



BR-6218Mg MIMO Wireless Broadband Router

User's Manual

Introduction	3
Features	3
Minimum Requirements	3
Package Content.....	3
Note.....	3
Get to know the Broadband Router	4
Back Panel	4
Front Panel.....	4
Setup Diagram	5
Getting started.....	6
Chapter 1	12
Quick Setup.....	12
Step 1) Time Zone.....	12
Step 2) WAN Settings	13
1.1 Dynamic IP	14
1.2 Static IP Address.....	15
1.3 PPPoE.....	15
1.4 PPTP	16
1.5 L2TP	18
Chapter 2	19
General Settings.....	19
2.1 System	20
2.1.1 Time Zone	20
2.1.2 Password Settings.....	21
2.1.3 Remote Management.....	22
2.2 WAN.....	23
2.2.1 Static IP	23
2.2.2 DHCP	23
2.2.3 PPPoE (PPP over Ethernet).....	23
2.2.4 PPTP	24
2.2.5 L2TP.....	24
2.2.6 DDNS	24
2.3 LAN	25
2.4 Wireless	26
2.4.1 Basic Settings.....	26
2.4.2 Advanced Settings	28
2.4.3 Security	30

2.4.3.1 WEP only.....	30
2.4.3.2 802.1x only	30
2.4.3.3 802.1x WEP Static key	31
2.4.3.4 WPA/WPA2 Pre-shared key	32
2.4.3.5 WPA/WPA2 Radius	33
2.4.4 Access Control	34
2.5 QoS	35
2.5.1 Port-based QoS.....	36
2.5.2 Rate Policing QoS	37
2.5.3 Guaranteed / Spare Class QoS.....	38
2.6 NAT	39
2.6.1 Virtual Server.....	40
2.6.2 Special Applications	41
2.6.3 ALG Settings	43
2.6.4 UPnP Settings.....	43
2.6.5 Static Routing	44
2.7 Firewall.....	45
2.7.1 Access Control List.....	46
2.7.2 URL Filter	48
2.7.3 Anti-DoS (Denial of Service).....	49
2.7.4 DMZ	50
Chapter 3	51
Status	51
3.1 Status and Information	52
3.2 Logs	52
3.2.1 System Log	52
3.2.2 ACL Log	53
3.2.3 URL Filter Log	53
3.2.4 DoS Log	53
3.2.5 New Connection Log	53
Chapter 4	54
Tool	54
Appendix A.....	55
Glossary	56

Introduction

Congratulations on purchasing this Wireless Broadband Router. This Wireless Broadband Router is a cost-effective IP Sharing Router that enables multiple users to share the Internet through an ADSL or cable modem. Simply configure your Internet connection settings in the Wireless Broadband Router and plug your PC to the LAN port and you're ready to share files and access the Internet. As your network grows, you can connect another hub or switch to the router's LAN ports, allowing you to easily expand your network. The Wireless Broadband Router is embedded with a IEEE 802.11g/b MIMO access point that allows you to build up a wireless LAN. The Wireless Broadband Router provides a total solution for the Small and Medium-sized Business (SMB) and the Small Office/Home Office (SOHO) markets, giving you an instant network today, and the flexibility to handle tomorrow's expansion and speed.

Features

- High Internet Access throughput (up to 100M)
- Allow multiple users to share a single Internet line
- Supports up to 253 users
- Internet Access via Cable or xDSL modem
- Access Private LAN Servers from the Public Network
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11g/b MIMO wireless LAN access point
- Support DHCP (Server/Client) for easy setup
- Support advance features such as: Special Applications, DMZ, Virtual Servers, 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 purposes
- 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)
- PCs with a Web-Browser (Internet Explorer 4.0 or higher, or Netscape Navigator 4.7 or higher)

Package Content

- One MIMO Broadband router unit
- One Quick Installation Guide
- One User Manual CD
- One Power Adapter
- 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 time used.

Get to know the Broadband Router

Back Panel

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

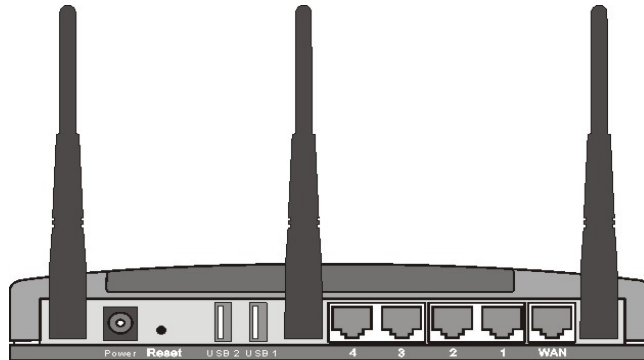


Figure 1.0

1) Local Area Network (LAN)

The Broadband router's 4 LAN ports are where you connect your LAN's PCs, printer servers, hubs and switches etc.

2) Wide Area Network (WAN)

The WAN port is the segment connected to your xDSL or Cable modem and is linked to the Internet.

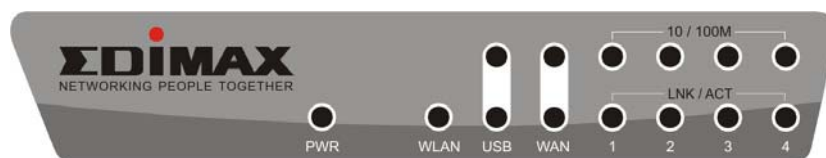
3) Reset

The Reset button allows you to do one of two things.

- 1) If problems occur with your router, press the router's reset button with a pencil tip (for less than 5 seconds) and the router will re-boot itself, keeping your original configurations.
- 2) If problems persist or you experience extreme problems or you forgot your password, press the reset button for longer than 5 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 LED lights that inform you of the router's current status. Below is an explanation of each LED and its description.



LED	Light Status	Description
PWR	ON	Router's power supply is on
WAN 10/100M	ON	WAN port 100Mbps is connected
	Off	WAN port 10Mbps is connected
WAN LNK/ACT	ON	WAN is connected
	Off	No WAN connection
	Flashing	WAN port is Activity (ACT)
LAN 10/100M (Port 1-4)	ON	LAN port 100Mbps is connected
	Off	LAN port 10Mbps is connected
LAN LNK/ACT (Port 1-4)	ON	LAN is connected
	Off	No LAN connection
	Flashing	LAN port is Activity (ACT)
WLAN-G	ON	Wireless LAN has been activated
	Off	Wireless LAN is disabled
	Flashing	Wireless LAN is Activity (ACT)

Setup Diagram

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

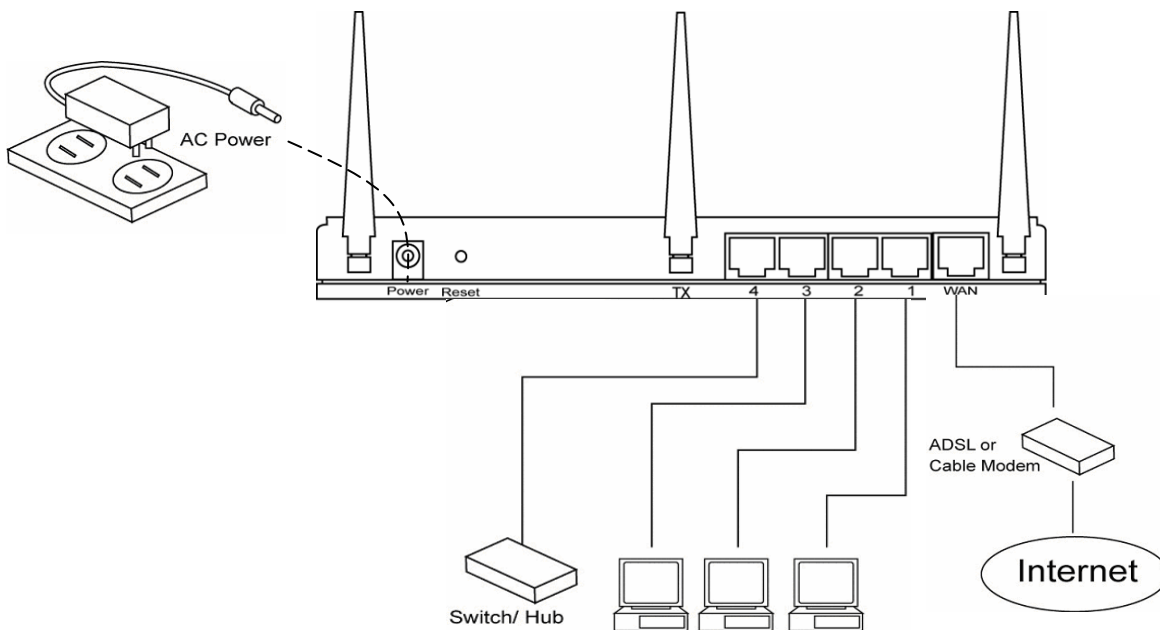


Figure 1.2

Getting started

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

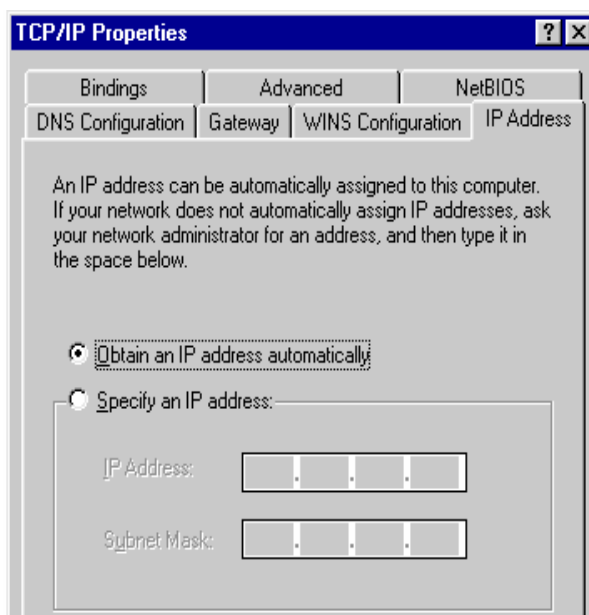
- 1) Setup your network as shown in the setup diagram above (fig 1.2).
- 2) You then need to set your LAN PC clients so that it can obtain an IP address automatically. All LAN clients require an IP address. Just like an address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP automatically then proceed to step 3, page 11)

Configure your PC to obtain an IP address automatically

By default the broadband router's DHCP is on, 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 now. If TCP/IP is installed, go 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 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*.



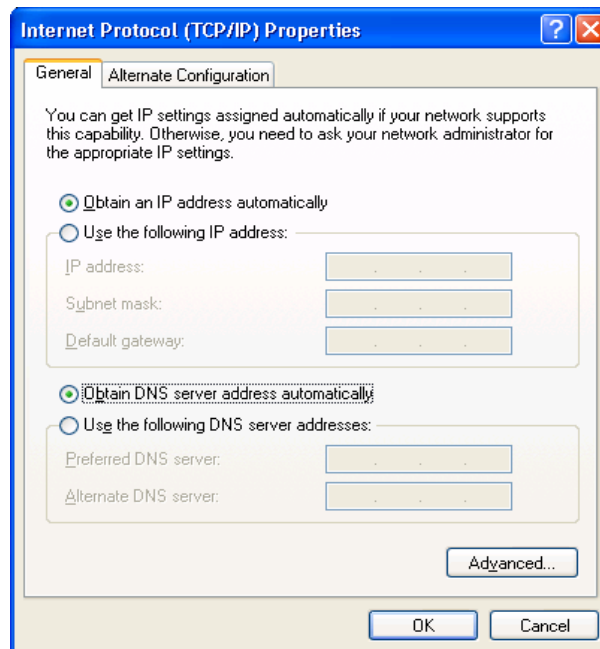
8: Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available 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.



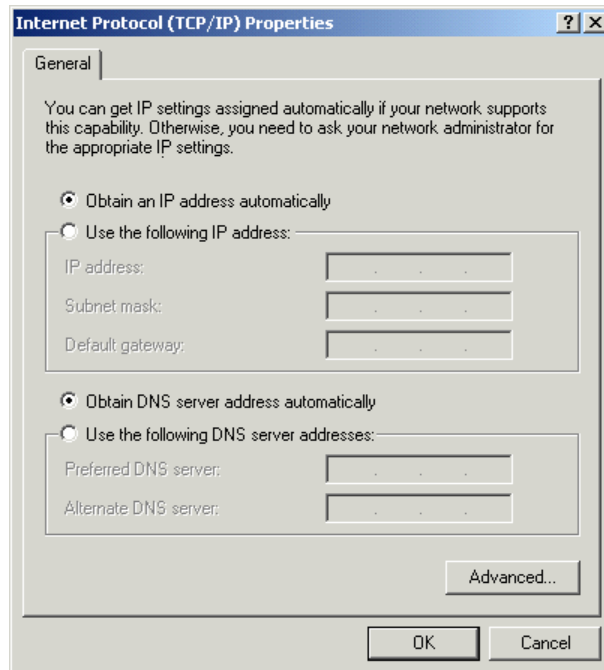
5: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available 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.



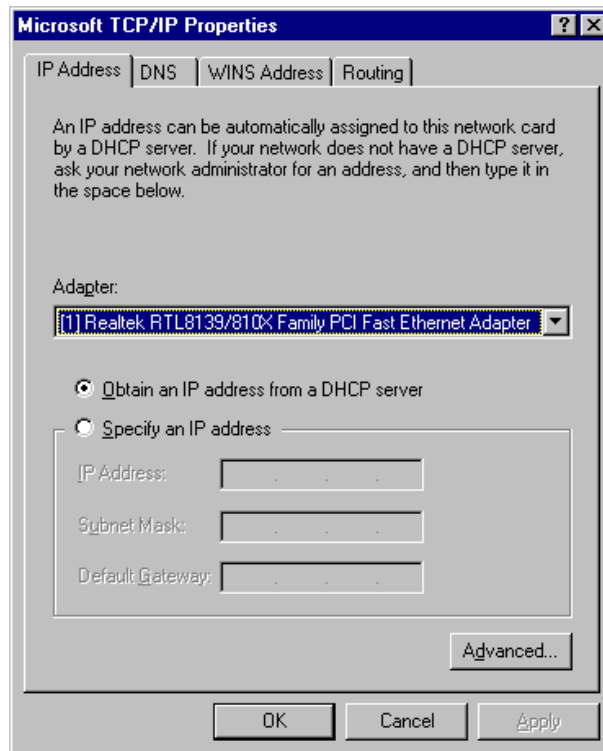
- 6: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available 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:** Let all fields are blank.
 - **WINS:** Let all fields are blank.
 - **Routing:** Let all fields are blank.



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

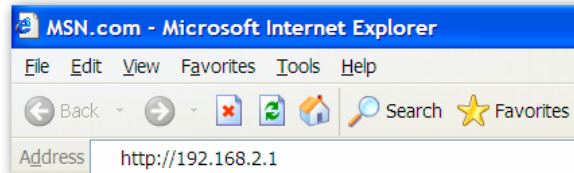
Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

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 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 available 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>

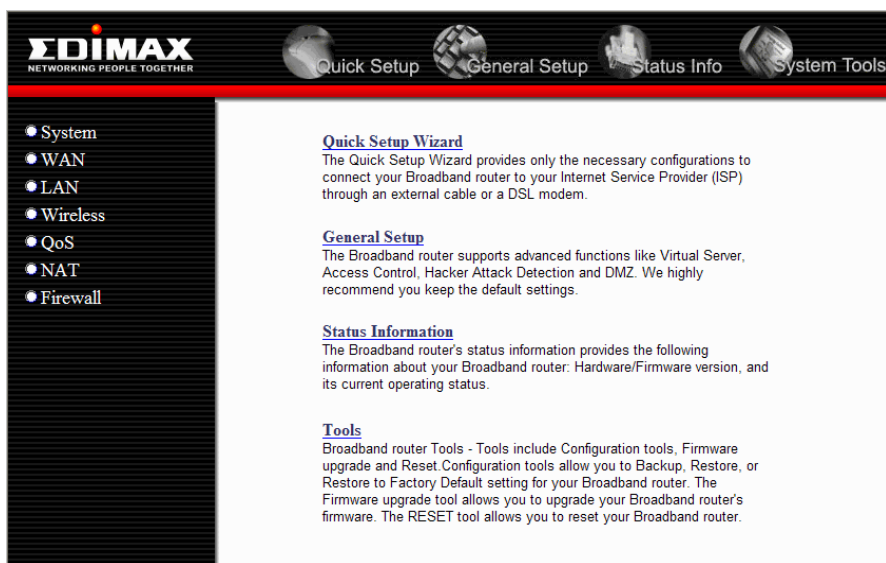


- 5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

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 Information** and **Tools**.



Menu	Description
Quick Setup Wizard <i>(Chapter 1)</i>	Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).
General Setup <i>(Chapter 2)</i>	This section contains configurations for the Broadband router's advance functions such as: Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements.
Status Information <i>(Chapter 3)</i>	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 <i>(Chapter 4)</i>	This section contains the broadband router's Tools - Tools include Configuration tools, 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 advance features/information.

Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter. Use the selections on the web management's top right hand page (see below) to navigate around the web-based management User Interface.

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.

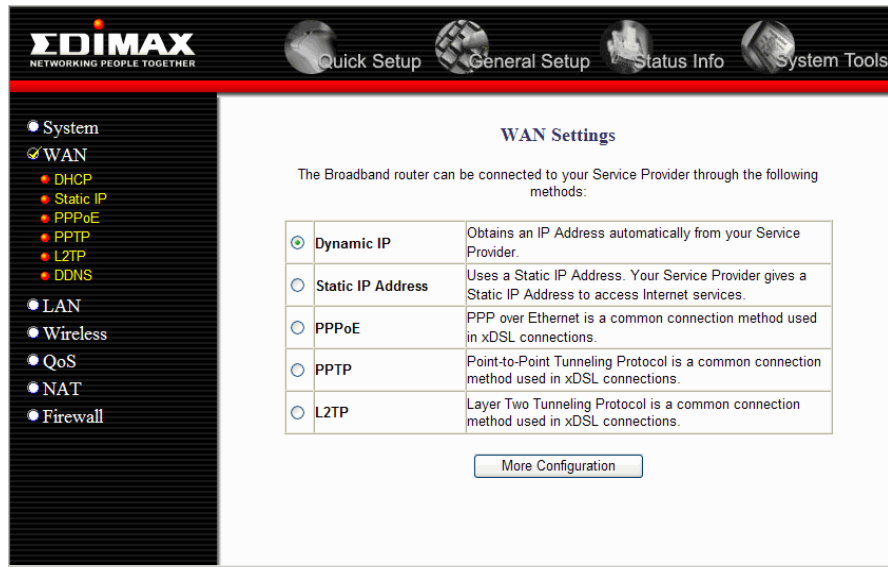
Parameter	Description
Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
NTP Server #	You can manually assign three time server addresses here.
Time	Here shows the time of current router setting.

Click on **NEXT** to proceed to the next page (step 2) WAN Settings.

Step 2) WAN Settings

In this section you have to select one of four 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.



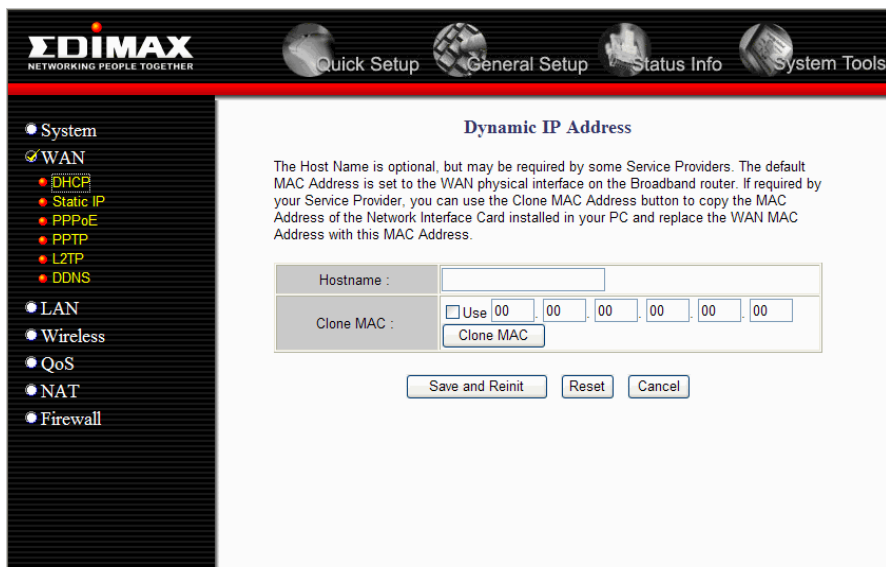
Parameter	Description
Dynamic IP	Your ISP will automatically give you an IP address
Static IP Address	Your ISP has given you an IP address already
PPPoE	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP	Your ISP requires you to use a Layer Two Tunneling Protocol (L2TP) connection.

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 Dynamic IP

Choose Dynamic IP if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as MAC address (see screen below).

Note: The MAC address section is optional and you can skip this section if your ISP does not require these settings for you to connect to the Internet.



Parameter	Description
Clone MAC	Your ISP may require a particular MAC address in order for you 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 Static IP Address

Select Static IP Address 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.

The screenshot shows the EDIMAX router configuration interface. The top navigation bar includes 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar lists various configuration options: System, WAN (selected), DHCP, Static IP, PPPoE, PPTP, L2TP, DDNS, LAN, Wireless, QoS, NAT, and Firewall. The main content area is titled 'Static IP Address' and contains the following text: 'If your Service Provider has assigned a Fixed IP address; enter the assigned IP Address, Subnet Mask and the Gateway IP Address provided.' Below this text is a form with four rows of input fields:

IP Address :	172	20	1	254
Subnet Mask :	255	255	255	0
Default Gateway :	172	20	1	250
DNS :	168	95	1	1

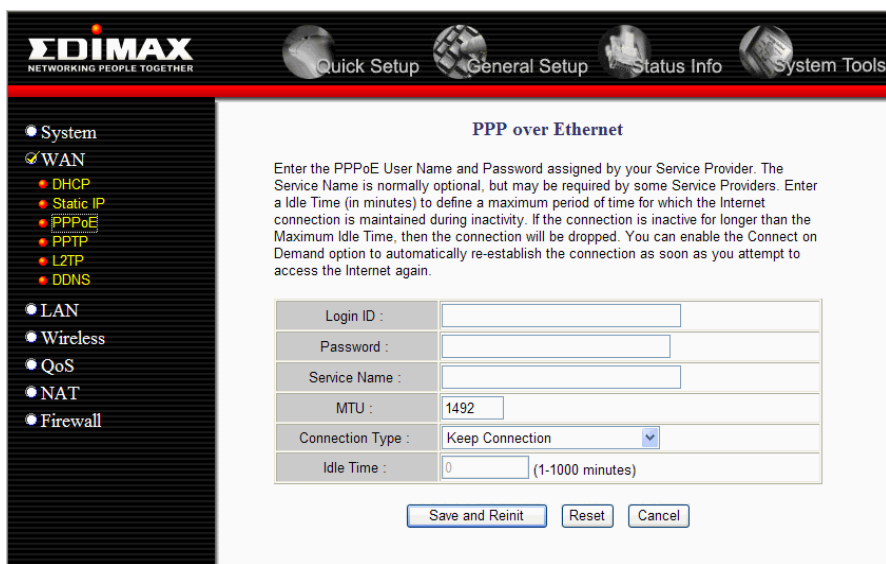
At the bottom of the form are three buttons: 'Save and Reinit', 'Reset', and 'Cancel'.

Parameter	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)
Default Gateway	This is the ISP's IP address gateway
DNS	This is the ISP's DNS server IP address

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, 4.

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.

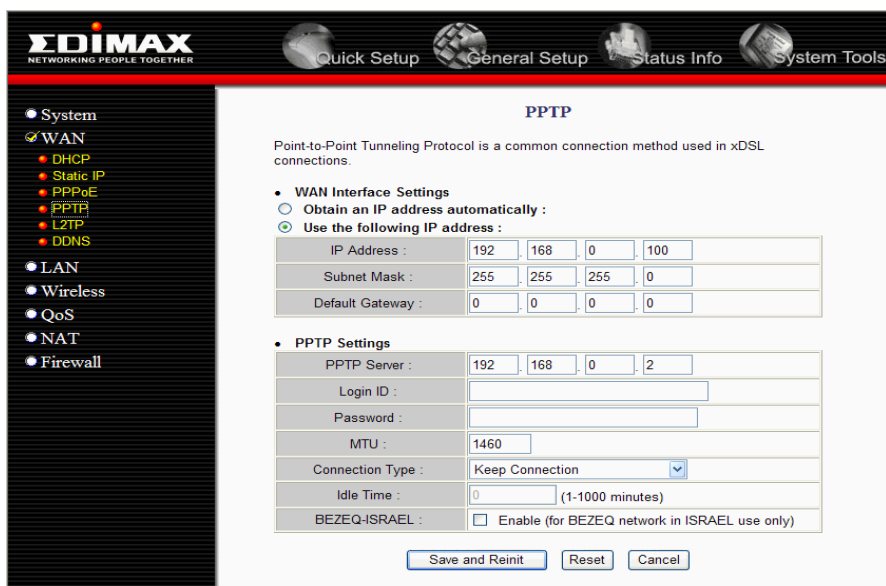


Parameter	Description
Login ID	Enter the Login ID provided by your ISP for the PPPoE connection
Password	Enter the Password provided by your ISP for the PPPoE connection
Service Name	This is optional. Enter the Service name should your ISP requires it, otherwise leave it blank.
AC Name	This is optional. Enter the AC Name should 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 a maximum packet size.
Dial On Demand	If checked, gateway won't dial this session until received a packet that requested Internet access. If unchecked, gateway dials this session immediately after system powered up.
Silent Timeout	If specified a non-zero value, gateway disconnects this session after specified idle time.
Auto Reconnect	If checked, gateway redials this session if session previously terminated by ISP.
Auth Type	Select PAP or CHAP for the authentication type requested by your ISP.

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 give you a static IP to be used to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given 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 Gateway
PPTP Server	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above
Login 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
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 a maximum packet size.
Silent Timeout	If specified a non-zero value, gateway disconnects this session after specified idle time.
Dial On Demand	If checked, gateway won't dial this session until received a packet that requested Internet access. If unchecked, gateway dials this session immediately after system powered up.
Auto Reconnect	If checked, gateway redials this session if session previously terminated by ISP.
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Auth Type	Select PAP or CHAP for the authentication type requested by your ISP.

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.
Use the following IP address	The ISP gives 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
L2TP Server	If your LAN has a L2TP Server, then enter that L2TP Server IP address here. If you do not have a L2TP Server then enter the ISP's Gateway IP address above
Login 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
MTU	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size.
Silent Timeout	If specified a non-zero value, gateway disconnects this session after specified idle time.
Dial On Demand	If checked, gateway won't dial this session until received a packet that requested Internet access. If unchecked, gateway dials this session immediately after system powered up.
Auto Reconnect	If checked, gateway redials this session if session previously terminated by ISP.
Auth Type	Select PAP or CHAP for the authentication type requested by your ISP.

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.

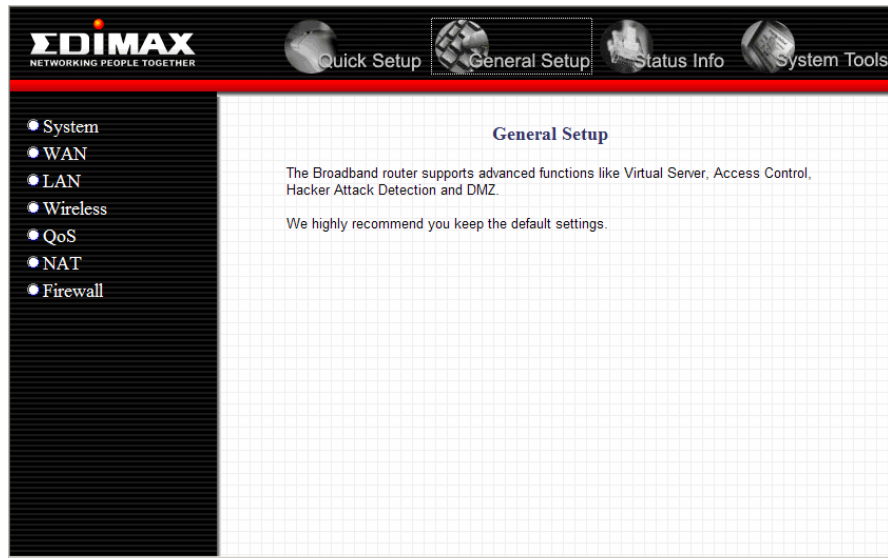
Chapter 2

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.



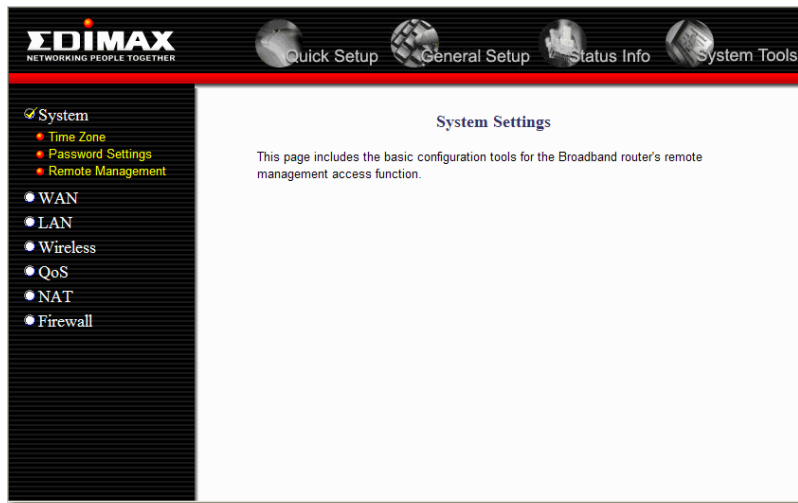
Below is a general description of what advance functions are available for this broadband router.

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	You can 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.

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.

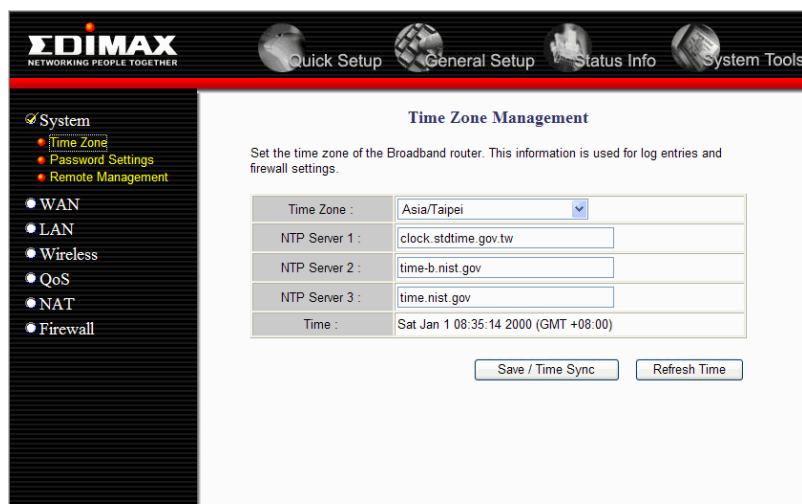


Parameter	Description
<i>System Settings</i>	
Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Password Settings	Allows you to select a password in order to access the web-based management website.
Remote Management	You can specify 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.

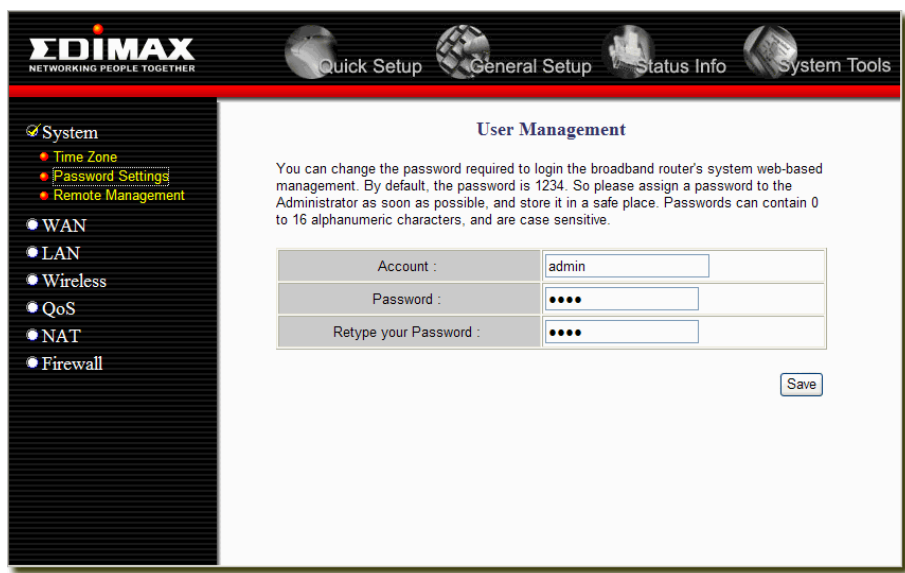


Parameter	Description
Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
NTP Server #	You can manually assign three time server addresses here.
Time	Here shows the time of current router setting.

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

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.

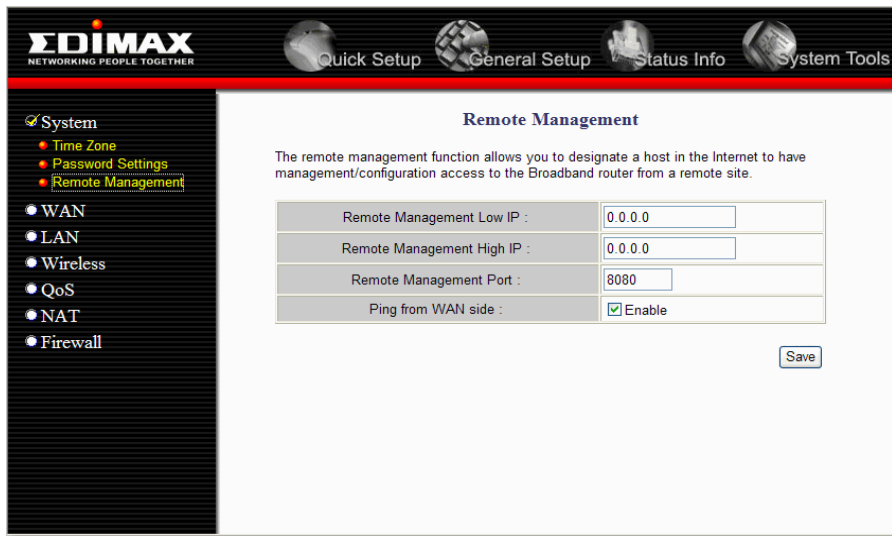


Parameter	Description
Account	Enter your account name to login to your Broadband router.
Password	Enter your password
Confirmed Password	Enter your password again for verification purposes Note: If you forget your password, you'll have to reset the router to the factory default (password is 1234) with the reset button (see router's back panel)

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

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.

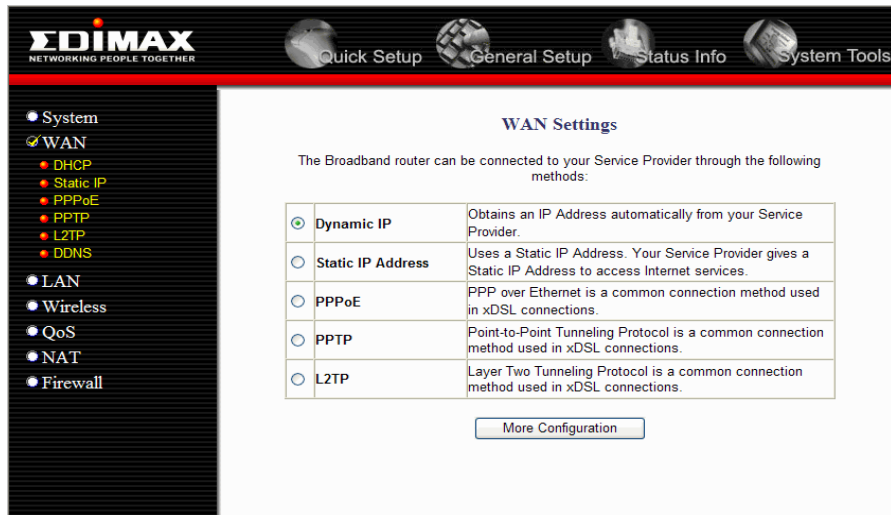


Parameter	Description
IP Address	Please specify the IP range to the Remote Management IP fields. All the Internet IPs that inside this range can manage this router from WAN side.
Port	To avoid conflict of virtual server at port 80, user can specify a different port in Remote Management Port for WAN side access.
Ping from WAN side	Ping from WAN side is turned on by default and could be turned off if the Enable checkbox is unchecked.

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

2.2 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** and **DDNS**.



Parameter	Description
Static IP	Your ISP has given you an IP address already
DHCP	Your ISP will automatically give you an IP address
PPPoE	Your ISP requires PPPoE connection.
PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP	Your ISP requires L2TP connection.
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

2.2.1 Static IP

Select Static IP address 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. (See chapter 1 "Static IP Address" for more detail)

2.2.2 DHCP

Choose the DHCP selection if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as MAC address (see chapter 1 "Dynamic IP" for more detail)

2.2.3 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)

2.2.4 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)

2.2.5 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. (See chapter 1 “L2TP” for more detail)

2.2.6 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.

The screenshot shows the DDNS configuration interface. At the top, there's a navigation bar with 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar lists various settings: System, WAN (selected), DHCP, Static IP, PPPoE, PPTP, L2TP, DDNS, LAN, Wireless, QoS, NAT, and Firewall. The main area is titled 'DDNS' and contains the following text: 'DDNS allows users to map the static domain name to a dynamic IP address. You must get a account, password and your static domain name from the DDNS service providers. Our products have DDNS support for www.dyndns.org and www.tzo.com now.' Below this is a form with four fields: 'Service Type' (a dropdown menu currently showing 'Disable'), 'Username', 'Password', and 'Hostname'. An 'Apply' button is located at the bottom right of the form.

Parameter	Description
Service Type	Select a DDNS service provider or select Disabled to disable DDNS function.
Username	The account that your DDNS service provider assigned to you
Password	The password you set for the DDNS service account above
Host Name	Your static domain name that use DDNS

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

2.3 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.

EDIMAX
NETWORKING PEOPLE TOGETHER

Quick Setup | General Setup | Status Info | System Tools

System
WAN
LAN
Wireless
QoS
NAT
Firewall

LAN Settings

You can enable the Broadband router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

IP Address :	192	.	168	.	2	.	1
Subnet Mask :	255	.	255	.	255	.	0
DHCP Server Status :	<input checked="" type="checkbox"/> Enable						
Start IP :	192	.	168	.	2	.	100
End IP :	192	.	168	.	2	.	199
1st WINS Server :	0	.	0	.	0	.	0
2nd WINS Server :	0	.	0	.	0	.	0
Provide Real DNS Server :	<input type="checkbox"/>						
Domain From Upper DHCP :	<input checked="" type="checkbox"/>						

Static DHCP leases

No.	Hardware Address				Assigned IP Address			
1	00	:00	:00	:00	000	:000	:000	:000
2	00	:00	:00	:00	000	:000	:000	:000
3	00	:00	:00	:00	000	:000	:000	:000
4	00	:00	:00	:00	000	:000	:000	:000
5	00	:00	:00	:00	000	:000	:000	:000
6	00	:00	:00	:00	000	:000	:000	:000
7	00	:00	:00	:00	000	:000	:000	:000
8	00	:00	:00	:00	000	:000	:000	:000

Save Reset

Dynamic DHCP Client List

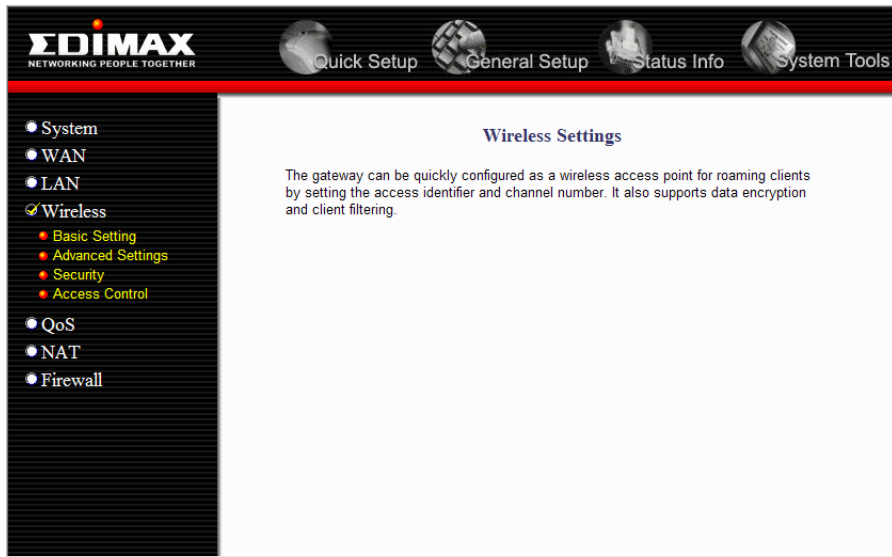
Hardware Address	Assigned IP	Hostname
00:13:D4:8F:AC:53	192.168.2.100	Joe

Parameter	Description
IP address	This is the router's LAN port IP address (Your LAN clients default gateway IP address)
IP Subnet Mask	Specify a Subnet Mask for your LAN segment
DHCP Server Status	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
IP Address Pool	You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.
WINS Server	You can specify the WINS server to assign to DHCP clients.
Provide Real DNS Server	When check this box, DHCP server will provide WAN DNS server to DHCP clients. Otherwise, DHCP server will provide itself as the DNS server.
Domain from upper DHCP	Enable this to assign the domain name from WAN connection.
Static DHCP leases	Static DHCP leases is for user to statically associate an IP address to a specific MAC address.
Dynamic DHCP Client List	Dynamic DHCP Client List shows all IP addresses already assigned and the corresponding LAN PC hostname and their MAC addresses.

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

2.4 Wireless

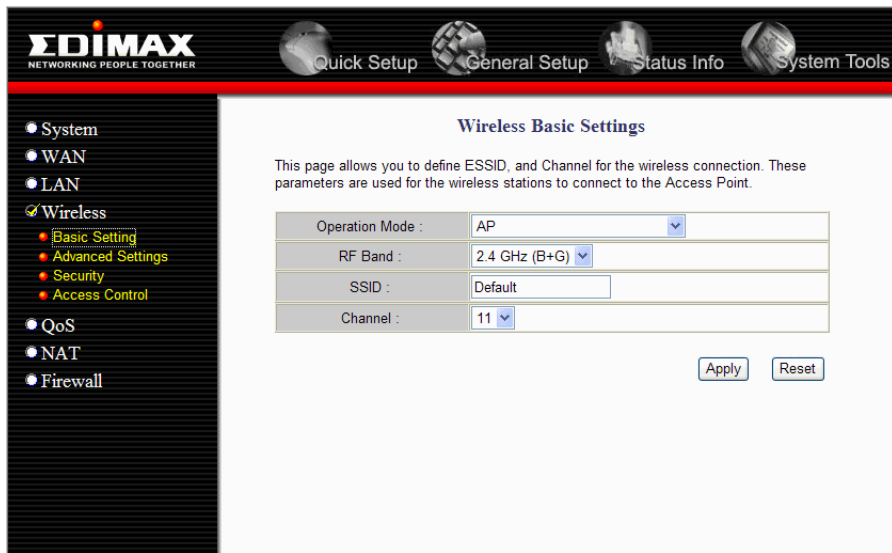
Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to your Intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.



2.4.1 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.

AP Mode setting Page



AP Bridge-Point to Point mode setting page

The screenshot shows the EDIMAX web interface for configuring wireless settings. The top navigation bar includes 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar lists various configuration categories: System, WAN, LAN, Wireless (selected), QoS, NAT, and Firewall. Under 'Wireless', sub-options include Basic Setting (selected), Advanced Settings, Security, and Access Control. The main content area is titled 'Wireless Basic Settings' and contains a descriptive paragraph: 'This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.' Below this is a form with the following fields: 'Operation Mode' (dropdown menu set to 'AP Bridge-Point to Point'), 'RF Band' (dropdown menu set to '2.4 GHz (B+G)'), 'Channel' (dropdown menu set to '11'), 'MAC Address 1' (text input field with '00 00 00 00 00 00'), and 'Set Security' (button labeled 'Set Security'). At the bottom right of the form are 'Apply' and 'Reset' buttons.

AP Bridge-Point to Multi-Point mode setting page

The screenshot shows the EDIMAX web interface for configuring wireless settings. The top navigation bar includes 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar lists various configuration categories: System, WAN, LAN, Wireless (selected), QoS, NAT, and Firewall. Under 'Wireless', sub-options include Basic Setting (selected), Advanced Settings, Security, and Access Control. The main content area is titled 'Wireless Basic Settings' and contains a descriptive paragraph: 'This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.' Below this is a form with the following fields: 'Operation Mode' (dropdown menu set to 'AP Bridge-Point to Multi-Point'), 'RF Band' (dropdown menu set to '2.4 GHz (B+G)'), 'Channel' (dropdown menu set to '11'), 'MAC Address 1' (text input field with '00 00 00 00 00 00'), 'MAC Address 2' (text input field with '00 00 00 00 00 00'), 'MAC Address 3' (text input field with '00 00 00 00 00 00'), 'MAC Address 4' (text input field with '00 00 00 00 00 00'), and 'Set Security' (button labeled 'Set Security'). At the bottom right of the form are 'Apply' and 'Reset' buttons.

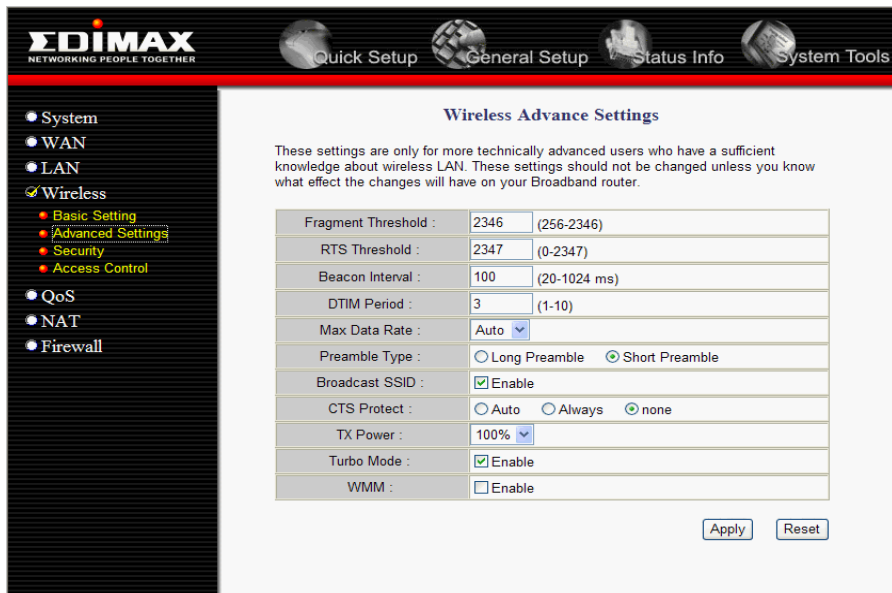
AP Bridge-WDS mode setting page

Parameter	Description
Operation Mode	It allows you to set the AP to AP, Bridge or WDS mode.
RF Band	It allows you to set the AP fix at 802.11b or 802.11g mode. You also can select B+G mode to allow the AP select 802.11b and 802.11g connection automatically.
SSID	This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.
Channel Number	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
MAC address	If you want to bridge more than one networks together with wireless LAN, 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 that join the bridging work.
Set Security	Click the "Set Security" button, then a "WDS Security Settings" will pop up. You can set the security parameters used to bridge access points together here when your AP is in AP Bridge modes. You can refer to section 4.3 "Security Settings" for how to set the parameters.

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

2.4.2 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 You should not change these parameters unless you know what effect the changes will have on this router.



Parameter	Description
Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this wireless router 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 still on the AP awaiting pickup.
Max Data Rate	The "Data Rate" is the rate this access point uses 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 can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast ESSID" can provide better security.
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 should be transmitted.
Tx Power	You can adjust the wireless transmit power here. By reduce the tx power can let the wireless signal only cover your working area.
Turbo Mode	By enable the turbo mode 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 above configurations. You can now configure other advance sections or start using the router.

2.4.3 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.

2.4.3.1 WEP only

When you select 64-bit or 128-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



Parameter	Description
Method	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 throughput will be lower.
Authentication	When using shared key, user must input 10 hexadecimal digits for WEP64 and 26 digits for WEP128. All the four WEP keys are set identical.
Key	The WEP keys are used to encrypt data transmitted in 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) as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) as the encryption keys.

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

2.4.3.2 802.1x 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.

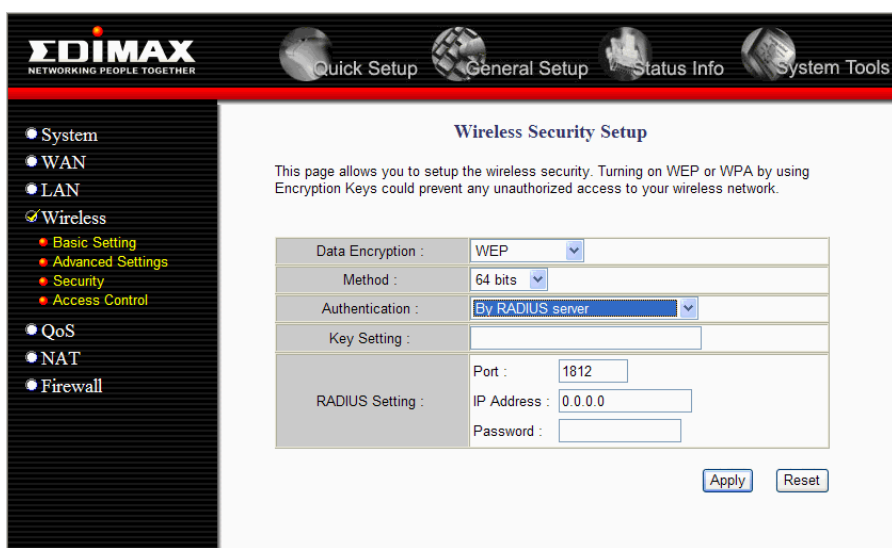


Parameter	Description
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

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

2.4.3.3 802.1x WEP Static key

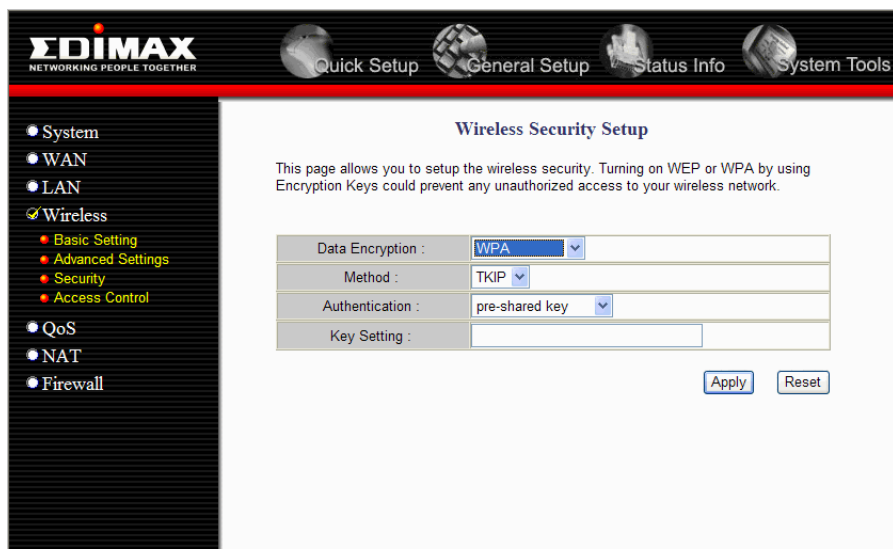
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.



For the 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".

2.4.3.4 WPA/WPA2 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 is not easy to be broken by hackers. This can improve security very much.



Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
Key Setting	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. At least 8 characters pass phrase as the pre-shared keys.

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

2.4.3.5 WPA/WPA2 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. This can improve security very much.

The screenshot shows the EDIMAX Wireless Security Setup page. The navigation menu on the left includes System, WAN, LAN, Wireless (selected), QoS, NAT, and Firewall. The main content area is titled 'Wireless Security Setup' and contains the following form fields:

- Data Encryption : WPA
- Method : TKIP
- Authentication : By RADIUS server
- RADIUS Setting :
 - Port : 1812
 - IP Address : 0.0.0.0
 - Password :

Buttons for 'Apply' and 'Reset' are located at the bottom right of the form.

Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
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 above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

2.4.4 Access Control

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



Parameter	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 "Apply". Then this wireless station will be added into the Access Control List. If you find any issues before adding it and want to retype again. Just click "Reset" 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 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, just click "Delete All" button. Click "Reset" will clear your current selections.

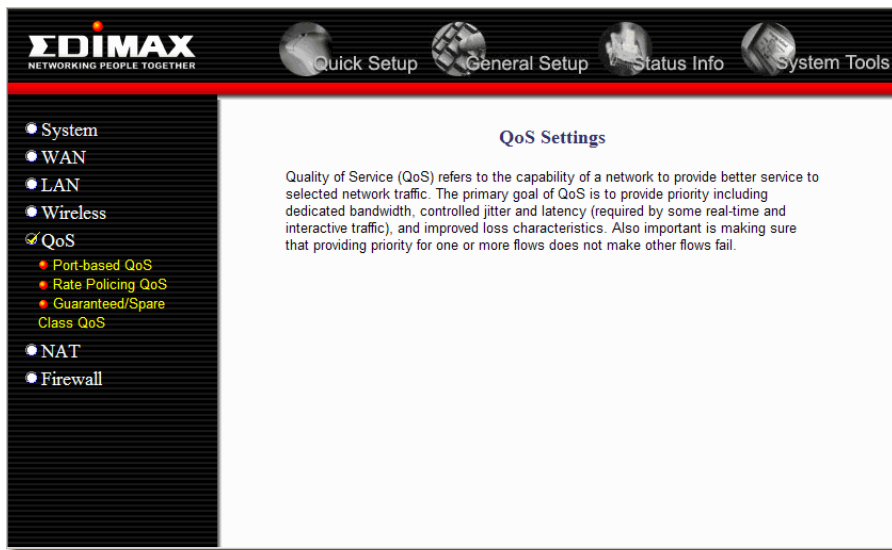
Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

2.5 QoS

This router supports various types of QoS – Port-based QoS, Rate Policing QoS, and Guaranteed/Spare Class QoS.

For Port based QoS, user can specify the High/Low queue priority for each Ethernet port and can apply total rate limit to any port from 128Kbps to 32Mbps or at Full-rate(100Mbps). Flow control can also be enabled/disabled on per-port basis.

For Application based QoS, user can specify a destination port number and associate it with a egress priority(High or Low). For example, in Fig 35, if user config port 7297 with high priority, then user would experience better service quality for such flows.



Parameter	Description
Port-based QoS	User can differentiate packet priority by L4 port number or by physical Ethernet port number.
Rate Policing QoS	User can specify a L3/4 criterion and associate it with a maximum token (packet rate or data rate based).
Guaranteed/Spare Class QoS	Your ISP requires PPPoE connection.

2.5.1 Port-based QoS

For Application based QoS, user can specify a destination port number and associate it with a egress priority(High or Low). For example, if user config port 7297 with high priority, then user would experience better service quality for such flows.

For Port based QoS, user can specify the High/Low queue priority for each Ethernet port and can apply total rate limit to any port from 128Kbps to 32Mbps or at Full-rate(100Mbps). Flow control can also be enabled/disabled on per-port basis.

Port-based QoS

Enable Hardware QoS by Application

Protocol	High Priority	Low Priority
TELNET	<input type="radio"/>	<input type="radio"/>
HTTP	<input type="radio"/>	<input type="radio"/>
POP3	<input type="radio"/>	<input type="radio"/>
SMTP	<input type="radio"/>	<input type="radio"/>

Enable Hardware QoS by device port number

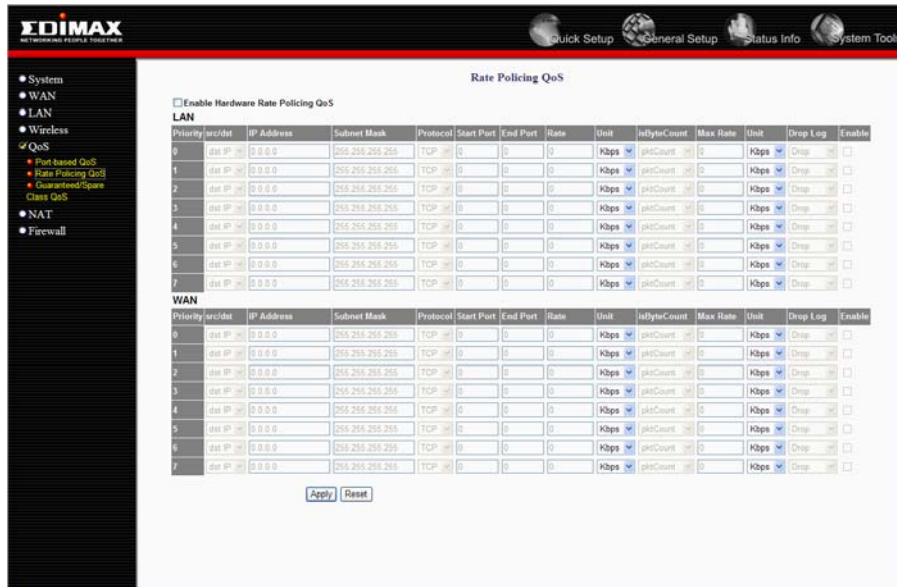
Port #	Flow Control	Incoming Rate Limit	Outgoing Rate Limit	Port-Based Priority
LAN 4	Disable	Full	Full	Low
LAN 3	Disable	Full	Full	Low
LAN 2	Disable	Full	Full	Low
LAN 1	Disable	Full	Full	Low
WAN	Disable	Full	Full	Low

Parameter	Description
Enable QoS by Application	Enable application-based QoS.
Protocol/Specific Port#	Set the priority of the specified protocol name or port number to higher or lower priority.
Enable QoS by device port	Enable Port-based QoS.

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

2.5.2 Rate Policing QoS

This router supports Rate Policing QoS. User can specify a L3/4 criterion and associate it with a maximum token (packet rate or data rate based). If a packet arrives and it matches to a rate policing entry, router decreases entry's allocated token by one (if pps based) or by packet length in bytes(if bps based). If unfortunately the packet just run out of allocated tokens, then it would be dropped directly or logged to software, depends on the setting of Drop Log field.



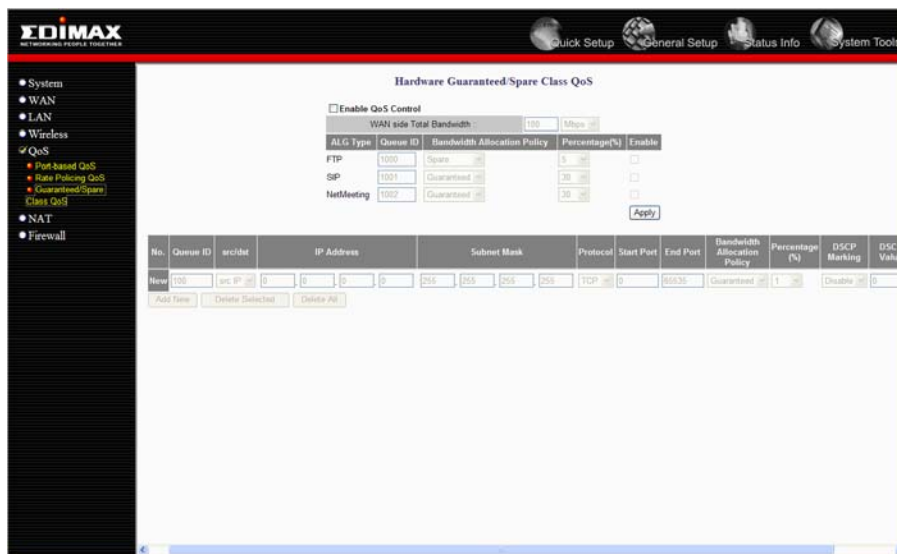
Parameter	Description
Src/dst	If you want to monitor the source IP of the packets, please select src IP. Otherwise, please select dst IP.
IP Address	Specify the IP Address that you want to limit the transmit/receive rate.
IP Mask	If you want to limit a subnet, you can specify the subnet mask here.
Protocol	Specify the protocol you want to monitor, it can be TCP / UDP / or IP only.
Start / End Port	Specify the port ranges that you want to monitor. To classify all TCP or UDP packets within same IP address / mask (regardless of port number) as same rate policy, set 0 to both Start Port and End Port.
Rate / Unit / isByteCount	Specify the rate, unit, and the type of the limitation.
Drop Log	Select the behavior when the flow is over limitation. You can just drop the packets or drop packet and log it.

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

2.5.3 Guaranteed / Spare Class QoS

User can first specify maximum WAN total bandwidth and then set bandwidth allocation rules according to two different classes: Guaranteed or Spared. Rules in Guaranteed class are guaranteed to have specified percentage of WAN Total bandwidth. At any period of time, if the aggregated bandwidth used by flows in guaranteed class doesn't exceed total bandwidth, the spared bandwidth is then available for allocating to the flows in Spared class, according to the percentage configured.

For example, 192.168.1.1 is guaranteed to have 50Mbps bandwidth if it needs and 192.168.1.2 has 25Mbps guaranteed on demand. If for a period of time, the aggregated bandwidth used by both hosts is 40Mbps , so only 40% WAN bandwidth is consumed by Guaranteed class flows, then all other hosts in 192.168.1.0 can compete to use the spared 60Mbps WAN bandwidth. If there exists another LAN on gateway, say, 192.168.2.0/24, then they can only use the rested bandwidth consumed by guaranteed and spared class.

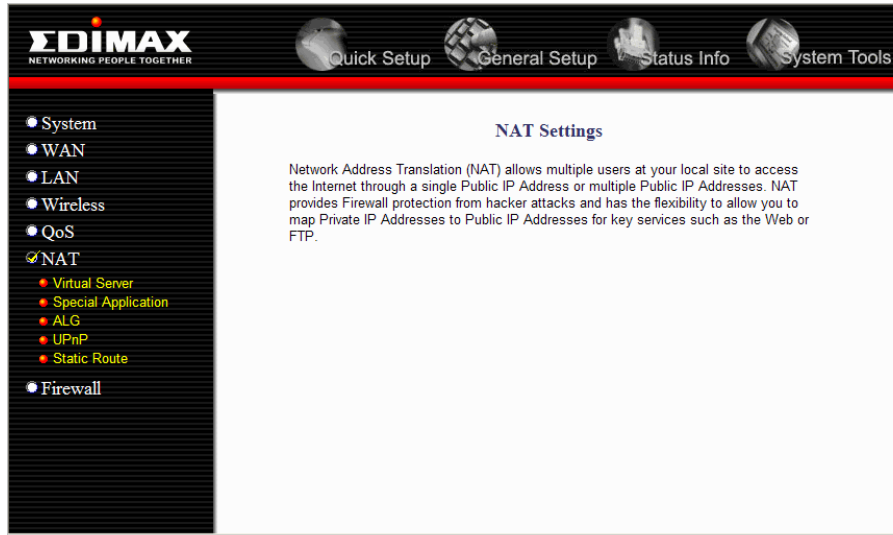


Parameter	Description
Queue ID	The Queue (Group) ID groups all the connections with the same Queue ID into one rule and these connections share the same bandwidth in this rule.
Src/Dst	If you want to monitor the source IP of the packets, please select src IP. Otherwise, please select dst IP.
IP Address	Specify the IP Address that you want to limit the transmit/receive rate.
IP Mask	If you want to limit a subnet, you can specify the subnet mask here.
Protocol	Specify the protocol you want to monitor, it can be TCP / UDP / or IP only.
Start / End Port	Specify the port ranges that you want to monitor. To classify all TCP or UDP packets within same IP address / mask (regardless of port number) as same rate policy, set 0 to both Start Port and End Port.
Bandwidth allocation policy	Guaranteed or Spare.
Percentage	Input the percentage of total bandwidth that this queue have.
DSCP Marking	Differentiated Services Code Point is a model in which traffic is treated by intermediate systems with relative priorities based on the type of services. If you want to mark this Queue to specified DSCP type, enable this option and filled a value in the DSCP value field.

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

2.6 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.

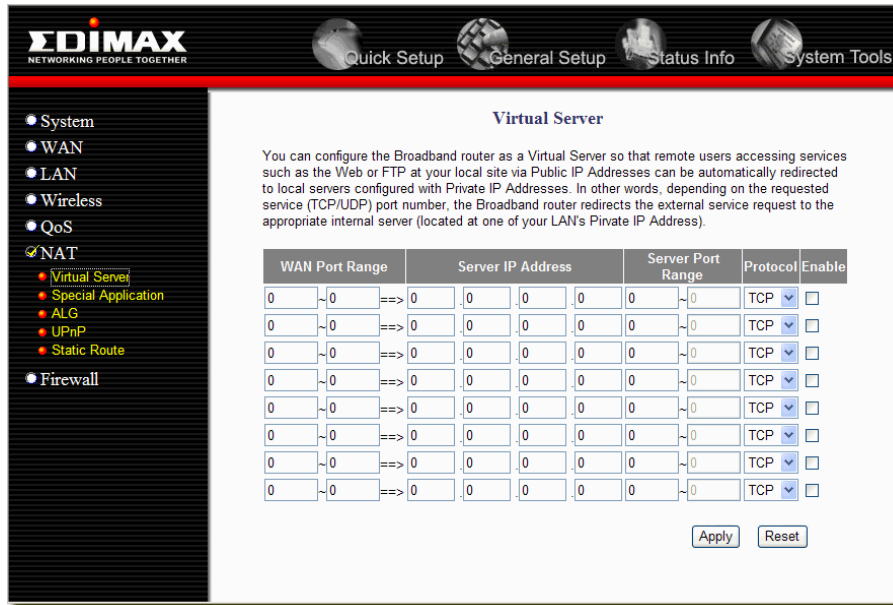


Parameter	Description
Virtual Server	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN IP address and its service 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.
ALG Setting	You can select special applications that need "Application Layer Gateway" to support here.
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 NAT port translation.
Static Routing	You can disable NAT function and setup the routing rules manually.

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

2.6.1 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 re-direct 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)



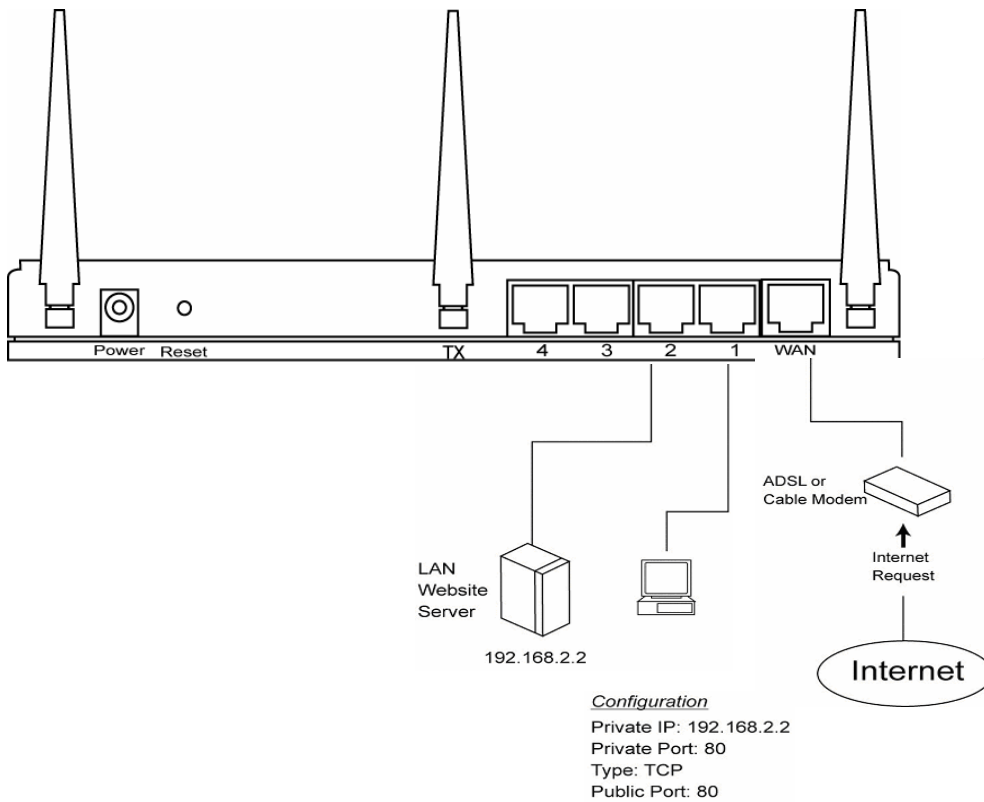
Parameter	Description
WAN Port Range	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN Note: Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Server IP Address	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 for Virtual Server to work properly.
Server Port Range	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)
Protocol	Select the port number protocol type (TCP, UDP).

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

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)



2.6.2 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.

EDIMAX
 NETWORKING PEOPLE TOGETHER

Quick Setup | General Setup | Status Info | System Tools

System
 WAN
 LAN
 Wireless
 QoS
 NAT
 Virtual Server
 Special Application
 ALG
 UPnP
 Static Route
 Firewall

Special Application

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the Trigger Port field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Name	Incoming Type	Incoming Port Range	Trigger Type	Trigger Start Port	Trigger Finish Port	Enable
Quick Time 4	UDP	6970-6999	TCP	554	554	<input type="checkbox"/>
MSN Gaming Zone	TCP	28800-29000	TCP	6667	6667	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>
	TCP		TCP	0	0	<input type="checkbox"/>

Apply Reset

Parameter	Description
Name	The description of this setting.
Incoming Type	Select the Inbound port protocol type: "TCP", "UDP" or both
Incoming Port Range	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, 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400)
Trigger Type	Select whether the outbound port protocol is "TCP", "UDP" or both.
Trigger Start/Finish Range	This is the out-going (Outbound) range of port numbers for this particular application
Enable	Enable the specified Special Application function.

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

Example: Special Applications

If you need to run applications that require multiple connections, then 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.

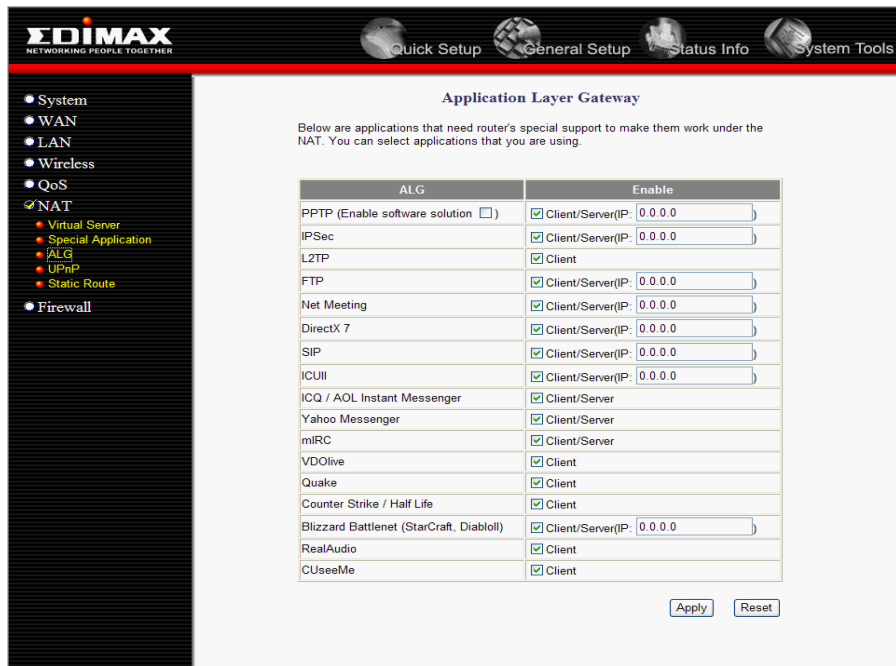
Example:

Name	Incoming Type	Incoming Port Range	Trigger Type	Trigger Start Port	Trigger Finish Port	Enable
MSN Game Zone	TCP	2300-2400, 47624	UDP	28800	28800	MSN Game Zone
Battle.net	UDP	6112	UDP	6112	6112	Battle.net

In the example above, when a user trigger's port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user. **Note:** Only one LAN client can use a particular special application at a time.

2.6.3 ALG Settings

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

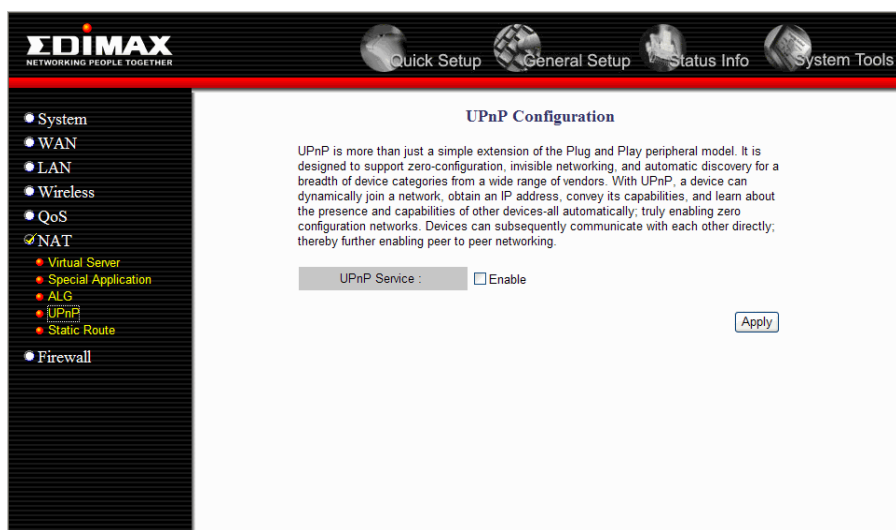


Parameter	Description
Enable	You can select to enable “Application Layer Gateway”, then the router will let that application correctly pass though the NAT gateway.

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

2.6.4 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 can access the Internet through this router easily.



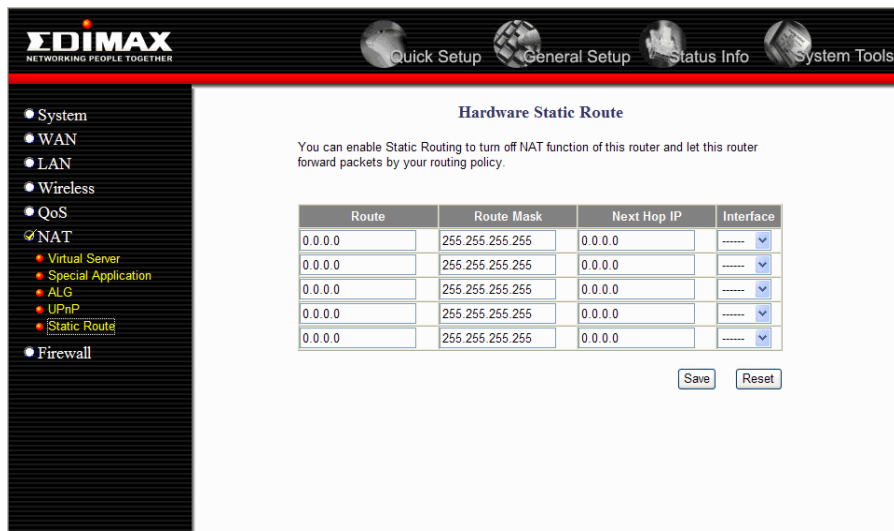
Parameter	Description
UPnP Feature	You can Enable or Disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function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

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

2.6.5 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.



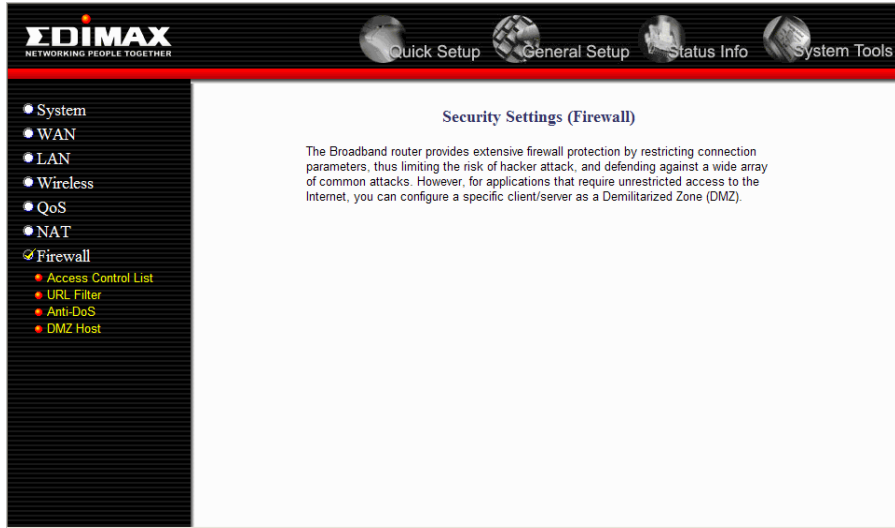
Parameter	Description
Route	The network address of destination LAN.
Route Mask	The subnet mask of destination LAN.
Next Hop IP	The next stop gateway of the path toward the destination LAN. This is the IP of the neighbor router that this router should communicate with on the path to the destination LAN.
Interface	The interface that go to the next hop (router).

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

2.7 Firewall

The 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 as a Demilitarized Zone (DMZ).

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



Parameter	Description
Access Control List	Access Control List allows you to specify which hosts users can or cannot have access to certain Internet applications
URL Filter	URL Filter allows you to specify which URLs can't be accessed by users.
Anti-DoS	The Broadband router's firewall can block common hacker attacks and can log the attack activities.
DMZ Host	The DMZ Host function allows you to re-direct 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

2.7.1 Access Control List

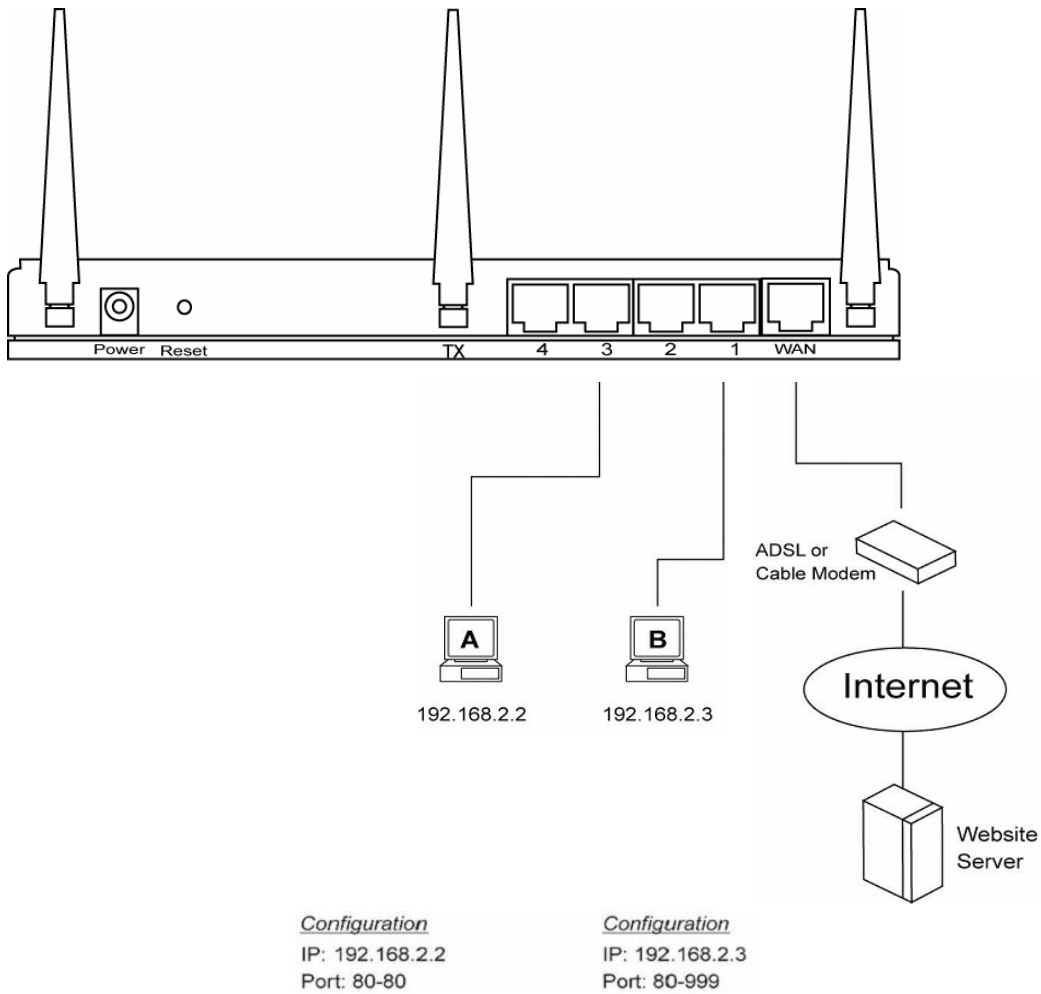
If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), then this is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access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

Parameter	Description
Policy	User can choose to log or not to log packets which match any configured ACL.
Direction/IP	Ingress means packets from LAN to Gateway and Egress means packets from Gateway to WAN. Pay special attention to the "Egress, source IP/port" direction group. The source IP address of an LAN-to-WAN packet will be already changed to gateway's public IP address. That means if you created a system-wise egress rule, please specifying the Gateway WAN IP address as the source IP.
Type	Specify the traffic type here. You can pick TCP for TCP traffic, UDP for UDP traffic, or IP for all kind of IP traffic.
Port	Specify the TCP/UDP port number for filtered traffic.
Day/Time	You can select a range of day and time that the specified PCs will not able to access the Internet on these time period.
Enable	You can Enable/Disable some policies by check their enable checkbox.

You can now configure other advance sections or start using the router (with the advance settings in place)

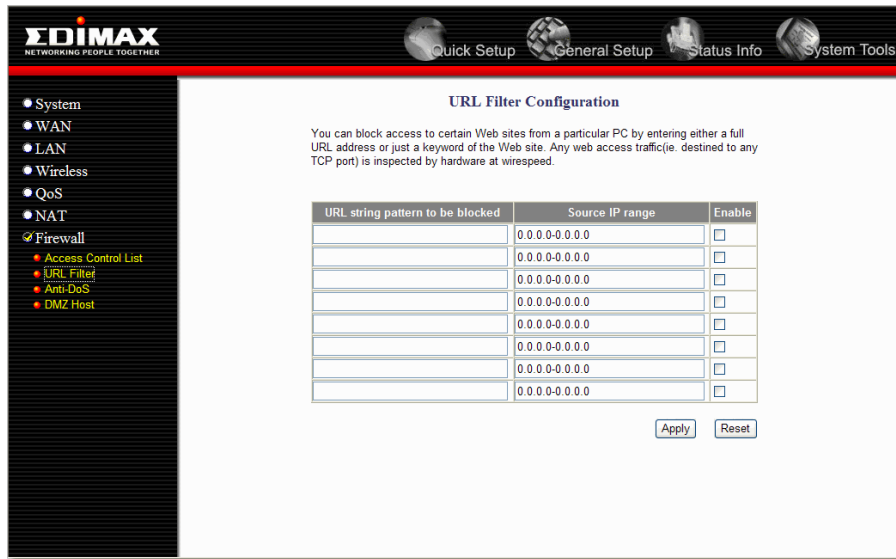
Example: Access Control

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.



2.7.2 URL Filter

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

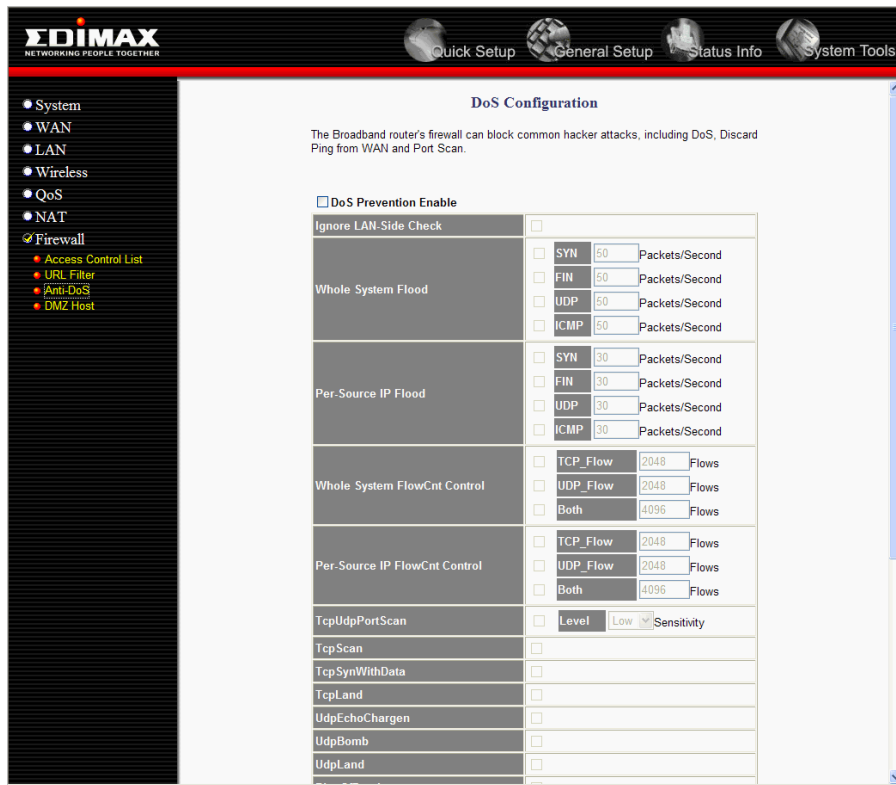


Parameter	Description
URL String Pattern	You can enter the full URL address or the keyword of the web site you want to block.
Source IP Range	You can specify a range of LAN PCs that apply to the URL filter feature.
Enable URL Blocking	Check the check box to Enable URL Blocking

You can now configure other advance sections or start using the router (with the advance settings in place)

2.7.3 Anti-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.

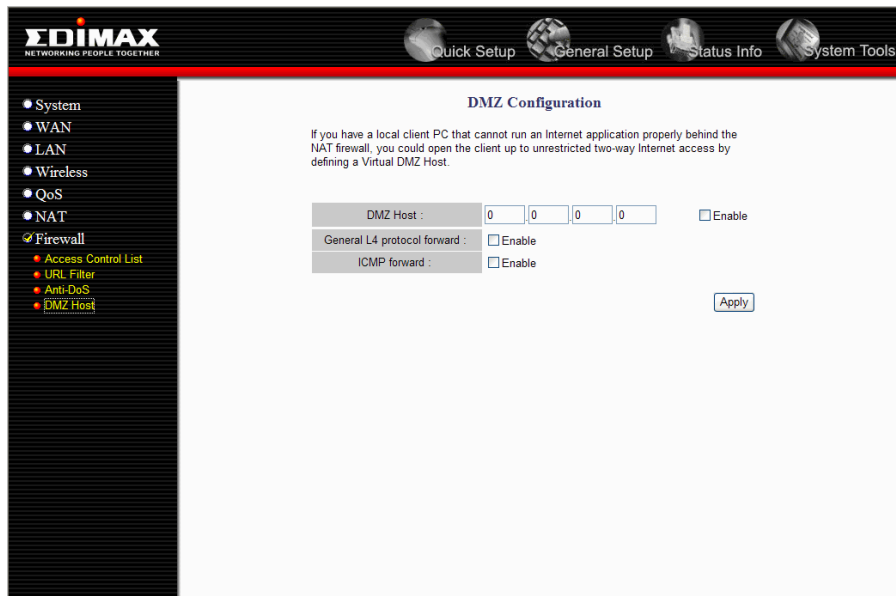


Parameter	Description
DoS Prevention Enable	Enables selected Anti-DoS features.
Ignore LAN-Side Check	Skip DoS checks for all LAN WAN packets.
Whole system flood	System-wide DoS threshold for SYN/FIN/UDP/ICMP flooding.
Per-source IP flood	SYN/FIN/UDP/ICMP flooding threshold per host. Offending host would be blocked for 120 seconds (default) if Source IP Blocking is enabled.
Whole system FlowCnt Control	System-wide Flow Count Control for TCP/UDP or both protocols.
Per-source IP FlowCnt Control	SYN/FIN/UDP/ICMP Flow Count Control per host. Offending host would be blocked for 120 seconds (default) if Source IP Blocking is enabled.
TcpUdpPortScan	Port scan detection. Sensitivity could be Low or High.
All DoS items	System-wide Dos detection.

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

2.7.4 DMZ

If you have a local client PC that cannot run an 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 re-direct 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 re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.



Parameter	Description
Enable DMZ	Enable/disable DMZ Note: If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function. DMZ Host 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 above Note: You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.
General L4 protocol forward	Check this to enable the general layer 4 protocol forwarding function.
ICMP forward	Check this to allow the ICMP packets forward to the DMZ host.

You can now configure other advance sections or start using the router (with the advance settings in place

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.

The screenshot displays the EDIMAX router's Status page. The top navigation bar includes 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. The left sidebar shows the 'Status' menu with sub-options: Internet Connection, Device Status, System Log, ACL Log, URL Filter Log, DoS Log, and New Connection Log. The main content area is divided into four sections: System, LAN, WAN, and Wireless.

System	
Firmware Version :	1.25
Firmware Date :	2006/09/18 13:56:04
Loader Version :	0.0.20
NAT :	Enable
L4 Switching :	Enable

LAN	
IP Address :	192.168.2.1
Subnet Mask :	255.255.255.0
MAC Address :	00:0E:2E:92:B2:4B
DHCP Server :	Enable
LAN 1 :	Link is Up. 100Mbps, full-duplex
LAN 2 :	Link is down. No cable detected
LAN 3 :	Link is down. No cable detected
LAN 4 :	Link is down. No cable detected
Received :	1626 packets, 146084 bytes
Transmitted :	565 packets, 349137 bytes
Dropped :	0 packets

WAN	
Connection Method :	DHCP Client
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0
DNS IP Address :	0.0.0.0
MAC Address :	00:0E:2E:92:B2:4C
WAN Port :	Link is down.
Received :	0 packets, 0 bytes
Transmitted :	0 packets, 0 bytes
Dropped :	2 packets

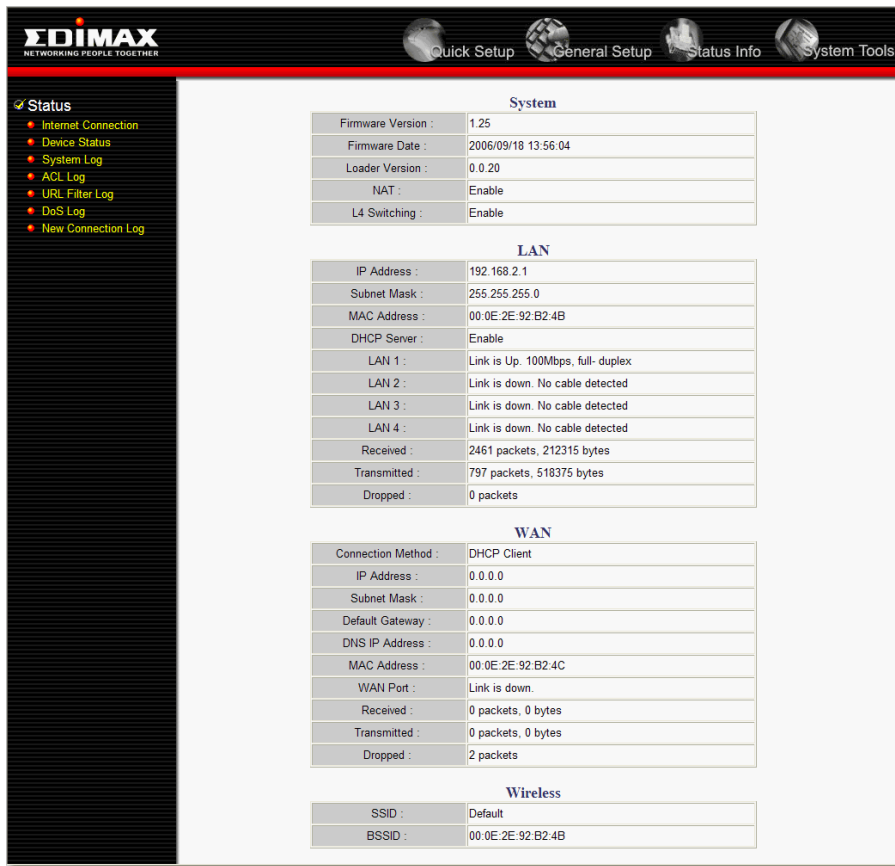
Wireless	
SSID :	Default
BSSID :	00:0E:2E:92:B2:4B

Parameter	Description
Status and Information	Shows the router's system information
Logs	This router supports five types of Log messages: System Log, ACL Log, URL filter, DoS Log and New connection Log.

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

3.1 Status and Information

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



Parameter	Description
Information	You can see the router's system information such as the router's: System Information, LAN Information, WAN Information, and Wireless Information.

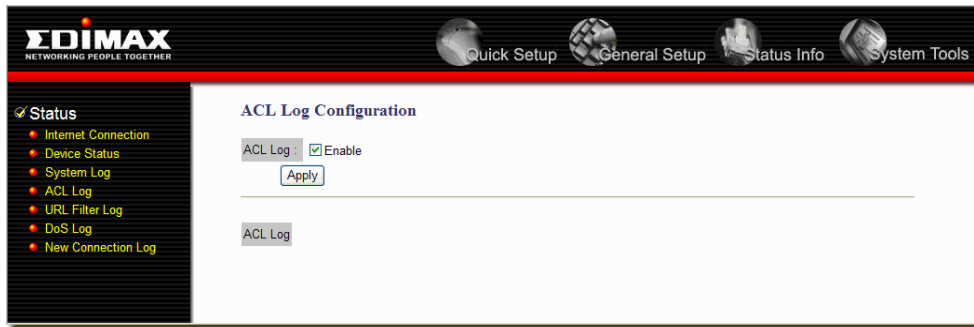
3.2 Logs

This router supports five types of Log messages: System Log, ACL Log, URL filter, DoS Log and New connection Log. You can Enable or Disable each of these Logs.

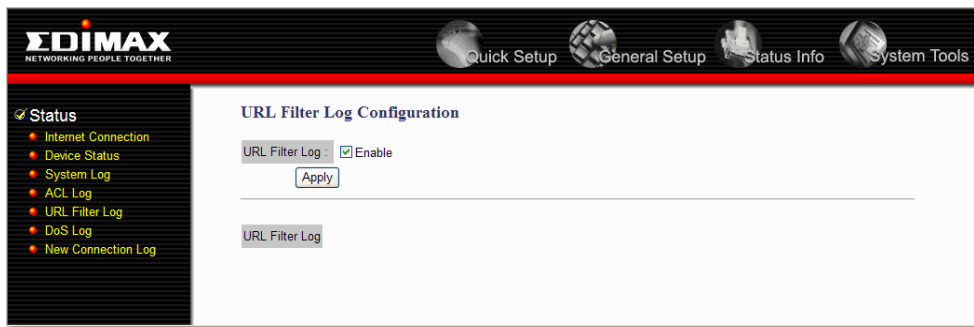
3.2.1 System Log



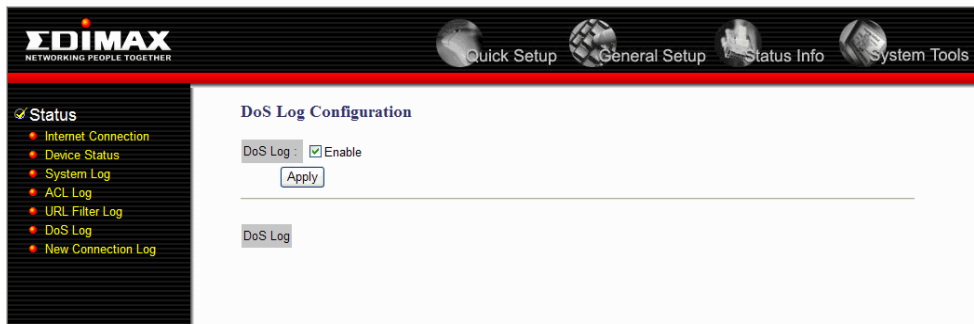
3.2.2 ACL Log



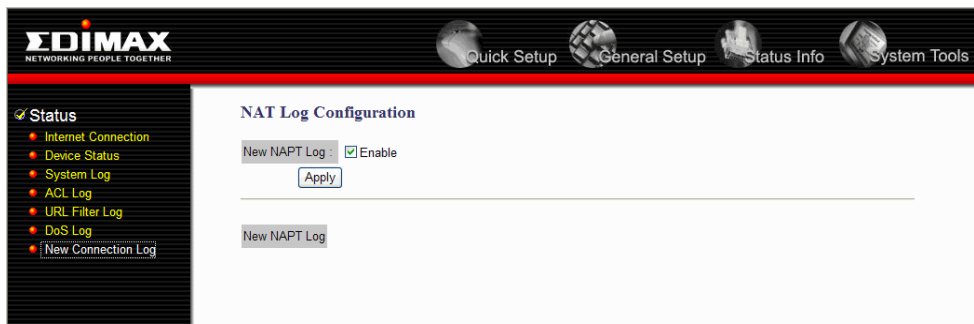
3.2.3 URL Filter Log



3.2.4 DoS Log



3.2.5 New Connection Log



Chapter 4

Tool

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



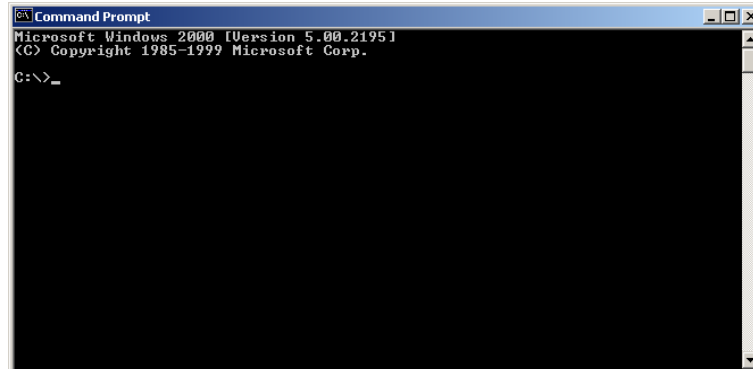
Parameter	Description
Firmware Version	This shows your current firmware version.
Firmware Upgrade	This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.
Factory Default	You can use the " Factory Defaults " tool to force the Broadband router to perform a power reset and restore the original factory settings.
System Restart	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the System Restart button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

Select one of the above three **Tools Settings** selection and proceed to the manual's relevant sub-section

Appendix A

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

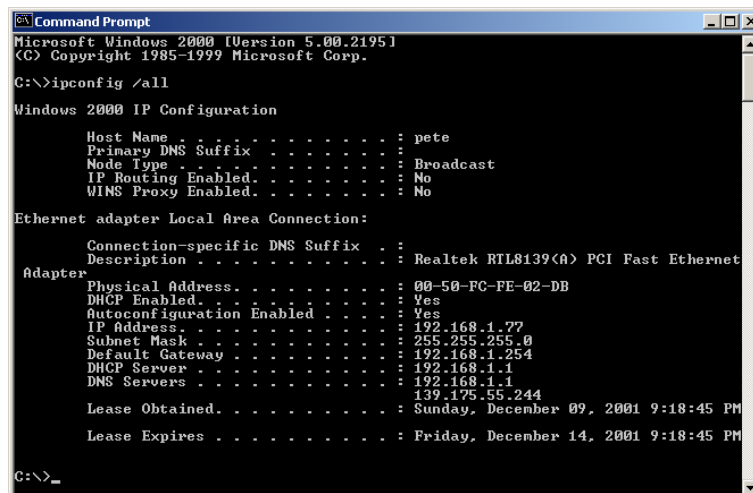
- 1) In Window's open the Command Prompt program



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>_
```

- 2) Type **Ipconfig /all** and <enter>



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : pete
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  :
    Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
    Adapter Physical Address . . . . . : 00-50-FC-FE-02-DB
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address . . . . . : 192.168.1.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
                             139.175.55.244
    Lease Obtained. . . . . : Sunday, December 09, 2001 9:18:45 PM
    Lease Expires . . . . . : Friday, December 14, 2001 9:18:45 PM

C:\>_
```

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

Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

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 keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper 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 standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

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

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that 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 for definition). 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 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 is

comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (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 distinguish one network application/protocol over 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 upon between multiple parties so that when they interface 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: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

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

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>