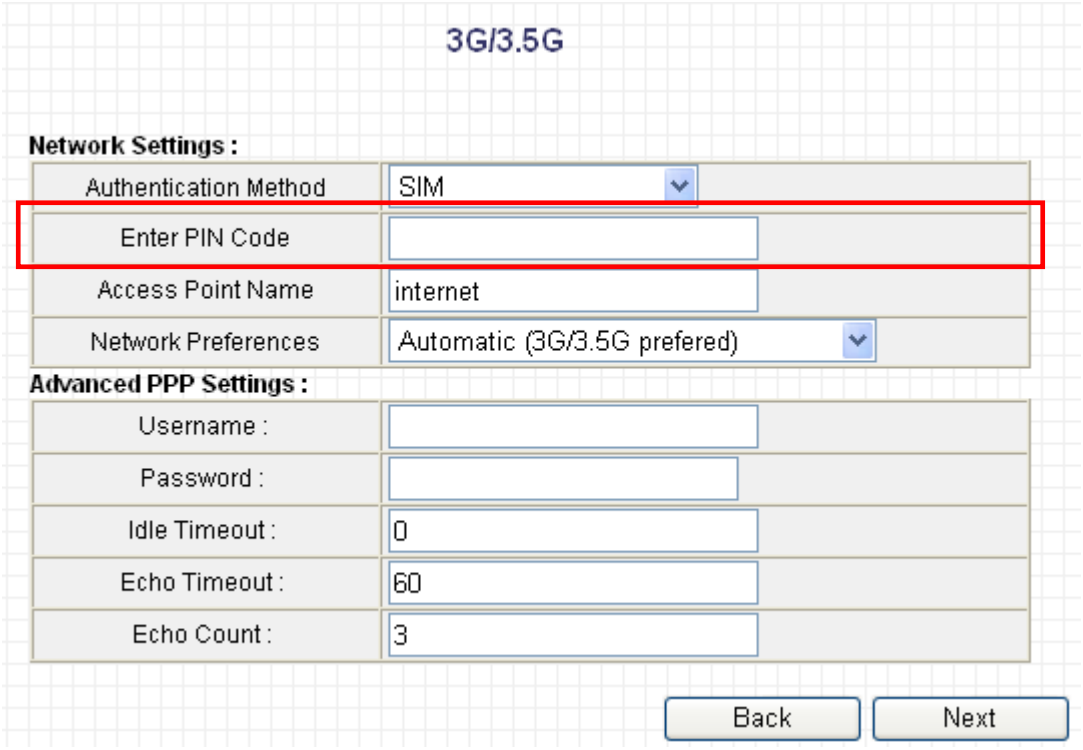
15. Plug in the C100S into the USB port of the 3G router.
16. The USB adapter will get the IP address from ISP automatically. You can check the Status of the 3G-6200Wg on the Web site (ex: 192.168.2.1).



17. Now you are able to connect to Internet successfully.



Note : If your SIM card requires entering the PIN code, please enter into the web management of the 3G router. In WAN setting web page, select 3G/3.5G. Enter the PIN code of the adapter.



Step 3) Broadband Type

3G-6200Wg provides two types of Internet connection method: wireless (3G/3.5G) or wired connection. You can access internet via USB 3G/3.5G modem card, or via wired xDSL / cable modem connection. However, only one connection method (wireless or wired) can be used at the same time.

In this section you have to select one of six types of connections that you will be using to connect your broadband router's WAN port to your ISP (see screen below).

Note: Different ISP's require different methods of connecting to the Internet, please check with your ISP as to the type of connection it requires.

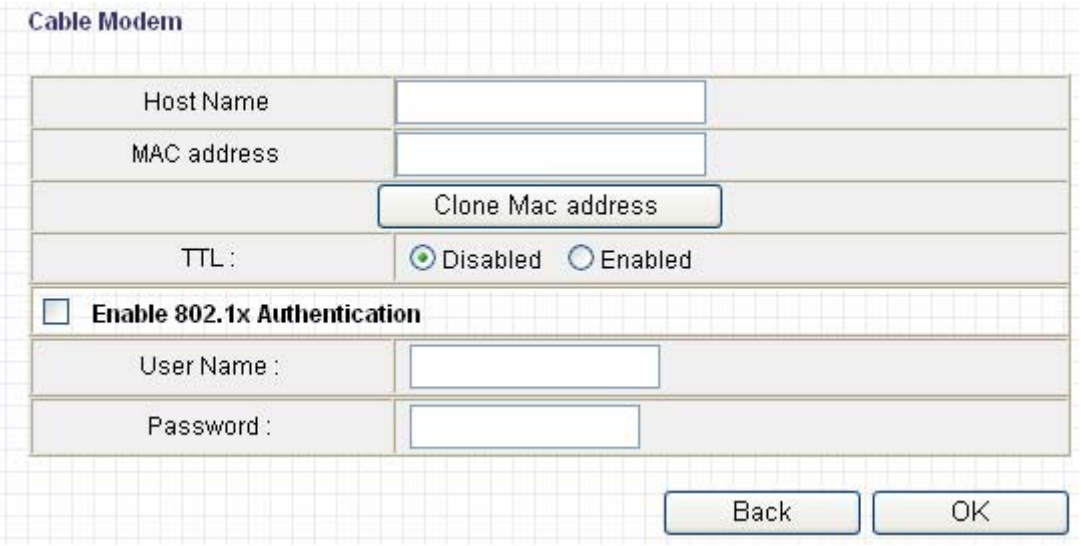
Menu	Description
Cable Modem	Your ISP will assign you with an IP address automatically
Fixed-IP xDSL	Your ISP gave you an IP address already
PPPoE xDSL	Your ISP requires you to use Point-to-Point Protocol over Ethernet (PPPoE)
PPTP xDSL	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP)
L2TP xDSL	Your ISP requires you to use a Layer Two Tunneling Protocol (L2TP)
Telstra Big Pond	This Protocol only used for Telstra Big Pond Internet service in Australia

Click on one of the WAN type and then proceed to the manual's relevant sub-section (**1.1**, **1.2**, **1.3**, **1.4**, **1.5** or **1.6**). Click on **Back** to return to the previous screen.

1.1 Cable Modem

Choose Cable Modem if your ISP will assign you with an IP address automatically **(i.e. DHCP)**. Some ISP's may also require that you fill in additional information such as host name and MAC address (see screen below).

Note: The Host Name and MAC address section is *optional* and you can skip this section if your ISP does not require these settings.



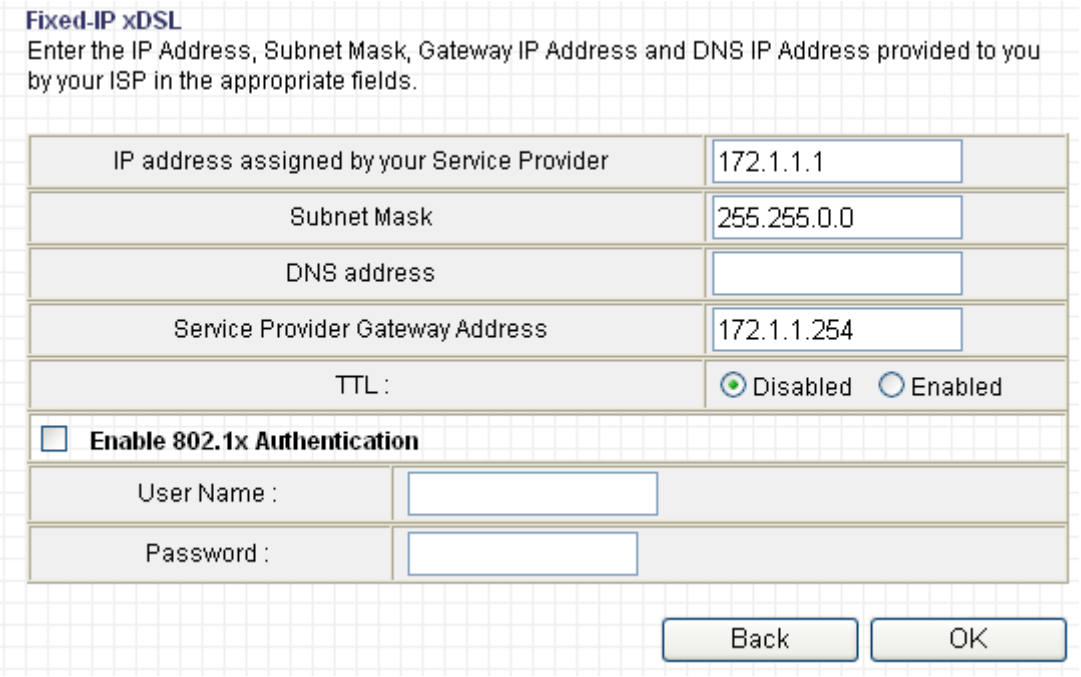
Parameters	Description
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP, otherwise leave it blank if your ISP does not require a Host Name.
MAC Address	Your ISP may require a particular MAC address to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address)

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the Cable Modem connection. You can start using the router now, if you wish to use some of the advance features

supported by this router see chapter 2, 3, 4.

1.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.

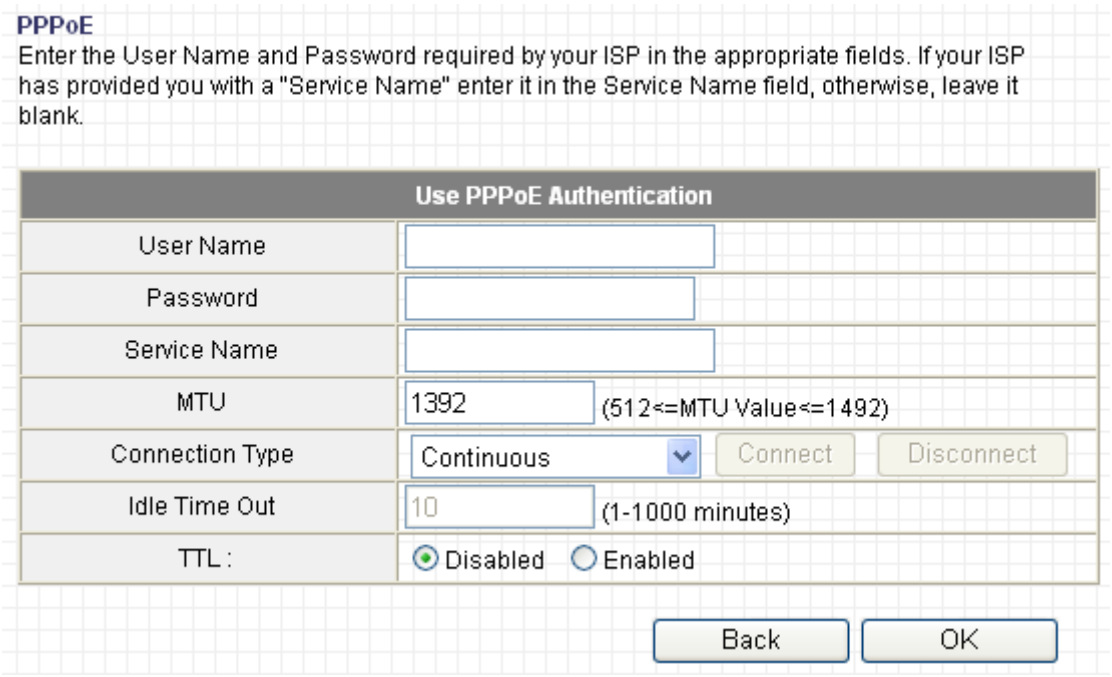


Parameters	Description
IP address	This is the IP address that your ISP has given you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
DNS address	This is the ISP's DNS server IP address
Gateway IP address	This is the ISP's IP address gateway

Click <OK> when you have finished the configuration above. Congratulations! You have completed the configuration for the Fixed-IP x DSL connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3,

1.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



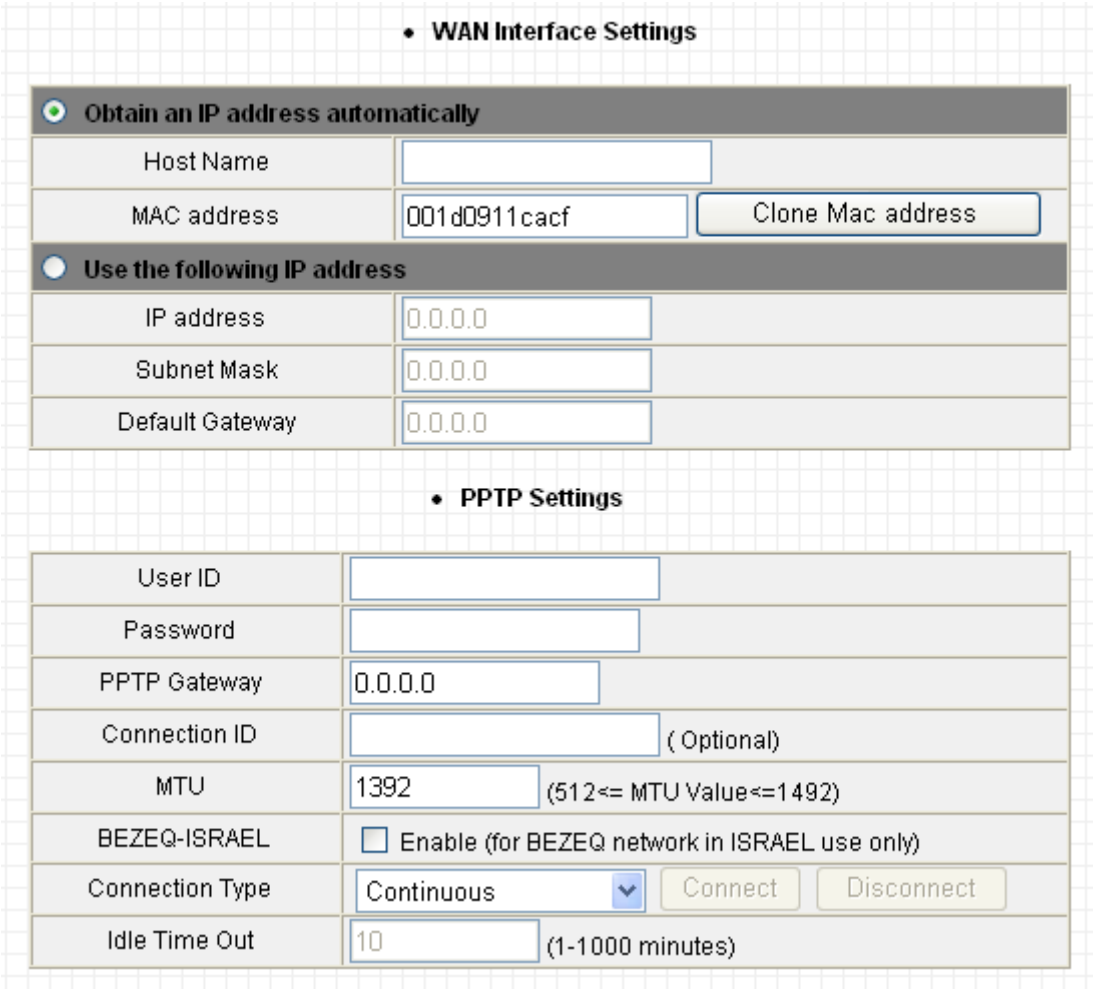
Parameter	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection
Password	Enter the Password provided by your ISP for the PPPoE connection
Service Name	This is optional. Enter the Service name of your ISP when your ISP requires it, otherwise leave it blank.
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you to not wish to set the maximum packet size. Please ask your ISP for detailed information.
Connection Type	If you select “Continuous”, the router will maintain the connection to the ISP. If the WAN connection drops, the router will reconnect to the ISP automatically. If you select “Connect On Demand”, the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will drop the WAN connection if the time period that no one is using the Internet exceeds the “Idle Time”.

	If you select “Manual”, the router will connect to ISP only when you click “Connect” manually from the Web management interface. The WAN connection will not disconnect because of idle timeout. If the WAN line drops and connected at a latter time again, the router will not connect to the ISP by itself.
Idle Time	You can specify an idle time (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection to your ISP. **Note:** This “idle timeout” function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends data to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially when your ISP charge you by the connection time.

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the PPPoE connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



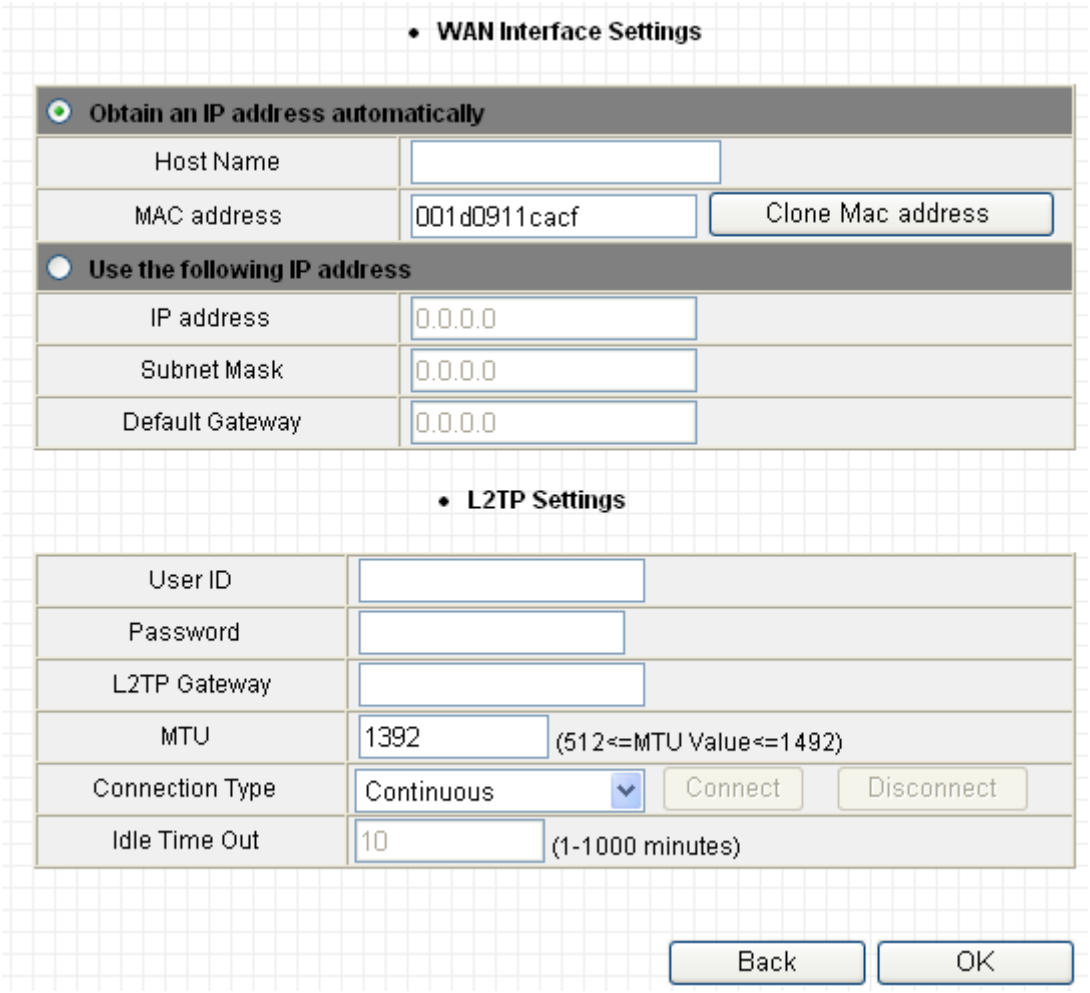
Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server.
Use the following IP Address	The ISP gave you a static IP to be used to connect IP address to the PPTP server
IP Address	This is the IP address that your ISP gave you to establish a PPTP connection
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway
User ID	Enter the User Name provided by your ISP for the PPTP

	connection. Sometimes called as Connection ID
Password	Enter the Password provided by your ISP for the PPTP connection
PPTP Gateway	If your LAN has a PPTP gateway, then enter that PPTP gateway's IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address, same as above
Connection ID	This is the ID given by your ISP, and this is optional.
BEZEQ-ISRAE	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select "Continuous", the router will maintain the connection to the ISP. If the WAN line breaks down and links again at a latter time, the router will reconnect to the ISP automatically; if you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web management interface. The WAN connection will not be disconnected because of idle timeout. If the WAN line breaks down and got connected again at a latter time, the router will not connect to the ISP by itself.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets has been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection to your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the PPTP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the L2TP server.
MAC Address	Your ISP may require a particular MAC address to connect to the Internet. This MAC address is the PC's MAC address that you originally made your Internet connection. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN

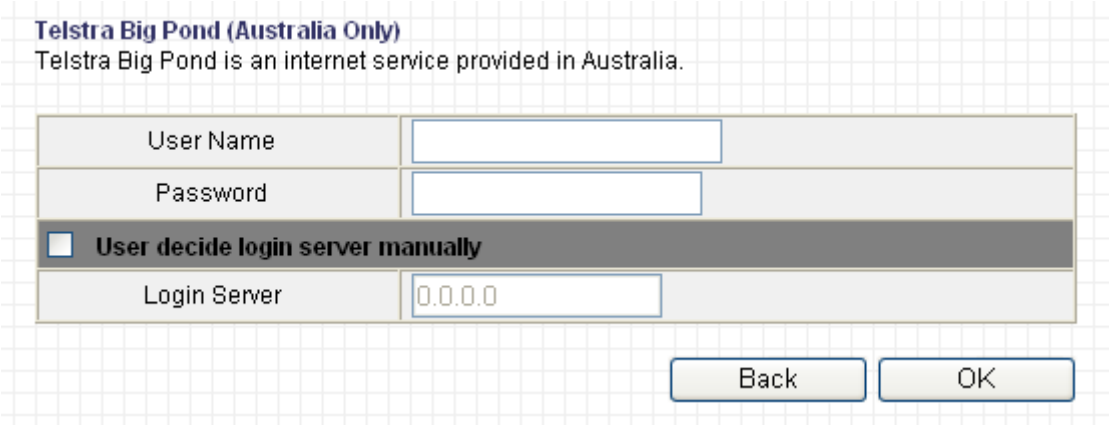
	MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address)
Use the following IP Address	The ISP gave you a static IP to be used to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP Gateway
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID
Password	Enter the Password provided by your ISP for the PPTP connection
L2TP Gateway	If your LAN has a L2TP gateway, then enter that L2TP gateway IP address here. If you do not have a L2TP gateway then enter the ISP’s Gateway IP address above
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Keep default value if you do not wish to set a maximum packet size.
Connection Type	If you select “Continuous”, the router will maintain the connection to the ISP. If the WAN line breaks down and links again at a latter time, the router will auto-reconnect to the ISP. If you select “Connect On Demand”, the router will connect to the ISP automatically when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the “Idle Time”. If you select “Manual”, the router will connect to ISP only when you click “Connect” manually from the Web user interface. The WAN connection will not be disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not connect to the ISP by itself.
Idle Time Out	The WAN “idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even

	when you are not using the Internet. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used. Due to the many uncontrollable issues, we do not guarantee the WAN “idle timeout" auto-disconnect function will always work. In order to prevent from extra connection fee, please **TURN OFF THE ROUTER WHEN YOU ARE NOT USING INTERNET**.

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the L2TP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.



Parameter	Description
User Name	Enter the User Name provided by your ISP for the Telstra Big Pond connection
Password	Enter the Password provided by your ISP for the Telstra Big Pond connection
User decide login server manually	Select if you want to assign the IP of Telstra Big Pond’s login server manually.
Login Server	The IP of the Login Server.

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the Telstra Big Pond connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

Chapter 2

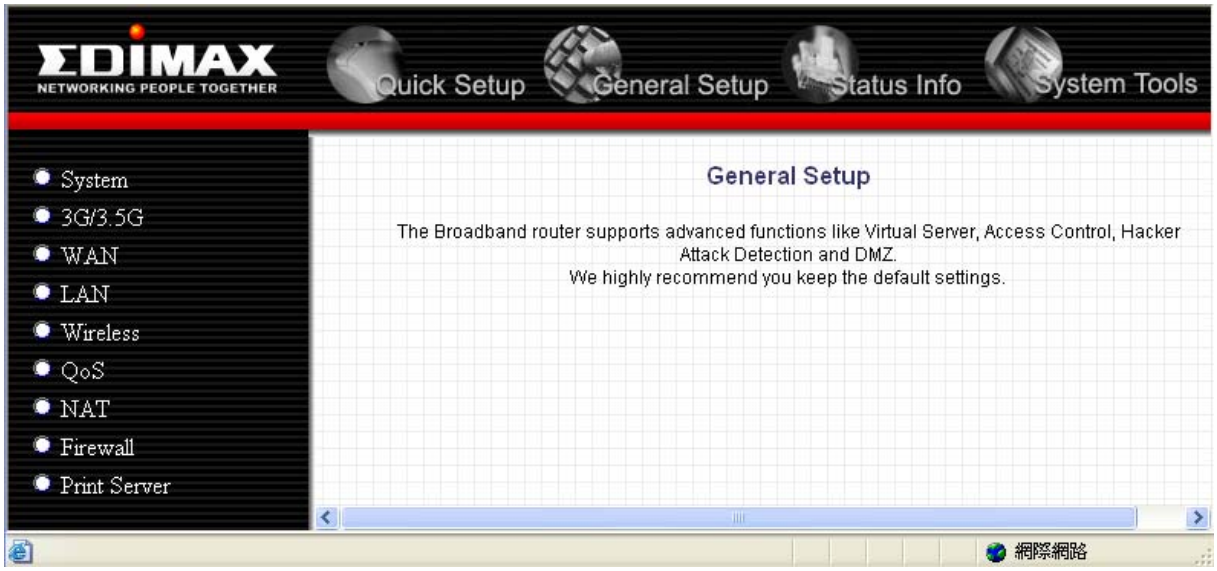
General Settings

Once you click on the **General Setup** button at the Home Page, you should see the screen below.

If you have already configured the Quick Setup Wizard, you **DO NOT** need to configure anything thing in the General Setup screen for you to start using the Internet.

The General Setup contains advanced features that allow you to configure the router to meet your network's needs such as: Wireless, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, Special Applications, DMZ and other functions.

Below is a general description of what advance functions are available in this broadband router.



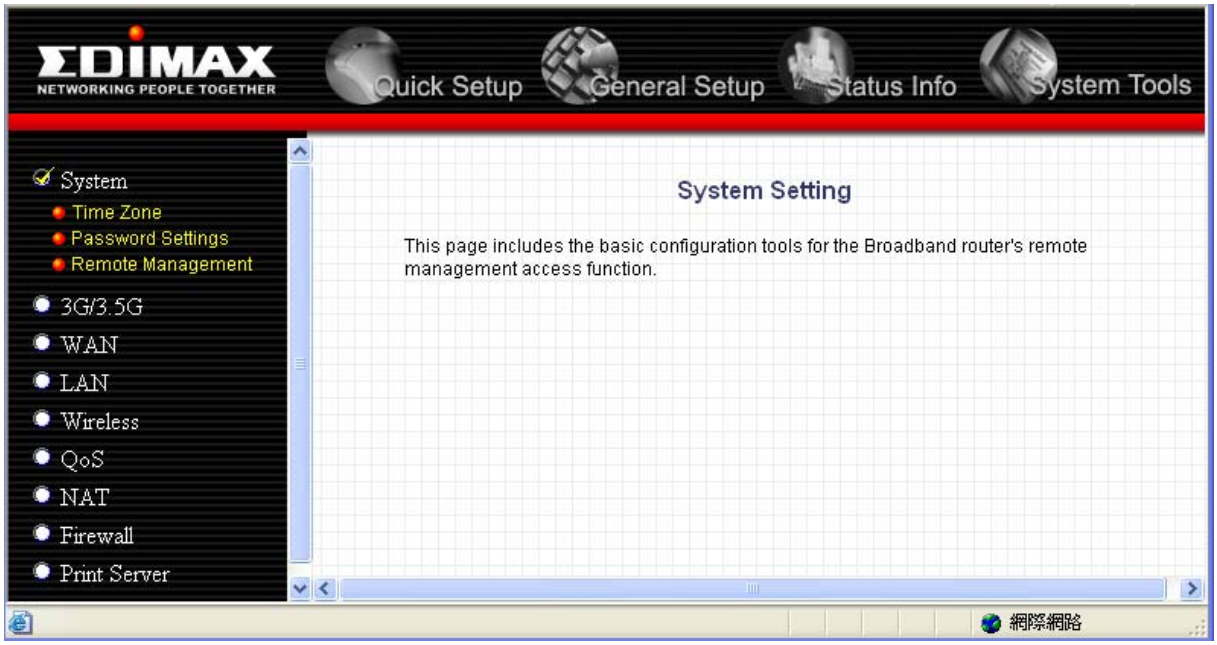
Menu	Description
System	This section allows you to set the Broadband router's system time zone, password and remote management administrator.
WAN	This section allows you to select the connection method in order to establish a connection with your ISP (same as the Quick Setup Wizard section)
LAN	You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP range for

	your LAN
Wireless	Setup the wireless LAN's SSID, WEP key, MAC filtering.
QoS	You can setup the QoS bandwidth control policy.
NAT	You can configure the Address Mapping, Virtual Server and Special Applications functions in this section. This allows you to specify what user/packet can pass your router's NAT.
Firewall	The Firewall section allows you to configure Access Control, Hacker Prevention and DMZ.
Print Server	The Print Server section allows you to enable the USB ports to support USB printer.

Select one of the above General Setup selections and proceed to the manual's relevant sub-section

2.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.

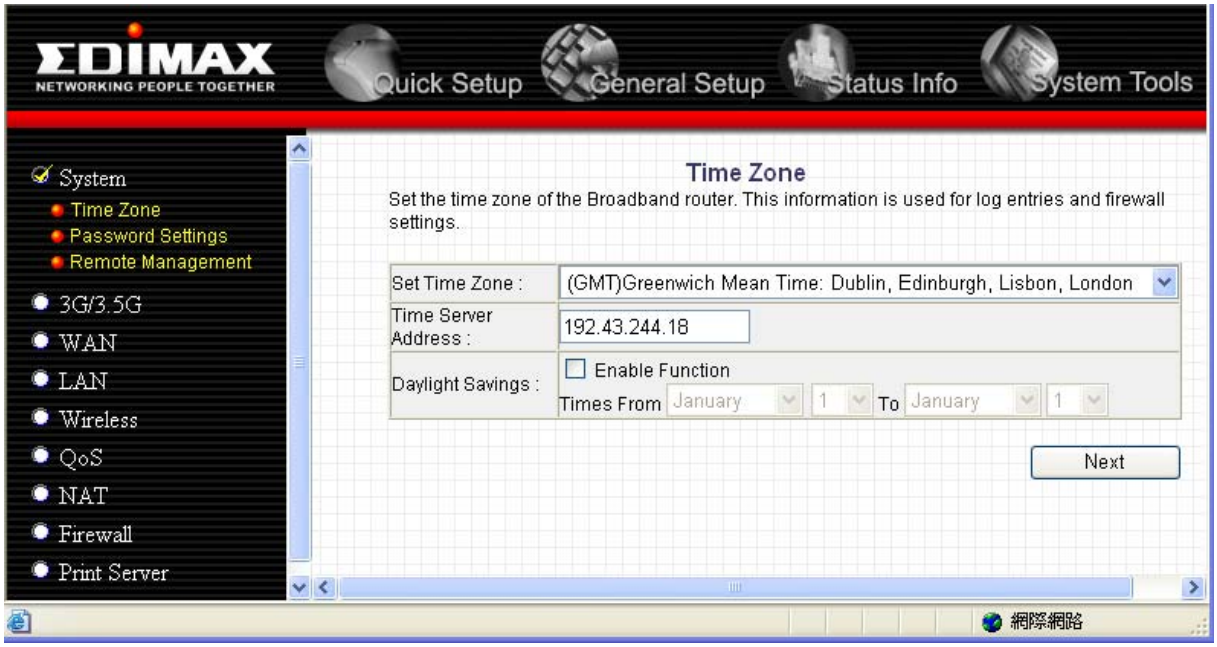


Parameters	Description
Time Zone	Select the time zone of the country you are living. The router will set its time based on your selection
Password Settings	Allows you to define a password in order to access the web-based management website.
Remote Management	You can specify a Host IP address that can perform remote management functions.

Select one of the above three system settings selections and proceed to the manual's relevant sub-section

2.1.1 Time Zone

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.



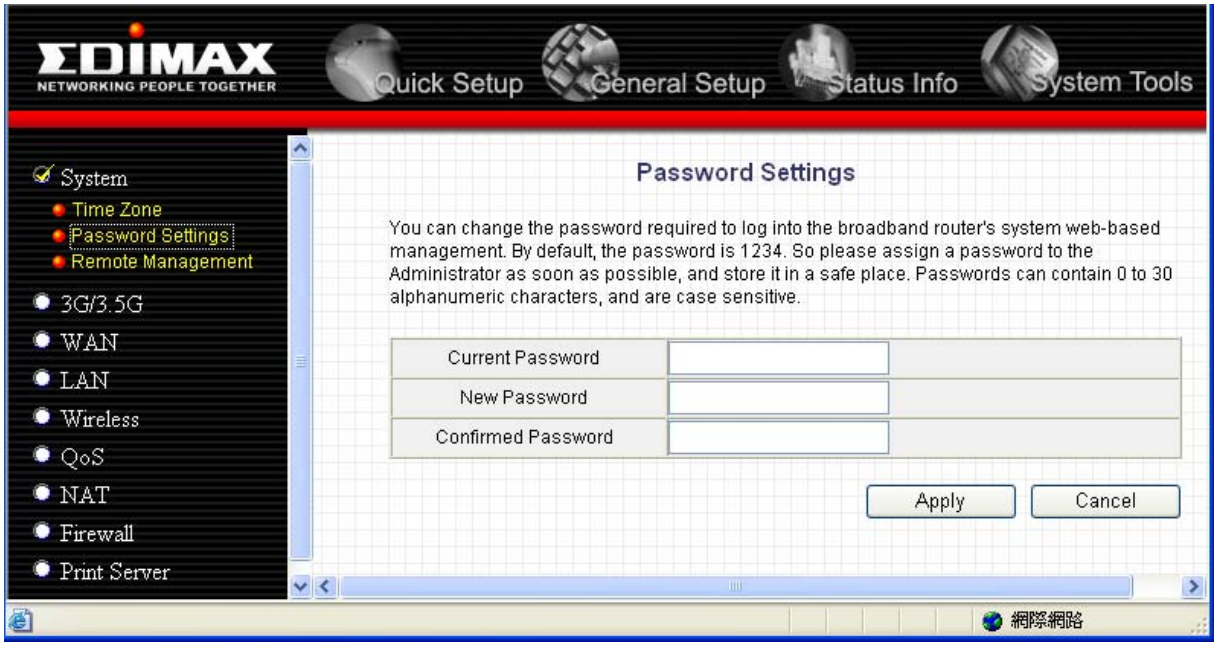
Parameter	Description
Set Time Zone	Select the time zone of the country you are living. The router will set its time based on your selection.
Time Server Address	The router default the “Time Server Address” is “192.43.244.18”
Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).
Times From	Select the period in which you wish to start using daylight Saving.
Times to	Select the period in which you wish to stop using daylight Saving.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.1.2 Password Settings

You can change the password required to log into the broadband router's system web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a

safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

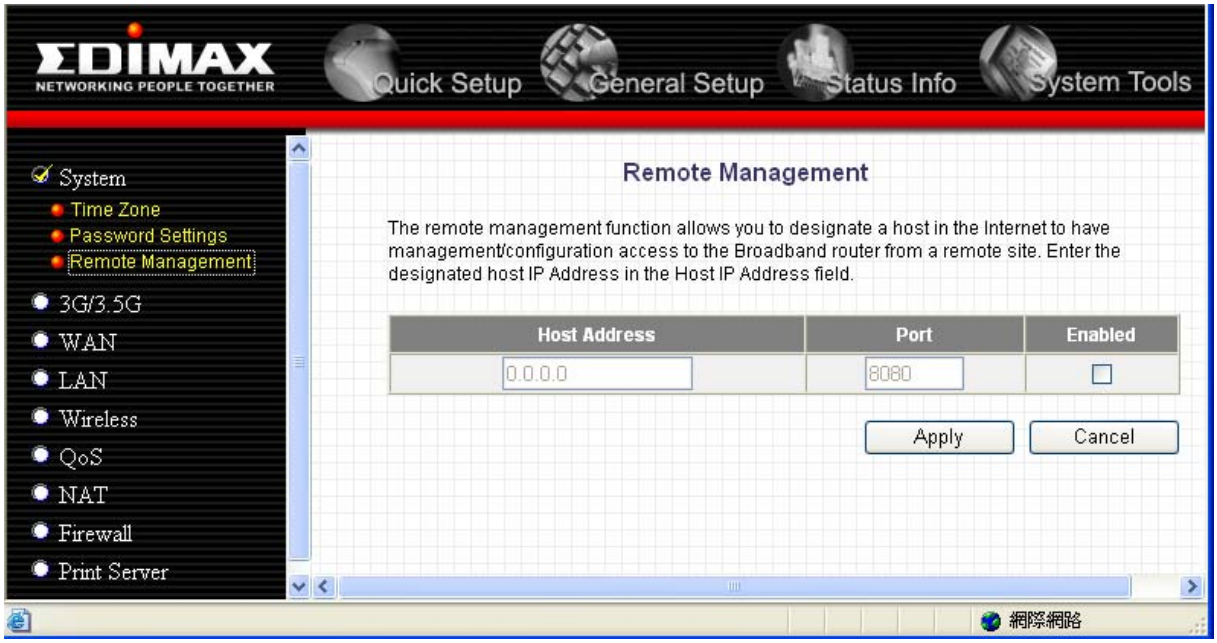


Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router. Note: By default there is NO password
New Password	Enter your new password
Confirmed Password	Enter your new password again for verification purposes **Note**: If you forget your password, you'll have to reset the router to the factory default (No password) with the reset button (see router's back panel)

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.1.3 Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.



Parameters	Description
Host Address	This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you'll be able to configure this router from your home. If the Host Address is **0.0.0.0,** means anyone can access the router's web-based configuration from a remote location, if they know the password. Click the **Enabled** box to enable the Remote Management function. **Note**: When you want to access the web-based management from a remote computer, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by colon and port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the router's web-based management.

	
Port	The port number of remote management web interface.
Enabled	Select “Enabled” to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advanced functions or start using the router (with the advanced settings in place)

2.2 3G/3.5G

3G-6200Wg provides two types of Internet connection method: wireless (3G/3.5G) or wired connection. You can access internet via USB 3G/3.5G modem card, or via wired xDSL / cable modem connection. However, only one connection method (wireless or wired) can be used at the same time. Related instructions will be given as follow.

3G-6200Wg supports most of 3G/3.5G modem cards, just connect the modem card to the USB port of 3G-6200Wg and 3G-6200Wg will recognize it automatically, no additional setup procedure required. However, some of modem cards require PIN code or account / password (you have to use 3G-6200Wg's web interface to input these information), and some modem cards requires you to connect the modem card with your PC and install driver / utility before you connect it with 3G-6200Wg (all PCs which need to access Internet by 3G-6200Wg requires to perform this procedure once). If you still not able to connect to Internet, please use wired Internet connection to access our website :http://www.edimax.com/ ,download latest version of firmware and upgrade 3G-6200Wg's firmware. If you still not be able to get connected by your 3G/3.5G modem card, please contact your dealer of purchase and provide the model name of the 3G/3.5G modem card you have, we'll try our best to help you to solve the problem.

Only one Internet connection (wireless / wired) can be used at the same time. Wireless connection (3G/3.5G) will be selected first, and use wired Internet connection as backup. Therefore, please DO NOT connect your 3G/3.5G modem card with 3G-6200Wg, or your telecomm service provider may charge you with high communication fee. For example, if you connect 3G/3.5G modem card with 3G-6200Wg when you're using wired Internet connection, wired connection will be dropped and use 3G/3.5G wireless connection instead. If 3G/3.5G wireless signal reception is poor and the connection can not be restored within 60 seconds, 3G-6200Wg will use wired Internet connection again, and will not switch back to wireless Internet connection (This only happens with wired Internet connection is available. If wired connection is unavailable, 3G-6200Wg will try to establish 3G/3.5G wireless connection again and again). If you want to use 3G/3.5G wireless connection again, you need to remove 3G/3.5G modem card from 3G-6200Wg and reconnect it back after 5 seconds.

(A) Plug and play, no setup procedure required.

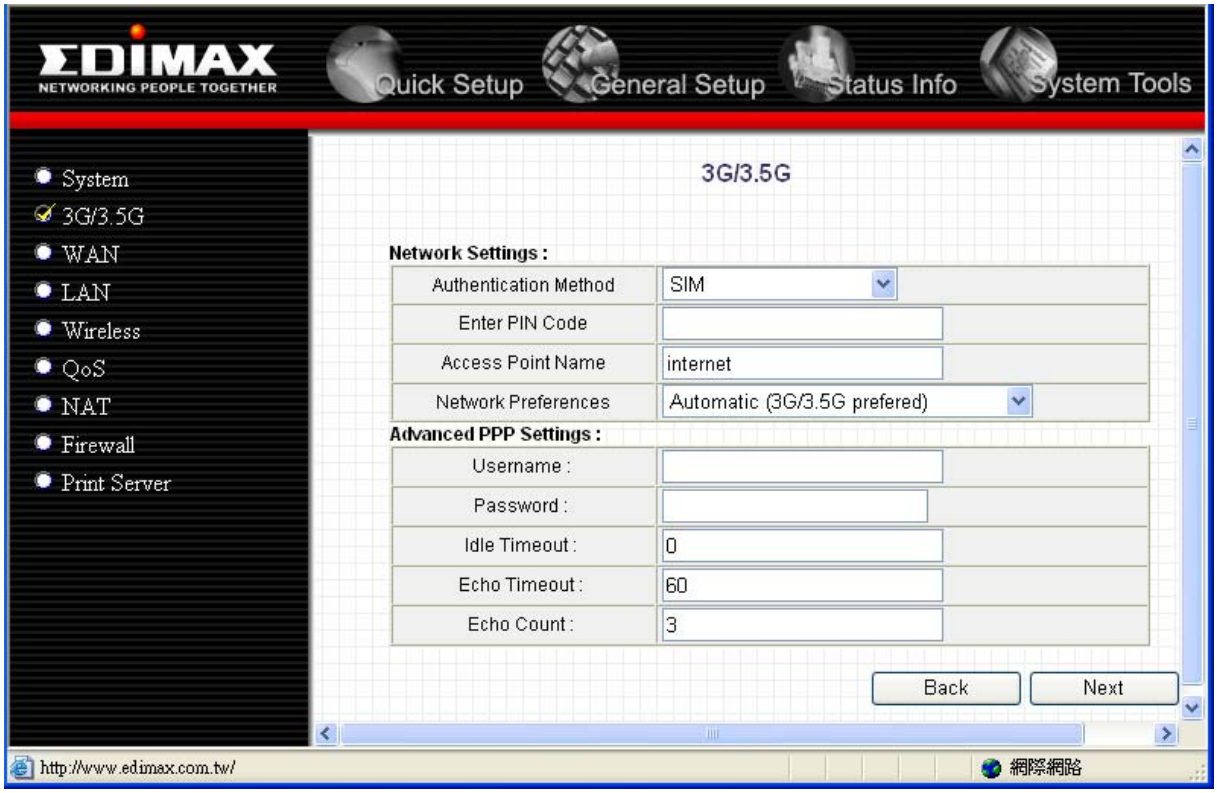
Connect the USB 3G/3.5G modem card with 3G-6200Wg and make sure the corresponding USB LED indicator of 3G-6200Wg lights up, then you can use the web browser to access Internet.

(B) PIN code or user name / password required:

Please check the authentication method you want to use. Most of telecomm service

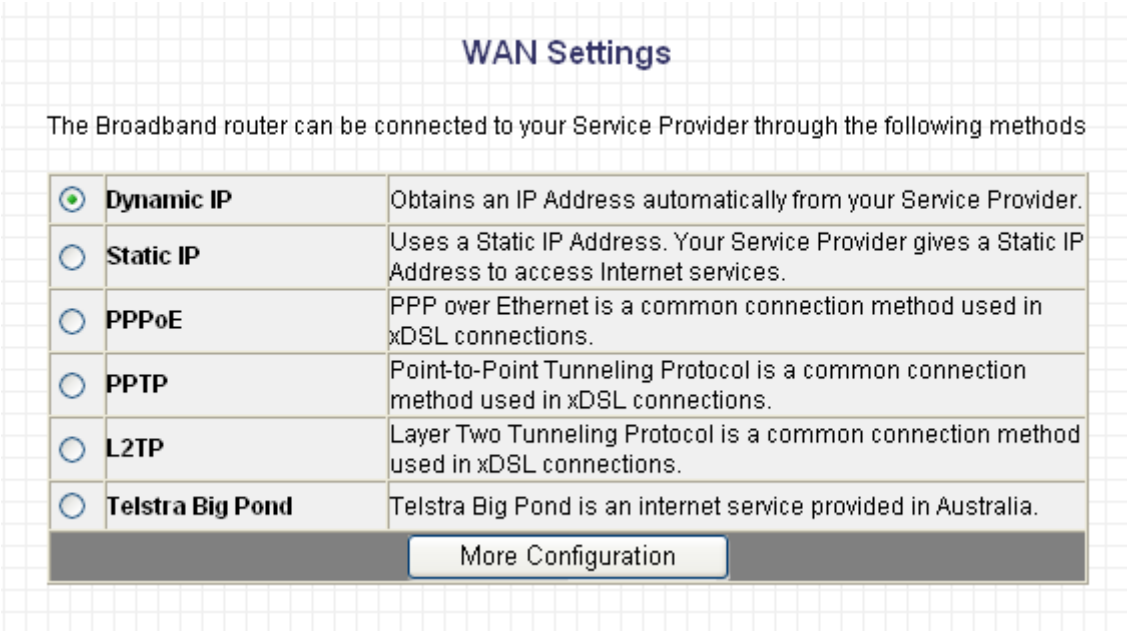
providers require you to input PIN Code, please check ‘SIM’ and input the PIN code provided by telecomm service provider. Most of options listed here are optional and you don’t have to provide those information if telecomm service provider doesn’t provide you with those information.

If telecomm provider provides you with username / password, please check /User Name / Password box and input the user name / password provided by telecomm service provider, then click ‘APPLY’ button. Wait for 1 minute (for 3G-6200Wg to



2.3 WAN

Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows to specify the type of WAN port connect you want to establish with your ISP. The WAN settings offer the following selections for the router’s WAN port, **Dynamic IP**, **Static IP Address**, **PPPoE**, **PPTP**, **L2TP**, **Telstra Big Pond**, **DNS** and **DDNS**.



Parameters	Description
Dynamic IP	Your ISP will assign you an IP address automatically
Static IP	Your ISP gave you an IP address already
PPPoE	Your ISP requires PPPoE connection.
PPTP	Your ISP requires you to use Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP	Your ISP requires L2TP connection.
Telstra Big Pond	Your ISP requires Telstra Big Pond connection.
DNS	You can specify a DNS server that you wish to use
DDNS	You can specify a DDNS server that you wish to use and configure the user name and password provided by you DDNS service provider.

Once you have made a selection, click <**More Configuration**> at the bottom of the screen and proceed to the manual's relevant sub-section

2.3.1 Dynamic IP

Choose the Dynamic IP selection if your ISP will assign you an IP address automatically. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address (see chapter 1 "Cable Modem" for more detail)

2.3.2 Static IP Address

Select Static IP address if your ISP assigned you with a specific IP address for you to use. Your ISP should provide all the information required in this section. (See chapter 1 “Fixed IP” for more detail)

2.3.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “PPPoE” for more detail)

2.3.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “PPTP” for more detail)

2.3.5 L2TP

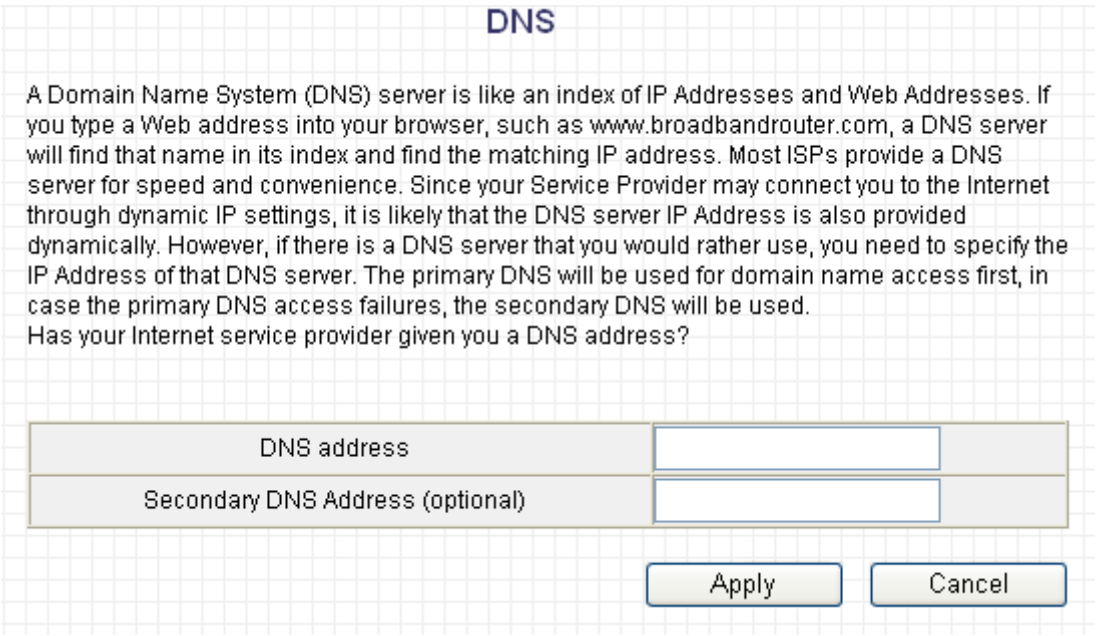
Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “L2TP” for detailed information)

2.3.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia. (See chapter 1 “Telstra Big Pond” for more detail)

2.3.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.



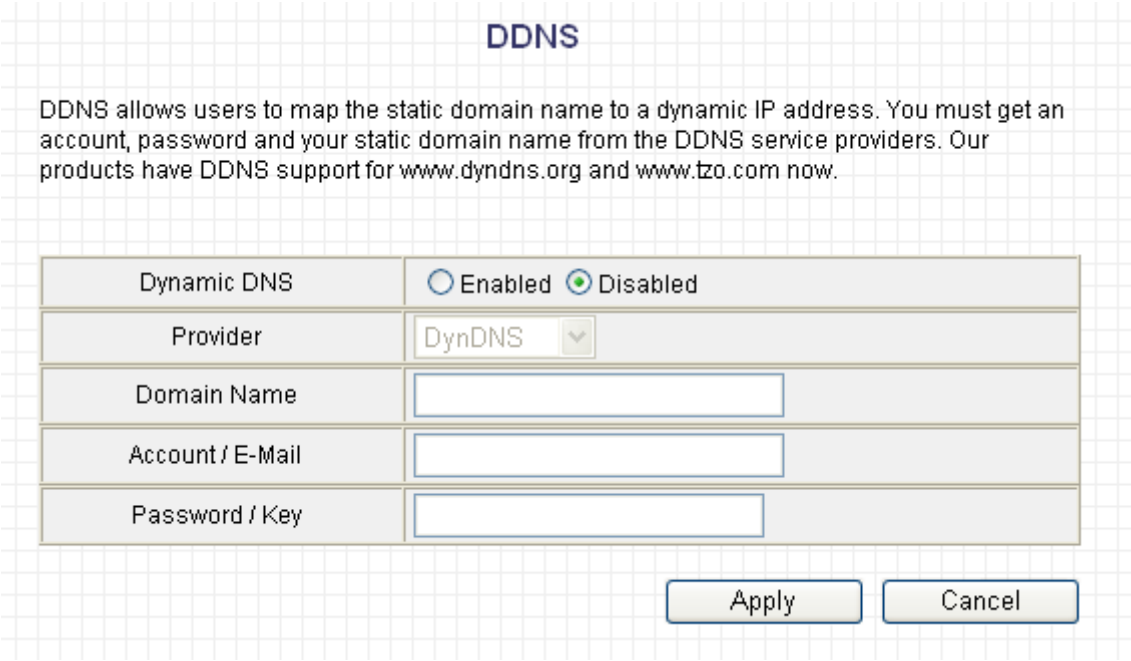
Parameters	Description
DNS address	Fill in the ISP's DNS server IP address; or you can specify your own preferred DNS server IP address
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used when the above DNS fail.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router (with the advanced settings in place)

2.3.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other

common DDNS service providers.

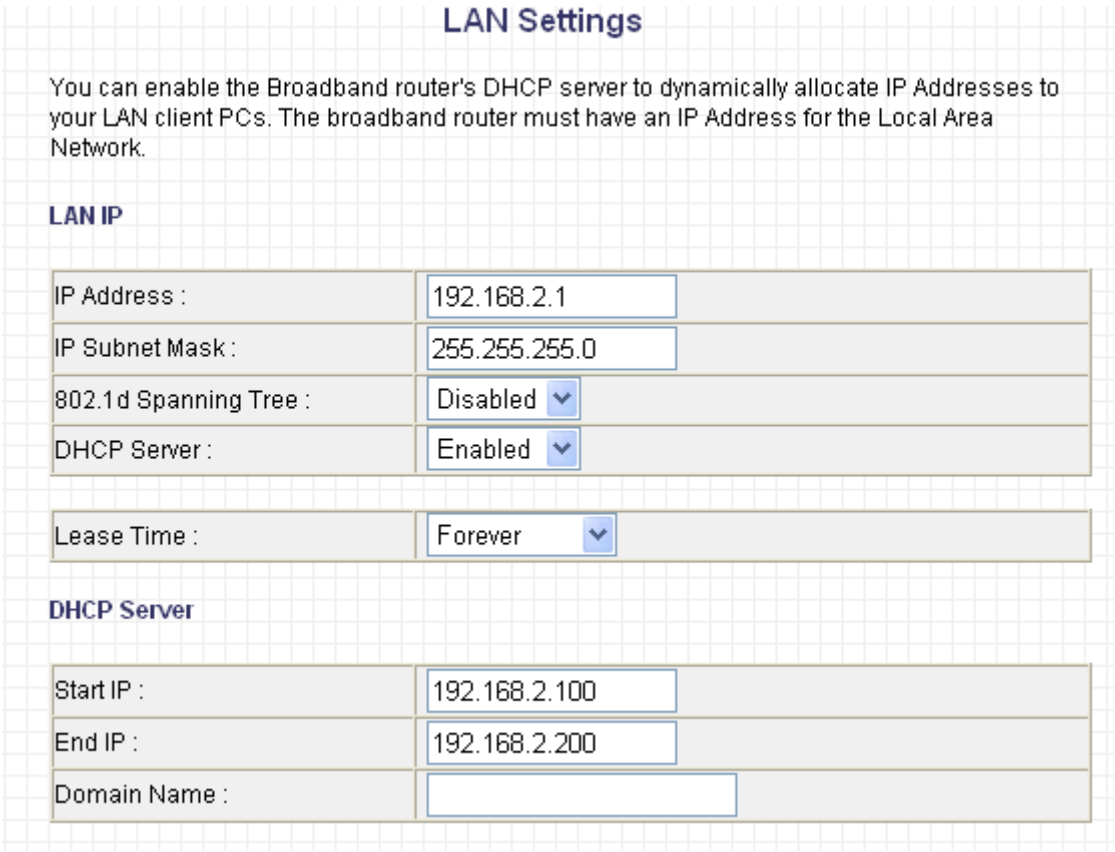


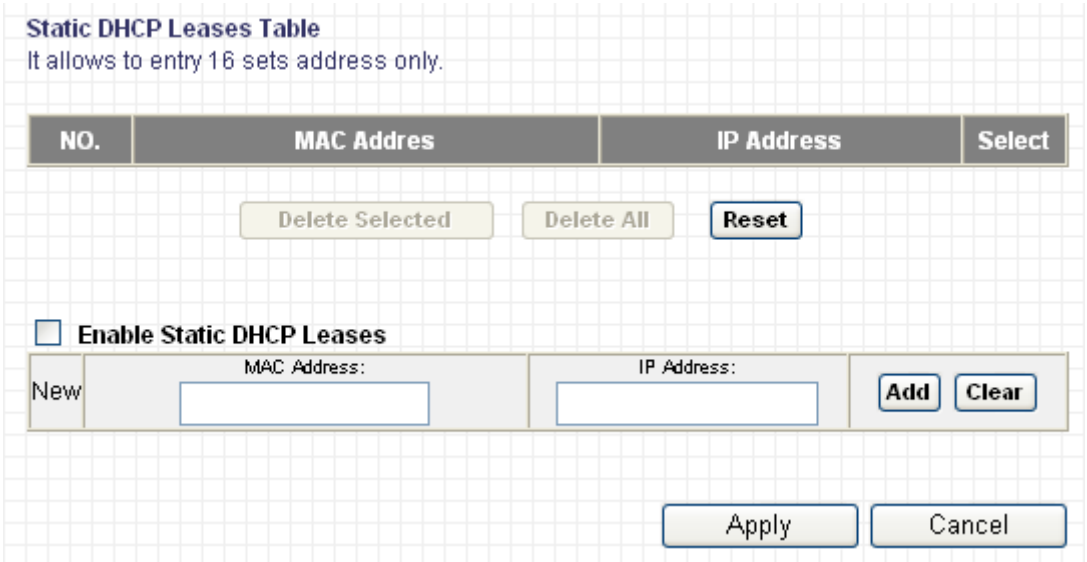
Parameters	Default	Description
Enable/Disable	Disable	Enable/Disable the DDNS function of this router
Provider		Select a DDNS service provider
Domain name		Your static domain name that use DDNS
Account/E-mail		The account that your DDNS service provider assigned to you
Password/Key		The password you set for the DDNS service account above

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.4 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.





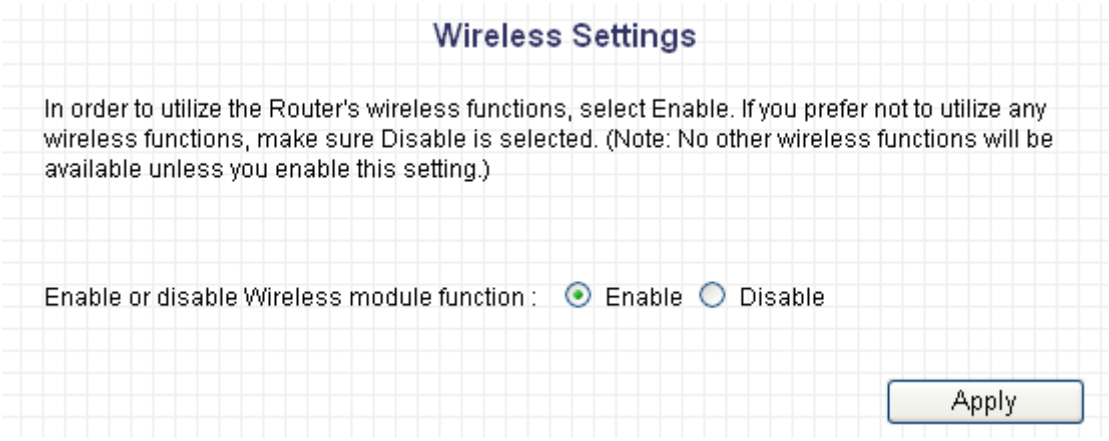
Parameters	Default	Description

IP address	192.168.2.1	This is the router's LAN port IP address (Your LAN clients default gateway IP address)
IP Subnet Mask	255.255.255.0	Specify a Subnet Mask for your LAN segment
802.1d Spanning Tree	Disabled	If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enabled	You can enable or disable the DHCP server. By enabling the DHCP server the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband router if you want the router to be your LAN client's default gateway
Lease Time		When enabled, DHCP service will temporarily give your LAN clients an IP address. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time period is reached
IP Address Pool		You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. **Note:** By default the IP range is from: **192.168.2.100** to **192.168.2.200**. If you want your PC to have a static/fixed IP address then you'll have to choose an IP address outside this IP address Pool.
Domain Name		You can specify a Domain Name for your LAN.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5 Wireless

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to your Intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.

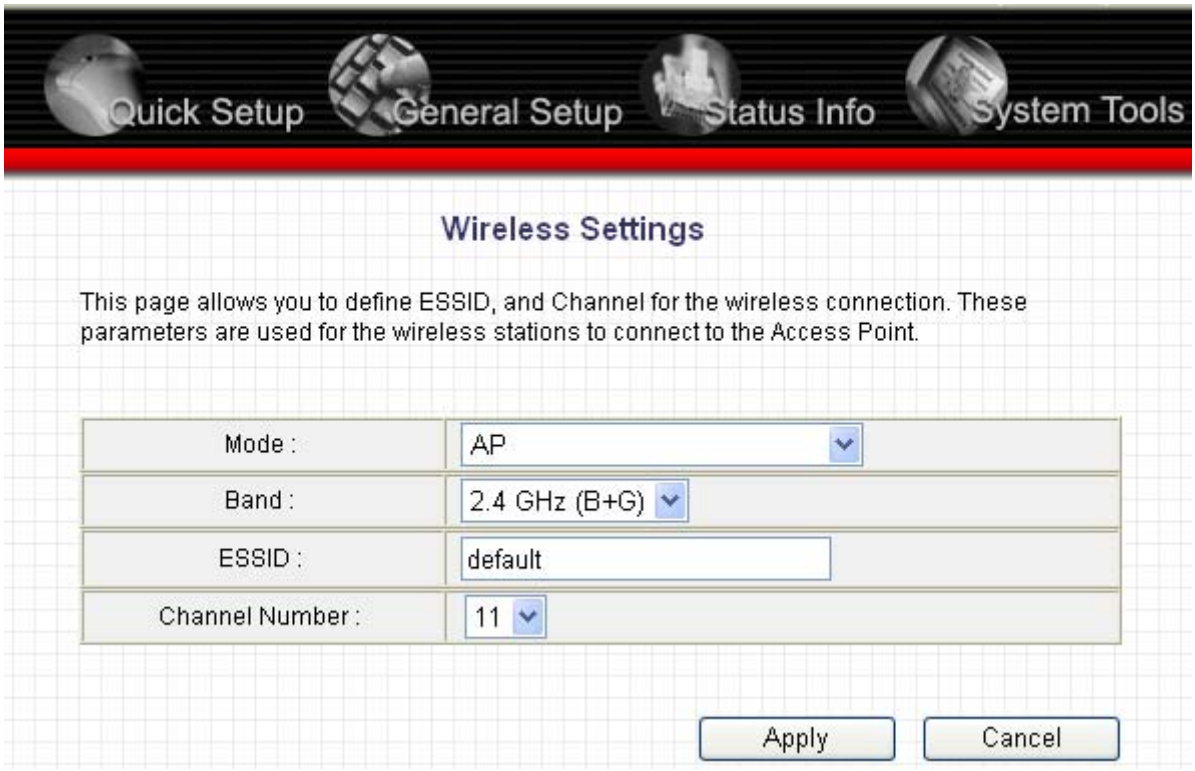


Parameters	Default	Description
Enable or disable Wireless module function	Enable	You can select to enable or disable the wireless access point module of this router.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.1 Basic Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.



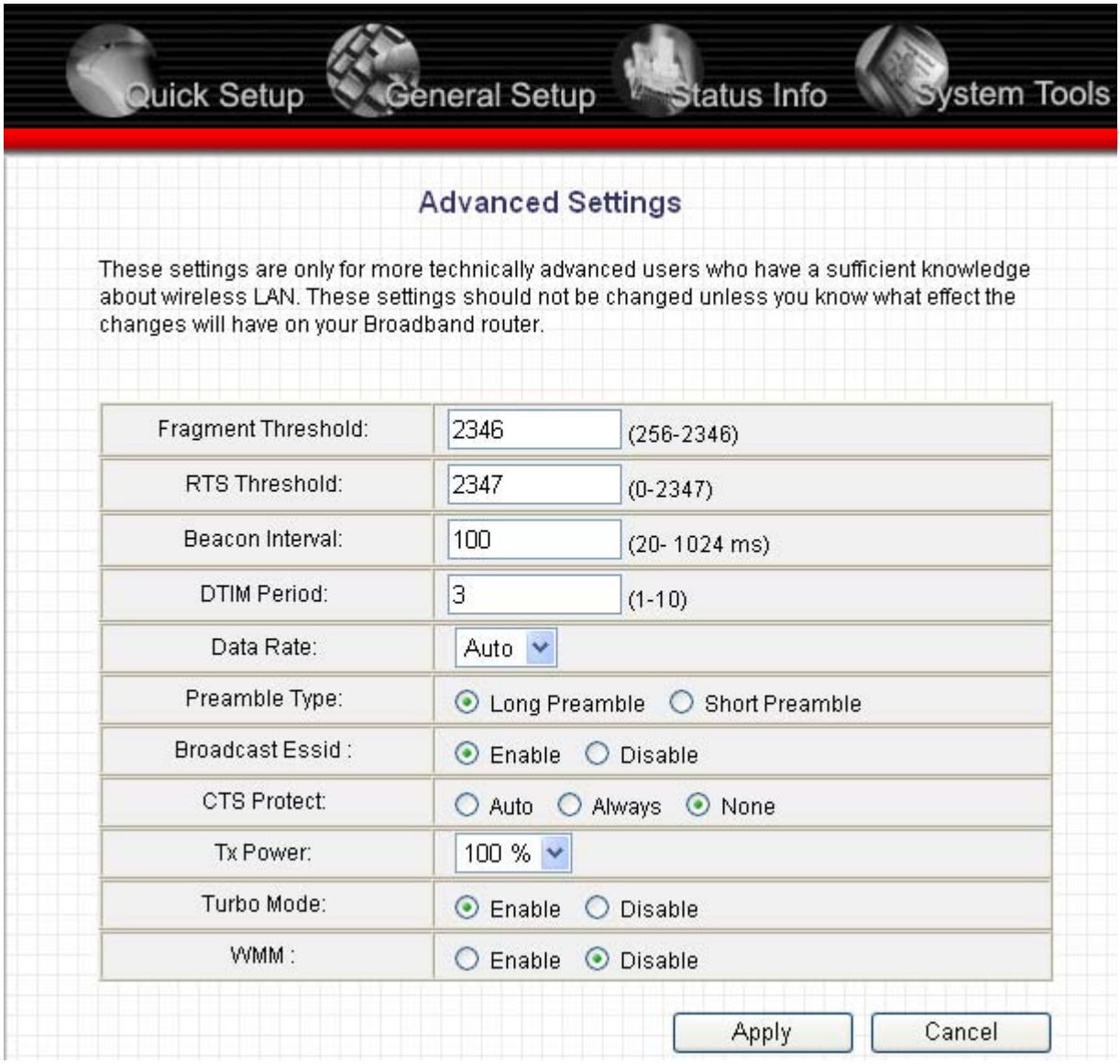
Parameters	Default	Description
Mode		It allows you to set the AP to AP, Bridge or WDS mode.
Band		It allows you to select the wireless band: 802.11b and / or 802.11g. You can select B+G mode to allow both 802.11b and 802.11g clients to connect to this wireless access point.
ESSID	default	This is the name of the wireless access point. All devices in the same wireless LAN should have the same ESSID.
Channel Number	11	The wireless channel used by the wireless access point. All devices in the same wireless LAN should use the same channel.
MAC address		If you want to combine more than one network, you have to set this access point to “AP Bridge-Point to Point mode”, “AP Bridge-Point

		to Multi-Point mode” or “AP Bridge-WDS mode”. You have to enter the MAC addresses of other access points which will join the same wireless network.
Set Security		Click the “Set Security” button, and then a “WDS Security Settings” will pop up. You can set the security parameters used to bridge access points together here, when you set your AP in AP Bridge mode. You can refer to section 4.3 “Security Settings” for detailed instructions.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place)

2.5.2 Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, preamble Type, etc. You should not change these parameters unless you know their function and effects.



Parameters	Description
Fragment Threshold	"Fragment Threshold" specifies the maximum fragmentation size of data packet to be transmitted. If this value is too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the

	wireless access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this wireless access point broadcast a beacon. Beacon is used to synchronize the wireless network.
DTIM Period	The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data which still exists on the AP and waiting for pickup.
Data Rate	The “Data Rate” is the rate this access point used to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point will discover this access point more easily. If you are building a wireless network which will open to the public, it’s recommended to enable this feature. Disabling “Broadcast ESSID” can provide better security.
IAPP	If you enable “IAPP”, it will allow wireless station roaming between IAPP enabled access points within the same wireless LAN.
CTS Protect	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic will be transmitted.
Tx Power	You can adjust the wireless transmit power here. By reduce the TX power, you can reduce the wireless coverage to make it only cover the area you need.
Turbo Mode	By enable the turbo mode, you can enhance the throughput up to 35Mbps.
WMM	WMM stands for Wi-Fi Multimedia. It is a standard created to define quality of service (QoS) in Wi-Fi networks. This adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring

	applications, each with different latency and throughput requirements, compete for network resources.

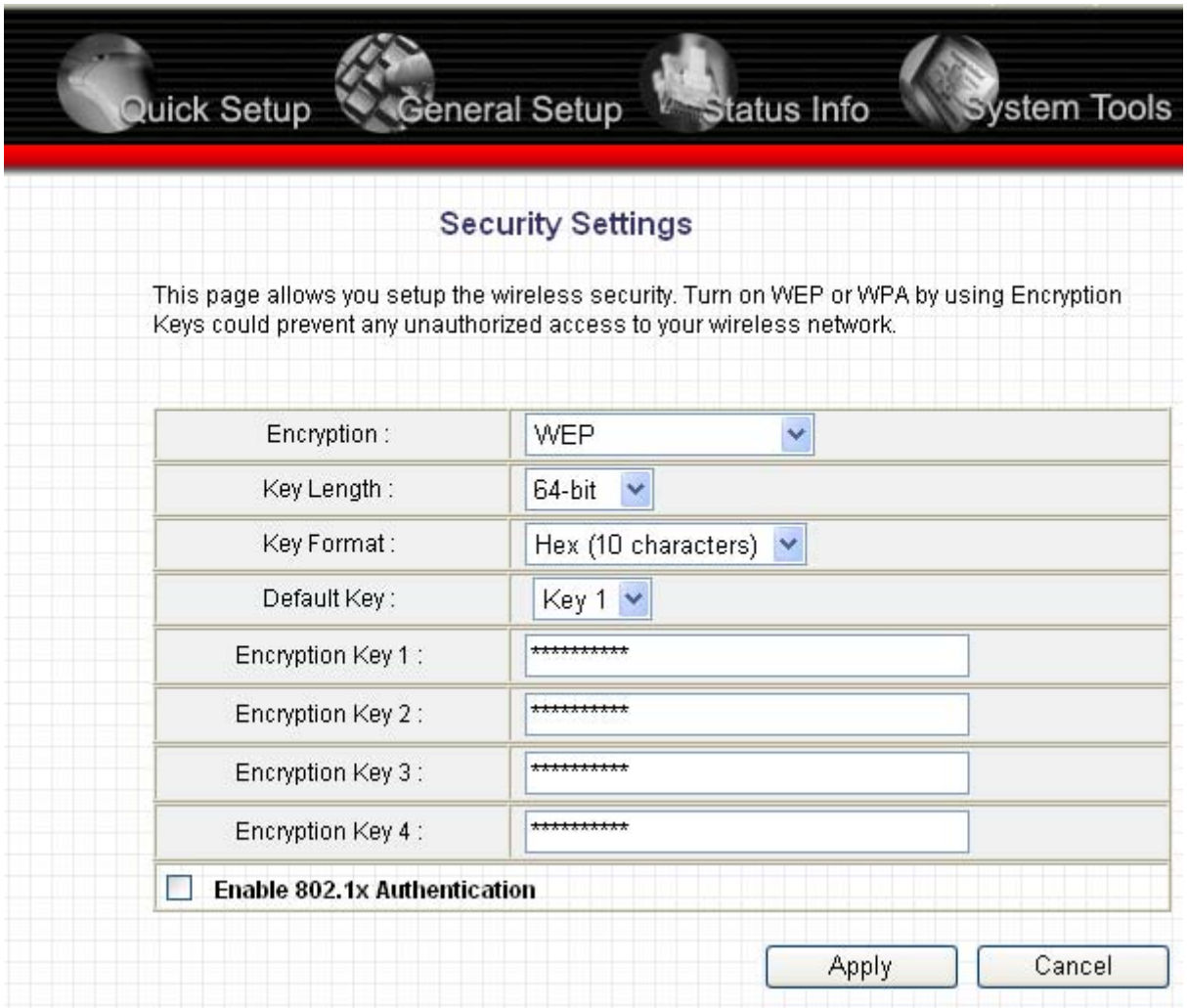
Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3 Security

This Router provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

2.5.3.1 WEP only

When you select 64-bit or128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys.



Parameters	Default	Description
Key Length	64-bit	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key

		length will provide higher level of security, but the data throughput will be lowered.
Key Format		You can select ASCII Characters (alphanumeric format) or Hexadecimal Digits ("A-F", "a-f" and "0-9") to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
Default Key		Select one of the four keys to encrypt your data. Only the key you select it in the "Default key" will be used.
Key 1 - Key 4		The WEP keys are used to encrypt data transmitted over the wireless network. Fill the text box by following the rules: 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values ("A-F", "a-f" and "0-9") or 13-digit ASCII characters as the encryption keys.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.2 802.1x only

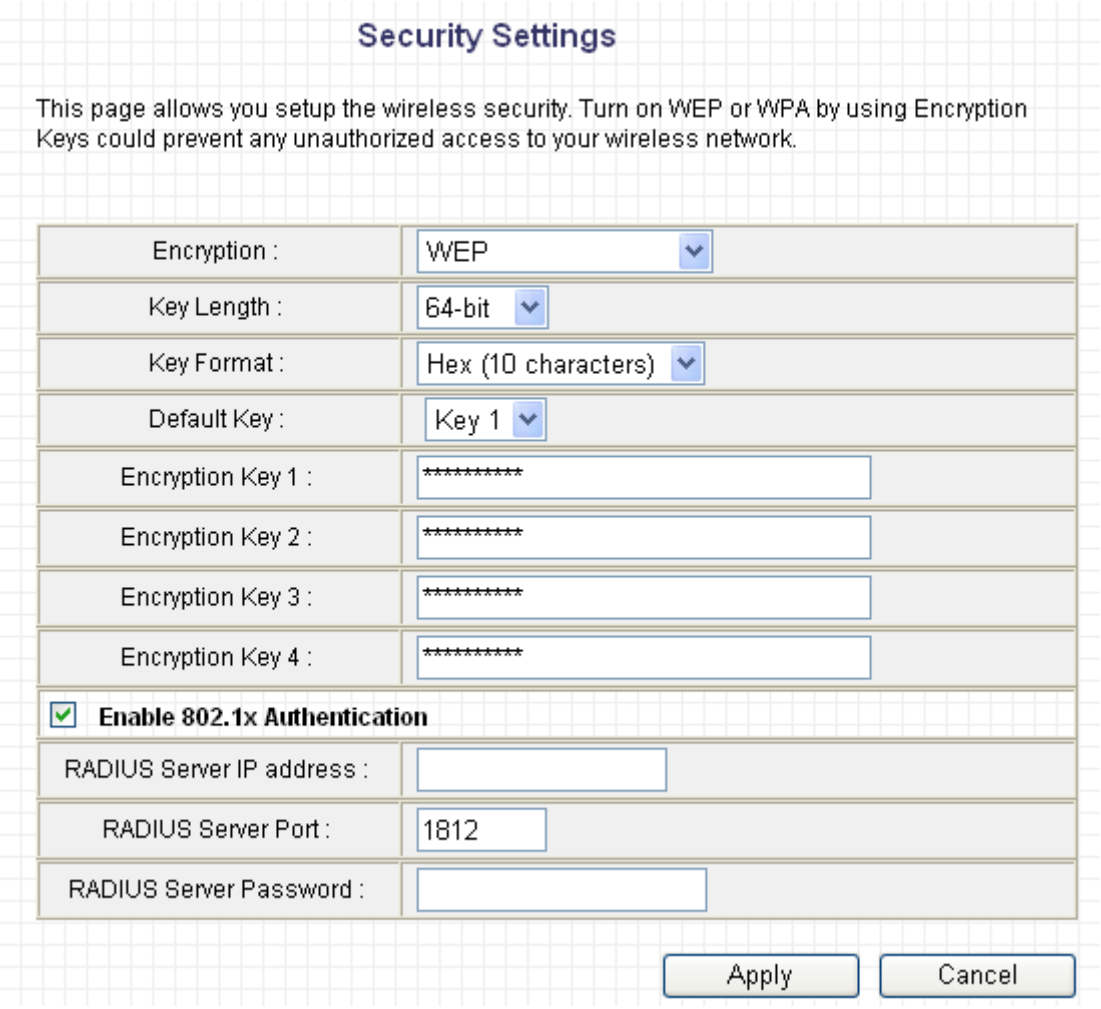
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication.

Parameters	Description
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.3 802.1x WEP Static key

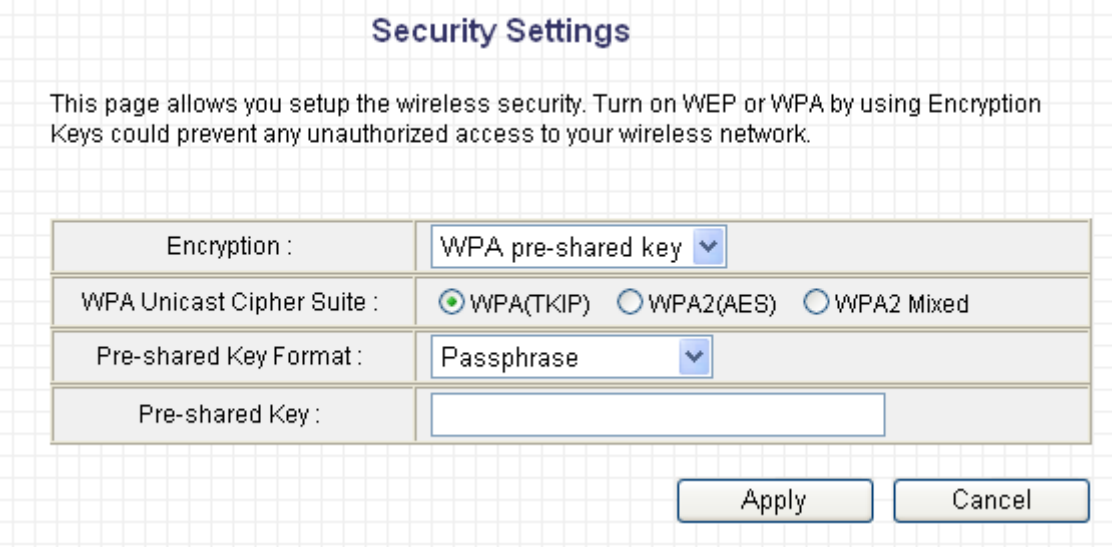
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.



For detailed instructions of WEP settings, please refer to section 2.4.3.1 “WEP only”. For the 802.1x settings, please refer to section 2.4.3.2 “802.1x only”.

2.5.3.4 WPA Pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key will not be known by hackers easily, and this will improve security.

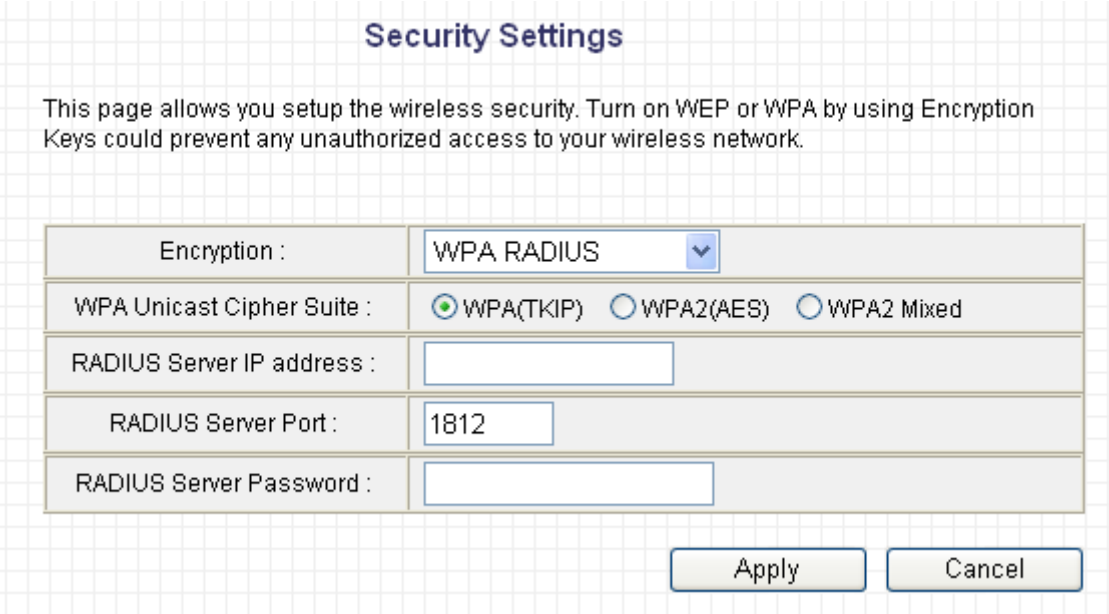


Parameters	Description
WPA(TKIP)	TKIP will change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	WPA2 AES uses CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	WPA2 Mixed will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format	You may select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted over the wireless network. Fill the text box by following the rules listed here: Hex WEP: input 64-digit Hex values (“A-F”, “a-f” and “0-9”) or at least 8 character pass phrase as the pre-shared keys.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.5 WPA Radius

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently, and this will improve security.

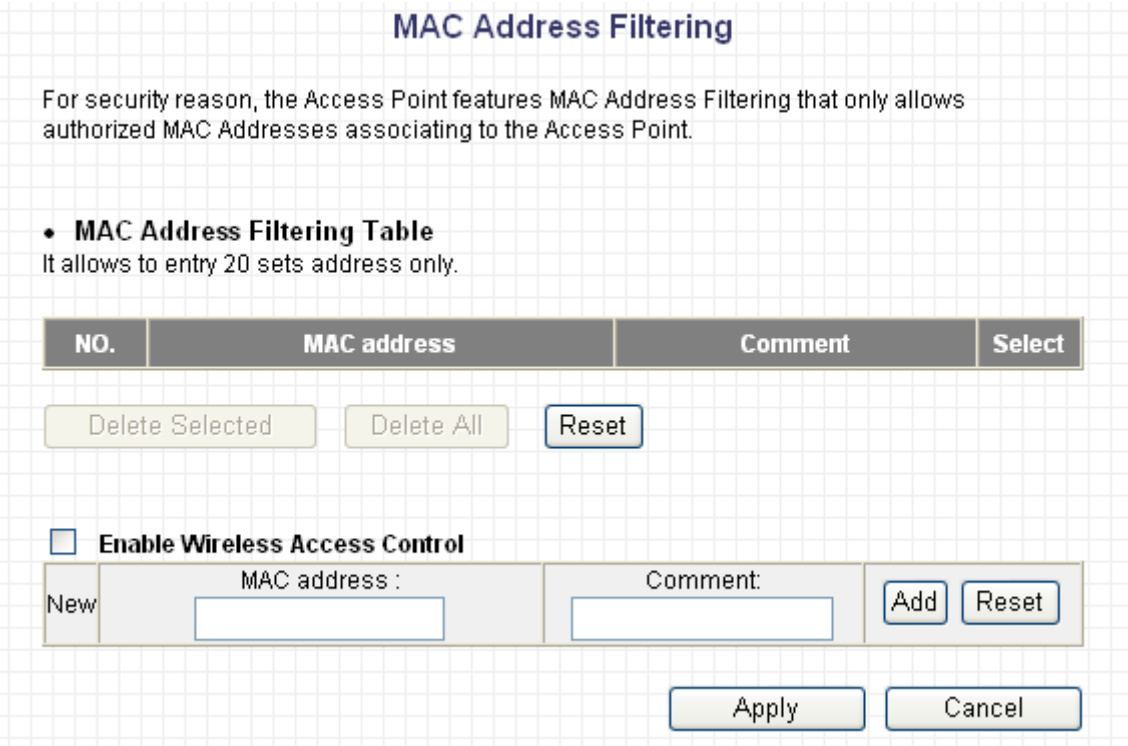


Parameters	Description
WPA(TKIP)	TKIP will change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	WPA2 AES uses CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	WPA2 MIXED will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.4 Access Control

This wireless router provides MAC Address Control, which prevents unauthorized MAC Addresses from accessing your wireless network.



Parameters	Description
Enable wireless access control	Enable wireless access control
Add MAC address into the list	Fill in the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". Then this wireless station will be added into the "Current Access Control List" below. If you find any issues before adding it and want to correct it. Just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.
Remove MAC address from list	If you want to remove some MAC address from the "Current Access Control List ", select the MAC addresses you want to remove in the list and then click "Delete Selected". If you want remove all MAC addresses from the table, click "Delete All" button. Click "Reset" will clear your current selections.

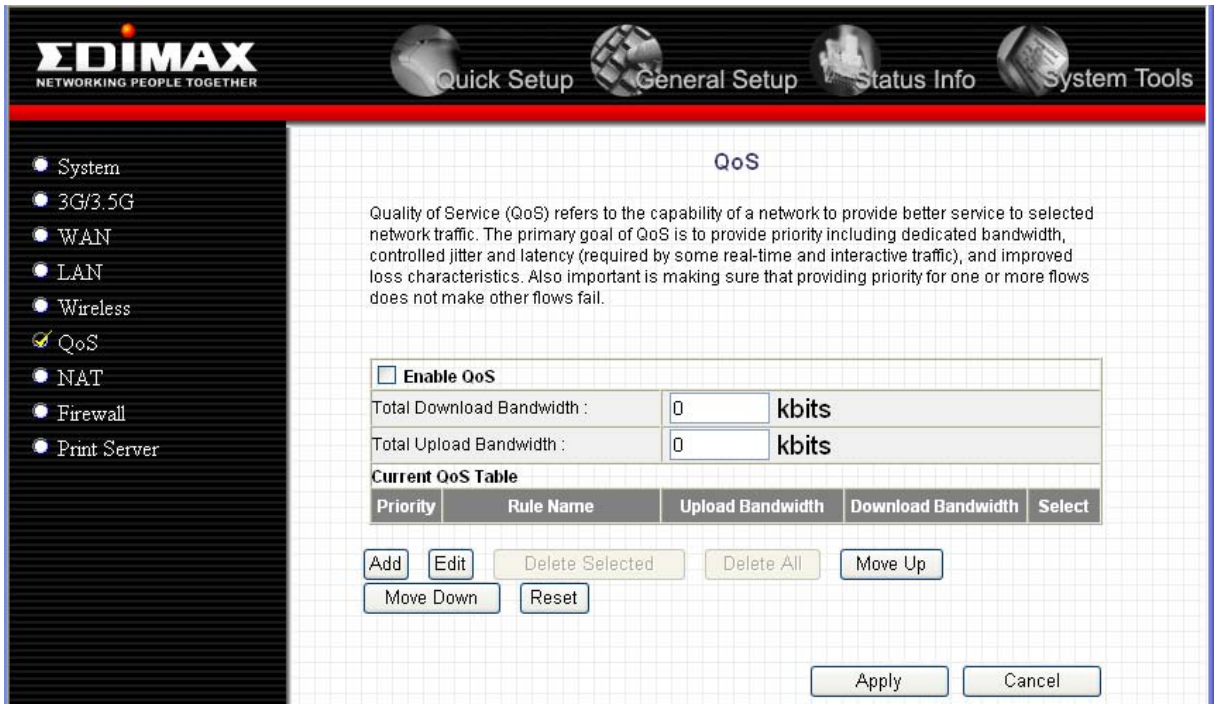
Click <**Apply**> at the bottom of the screen to save the configurations. You can

now configure other advance sections or start using the router.

2.6 QoS

The QoS function can classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using delay-sensitive services like Internet phone, video conference …etc. All the applications not specified by you are classified as rule name “Others”. The rule with smaller priority number has higher priority; the rule with larger priority number has lower priority. You can adjust the priority of the rules by moving them up or down.

Note: If the total assigned bandwidth of higher priority applications is larger than the maximum bandwidth provided by the WAN port, then other applications will not get any bandwidth.

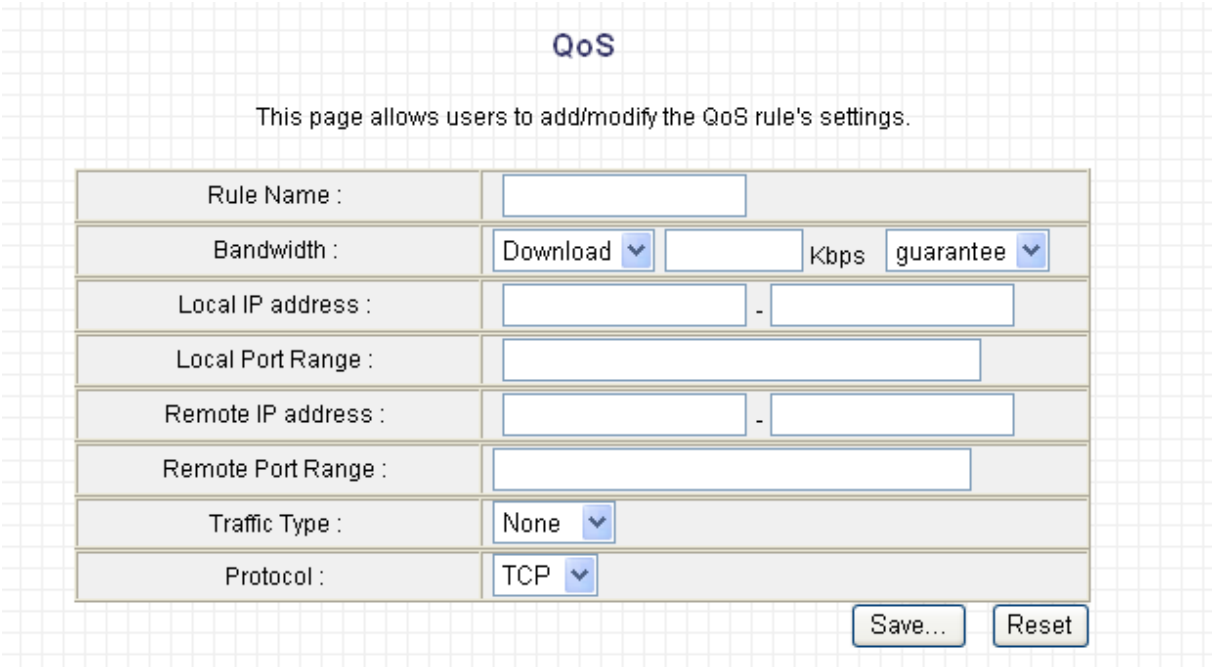


Parameters	Description

Enable/Disable QoS	You can check “Enable QoS” to enable QoS function for the WAN port. You also can uncheck “Enable QoS” to disable QoS function for the WAN port.
Total Download Bandwidth	Here you can set maximum download bandwidth for all the users of the router.
Total Upload Bandwidth	Here you can set the maximum upload bandwidth for all the users of the router.
Add a QoS rule into the table	Click “Add”, and the QoS rule form will appear. Click “Apply” after filling the form and the rule will be added into the table.
Remove QoS rules from table	If you want to remove some QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want to remove all QoS rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections.
Edit a QoS rule	Select the rule you want to edit and click “Edit”, then the detailed information of the selected QoS rule will appear. Click “Apply” after editing the form and the rule will be saved.
Adjust QoS rule priority	You can select the rule and click “Move Up” to make its priority higher. You also can select the rule and click “Move Down” to make its priority lower.

Edit QoS Rule:

You can assign packet classification criteria by its local IP range, remote IP range, traffic type, protocol, local port range and remote port range parameters. The parameters you leave blank will be ignored. The priority of this rule will be applied to packets that match the classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.



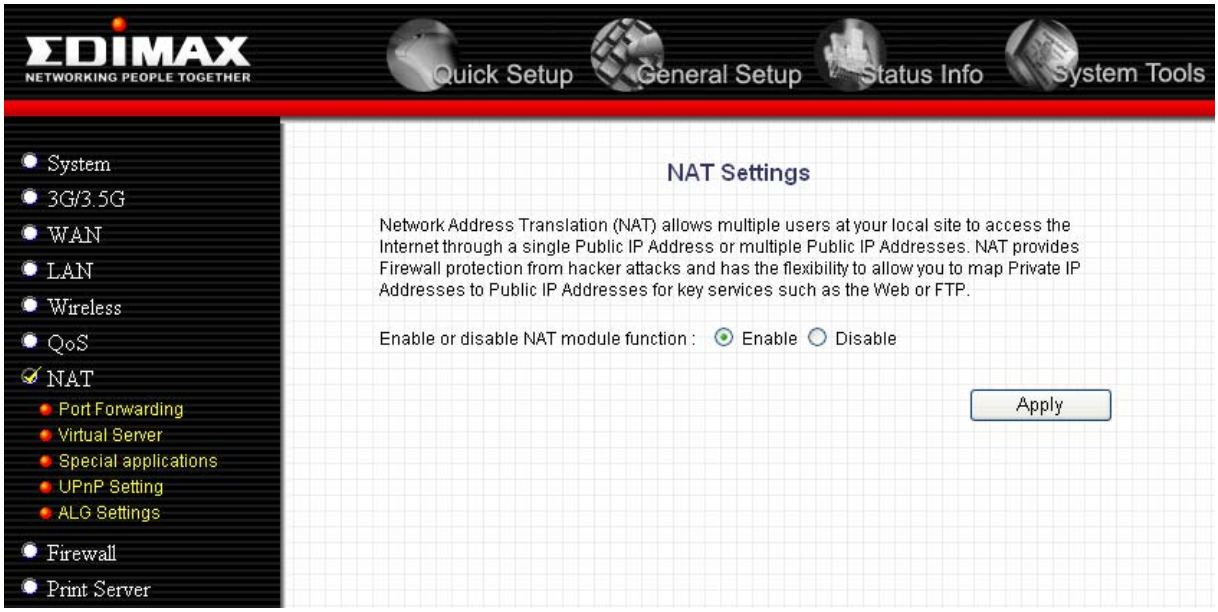
Parameters	Description
Rule Name	The name of this rule.
Bandwidth	You can assign the download or upload bandwidth in Kbps (1024 bit per second). You can limit the maximum bandwidth consumed by this rule by selecting “Maximum”. You also can reserve enough bandwidth for this rule by selecting “Guarantee”.
Local IP Address	Enter the local IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5
Local Port Range	Enter the local port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash “-“, for example “101-150” means from port number 100 to port number 150 – the range of 50 port numbers.
Remote IP Address	Enter the remote IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5

Remote Port Range	Enter the remote port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash “-“, for example “101-150” means from port number 101 to port number 150, which indicates 50 port numbers.
Traffic Type	Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination port number, if you are familiar with the application protocol.
Protocol	Select the protocol type of the packets that this rule will apply to.
Apply	Apply and exit the form.
Reset	Clear the content of this form.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map private IP addresses to public IP addresses for key services such as Websites and FTP.



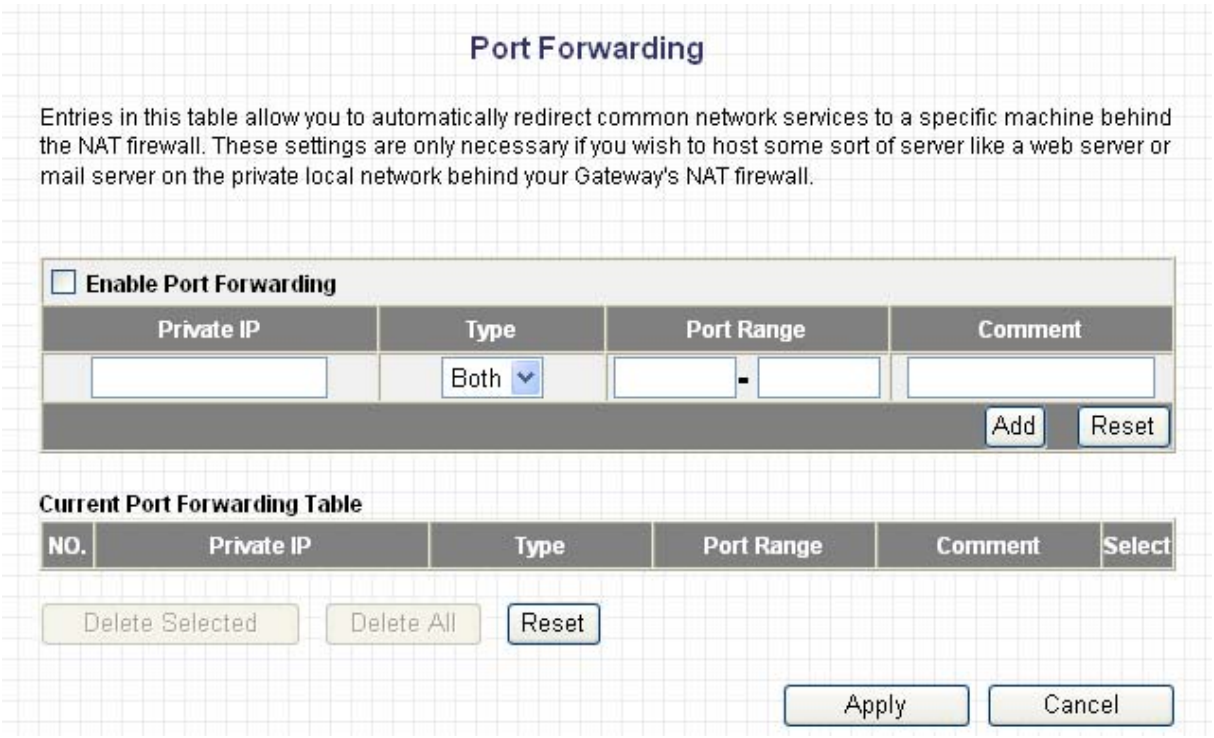
Parameters	Description
Port Forwarding	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Port Forwarding function allows you to redirect a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.
Virtual Server	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Virtual Server allows you to redirect a particular service port number (from the Internet/WAN Port) to a particular LAN IP address and its service port number.
Special Applications	Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support these types of applications.
UPnP Setting	It allows to enable or disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router

	automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAPT port translation.
ALG Setting	You can let special applications that require “Application Layer Gateway” to be supported here.
Static Routing	You can disable NAT function and setup the routing rules manually.

Click on one of the above NAT selections and proceed to the manual's relevant sub-section.

2.7.1 Port Forwarding

The Port Forwarding allows you to redirect a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.



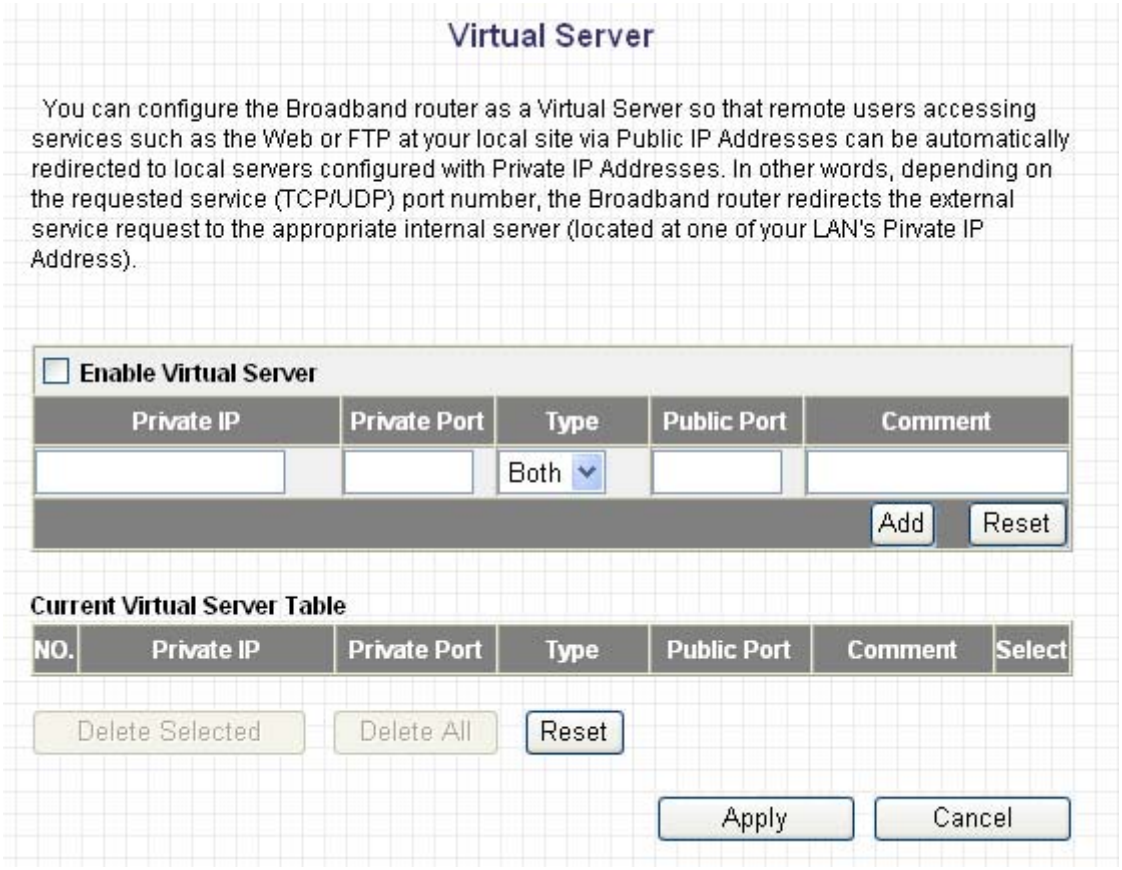
Parameters	Description
Enable Port Forwarding	Enable Port Forwarding
Private IP	This is the private IP of the server behind the NAT firewall. **Note:** You need to give your LAN PC clients a fixed/static IP address in order to make port forwarding function working properly.
Type	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add Port Forwarding	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you found any

	typo before adding it and want to correct it, just click "Clear" and the fields will be cleared.
Remove Port Forwarding	If you want to remove some Port Forwarding settings from the “Current Port Forwarding Table", select the Port Forwarding settings you want to remove in the table and then click "Delete Selected". If you want remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.2 Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to redirect a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number)



Parameters	Description
Enable Virtual Serve	Enable Virtual Server.
Private IP	***This is the LAN client/host IP address that the Public Port number packet will be sent to.*** **Note:** You need to give your LAN PC clients a fixed/static IP address in order to make Virtual Server working properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the

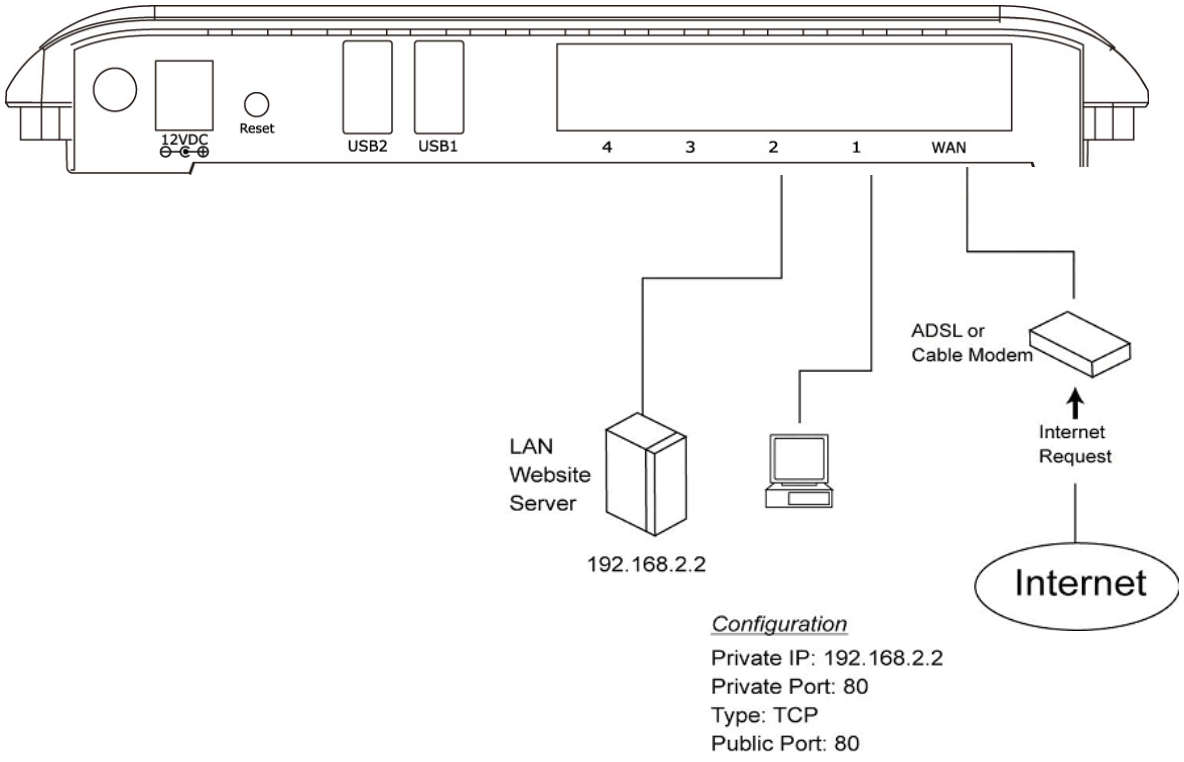
	packet enters your LAN (to the LAN Server/Client IP)
Type	Select the port number protocol type (TCP, UDP or both). If you are unsure, keep it untouched.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be redirected to the above Private IP address host in your LAN **Note**: Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Comment	You can enter the description of this setting here.
Add Virtual Server	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you found any typo before adding it and want to correct it, just click "Clear" and the fields will be cleared.
Remove Virtual Server	If you want to remove some Virtual Server settings from the “Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want remove all Virtual Server settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

Example: Virtual Server

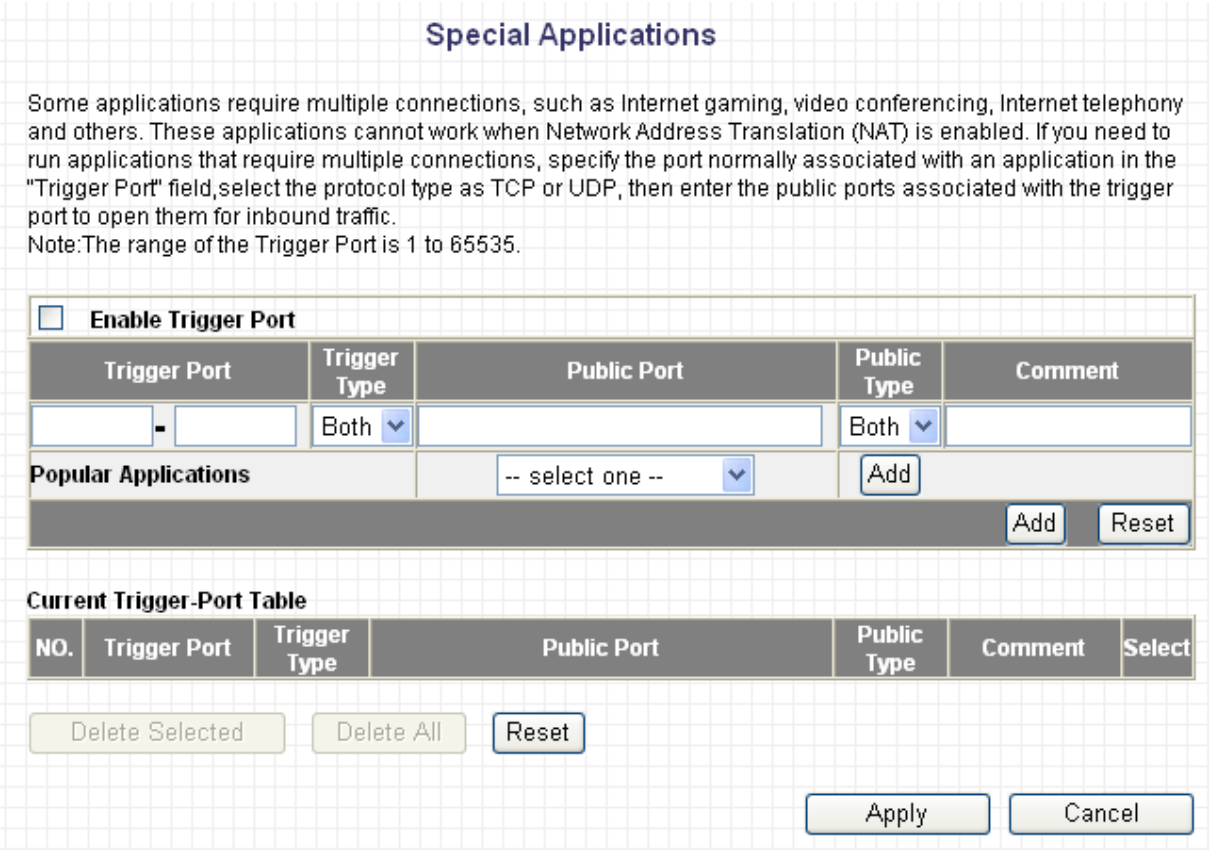
The diagram below demonstrates one of the ways you can use the Virtual Server function. Use the Virtual Server when you want the web server located

in your private LAN to be accessible to Internet users. The configuration below means that any request coming form the Internet to access your web server will be translated to your LAN's web server (192.168.2.2).
Note: For the virtual server to work properly Internet/remote users must know your global IP address. (For websites you will need to have a fixed/static global/public IP address)



2.7.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Parameters	Description
Enable Trigger Port	Enable the Special Application function.
Trigger Port	This is the outgoing (Outbound) range of port numbers for this particular application
Trigger Type	Select whether the outbound port protocol is “TCP”, “UDP” or both.
Public Port	***Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)*** **Note**: Individual port numbers are separated by a comma (e.g. 47624, 5775, and 6541 etc.). To input a port range use a “dash” to separate the two port number range (e.g. 2300-2400)
Public Type	Select the Inbound port protocol type: “TCP”, “UDP” or both
Comment	The description of this setting.
Popular applications	This section lists many popular applications that require multiple connections. Select an application from the

	Popular Applications selection and click “Add”. It will automatically list the Public Ports required for this popular application you’d specified.
Add Special Application	Fill in the "Trigger Port", "Trigger Type”, “Public Port”, "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Special Application setting will be added to the "Current Trigger-Port Table" below. If you found any typo before adding it and want to correct it, just click "Clear" and the fields will be cleared. If you want to add a popular application, select one “Popular Application” and then click “Add”.
Remove Special Application	If you want to remove some Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Applications settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

Example: Special Applications
If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

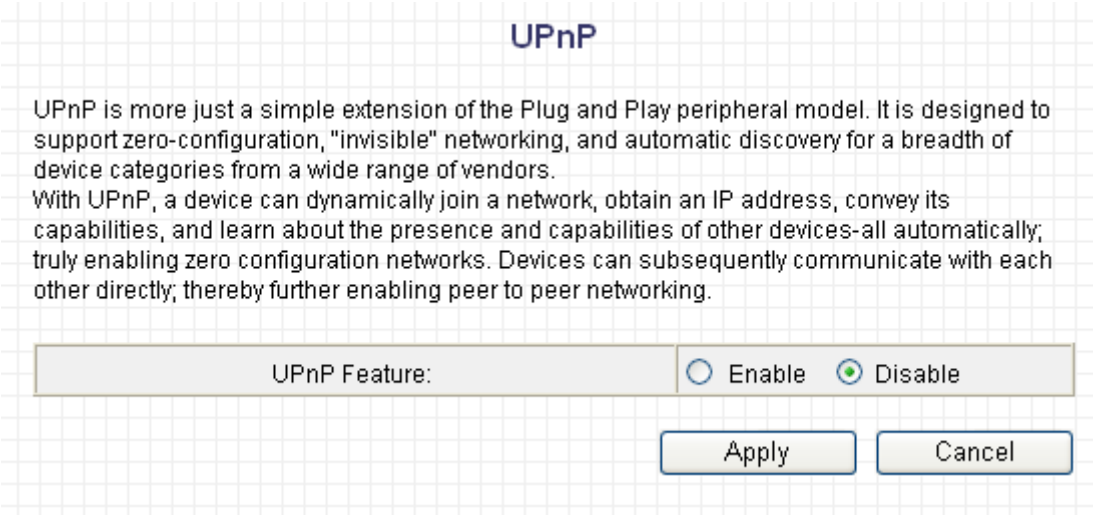
ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example listed above, when a user triggered port 28800 (outbound) for MSN Game Zone then the router will direct incoming packets for ports 2300-2400 and 47624 to that user.

Note: Only one LAN client can use a particular special application at a time.

2.7.4 UPnP Settings

With UPnP, all PCs in you Intranet will discover this router automatically. So you do not have to do any configuration for your PC, and they can access the Internet through this router automatically.

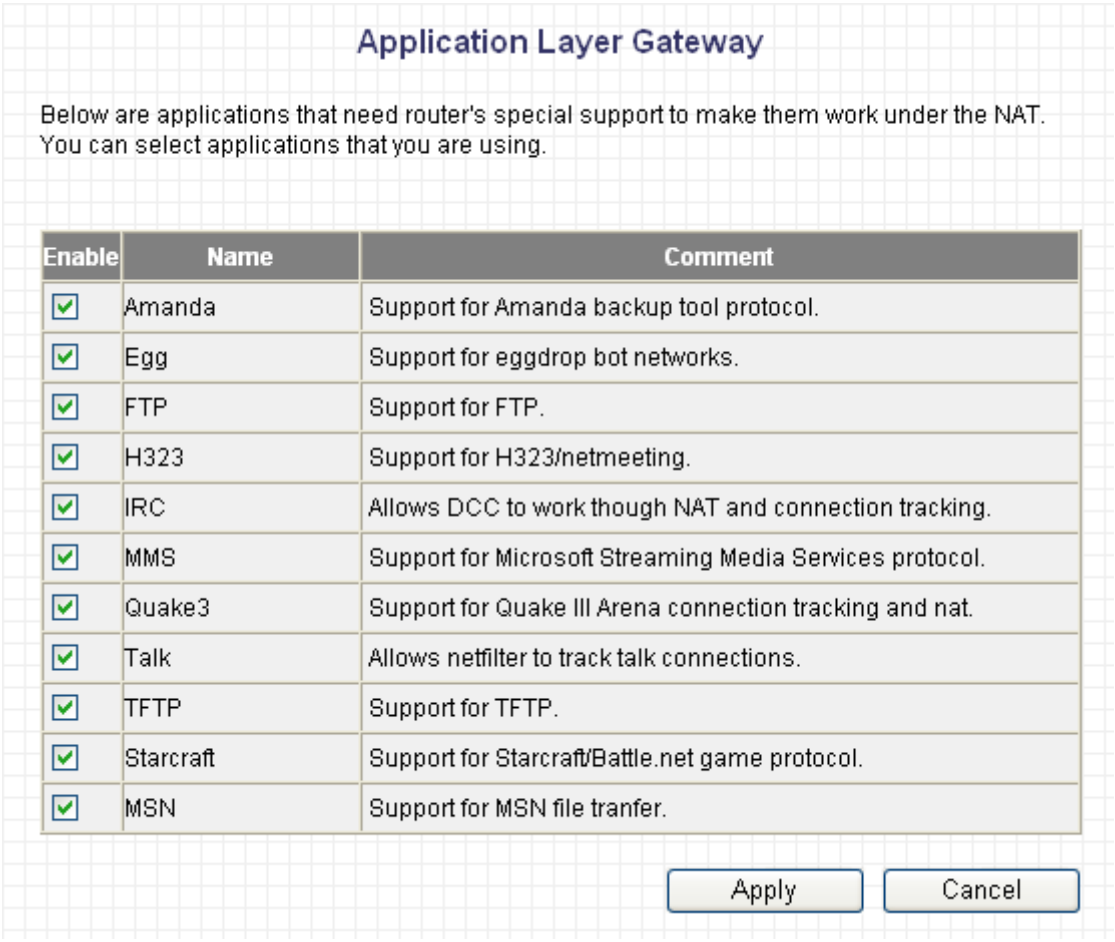


Parameters	Default	Description
UPnP Feature	Disable	You can Enable or Disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications which support UPnP smoothly connect to Internet websites and avoid any incompatibility problem due to the NAPT port translation.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.5 ALG Settings

You can select applications that require “Application Layer Gateway” support.



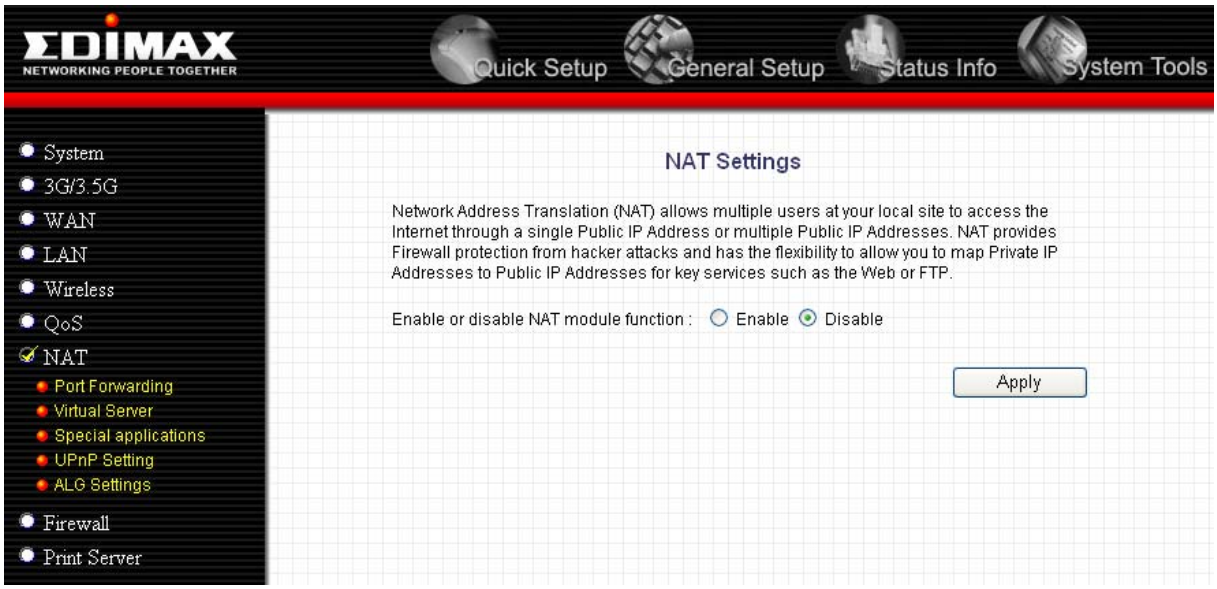
Parameters	Default	Description
Enable		You can enable “Application Layer Gateway” function, and the router will let selected application correctly pass though the NAT gateway.

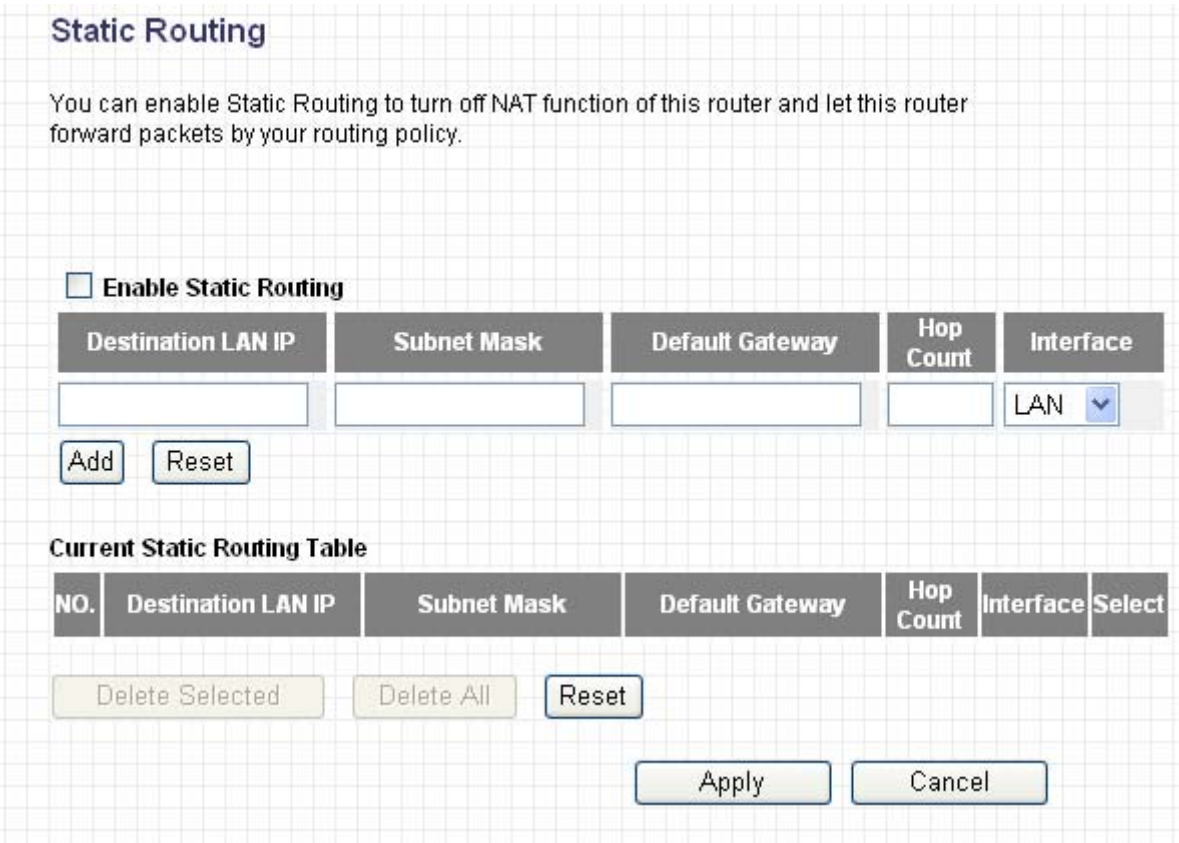
Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.6 Static Routing

This router provides static routing function when NAT is disabled. With static routing, the router can forward packets according to your routing rules. The IP sharing function will not work any more in static routing mode.

Note: The DMZ function of firewall will not work if static routing is enabled.





Parameters	Description
Enable Static Routing	Static routing function is disabled by default. You have to enable the static routing function, to make your routing rules take effect.
Destination LAN IP	The network address of destination LAN.
Subnet Mask	The subnet mask of destination LAN.
Default Gateway	The next stop gateway of the path toward the destination LAN. This is the IP of the neighbor router that this router should communicate with on the path to the destination LAN.
Hop Count	The number of hops (routers) to pass through to reach the destination LAN.
Interface	The interface that go to the next hop (router).
Add a Rule	Fill in the "Destination LAN IP", "Subnet Mask", "Default Gateway", "Hop Count" and "Interface" of the rule to be added and click "Add". Then this static routing rule will be added to the "Static Routing Table" listed below. If you found any typo before adding it and want to correct it, just click "Reset" and the fields will be cleared.
Remove a Rule	If you want to remove some routing rules from the "Static Routing Table", select the rules you want to remove in the table and click "Delete Selected". If you want remove all rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.8 Firewall

This broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server to be located in Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select **Enable** and click **Apply**

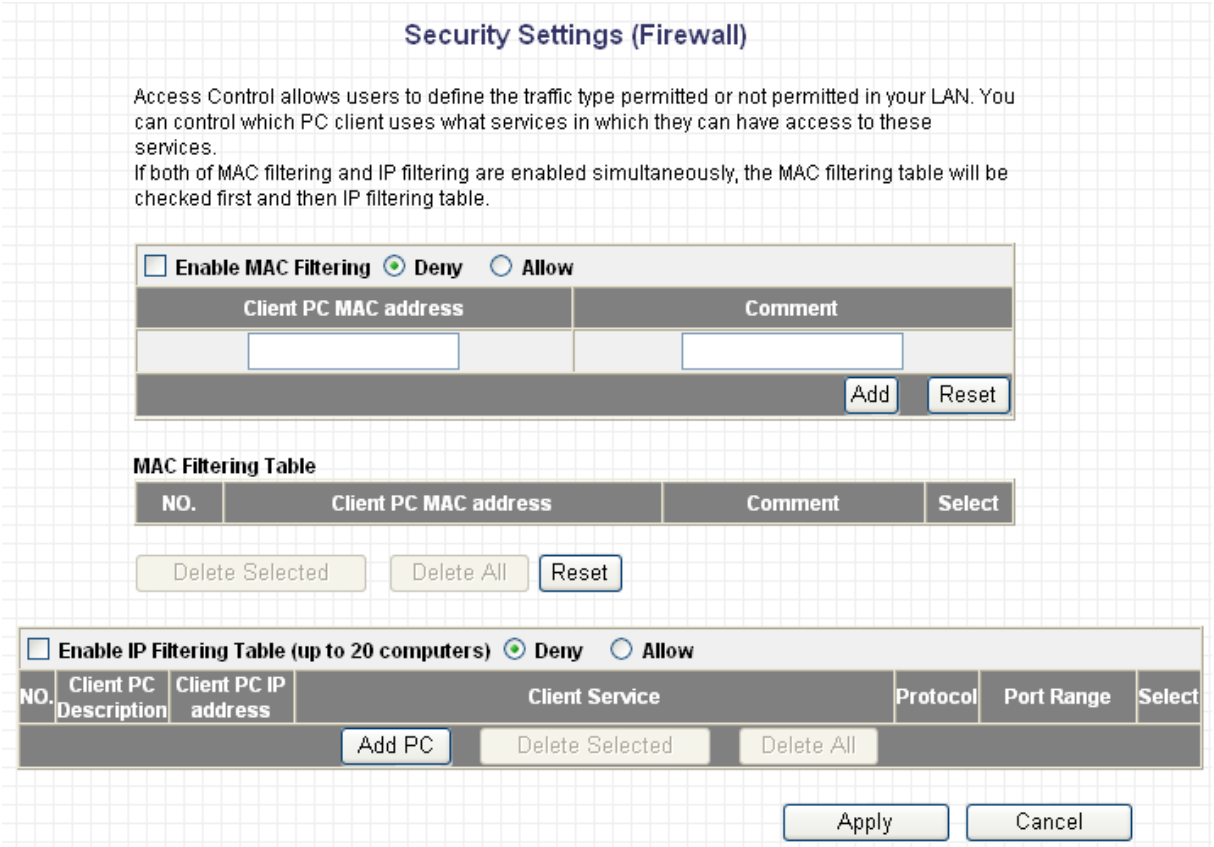
Parameters	Description
Access Control	Access control allows you to specify which computer can or cannot access to certain Internet applications
URL Blocking	URL Blocking allows you to specify which URLs can not be accessed by users.
DoS	The Broadband router's firewall can block common hacker attacks and can log the attack activities.
DMZ	The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN.

Click on one of the firewall selections and proceed to the manual's relevant sub-section

2.8.1 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), this is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to

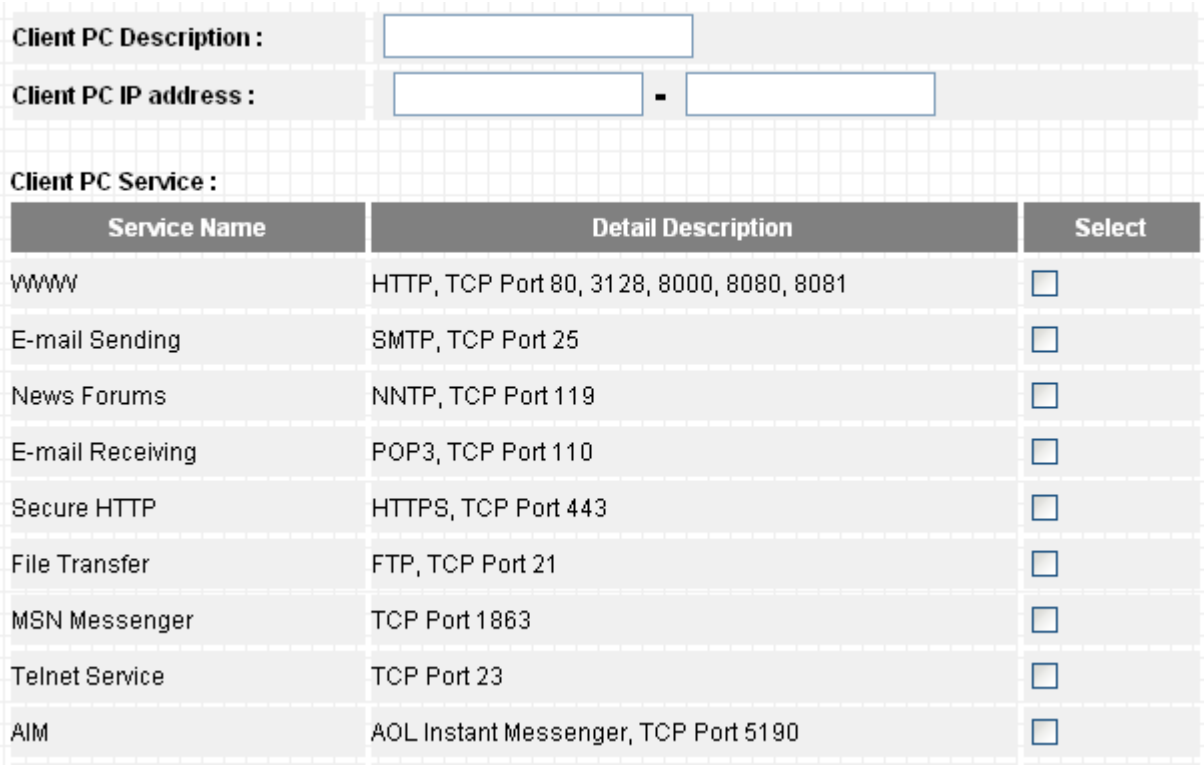
these services.

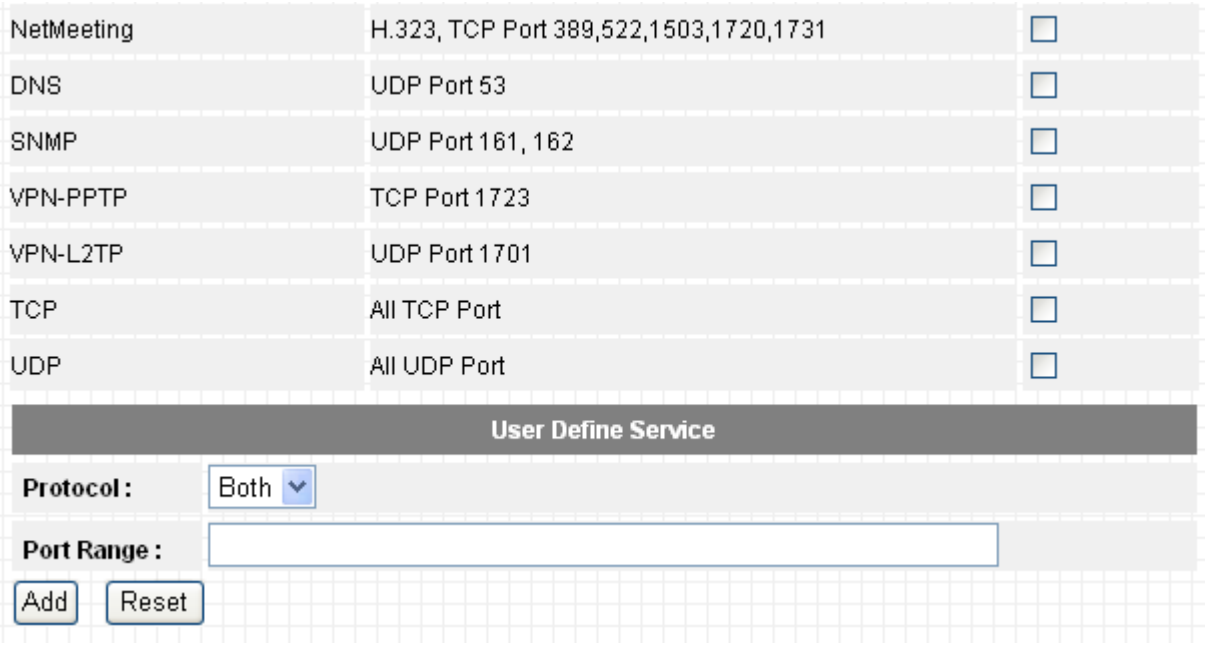


Parameters	Description
Deny	If you select “Deny”, then all PCs will be allowed to access Internet, except those PCs listed in the list below.
Allow	If you select “Allow”, then all PCs will be denied to access Internet. expect those PCs listed in the list below.
Filter client PCs by IP	Fill “IP Filtering Table” to filter PC clients by IP.
Add PC	You can click Add PC to add an access control rule for users by IP address.
Remove PC	If you want to remove some PC from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button.
Filter client PC by MAC address	Check “Enable MAC Filtering” to enable MAC Filtering.

Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC which is allowed to access the Internet, and then click “Add”. If you found any typo before adding it and want to correct it, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

You can now configure other advance sections or start using the router.

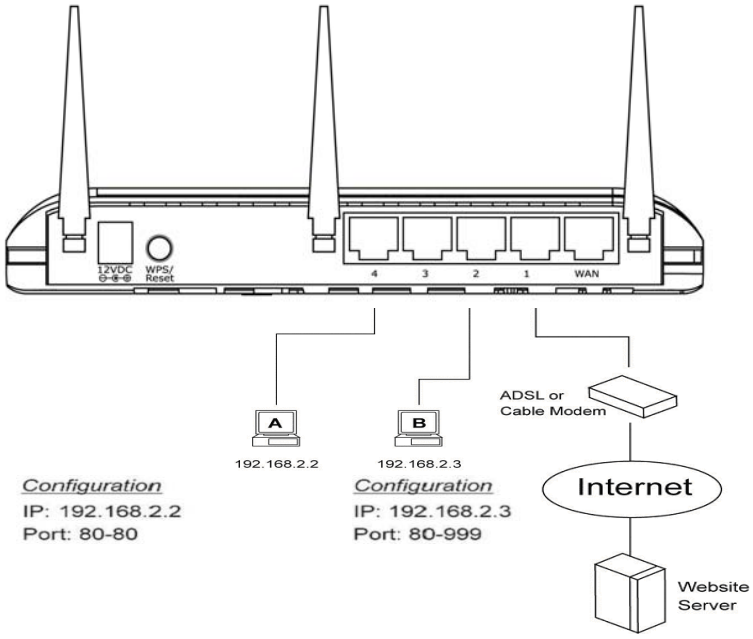




Parameters	Description
Client PC Description	The description for this client PC rule.
Client PC IP Addresses	Enter the IP address range that you wish to apply this access control rule. This is the user's IP address(es) that you wish to setup an access control rule. **Note:** You need to give your LAN PC clients a fixed/static IP address, to make the access control rule working properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select UDP, TCP or both protocol types you want to block.
Port Range	You can assign up to five port ranges. The router will block clients from accessing Internet services which will use these ports.
Apply Changes	Click "Apply Changes" to save the setting.
Reset	Click "Reset" to clear all fields.

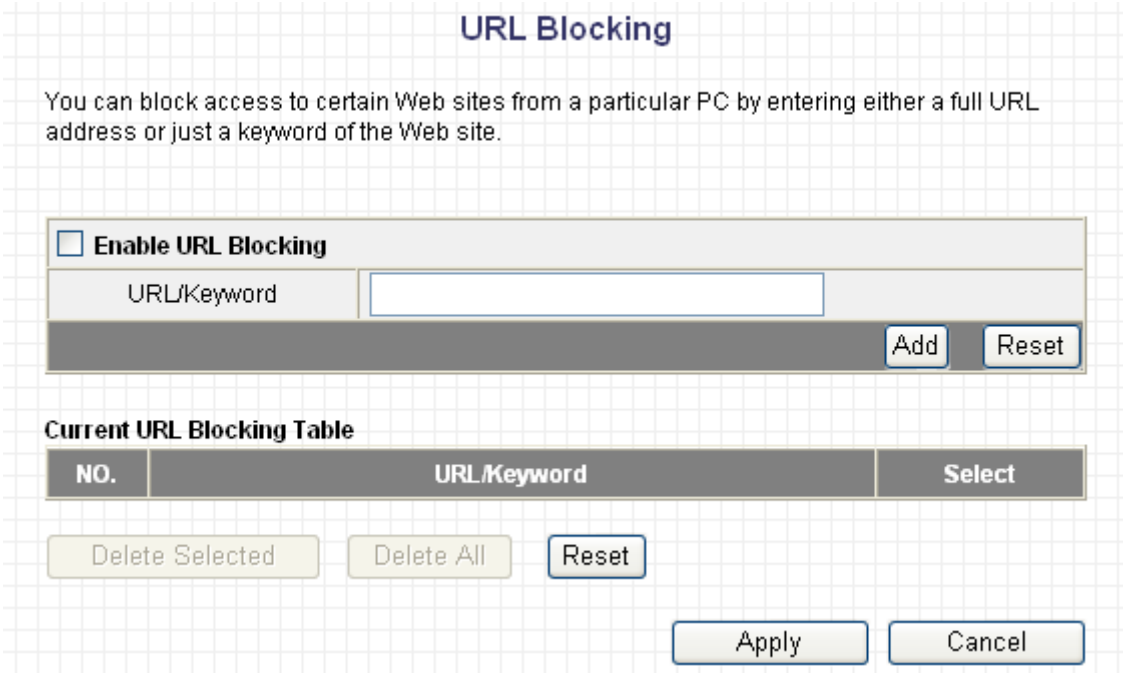
Click <**Apply Changes**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

Example: Access Control
In the example below, LAN client A can only access websites that use Port 80. However, LAN client B is able to access websites and any other service that uses ports between 80 and 999.



2.8.2 URL Blocking

You can block access to some web sites from particular PCs by entering a full URL address or just keyword of the Web site.

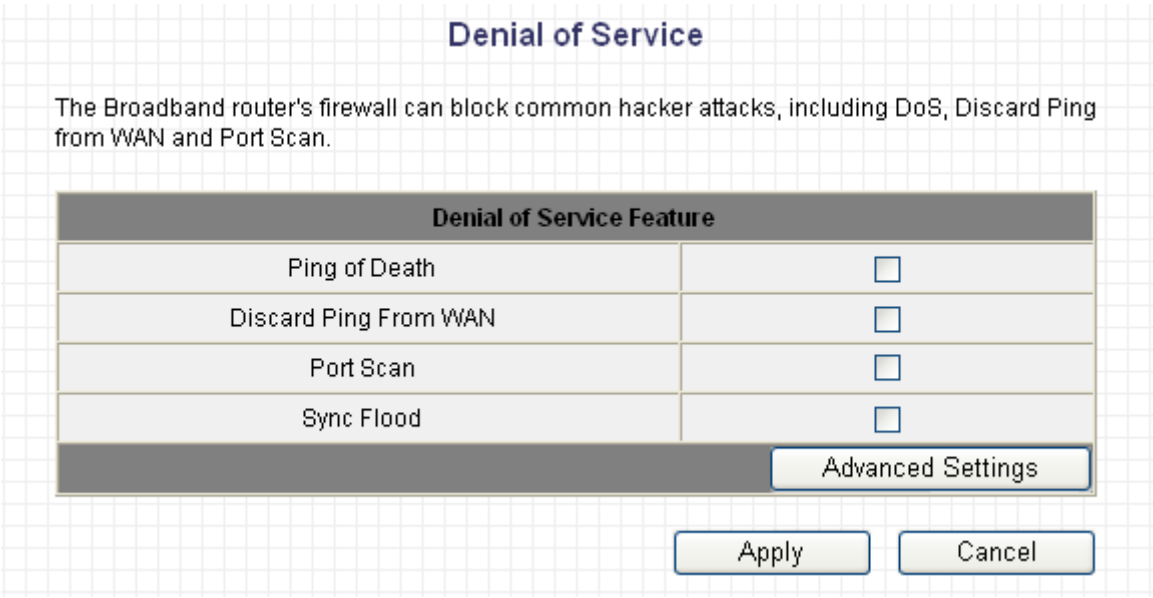


Parameters	Description
Enable URL Blocking	Enable/disable URL Blocking
Add URL Keyword	Fill in “URL/Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block. If you found any typo before adding it and want to correct it, just click "Reset" and the field will be cleared.
Remove URL Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

You can now configure other advance sections or start using the router.

2.8.3 DoS (Denial of Service)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

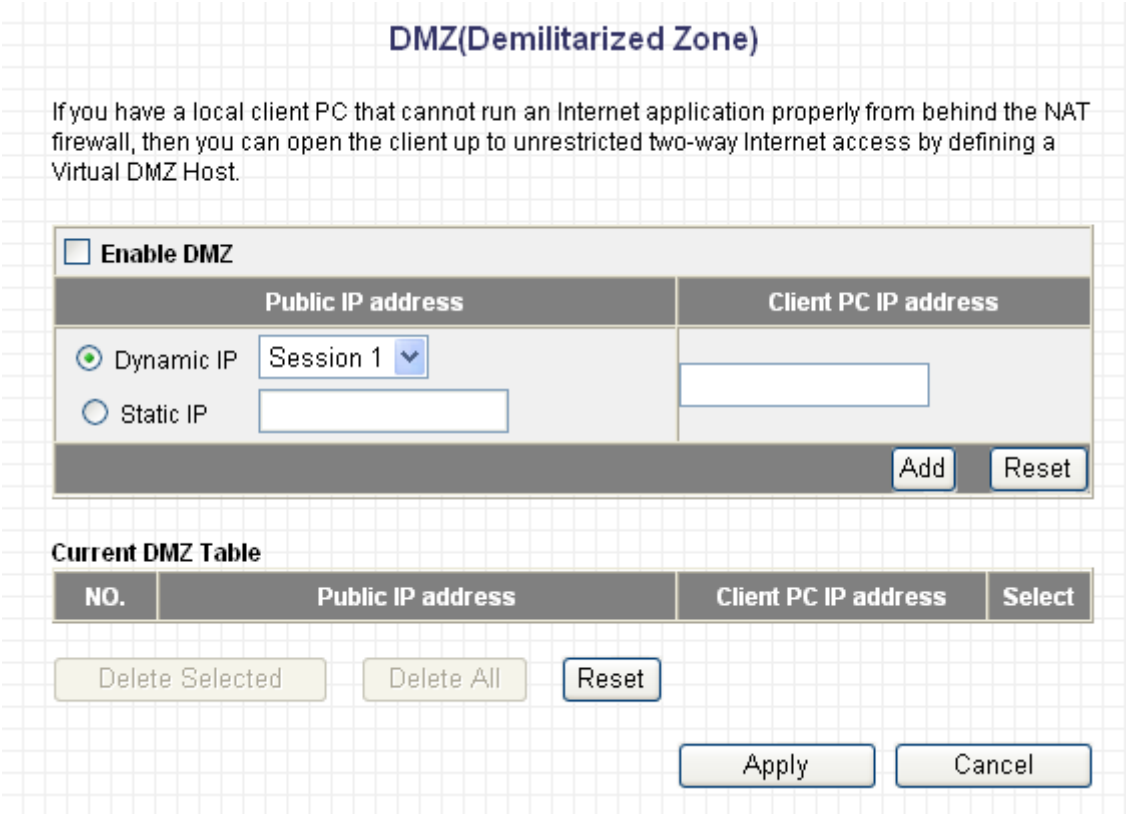


Parameters	Description
Ping of Death	Protect from Ping of Death attack
Discard Ping From WAN	The router’s WAN port will not respond to any Ping requests
Port Scan	Protect the router from Port Scan.
Sync Flood	Protect the router from Sync Flood attack.

Click **<Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.8.4 DMZ

If you have a local client PC that cannot run some specific Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server redirects a particular service/Internet application to a particular LAN client/server, whereas DMZ redirects all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

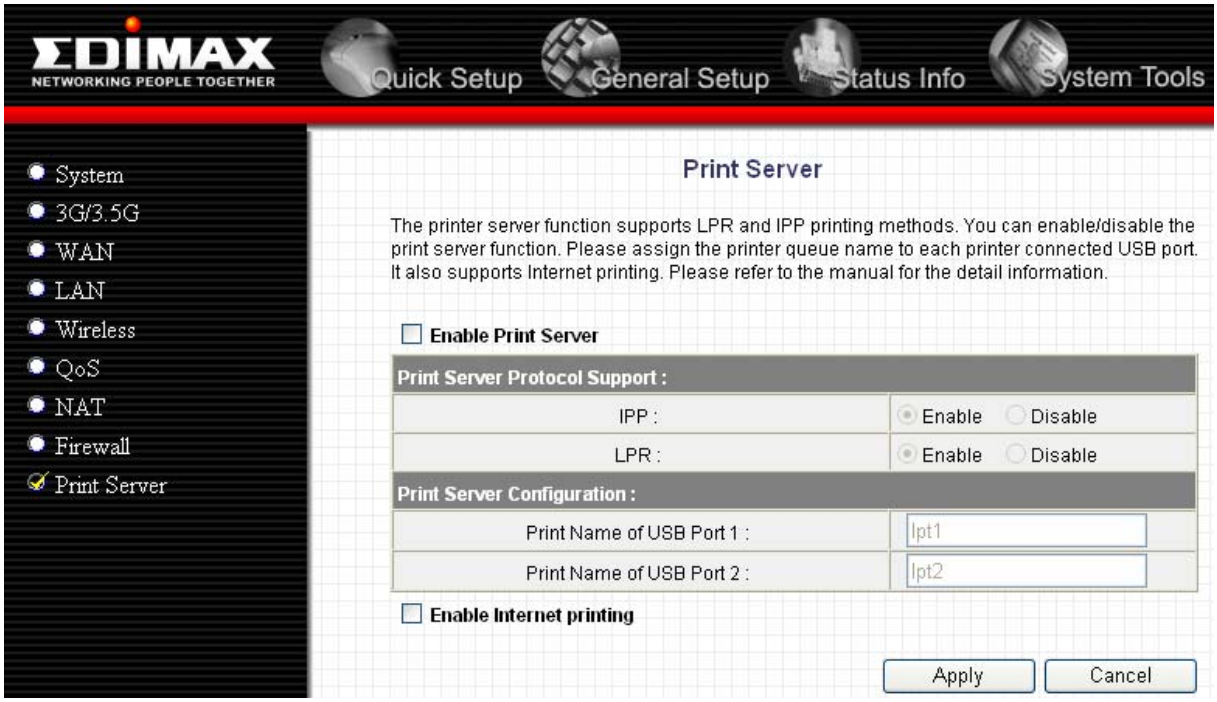


Parameters	Description
Enable DMZ	Enable/disable DMZ **Note**: If there's confliction between the virtual server and the DMZ setting, the virtual server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other public IP addresses assigned to you by your ISP.

Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address listed above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

2.9 Print Server

The router provides Print Server function that let you share a printer to all PCs in your Intranet. It supports LPD and IPP printing protocol.



Parameters	Description
Enable Print Server	Enable/disable USB print server.
IPP	Enable to support the Internet Printing Protocols.
LPR	Enable to support the Local Printing Remote Protocols.
Print Name of USB Port 1	It is the port name of the printer connected to USB port 1.
Print Name of USB Port 2	It is the port name of the printer connected to USB port 2.
Enable Internet printing	You can check “Enable Internet printing” to share the printer on internet, you can uncheck this option to use

	printer on intranet only.

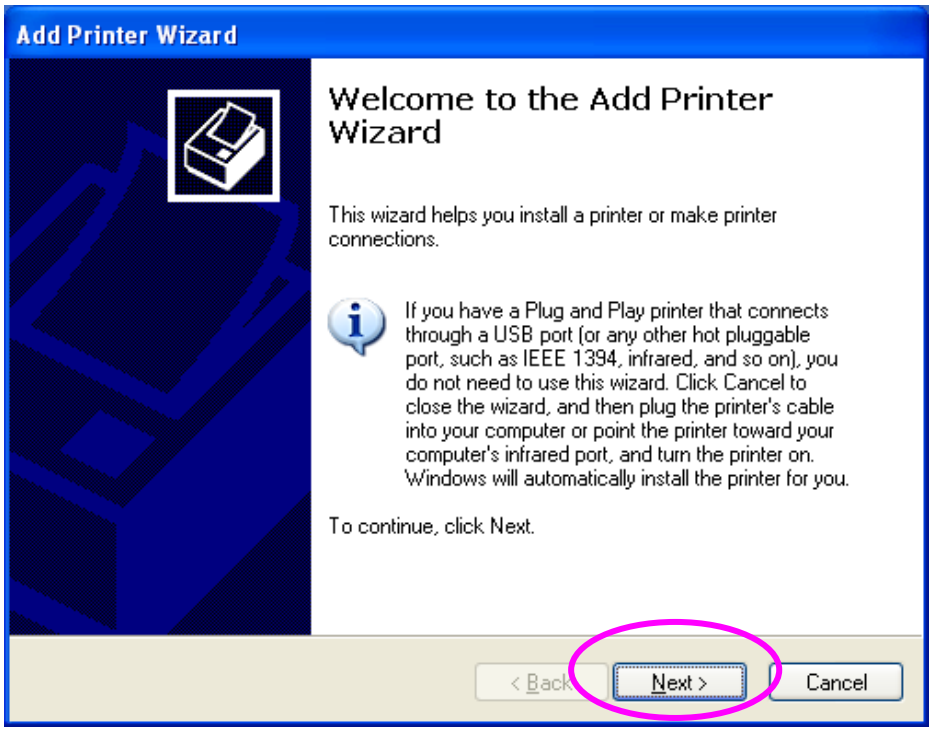
Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.9.1 LPR Printing

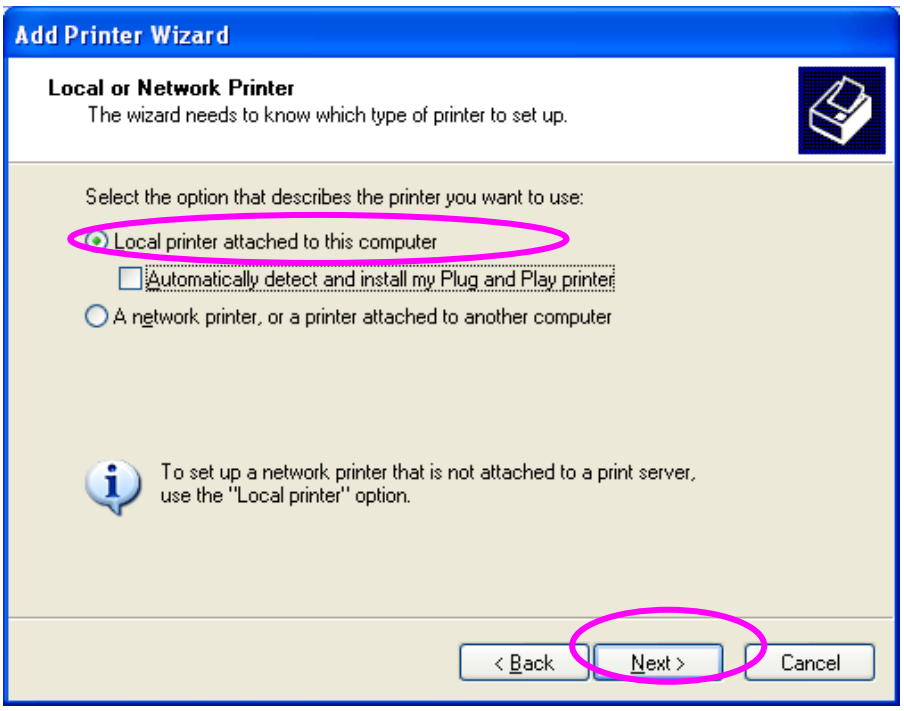
LPR Printing (Line Printer Remote technology) allows user to connect to printers via TCP/IP protocol for printing sharing. Computer with Windows 98SE/Me/NT/2000/XP/2003 operating system can use the protocol to share printer over the network.

To configure the LPR setting in Windows 2000/XP/2003, please follow the instructions listed below:

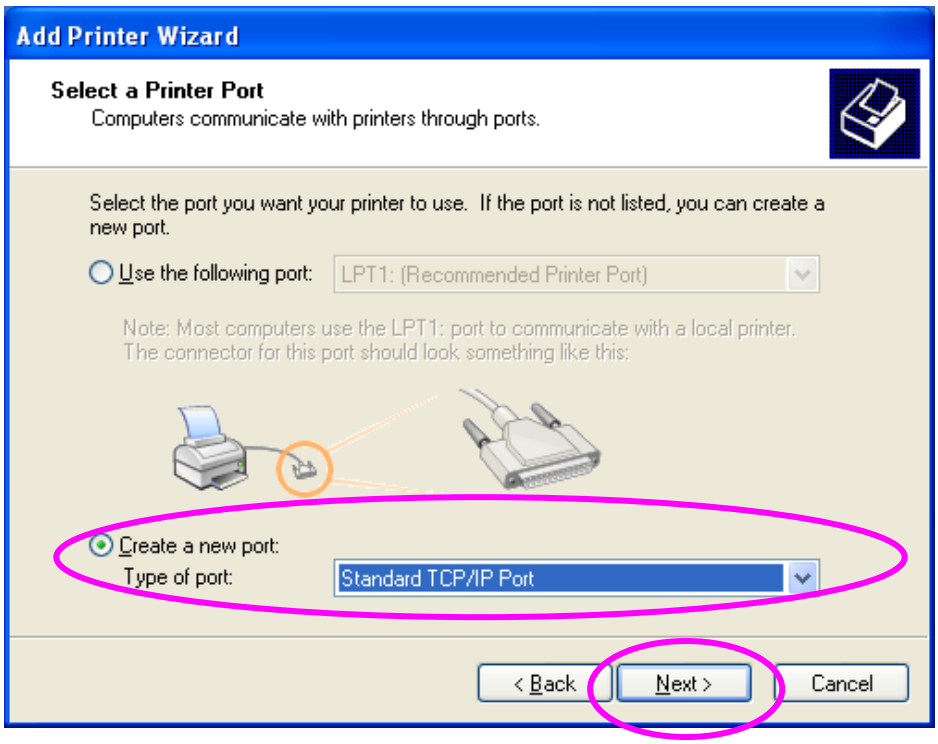
1) Click “Start”, choose “Settings” and select “Printers and Faxes”.
2) Click “Add a Printer”.
3) The “Add Printer Wizard” will appear, then Click “Next”.



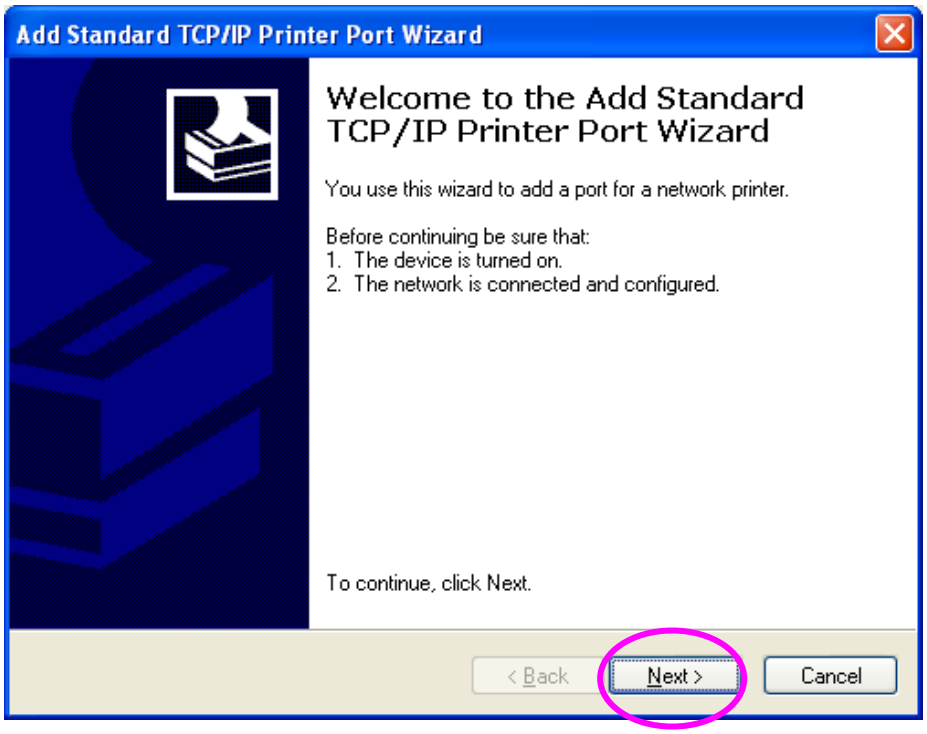
4) Select “Local Printer attached to this computer” and click “Next”.



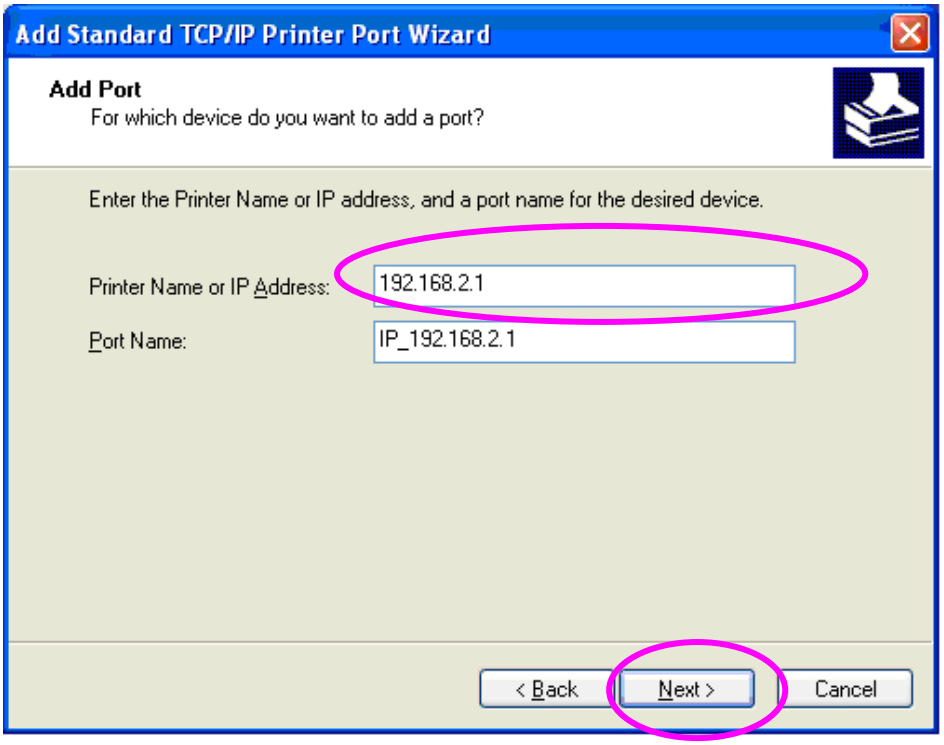
5) Choose “Create a new port” and “Standard TCP/IP Port”. Click “Next”.



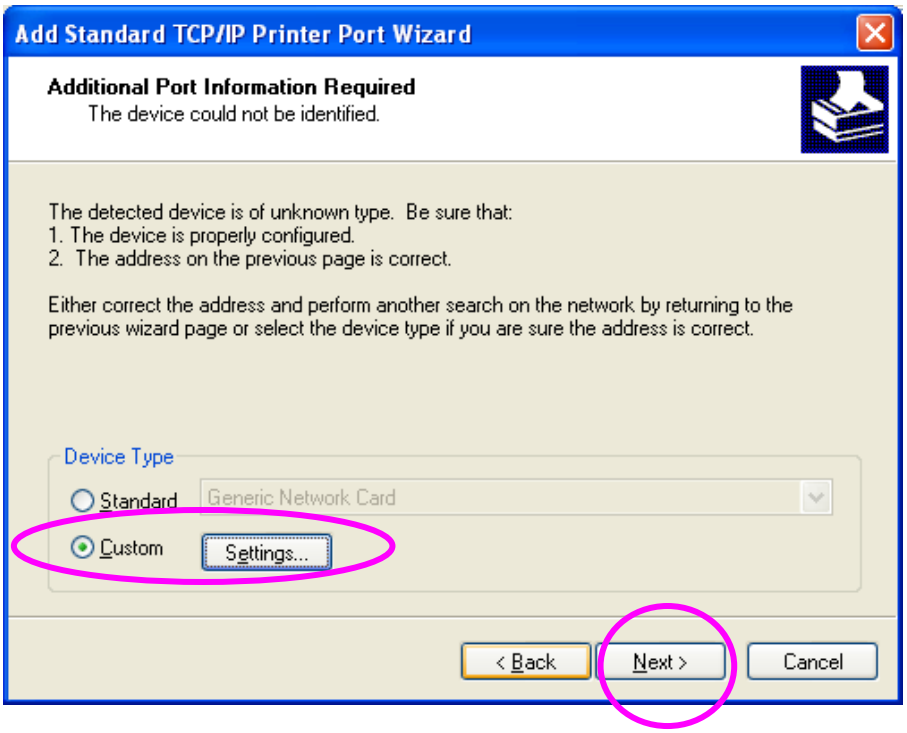
6) Please make sure that the Print Server and the Printer have turned on and connected to the network correctly before you continue. Click “Next”.



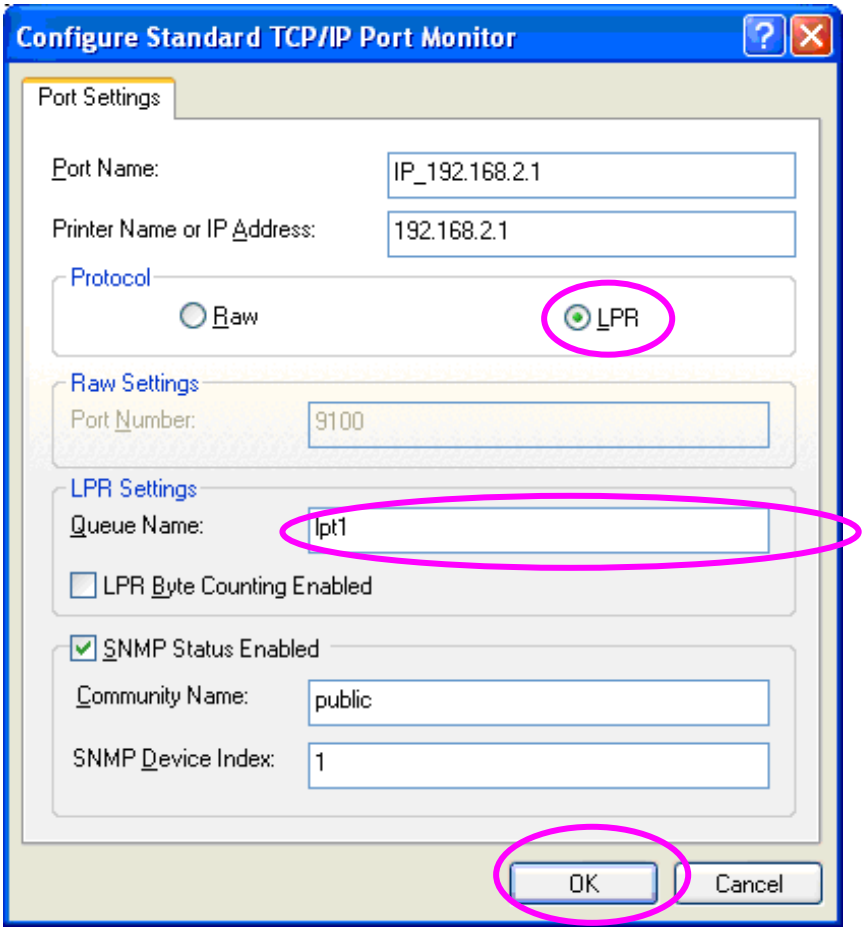
7) Enter the IP Address of the Print Server in the “Printer Name or IP Address”. Click “Next”.



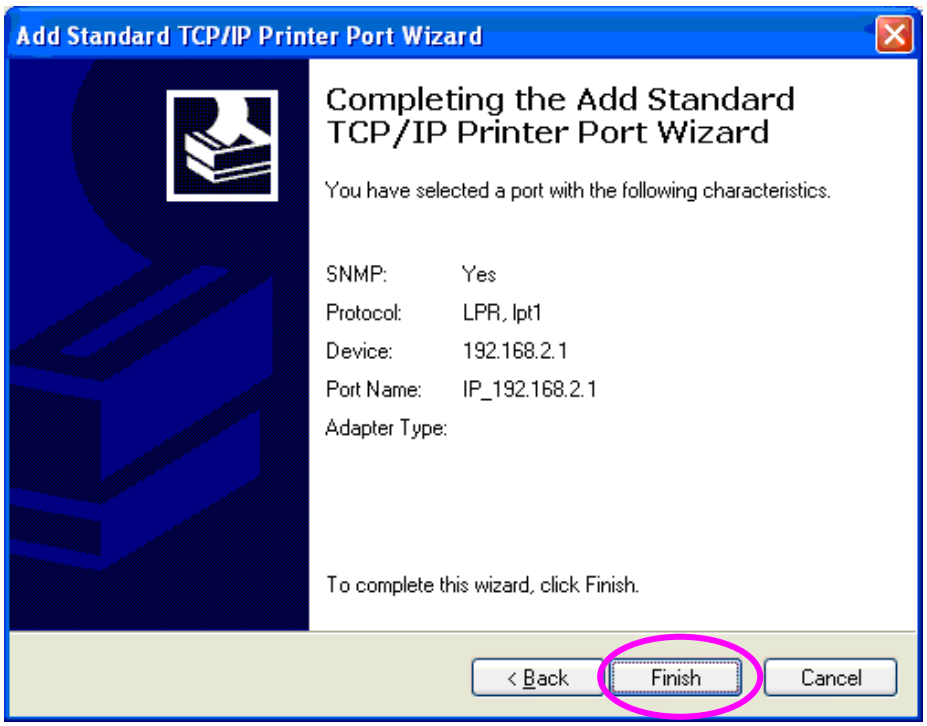
8) Select “Custom” and click “Settings”. When you have finished the settings at step 9, click “Next” to continue.



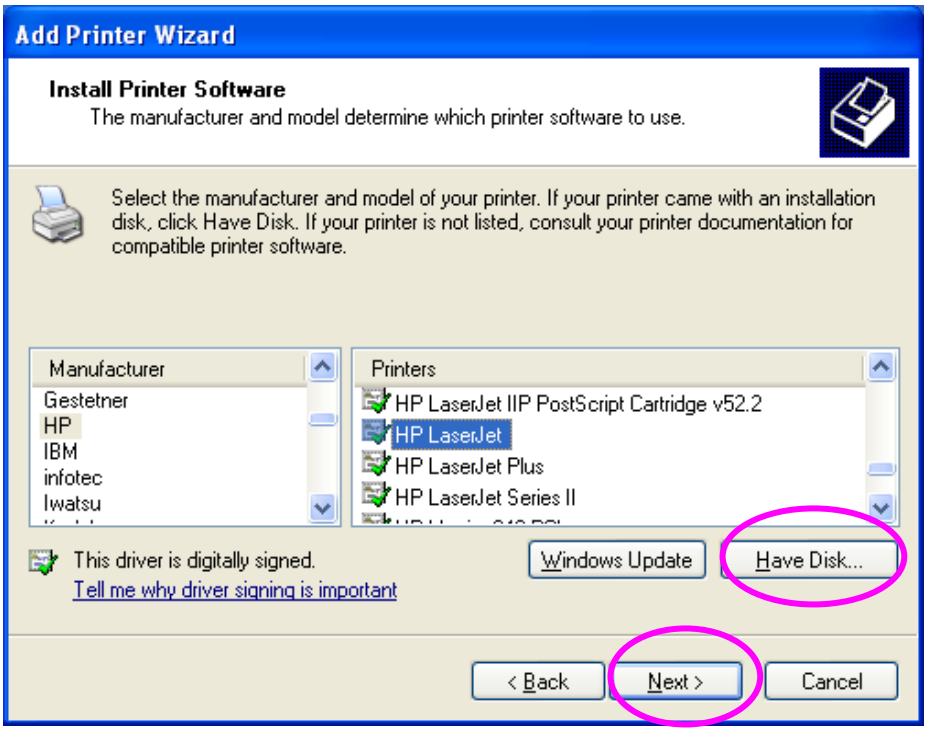
9) Select “LPR” and enter “lpt1” in the “Queue Name”, click “OK”. By default the queue name of the Print Server is “lpt1”.


Configure Standard TCP/IP Port Monitor
Port Settings
Port Name:
IP_192.168.2.1
Printer Name or IP Address:
192.168.2.1
Protocol
Raw
LPR
Raw Settings
Port Number:
9100
LPR Settings
Queue Name:
lpt1
LPR Byte Counting Enabled
SNMP Status Enabled
Community Name:
public
SNMP Device Index:
1
OK
Cancel

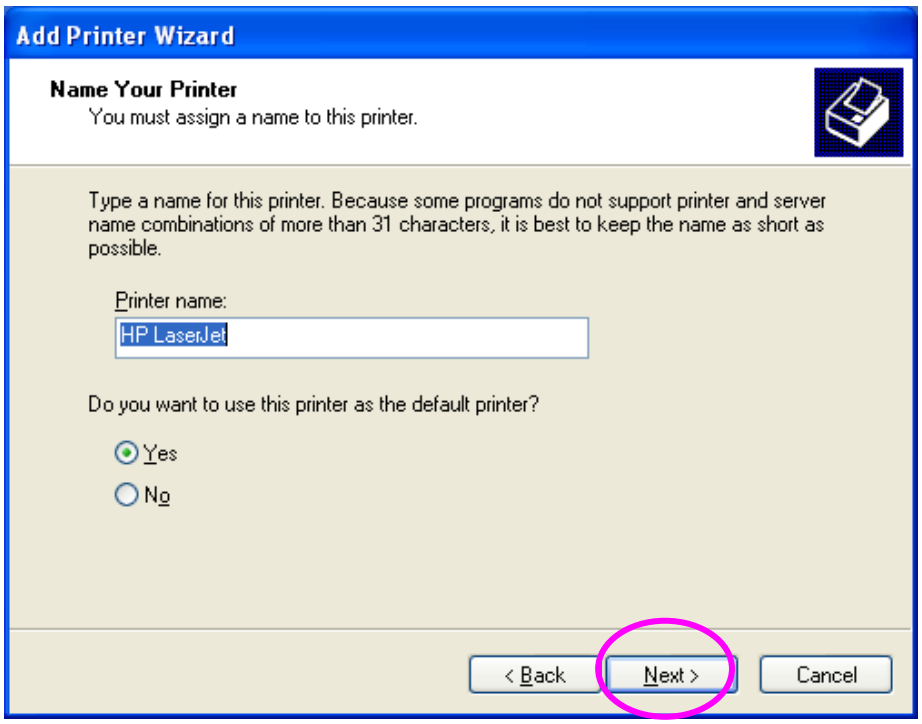
10) Click “Finish”.



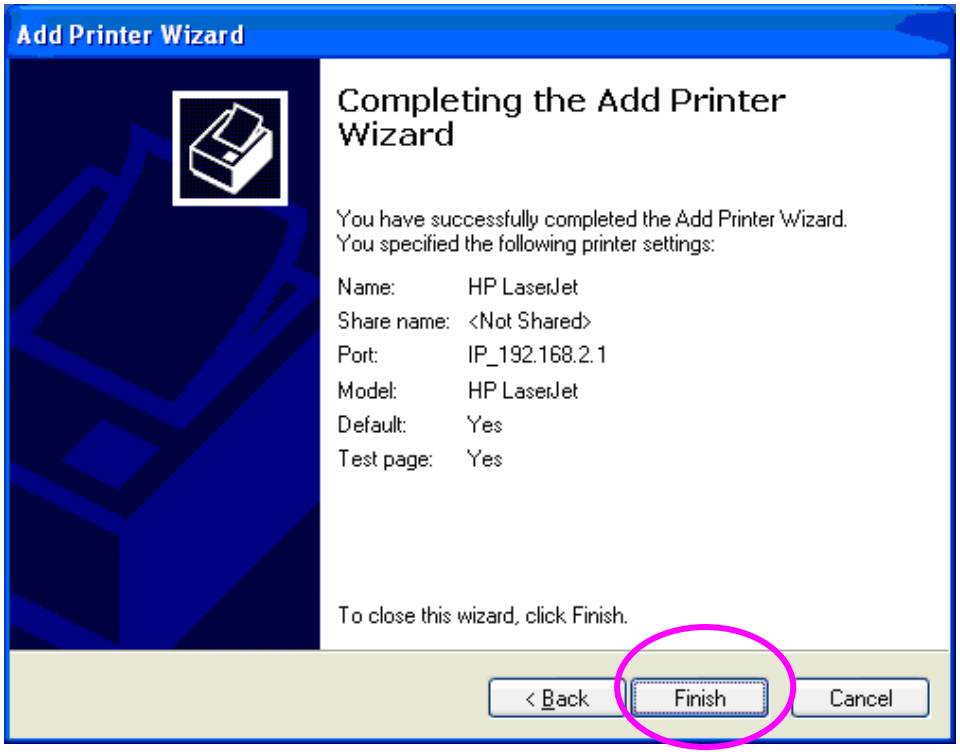
11) Select a suitable printer manufacturer and the printer model and click “Next”. If your printer is not in the list, click “Have Disk…” to install the driver of the printer. After installation, the printer model will be added to the list.



12) Choose to set the print whether as a default printer or not. Click “Next”.



13) You have added the network printer to the PC successfully. The information of the printer is displayed in the windows. Click “Finish”.



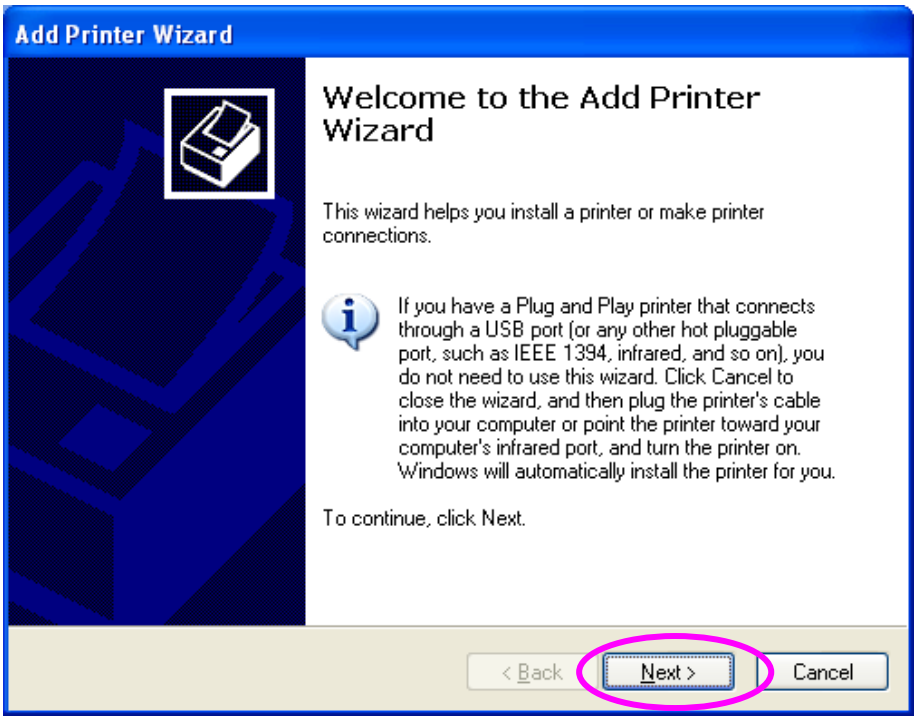
2.9.2 IPP Printing

IPP (Internet Printing Protocol) Printing provides a convenient way of remote printing service by TCP/IP. The Print Server can support IPP printing in Windows 2000/XP/2003 by default. By using the IPP printing, you can share the printer to all the PC's that can access the Print Server by Internet Protocol (IP).

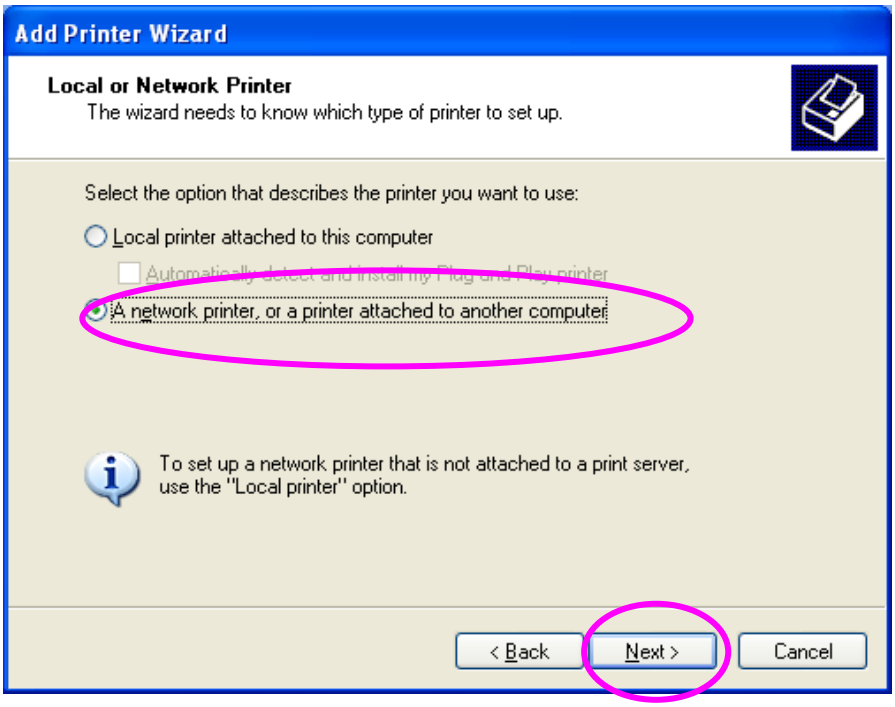
To configure the IPP Printing on Windows 2000/XP/2003, you have to make sure the print server has correct IP settings. If you want to share the printers to Internet users, you have to set a valid Internet IP address to the Print Server. You also have to make sure that there's no gateway, router or firewall blocking IPP protocol if you have these gateway devices installed in your network.

At client side, please follow the steps below to configure the LPR setting in Windows 2000/XP/2003.

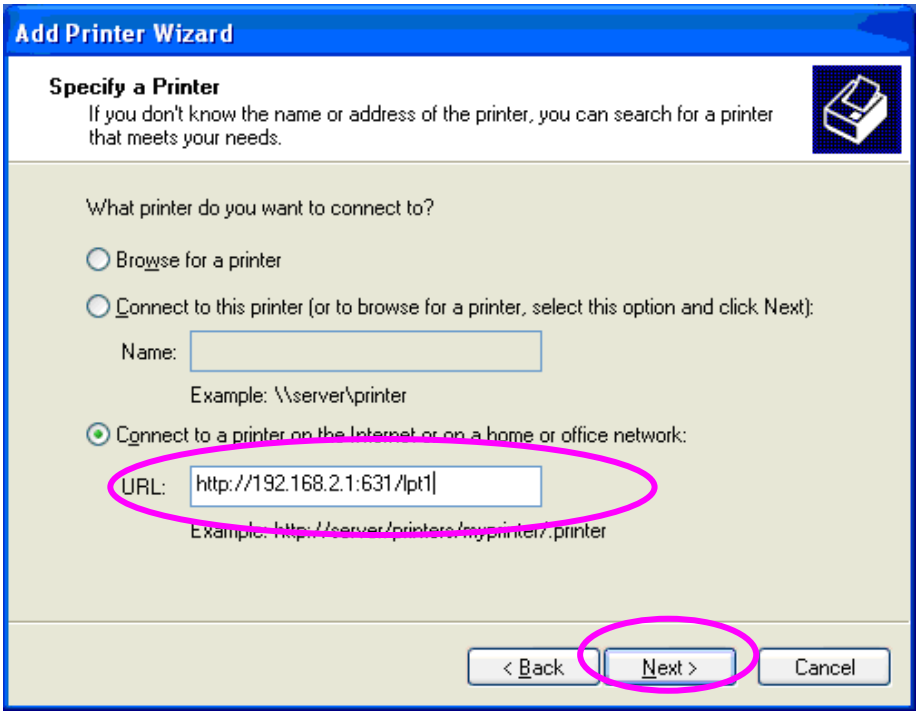
1) Click "Start", choose "Settings" and select "Printers and Faxes".
2) Click "Add a Printer".
3) The "Add Printer Wizard" is displayed. Click "Next".



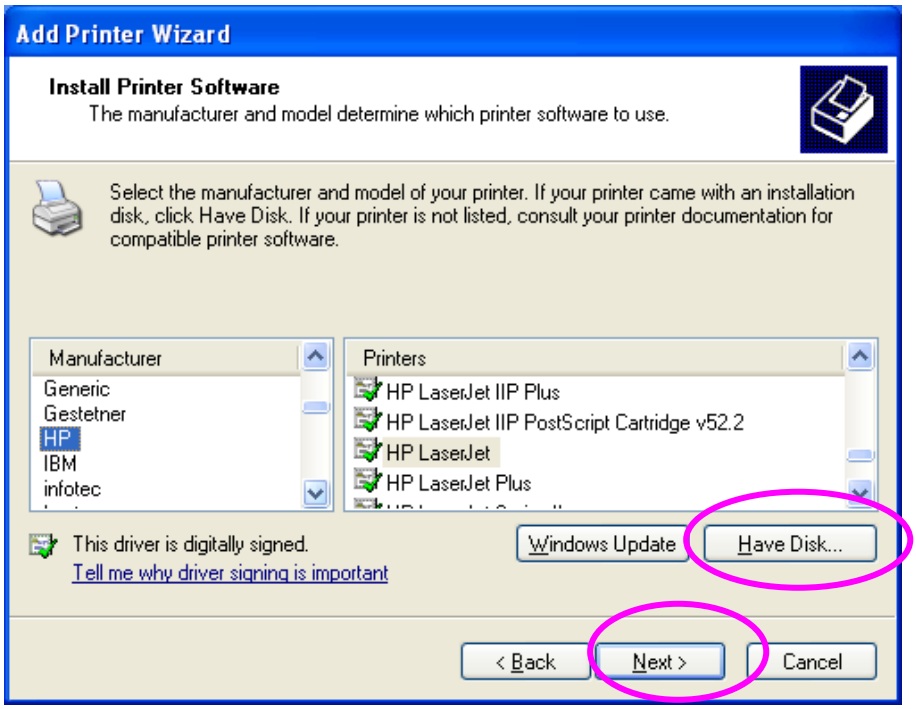
4) Select “A network printer, or a printer attached to another computer”, then click “Next”.



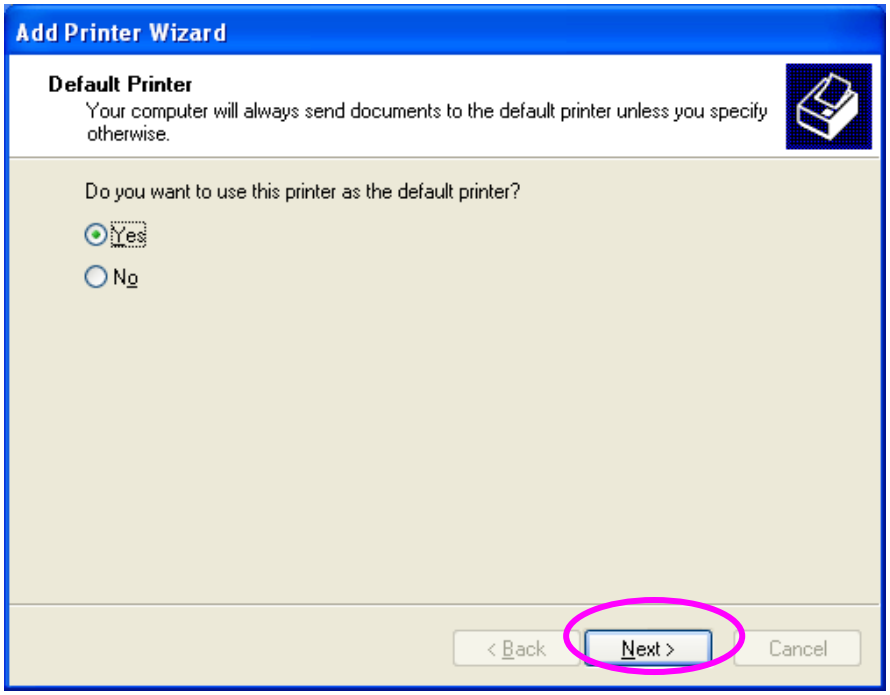
5) Select “Connect to a printer on the Internet or on a home or office network” and enter the URL of Print Server. The URL format is “http://IP:631/Port Name”. The IP should be the Print Server’s IP. The number 631 is IPP standard port number. Port Name is the port name of Print Server that your printer is connected to. The default port name is “lpt1”. One example of the URL is http://192.168.2.1:631/lpt1. After entering the URL of Print Server, click “Next”.


Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Browse for a printer
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
http://192.168.2.1:631/lpt1
< Back
Next >
Cancel

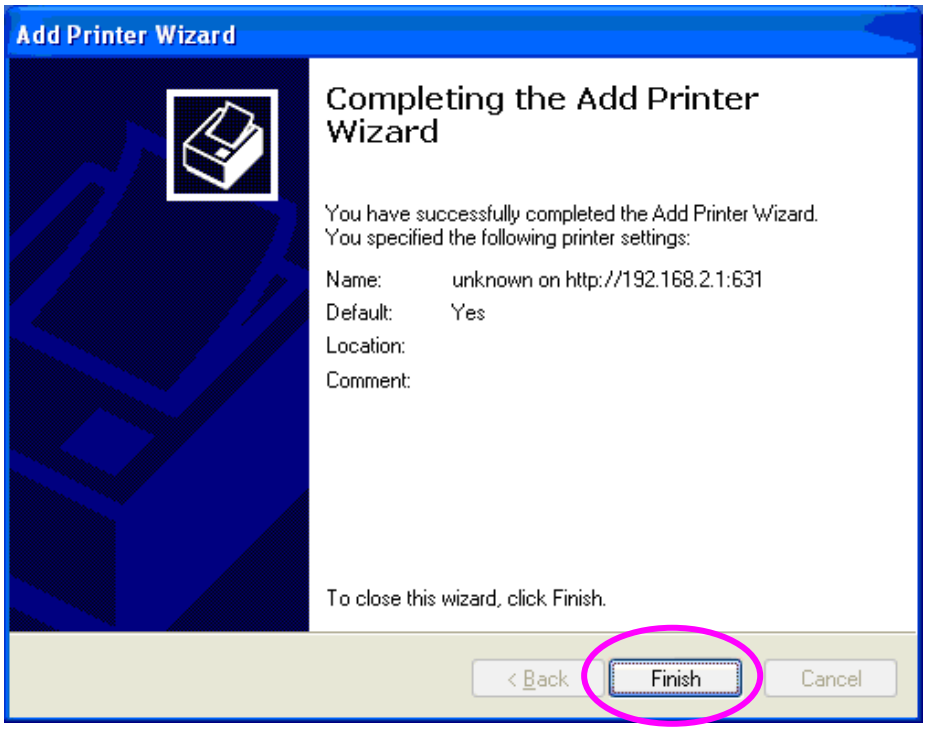
6) Select a suitable printer manufacturer and the printer model and click “Next”. If your printer is not in the list, click “Have Disk…” to install the driver of the printer. After installation, the printer model will be added to the list.



7) Choose to set the print whether as a default printer or not. Click “Next”.



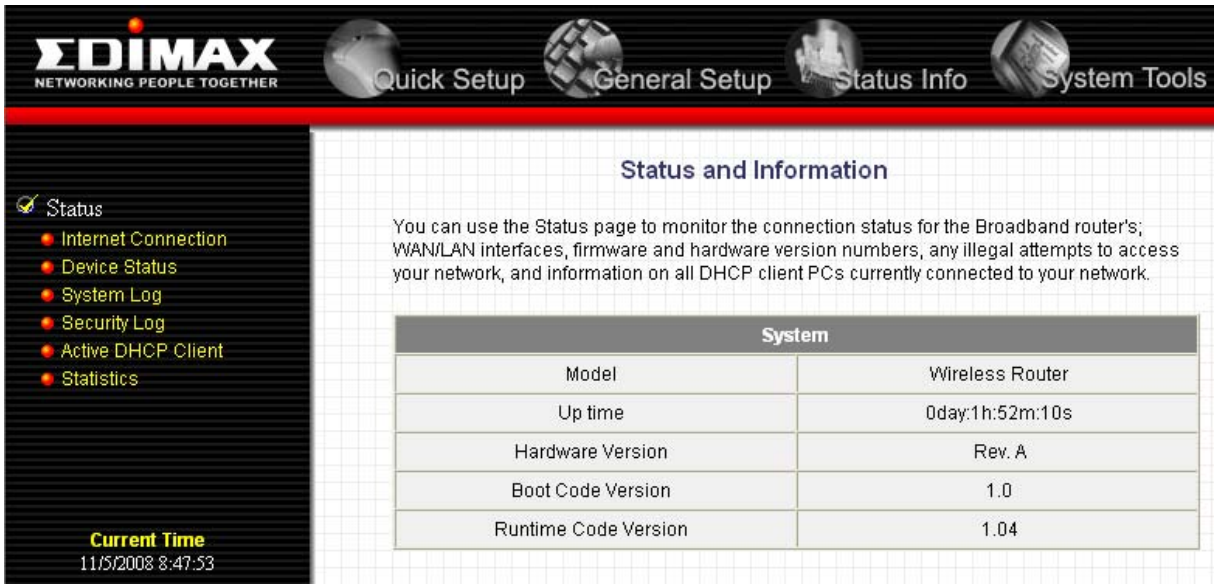
8) Now you have successfully added the network printer to your PC. The information of the printer will be displayed in the window. Click “Finish”.



Chapter 3

Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the Broadband router's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

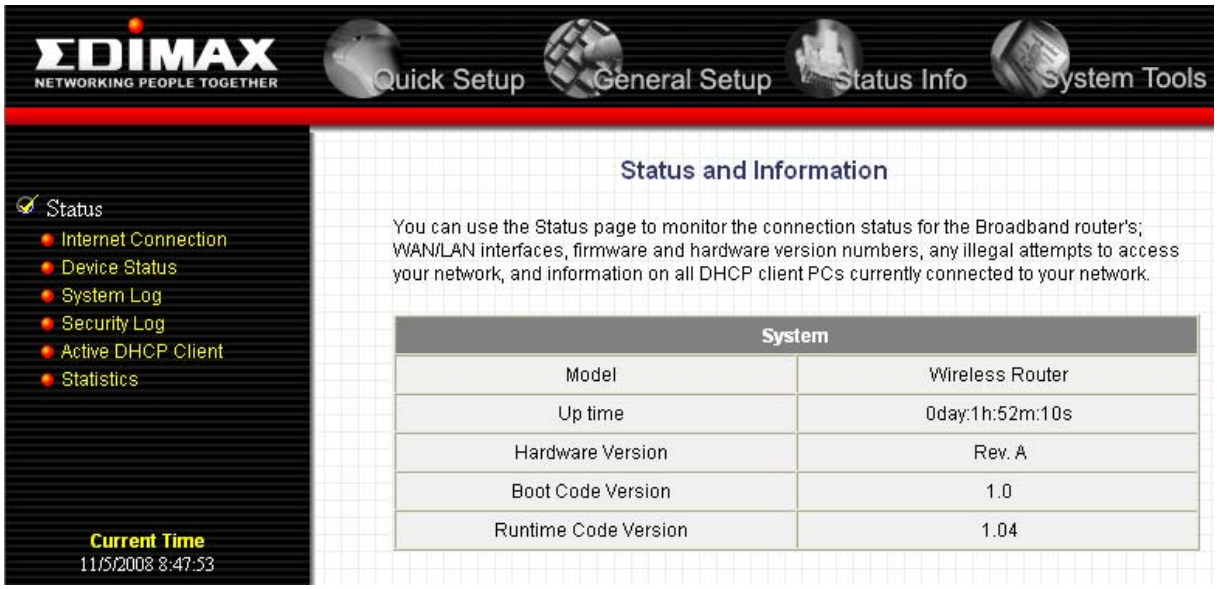


Parameters	Description
Status and Information	Shows the router’s system information
Internet Connection	View the Broadband router’s Internet connection status and other related information
Device Status	View the Broadband router’s current settings
System Log	View the Broadband router’s system log
Security Log	View any attempts that have been made to gain access to your network.
Active DHCP Client	View your LAN client's information that is currently linked to the broadband router
Statistics	Shows the statistics

Select one of the above Status selections and proceed to the manual's relevant sub-section

Status and Information

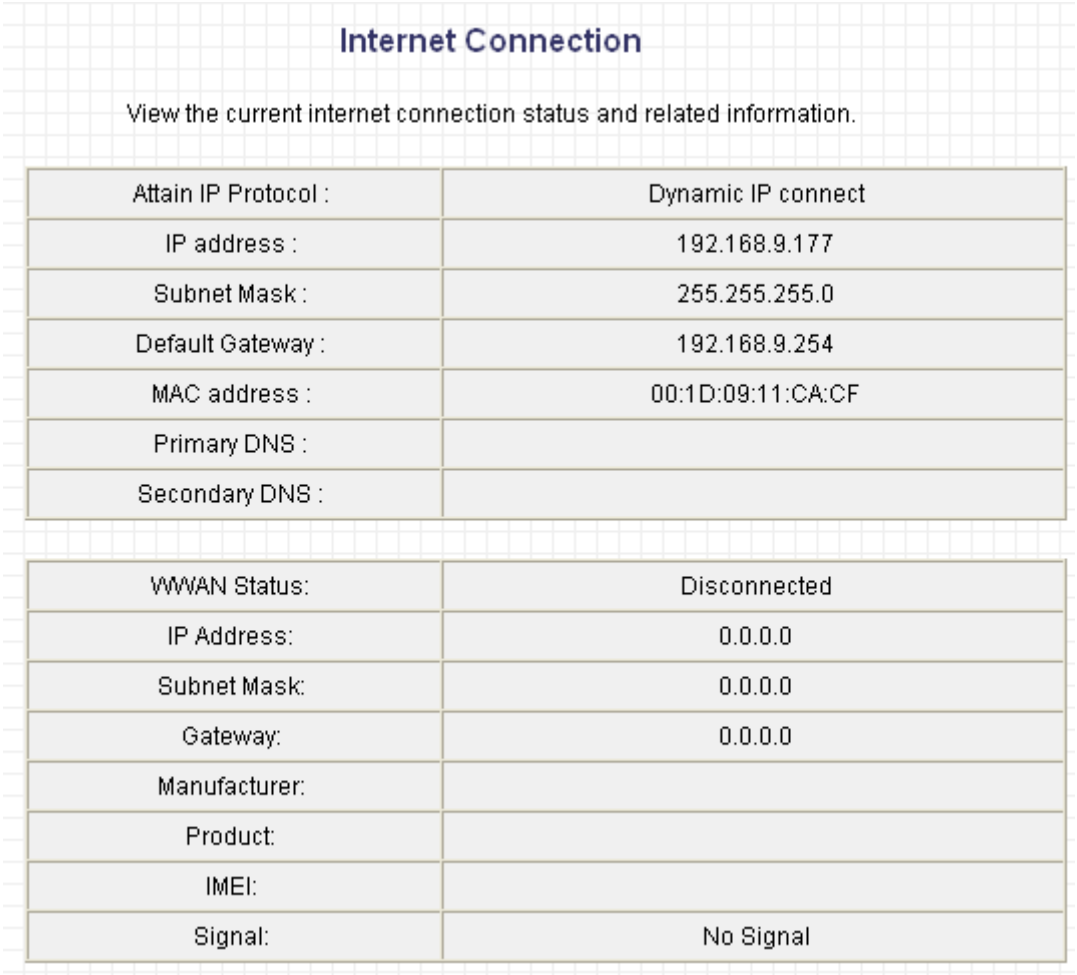
The Status and Information section allows you to view the router's system information



Parameters	Description
Information	You can see the router's system information, such as the router's LAN MAC address, WAN MAC address, hardware version, serial number, boot code version, runtime code version

3.1 Internet Connection

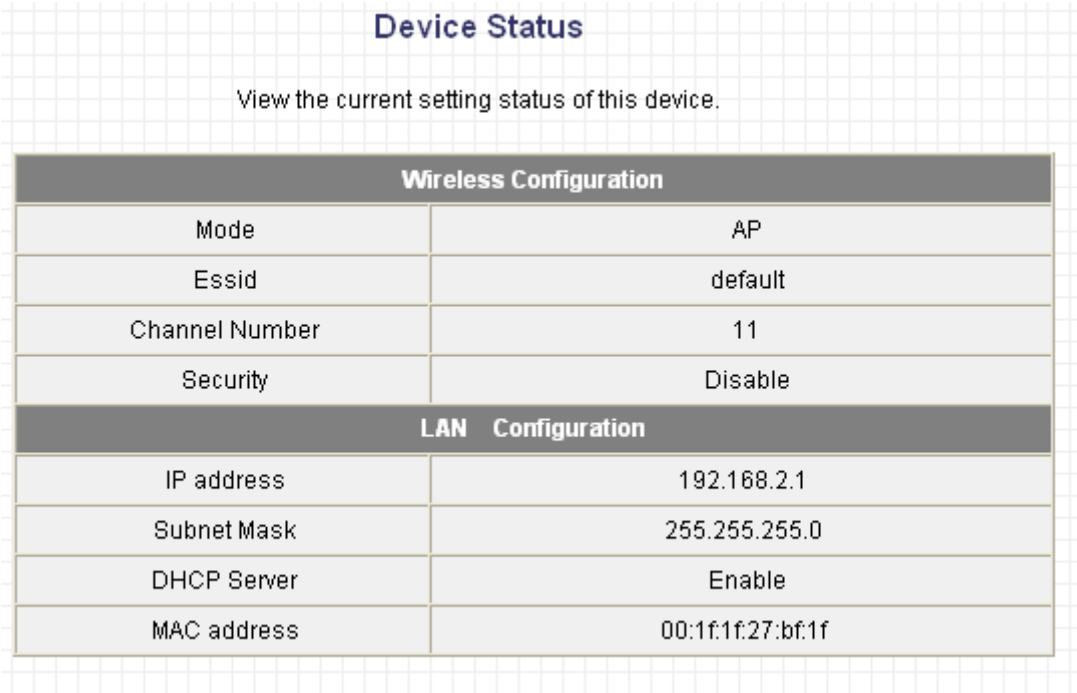
View the Broadband router's current Internet connection status and other related information



Parameters	Description
Internet Connection	This page displays the router's WAN port and 3G/3.5G Internet (WWAN)connection information, including: WAN IP address, subnet mask, and ISP gateway as well as the primary DNS and secondary DNS being used.

3.2 Device Status

View the broadband router's current configuration settings. The device status displays the configuration settings you've configured in the Quick Setup Wizard/General Setup section.



Device Status

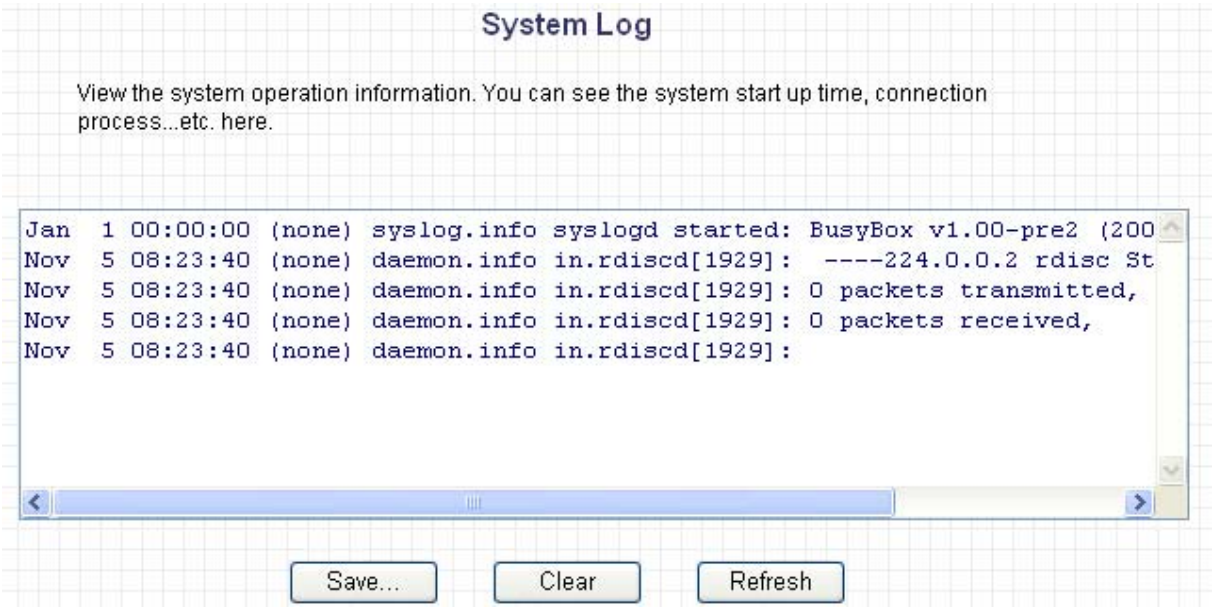
View the current setting status of this device.

Wireless Configuration	
Mode	AP
Essid	default
Channel Number	11
Security	Disable
LAN Configuration	
IP address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC address	00:1f:1f:27:bf:1f

Parameters	Description
Device Status	This page shows the broadband router's current device settings, including: broadband router LAN port's current LAN IP address and subnet mask. It also shows whether the DHCP server function is enabled / disabled.

3.3 System Log

View the operation log of the system.



Parameters	Description
System Log	This page shows the system log of the broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved <**Save**> as a local file, you can clear the log by click <**Clear**> button, too. You can also click <**Refresh**> button to get the most updated information. When the system is powered down, the system log will disappear if it's not saved as a local file.

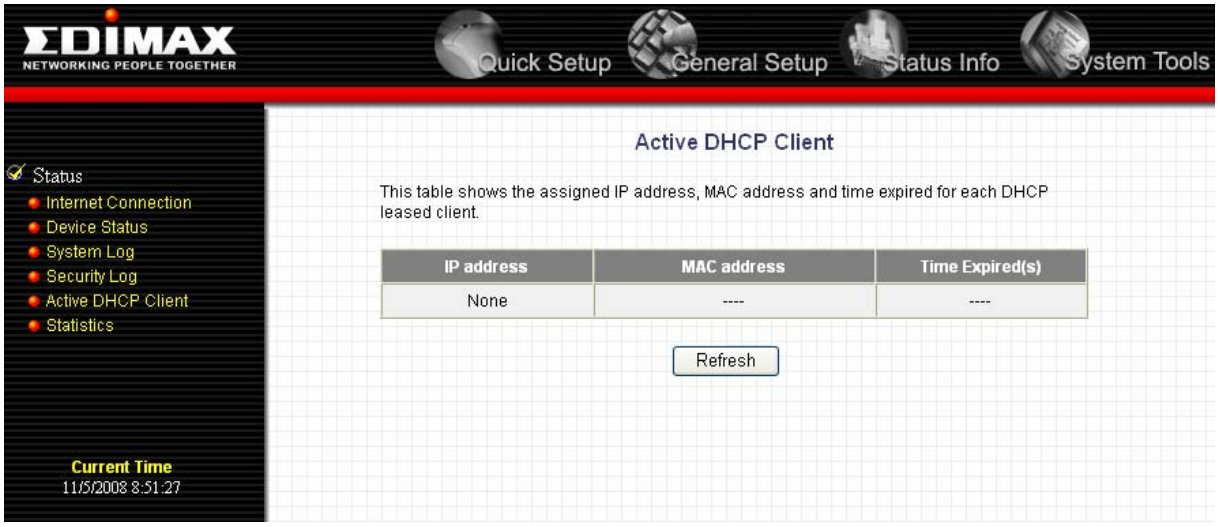
3.4 Security Log

View any attempts that have been made to gain access to your network.

Parameters	Description
Security Log	This page shows the current security log of the Broadband router. It displays all attempts tried to access your network. At the bottom of the page, the security log can be saved <**Save**> as a local file, you can clear the log by clicking <**Clear**>, too. You can also click <**Refresh**> button to get the most updated information. When the system is powered down, the security log will disappear if it's not saved as a local file.

3.5 Active DHCP Client

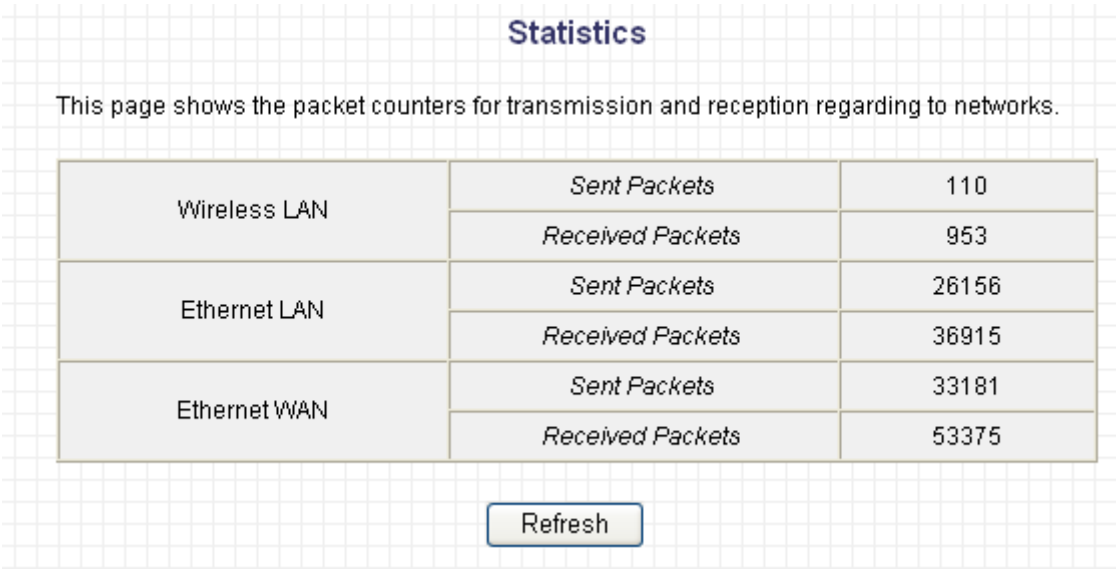
This page lists all DHCP clients.



Parameters	Description
Active DHCP Client	This page shows all DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the **IP** address and the **MAC** address and expiry time of each LAN Client. Use the **Refresh** button to get the most updated information.

3.6 Statistics

View the statistics of packets sent and received on WAN, LAN and Wireless LAN interface.

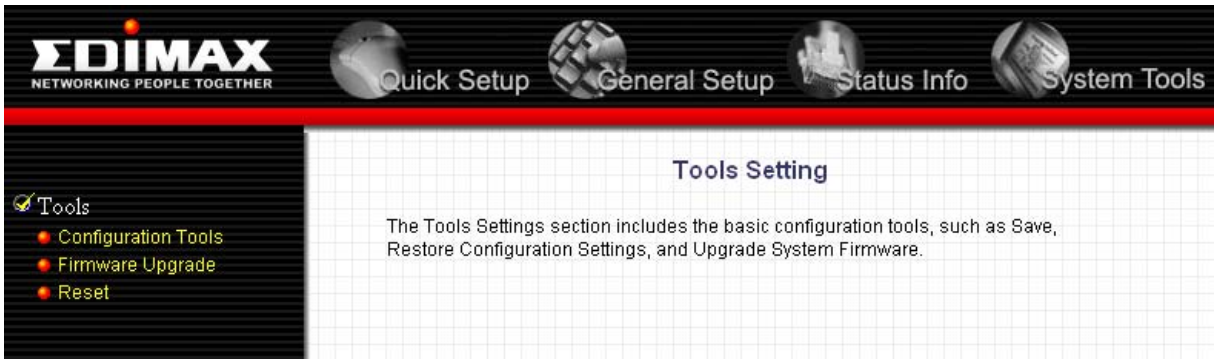


Parameters	Description
Statistics	Shows the statistics of packets sent and received on WAN, LAN and Wireless LAN interface.

Chapter 4

Tool

This page includes basic configuration tools of this broadband router, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.

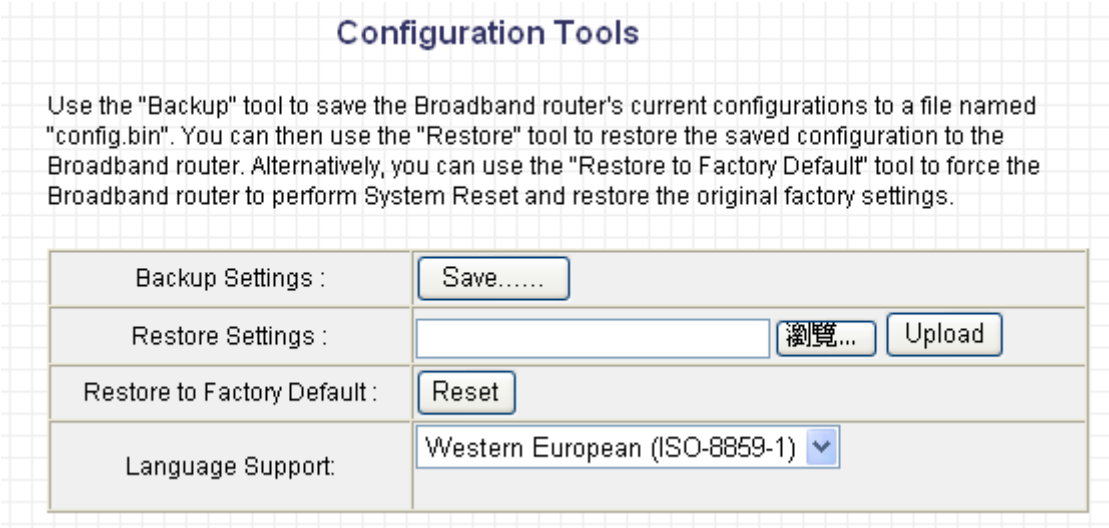


Parameters	Description
Configuration Tools	You can save the router's current configuration, restore the configuration from previously saved configuration files, and restore the router's factory default settings
Firmware Upgrade	This page allows you to upgrade the router's firmware
Reset	When you encounter any problem using this broadband router, you can reset the router by this function

Select one of the above **Tools Settings** selections and proceed to the relevant sub-section

4.1 Configuration Tools

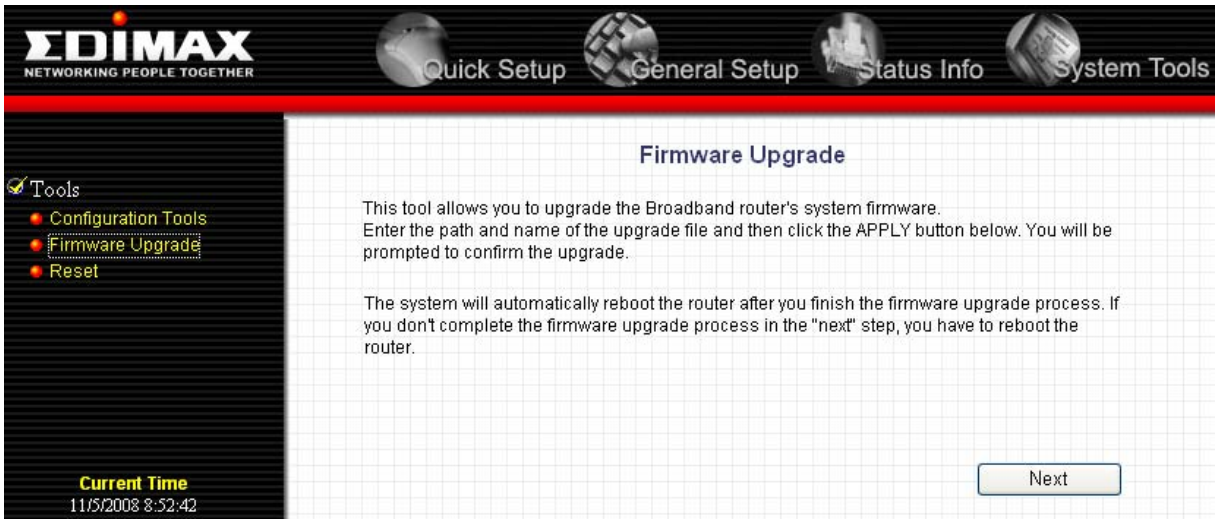
The Configuration Tools screen allows you to save (**Backup**) the router's current settings. Saving the configuration settings provides an added protection and convenience when there're some problems with the router, and you have to reset to factory default to solve the problem. When you save the configuration setting (Backup), you can reload the saved configuration to the router through the **Restore** selection. If extreme problems occur you can use the **Restore to Factory Defaults** selection, this will set all configurations to its original default settings (e.g. when you purchased the router).



Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save the broadband router's current configuration to a file named "config.bin" on your PC. You can then use the "**Restore**" tool to restore the saved configuration to the broadband router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the broadband router to perform a power reset and restore to original factory settings.

4.2 Firmware Upgrade

This page allows you to upgrade the router's firmware



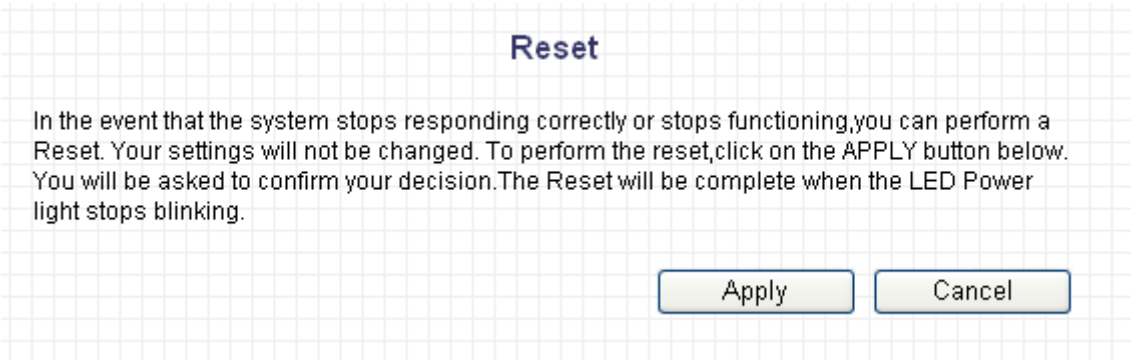
Parameters	Description
Firmware Upgrade	This tool allows you to upgrade the broadband router's system firmware. To upgrade the firmware of your broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also click the browse button to locate the firmware file on your PC.

After you selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process. (You may have to wait few minutes for the upgrade to complete). Once the upgrade is complete you can start using the router.

Warning: When upgrading firmware, be sure not to switch the computer off, or restart your computer.

4.3 Reset

You can reset the router's system when there's something wrong with the router. The reset function will reboot your router.

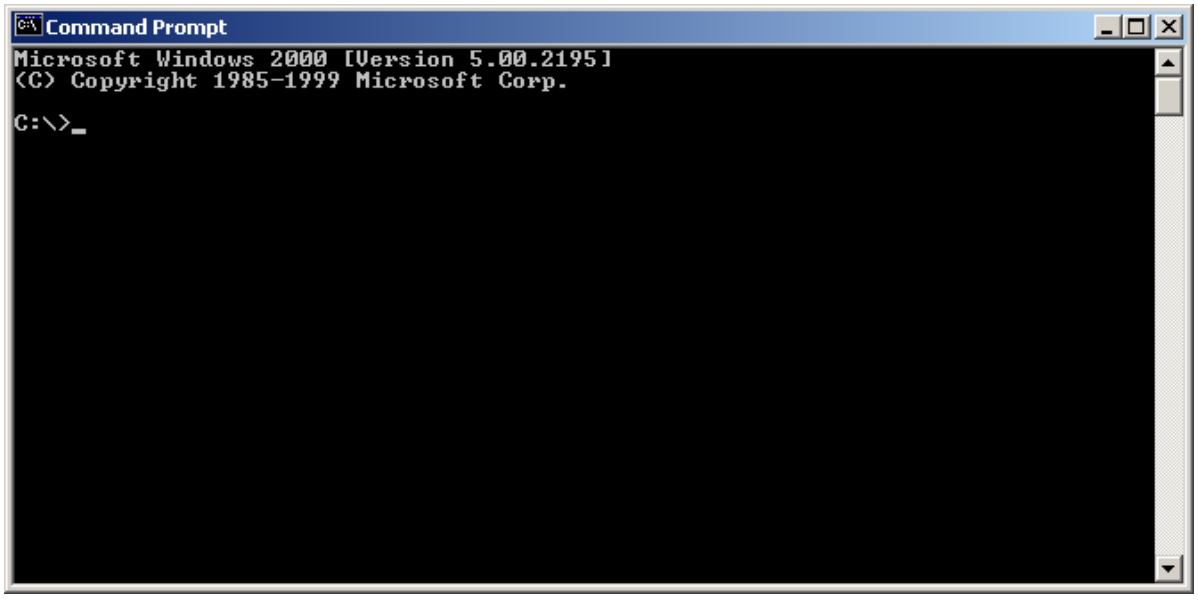


Parameters	Description
Reset	In the event that the system stops responding or stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the <APPLY> button. You will be asked to confirm your decision. The reset will be complete when the power LED stops blinking. Once the reset process is complete you may start using the router.

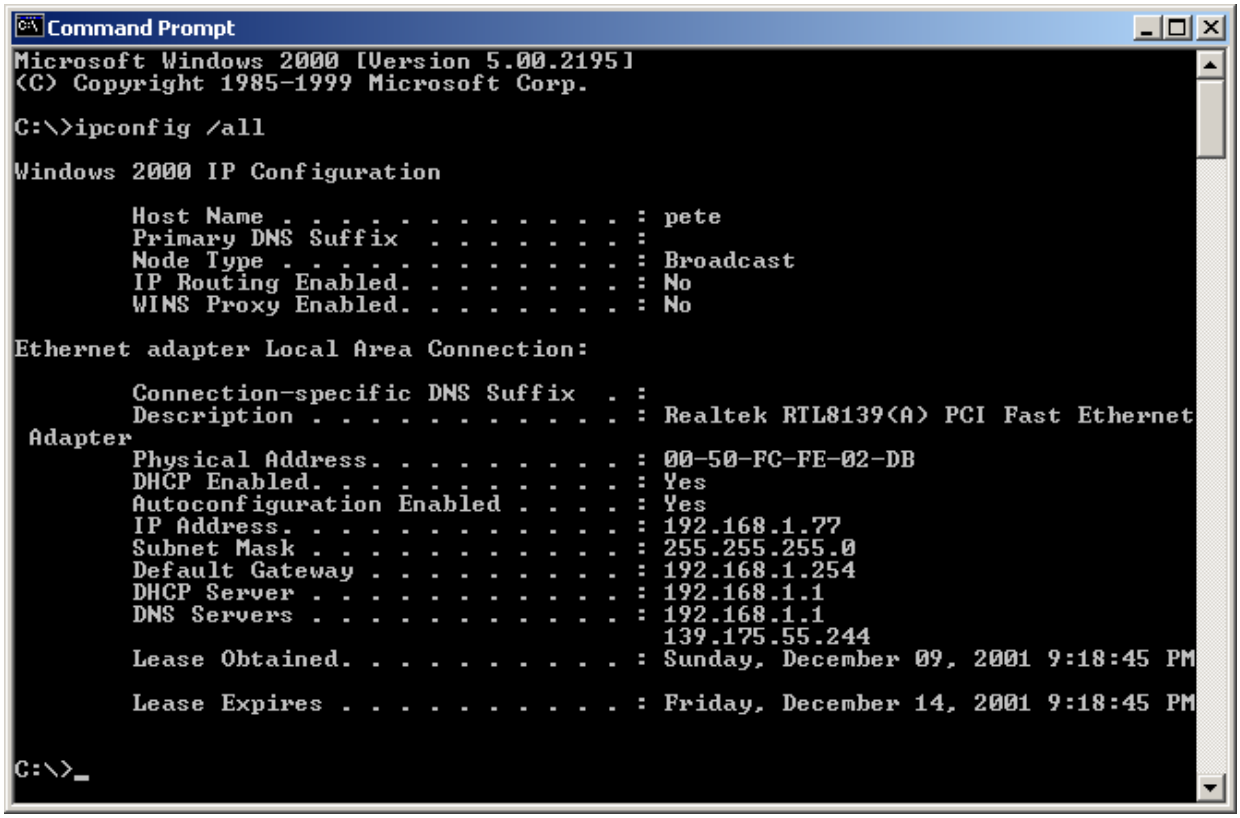
Appendix A

How to find your PC's IP and MAC address manually

1) In Window's open the Command Prompt program



2) Type Ipconfig /all and <enter>



- Your PC's IP address is the one titled as **IP address** (192.168.1.77 in this example)
- The router's IP address is the one titled as **Default Gateway** (192.168.1.254 in this example)
- Your PC's MAC Address is the one titled as **Physical Address** (00-50-FC-FE-02-DB in this example)

Glossary

Default Gateway (Router): Every non-router IP device needs a default gateway. When the device sends out an IP packet, if the destination is not in the same network, the device will send the packet to default gateway, which will then forward it to the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer in your network.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server will maintain a database of domain names and respective IP addresses, so when a domain name is requested (like typing "Broadbandrouter.com" in your Internet browser), the user will get the corresponding IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A kind of standard of computer networks. Ethernet networks are connected by special cables and hubs, and transfers data at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle timeout is designed so that after no traffic has been transferred to the Internet for a pre-configured amount of time, the connection will be disconnected automatically.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists four sets of numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading
1's followed by consecutive trailing 0's, such as

11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as “x” number of leading 1’s.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1’s in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,
11011001.10110000.10010000.00000111, and if its network mask is,
11111111.11111111.11110000.00000000
It means the device’s network address is
11011001.10110000.10010000.00000000, and its host ID is,
00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP listed below for explanations). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered as a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It comprises two parts: 3 bytes of data that corresponds to the Manufacturer ID (which is unique for each manufacturer), plus 3 bytes that are often used as the product’s serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband router’s NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to identify one network application/protocol from another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23

FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed between multiple parties so that when they communication with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Stands for Wide Area Network. A network that connects computers located in geographically separated areas (e.g. different buildings, cities,

countries). The Internet is a wide area network, too.

Web-based management Graphical User Interface (GUI): Many devices support graphical user interface that is based on the web browser. This means the user can use their familiar web browser (ex. Netscape or Microsoft Internet Explorer) to control/configure or monitor the device being managed.

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 complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.
Federal Communications Commission (FCC) RF Exposure Requirements
SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for Certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such a PDAs or lappads is not authorized.
This transmitter is restricted for use with the specific antenna tested in the application for Certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

EDIMAX

NETWORKING PEOPLE TOGETHER

EDIMAX Technology Co., Ltd.

www.edimax.com