NEXXT
SOLUTIONS

Acrux300
USER MANUAL

Model: **ARN03304U1**

Copyright Statement

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the 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:

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

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.
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 user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CONTENTS

Package contents

Upon opening the box, make sure that the following items are included:

*One ARN03304U1 Wireless N Gigabit Router
*One DC Power Adapter
*One Quick Installation Guide
*One resource CD-ROM with a digital copy of the Quick installation Guide and the User Manual

Note:

If any of the listed items is missing, mismatched, damaged or broken, contact your local dealer immediately for replacement.

Chapter 1. Introduction

Thank you for purchasing the ARN03304U1 Wireless N Gigabit Router from Nexxt Solutions.

1.1 Product overview

The ARN03304U1 Gigabit N Router is a combined wired/wireless network connection device integrated with an internet-sharing router and a 4-port switch. Based on 802.11 N specifications, this router ensures ultimate performance for HD video streaming, online games, intense data transfers, and heavy internet use, with no lag or interference. Featuring an innovative Network Storage Capability known as NAS, this router can fully meet the needs of Small Office/Home Office environments, by allowing access from any computer linked to the network to the data stored in any hard drive, flash drive or a memory card reader attached to the router's USB port.

Incredible speed

The ARN03304U1 Wireless N Gigabit Router delivers up to 300Mbps wireless speeds with other 802.11n connected clients. Such transmission rate makes it ideal for handling multiple data streams at the same time, which ensures the stability and the smooth operation of the network. The performance of this 802.11n wireless router will enhance your networking experience by achieving speeds up to 6 times faster than 802.11g devices. It also offers backward compatibility with all IEEE 802.11g and IEEE 802.11b products.

Multi-Level security

The Wireless N Gigabit Router provides complete data privacy. It supports multiple protection methods, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protection.

Flexible access control

The Wireless N Gigabit Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, so that the network administrators can manage and monitor the network in real time using the remote management function.

Hassle-free installation

As it is compatible with virtually all the major operating systems, management of the router is very simple. A Quick Setup Wizard is supported, which provides easy-to-follow step by step instructions that are later described in detail in this manual. Before installing the router, please read the user guide carefully, to become familiar with all the features and functions of the router.

1.3 Main Features

* Complies with IEEE 802.11n to provide a wireless data rate of up to 300Mbps.
* One 10/100/1000M auto-negotiation RJ45 WAN port, four 10/100/1000M auto-negotiation RJ45 LAN ports, supporting auto MDI/MDIX.

* Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
* Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access.
* Supports Virtual Server, Special Application and DMZ host.
* Supports UPnP, Dynamic DNS, Static Routing.
* Provides automatic and scheduled internet connection to the internet on certain times.
* Built-in NAT and DHCP server supports static IP address distributing.
* Supports Parental Control and Access Control.
* Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
* Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
* Supports Flow Statistics.
* Supports firmware upgrade and Web management.

1.4 Panel Layout

1.4.1 The Front Panel

Figure 1-1 Front Panel

The router's LEDs and the WPS button are located on the front panel. (Viewed from left to right).

Name	Status	Indication
Power	Off	Power is off
	On	Power is on
System	On	Router is initializing or there may be a system error
	Flashing	Router is working properly
	Off	Router has a system error
WLAN	Off	The wireless function is disabled
	Flashing	The wireless function is enabled
WAN, LAN 1-4	Off	There is no device linked to the corresponding port
	On	There is a device linked to the corresponding port, but no activity is detected
	Flashing	There is an active device linked to the corresponding port
WPS	Slow Flash	A wireless device is connecting to the network by WPS function. This process will takes 2 minutes to complete
	On	A wireless device has been successfully added to the network by WPS function
	Quick Flash	A wireless device failed to be added to the network by WPS function

Table 1-1 LEDs description

Note:

After a device is successfully added to the network by WPS function, the WPS LED will remain illuminated for about 5 minutes before going off.

1.4.2 Rear panel

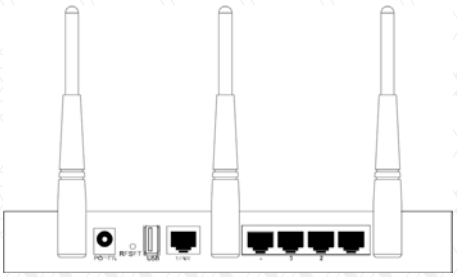


Figure 1-2 Rear Panel sketch

The following parts are located on the rear panel (View from left to right).

* **POWER:** This is the power socket where you will connect the power adapter. Please use only the power adapter supplied to connect the device to the AC mains.
* **RESET:**
  Two methods are available to reset to the router to its factory default configuration:
  1) Go to the Factory Default option on System Tools -> Factory Default page included in the router's Web-based Utility.
  2) Use the Factory Default Reset button: Press the Reset button for five seconds and then wait for the Router to reboot.
* **USB:** Connect with USB Mass Storage Device.
* **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet
* **1,2,3,4 (LAN):** These ports (1, 2, 3, 4) connect the Router to the local PC(s)
* **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2
Connecting the router

2.1 System requirements

* Broadband Internet Access Service (DSL/Cable/ Ethernet)
* One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the Router is connected directly to the Ethernet.)
* PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
* TCP/IP protocol on each PC
* Web browser, such as Microsoft Internet Explorer 5.0 , Netscape Navigator 6.0 or above.

2.2 Installation environment requirements

* Place the router in a well ventilated place, far away from any heat generating device, heater or heating vents.
* Avoid t exposure to direct light (such as sunlight) or excessive heat.
* Allow at least 2 inches (5 cm) of clearance around the unit.
* Operating temperature: 0°C~40°C (32°F~104°F)
* Operating humidity: 10%~90%RH, non-condensing.

2.3 Connecting the router

Before installing the router, make sure your PC is successfully connected to the Internet using the broadband service. If any problems arise during the process, please contact your ISP directly. Proceed with the router installation, according to the following steps. Do not forget to unplug the power adapter, making sure to keep your hands always dry.

1. Power off your PC, Cable/DSL modem, and the router.
2. Choose the optimum location for the router. The best place is usually near the center of the area in which your PC(s) will wirelessly connect.
3. Adjust the direction of the antenna. Placing the antenna in the upright position often provides the best performance.
4. Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the router, as shown in figure 2-1. (If you have a wireless NIC and want to use the wireless function, you can skip this step.)
5. Connect the DSL/Cable Modem to the WAN port on the Router, as shown in figure 2-1.
6. Connect the power adapter to the power socket on the router, and the other end into an electrical outlet. The Router will start to work automatically.
7. Power on your PC and Cable/DSL Modem.

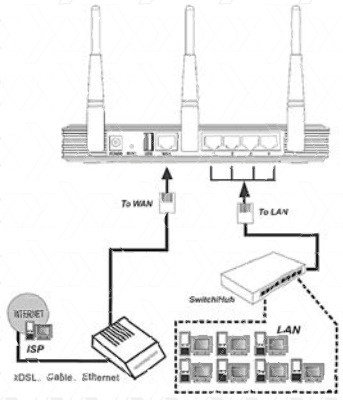


Figure 2-1 Hardaware Installation
of the Wireless N Gigabit Router

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of you Wireless N Gigabit Router in minutes using the Quick Setup Wizard.

3.1 TCP/IP Configuration

The default IP address of the router is 192.168.0.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. Default values are used in the description included in this manual.

Connect the local PC to the LAN ports of the router. You can now start configuring the IP address for your PC as described below.

* Configure the IP address manually.

1. Set up the TCP/IP Protocol for your PC. If you need further instructions regarding this feature, please refer to Appendix B: "Configuring the PC."
2. Configure the network parameters. The IP address is 192.168.0.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168. 0.1 (The router's default IP address).

* Obtain an IP address automatically.

1. Set up the TCP/IP Protocol in "Obtain an IP address automatically" mode on your PC. If you need further instructions regarding this feature, please refer to Appendix B: "Configuring the PC."
2. The built-in DHCP server will then assign an IP address to the PC.

The user can now run the Ping command in the command prompt to verify the network connection between your PC and the Router. The following

example is based on Windows 2000 operating system.

After opening a command prompt, type ping 192.168.0.1, followed by Enter.

* If the result displayed is similar to the illustration in Figure 3-1, it means the connection has been established correctly between your PC and the router.

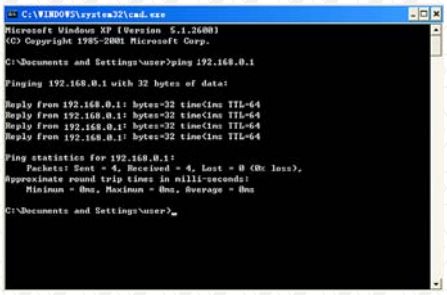


Figure 3-1 Successful message of Ping command

* If the result displayed is similar to the illustration in figure 3-2, it means the connection between your PC and the router has failed.

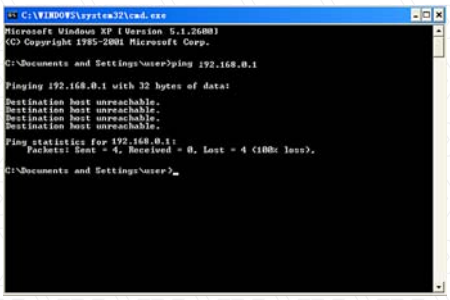


Figure 3-2 Failure message of Ping command

Check the connection by executing the following steps:

1. Is the connection between your PC and the router correct?
   Note:
   The 1/2/3/4 LEDs of LAN ports on the router which your computer is linked to, and the LEDs on your PC's adapter should be lit.
2. Is the TCP/IP configuration for your PC correct?
   Note:
   If the router's IP address is 192.168.0.1, your PC's IP address must be within 192.168.0.2 ~ 192.168. 0.254 range.

3.2 Quick Installation Guide

The configuration and management of the Wireless N Gigabit Router is made simple through a Web-based (Internet Explorer or Netscape® Navigator) utility. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.0.1 in the address field of the page.

Figure 3-3 Login the router

Within seconds, a login window will appear, similar to the one shown in Figure 3-4. Enter admin for the User Name and Password, both in lower case letters. Then click the OK button or press the Enter to continue.

Figure 3-4 Login Windows

Note:
If the above screen does not pop-up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

2. After successfully logging in, you can click the Quick Setup to quickly configure the router.

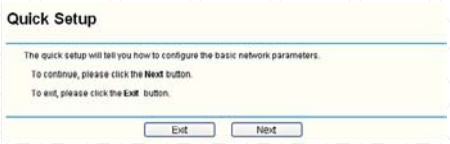


Figure 3-5 Quick Setup

3. Click Next, and then the WAN Connection Type page will appear, as shown in Figure 3-6.

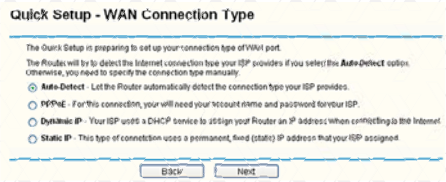


Figure 3-6 WAN connection types

The router combines the Auto-Detect functionality with three widely used types of internet connections: PPPoE, Dynamic IP and Static IP. The Auto-Detect setting is recommended. However, if you are certain of what kind of connection type your ISP provides, check it now and continue with the router configuration as prompted.

4. If you select **Auto-Detect**, the router will automatically discover the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection.
   The appropriate configuration page will be displayed when an active Internet service is successfully detected by the router.

   1. If the connection type detected is PPPoE, the next screen will appear, as shown in Figure 3-7.

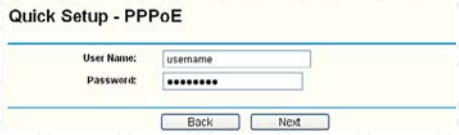


Figure 3-7 Quick Setup - PPPoE

* **User Name and Password** - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have any problems during this process, please contact your ISP directly.

2. If the connection type detected is Dynamic IP, the next screen will appear, as shown in Figure 3-9. Afterwards, you may continue with the wireless configuration.

3. If the connection type detected is Static IP, the next screen will appear, as shown in Figure 3-8.

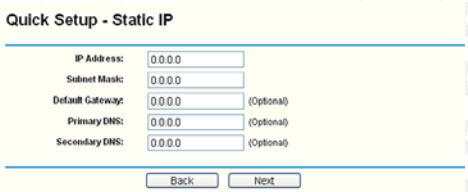


Figure 3-8 Quick Setup - Static IP

* **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into this field.
* **Subnet Mask** - The Subnet Mask is used for the WAN IP address, usually 255.255.255.0. is used.
* **Default Gateway** - Enter the gateway IP address into the box, if required.
* **Primary DNS** - Enter the DNS Server IP address into the box, if required.
* **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

5. Click **Next** to continue, the Wireless settings page will appear, as shown in Figure 3-9.

Figure 3-9 Quick Setup – Wireless

* **Wireless Radio** – Use the drop-down menu to enable or disable wireless radio.
* **SSID** - Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be Nexxt_xxxxxx (in which xxxxxx represent the last six unique characters of each router's MAC address). This value is case-sensitive. For example, TEST is NOT the same as test.
* **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region different from those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

* **Channel** - This field determines the operating frequency to be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
* **Mode** - This field determines the wireless mode which the Router works on.
* **Channel Width** - Select a channel width from the pull-down list. The default setting is automatic, designed to instantly adjust the channel width of clients.
* **Max Tx Rate** - You can limit the maximum transmission rate of the router through this field.
* **Disable Security** - The wireless security function can be enabled or disabled.
  If disabled, the wireless stations will be able to connect with the router without encryption.
  It is strongly recommended that you choose one of following options to enable security.
* **WPA-PSK/WPA2-PSK** - Select WPA based on pre-shared passphrase.
  * **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters.
    For ASCII, the key can be made up of any number, from 0 to 9, and any letter, from A to Z. This string should be between 8 and 63 characters long.
    For Hexadecimal, the key can be made up of any number, from 0 to 9, and any letter, from A to F. This string should be between 8 and 64 characters long.

Please note that the key is also case sensitive, this means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings for future reference.

* **No Change** - If you chose this option, wireless security configuration will remain unchanged. These settings only refer to the basic wireless parameters. For advanced settings, please refer to Section 4.6: "Wireless".

6. Click the **Next** button. The Finish page will appear in this case.
   If you don't make any changes on the Wireless page, you will see the Finish page as shown in Figure 3-10. Click the Finish button to complete the **Quick Setup** procedure.

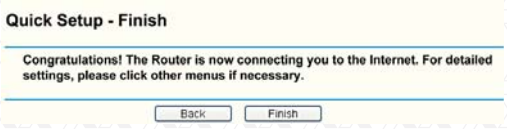


Figure 3-10 Quick Setup – Finish

If any changes are made on the Wireless page, the Finish page will pop up, as shown in figure 3-11. Click the Reboot button to make your wireless configuration to take effect and complete the Quick Setup.

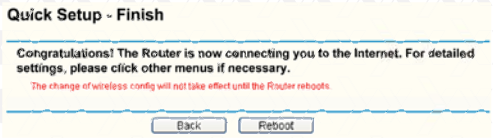


Figure 3-11 Quick Setup - Finish

Chapter 4. Configuring the router

This chapter includes a detailed description of key functions and the configuration procedure of each Web page.

4.1 Login

After successfully logging in, you will see the sixteen main menus on the left of the Web-based utility. On the right column, the corresponding explanations and instructions will be displayed.

Each Web page's key functions are explained in detail in the section below.

4.2 Status

The Status page displays the current state of the router. All information is read-only.

Figure 4-1 Router Status

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

4.4 WPS

This section will guide you on how to add a new wireless device quickly to an existing network using the WPS (Wi-Fi Protected Setup) function.

a. Open the "WPS" menu. The following screen (shown in Figure 4-2) will appear.

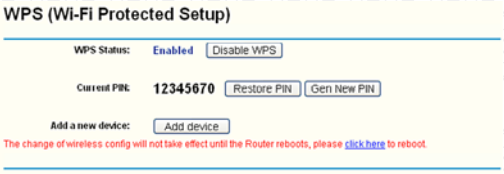


Figure 4-2 WPS

* **WPS Status** – Enables or disables the WPS function.
* **Current PIN** - The current PIN of the Router is displayed on this screen. The default PIN of the Router can be found in the label or User Guide.
* **Restore PIN** - Restores the PIN of the Router to its default value.
* **Gen New PIN** - Click this button to obtain a new random value as the router's PIN. You can better protect your network by generating a new PIN.
* **Add device** - You can add a new device to the existing network manually by clicking this button.

b. **To add a new device:**

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between the wireless adapter and the router using either the Push Button Configuration (PBC) method or the PIN method.

Note:

To build a successful connection via WPS, you

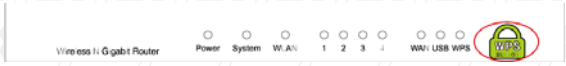
should also configure the new device for WPS in the meantime.
In order to configure the new device, we are going to use the Lynx Wireless Adapter from Nexxt Solutions as an example.

I. PBC configuration

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC), you can add the device to the network by executing any of the two following methods.

First method:

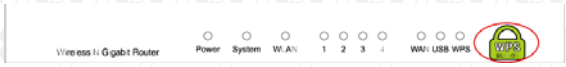
Step 1: Press the WPS button on the front panel of the router.



Step 2: Press and hold the WPS button of the router 2 or 3 seconds. The adapter will then connect to the router via WPS automatically.

Second method:

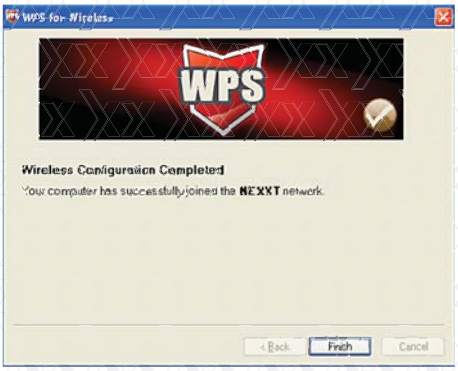
Step 1: Press the WPS button on the front panel of the router.



Step 2: In order to configure the wireless adapter, select **Push the button on my access point** in the configuration utility of the WPS, as shown below. Click **Next** to continue.

WPS Configuration Screen for the Wireless Adapter

Step 3: Wait until the next screen appears. Click Finish to complete the WPS configuration.



WPS Configuration Screen for the Wireless Adapter

Third method:

Step 1: Keep the default WPS Status as Enabled and click the Add device button as shown in Figure 4 2. The following screen will appear.

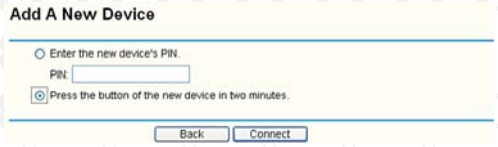
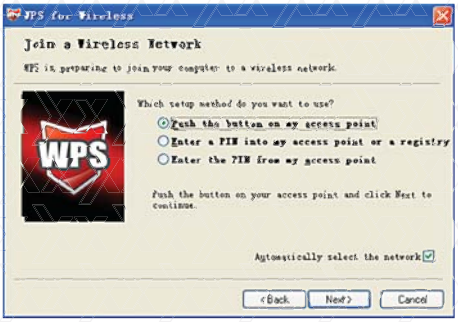


Figure 4-3 Add A New Device

Step 2: Choose **Press the button of the new device in two minutes**, and click Connect.
Step 3: In order to configure the wireless adapter, select **Push the button on my access point** in the configuration utility of the WPS, as shown below. Click **Next** to continue.



WPS Configuration Screen for the Wireless Adapter

Step 4: Wait until the next screen appears. Click **Finish** to complete the WPS configuration.

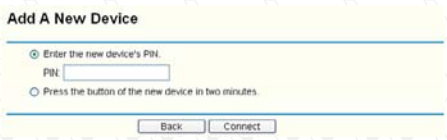
WPS Configuration Screen for the Wireless Adapter

II. PIN configuration

If the wireless adapter supports Wi-Fi Protected Setup and the PIN Configuration, you can add the device to the network by executing any of the two following methods.

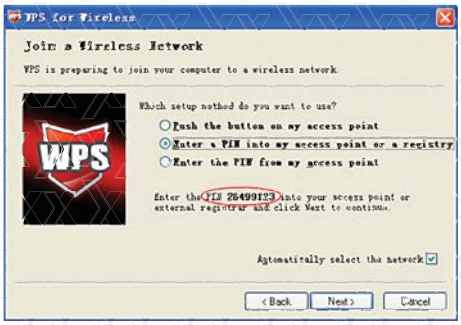
First method: Enter the PIN into the router.

Step 1: Keep the default WPS Status as Enabled and click the Add device button, as shown in Figure 4-2. The following screen will appear.



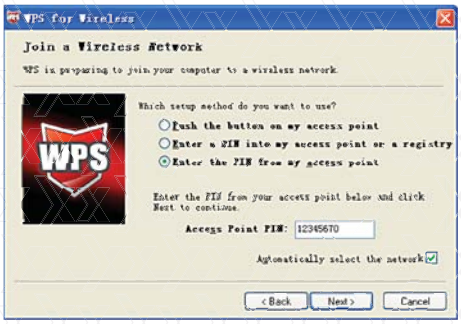
Step 2: Select **Enter the new device's PIN** and input the code of the wireless adapter in the field next to PIN. When done, click Connect.

Note:
The PIN code of the adapter is always displayed on the WPS configuration screen.
Step 3: In order to configure the wireless adapter, select **Enter a PIN into my access point or a registrar** in the configuration utility of the WPS, as shown below. Click **Next** to continue.



WPS Configuration Screen of the Wireless Adapter

Note:
The default PIN code of the adapter is 26499123, as displayed in this example.
Second method: Enter the PIN from my Router.
Step 1: Get the Current PIN code of the Router, as shown in Figure 4-2 (each Router has its unique PIN code. We are using 12345670 as the PIN code in this example).
Step 2: In order to configure the wireless adapter, select Enter a PIN from my access point in the configuration utility of the WPS, as shown below. Enter the PIN code of the router into the field next to **Access Point PIN**. Click **Next** to continue.



WPS Configuration Screen for the Wireless Adapter

Note

The default PIN code of the Router can be found in its label or on the WPS configuration screen, as shown in Figure 4-2.

c). Once the new device has been successfully connected to the network, the following screen will appear.

Note:
a. The status LED on the Router will be solid green if the device has been successfully added to the network.
b. The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

4.5 Network

Figure 4-4 Network menu

As shown in Figure 4-4, there are three submenus under **Network: LAN, WAN** and **MAC Clone**. Click on any of these items in order to configure the corresponding function.

4.5.1 LAN

Go to "**Network → LAN**" in the menu, in order to configure the IP parameters of the LAN on the screen, as shown below.

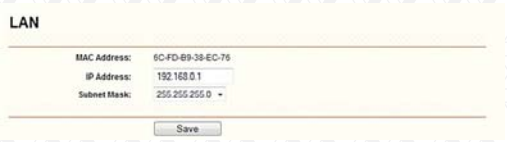


Figure 4-5 LAN

- **MAC Address -** The physical address of the router, as seen from the LAN. This value cannot be changed.
- **IP Address -** Enter the IP address of your router or reset it in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally, use 255.255.255.0 as the subnet mask.

Note:

a. If you change the IP Address of the LAN, you must use the new IP Address to login to the router.

b. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.5.2 WAN

Go to "**Network → WAN**" in the menu, in order to configure the IP parameters of the WAN on the screen, as shown below.

1. If your ISP provides the DHCP service, please select Dynamic IP, so that the Router will automatically get IP parameters from your ISP. The page that pops up at this stage looks like the one below (Figure 4-6):

Figure 4-6 WAN - Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the Renew button to renew the IP parameters from your ISP. Click the Release button to release the IP parameters.

* **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
* **Use These DNS Servers** - If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Note:
If you find an error when you go to a Web site after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

* **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select Static IP. The Static IP settings page will appear, as shown in Figure 4-7.

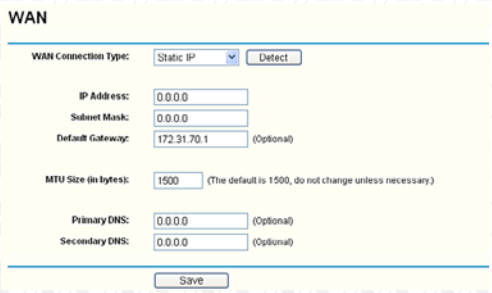


Figure 4-7 WAN - Static IP

* **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
* **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually this is 255.255.255.0.
* **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.

* **MTU Size -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
* **Primary/Secondary DNS -** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

3. If your ISP provides a PPPoE connection, select PPPoE option. In that case, you must fill in following parameters (Figure 4-8):

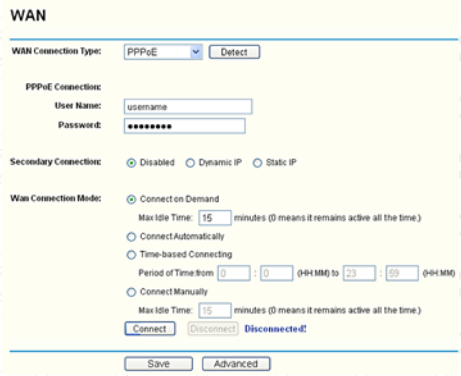


Figure 4-8 WAN - PPPoE

* **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
* **Secondary Connection** - It is available only for PPPoE Connection. If your ISP provides an additional Connection method such as Dynamic/Static IP to gain access to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.

* **Disabled** - The Secondary Connection is disabled by default, so there is only the PPPoE connection available, this being the recommended setting for this feature.
* **Dynamic IP** - You can check this radio button to use Dynamic IP as the secondary connection to gain access to the local area network provided by ISP.
* **Static IP** - You can check this radio button to use Static IP as the secondary connection to gain access to the local area network provided by ISP.

* **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified period of inactivity (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want to keep your Internet connection active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
* **Connect Automatically** - The connection can be re-established automatically after being disabled.
* **Time-based Connection** - The connection will only be established within the period ranging from the start time to the end time (both are in HH:MM format).

Note:
The Time-based Connection feature can work only after the system time on the System Tools -> Time page has been configured.

* **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the Max

Idle Time function as the Connect on Demand mode. The Internet connection can be disconnected automatically after a specified period of inactivity, and re-established when you attempt to access the Internet once again.

Caution: Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background. If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-9 will appear:

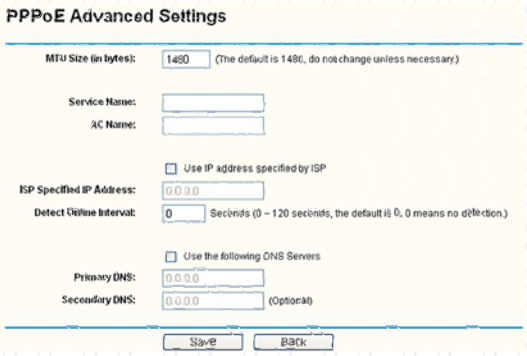


Figure 4-9 PPPoE Advanced Settings

* **MTU Size** - The default MTU size is "1480" bytes, which is usually fine. It is not recommended that you change the default MTU Size, unless required by your ISP.
* **Service Name/AC Name** - The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is

necessary for your ISP. In most cases, leaving these fields blank will work.

* **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the router during login, please click "Use IP address specified by ISP" check box and enter the IP address provided by your ISP in dotted-decimal notation.
* **Detect online interval** - Access Concentrator online detection that the router will run at the specified interval. The default value is "0". You can select any number between "0" and "120". A "0" setting means no detection.
* **DNS IP address** - If your ISP does not automatically assign DNS addresses to the router during login, please click "Use the following DNS servers" check box and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the Save button to store your settings.

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select BigPond Cable. Proceed to fill in the following parameters, as shown below (Figure 4-10):

Figure 4-10

* **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
* **Auth Server** - Enter the authenticating server IP address or host name.
  Auth Domain - Type in the domain suffix server name based on your location.

  For example
  NSW / ACT - **nsw.bigpond.net.au**
  VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
  QLD - **qld.bigpond.net.au**
* **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
* **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after

a specified period of inactivity (Max Idle Time) and be re-established when you attempt to access the Internet once again. If you want to keep your Internet connection active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

* **Connect Automatically** - The connection can be re-established automatically when it was down.
* **Connect Manually** - You can click this button to instantly Connect/Disconnect the device. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be cancelled automatically after a specified period of inactivity and re-established when you attempt to access the Internet once again.

  Click the **Connect** button to connect immediately.
  Click the **Disconnect** button to disconnect immediately.

Caution: Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.
Click the **Save** button to store your settings.

5. If your ISP provides L2TP connection, please select L2TP option. In that case, you must fill in the following parameters (Figure 4-11):

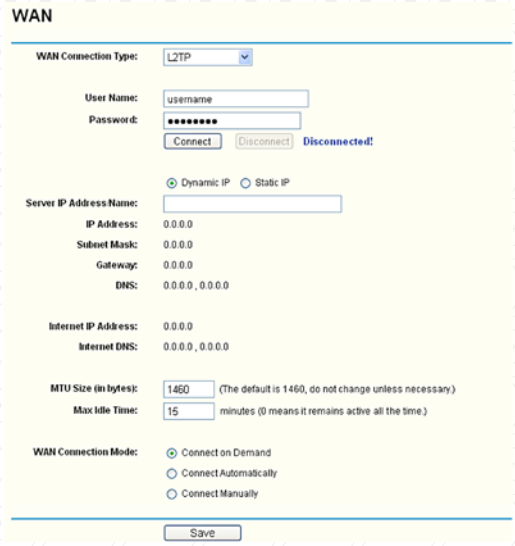


Figure 4-11 L2TP Settings

* **User Name/Password** - Type the User Name and Password provided by your ISP. These fields are case-sensitive.
* **Dynamic IP/ Static IP** - Select the one as provided by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
* **Connect on Demand** - You can configure the router to cancel your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the

router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection is terminated.

* **Connect Automatically** - Connects automatically after the router is disconnected. To use this option, click the radio button.
* **Connect Manually** - You can set up the router so as to connect or disconnect it manually. After a specified period of inactivity (**Max Idle Time**), the router will cancel your Internet connection, in which case you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to keep the connected status active, unless a new link is requested.

Caution: Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.

6. If your ISP provides a PPTP connection, please select the PPTP option. Then proceed to fill in the corresponding parameters (Figure 4-12):

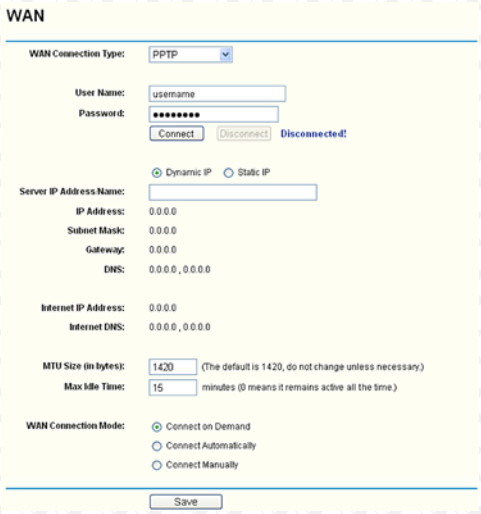


Figure 4-12 PPTP Settings

* **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
* **Dynamic IP/ Static IP** - Select the one as provided by your ISP. Then enter the ISP's IP address or the domain name.
  If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. Click **Save** to keep your changes.
  Click the **Connect** button to connect immediately.
  Click the **Disconnect** button to disconnect immediately.
* **Connect on Demand** - You set up the router so as to disconnect from the Internet after a speci-

fied period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet once again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

* **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
* **Connect Manually** - You can set up the router so as to connect or disconnect it manually. After a specified period of inactivity (**Max Idle Time**), the router will cancel your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet once again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to keep the connected status active, unless a new link is requested.
Caution: Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.

Note:
If you do not know how to choose the appropriate connection type, click the **Detect** button to allow the router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the router. This report is for your reference only. To verify the connection type your ISP provides, please refer to your ISP directly. The various types of Internet connections that the router can detect are as follows:

* **PPPoE** - a PPPoE-based internet connection requires a user name and password.
* **Dynamic IP** - an IP- based internet connection uses dynamic IP address assignment.
* **Static IP** - a Static-based internet connection uses static IP address assignment.

The router cannot detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.5.3 MAC Clone

Go to "**Network → MAC Clone**" in the menu, in order to configure the MAC address of the WAN on the screen as shown in figure 4-13 below.

Figure 4-13 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

* **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires that you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format (X is any hexadecimal digit).
* **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address To** button and this MAC address will be copied into the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value. Click the **Save** button to store your settings.

Note:

Only the PC on your LAN can use the **MAC Address Clone** function.

4.6 Wireless

Figure 4-14 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-14): **Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics**. Click on any of these items in order to configure the corresponding function.

4.6.1 Wireless Settings

Go to "Wireless→Wireless Setting" in the menu, in order to configure the basic settings for the wireless network on this page.

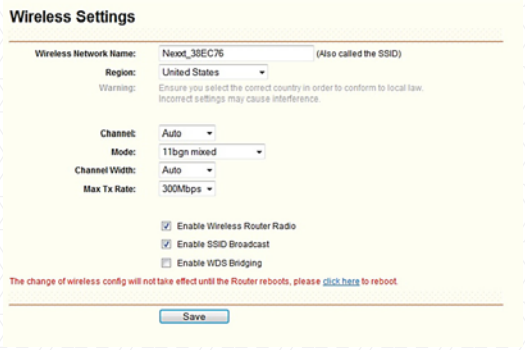
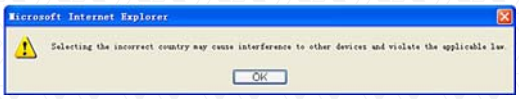


Figure 4-15 Wireless Settings

* **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be NEXXT_XXXXXX (in which xxxxxx represent the last six unique characters of each router's MAC address). This value is case-sensitive. For example, TEST is NOT the same as test.

* **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region different from those specified in this field. If your country or region is not listed, please contact your local government agency for assistance. When you select your local region from the pull-down list, click the **Save** button. The dialog box with this note will be displayed. Click **OK** to continue.



Dialog box

Note:
Based on local regulations, the North America version does not have the region selection option available.

* **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
* **Mode** - Select the desired mode. The default setting is 11bgn mixed.
  11b only - Select it when all of your wireless clients are 802.11b.
  11g only - Select it when all of your wireless clients are 802.11g.
  11n only - Select it when all of your wireless

clients are 802.11n.
11bg mixed - Select it when you are using both 802.11b and 802.11g wireless clients.
11bgn mixed - Select it when you are using a mix of 802.11b, 11g, and 11n wireless clients.
Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

* **Channel width** - Select any channel width from the pull-down list. The default setting is automatic, designed to instantly adjust the channel width of clients

Note:
When 11b only, 11g only, or 11bg mixed is selected in the Mode field, the **Channel Width** field will turn grey, showing a fixed setting of 20M, which remains unchanged.

* **Max Tx Rate** - Use this field to limit the maximum Tx rate of the router.
* **Enable Wireless Router Radio** - The wireless radio of this router can be enabled or disabled to allow wireless stations access.
* **Enable SSID Broadcast** - When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select the **Enable SSID Broadcast** checkbox, the wireless router will start broadcasting its name (SSID) over the air.

4.6.2 Wireless Security

Go to "**Wireless → Wireless Security**" in the menu, in order to configure the security settings of your wireless network.

There are five wireless encryption methods supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key), WPA-PSK (Pre-Shared Key).

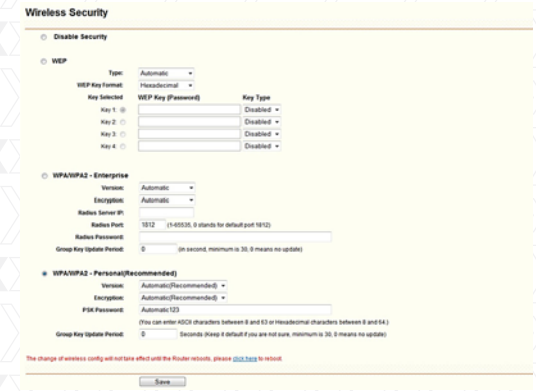


Figure 4-16

* **Disable Security** - If you do not want secure your network, check this box. However, it is strongly recommended to opt for one of the following encryption methods, to better protect your network traffic.
* **WEP** - It is based on the IEEE 802.11 standard. If you check this box, a notice in red will be displayed, as shown in Figure 4-17.

Figure 4-17

- **Type** - Choose the type for the WEP security from the pull-down list. The default setting is **Automatic**, which sets **Open System** or **Shared Key authentication** form automatically, based on the wireless station's capability and request.
- **WEP Key Format** - Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.
  64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not supported) or 5 ASCII characters.
  128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not supported) or 13 ASCII characters.
  152-bit - You can enter 32 hexadecimal digits

(any combination of 0-9, a-f, A-F, zero key is not supported) or 16 ASCII characters.

Note:
If you do not set a passkey, the wireless encryption feature remains disabled even if you have selected **Shared Key**, as your Authentication Mode.

* **WPA/WPA2 Enterprise** - It is based on the radius server.

- **Version** - Choose the WPA encryption method from the pull-down list. The default setting is **Automatic**, which automatically sets **WPA** (Wi-Fi Protected Access) or **WPA2** (WPA version 2), based on the wireless station's capability and request.
- **Encryption** - You can either select Automatic, or TKIP or AES.

Note:
If you check the **WPA/WPA2** radio button and choose **TKIP** encryption, a notice in red will be displayed, as shown below in Figure 4-18.

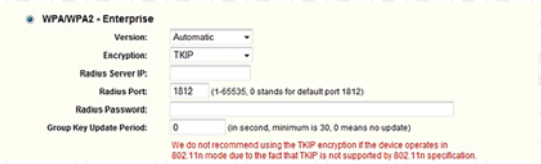


Figure 4-18

- **Radius Server IP** - Enter the IP address of the radius server.
- **Radius Port** - Enter the port used by the radius server.

- **Radius Password** - Enter the password for the radius server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or higher. Enter 0 to disable the update.

* **WPA-PSK/WPA2-PSK Personal** - It is the WPA/WPA2 authentication type based on pre-shared passphrase.

- **Version** - Choose the WPA-PSK encryption method from the drop-down list. The default setting is **Automatic**, which instantly sets **WPA-PSK** (Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA), based on the wireless station's capability and request.
- **Encryption** - When **WPA-PSK** or **WPA** is set as the Authentication Mode, you can either select **Automatic**, or **TKIP** or **AES** as your Encryption type.

Note:

If you check the **WPA-PSK/WPA2-PSK** radio button and choose TKIP encryption, the following window will be displayed.

Figure 4-19

- **PSK Passphrase** - You can enter an ASCII string between 8 and 63 characters long, or 8 to 64 Hexadecimal characters.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or higher. Enter "0" to disable the update.

Be sure to click the **Save** button to store your settings on this page.

4.6.3 Wireless MAC Filtering

Go to "**Wireless → MAC Filtering**" in the menu, so that you can control the wireless access by configuring the Wireless MAC Address Filtering feature, as shown in Figure 4-20.

Figure 4-20 Wireless MAC address Filtering

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disable**.

* **MAC Address** - The wireless station's MAC address that you want to filter.
* **Status** - It displays the current status of this entry, either Enabled or Disabled.
* **Description** - A short description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The "Add or Modify Wireless MAC Address Filtering entry" page will appear, as shown in Figure 4-21 below:

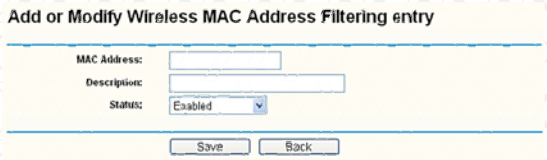


Figure 4-21 Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the **MAC Address** is XX-XX-XX-XX-XX-XX (X represents any hexadecimal digit). For example: 00-0A-EB-00-07-8A.
2. Enter a short description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Status** – Select **Enabled** or **Disabled** as the status for this entry, from the **Status** pull-down list.
4. Click the **Save** button to store this entry.

To modify or delete an existing entry:

1. Click the **Modify** button next to in the entry you want to change. If you want to erase this entry, click on **Delete**.
2. Proceed with the changes you want to make.
3. Click the **Save** button to save your settings.

Click the **Enable All** button to activate all entries
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries
Click the **Next** button to go to the following page
Click the **Previous** button to return to the last page.
For example: If you want wireless station A with MAC address 00-0A-EB-00-07-8A and wireless

station B with MAC address 00-0A-EB-00-23-11 to be able to access the Router, while all the other wireless stations are denied access, you must configure the Wireless **MAC Address Filtering feature** using the steps detailed below:

1. Click the **Enable** button to activate this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for Filtering Rules.
3. Delete all or disable all entries, if there are any entries already.
4. Click the **Add New** button and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the **MAC Address** field; then enter wireless station A/B in the Description field, while selecting **Enabled** in the Status field. Click the **Save** and the **Back** button to complete this procedure.
   The filtering rules just configured should look similar to the following list:

4.6.4 Wireless Advanced Settings

Go to "**Wireless →Wireless Advanced**" in the menu, in order to configure the advanced settings of your wireless network.

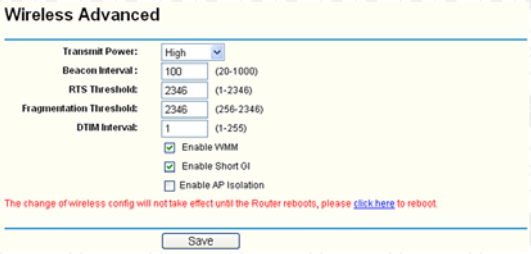


Figure 4-22 Wireless Advanced

* **Transmit Power** - You can specify the transmit power of the router in this field. The available settings are High, Middle or Low. High is the default setting, which is also recommended.
* **Beacon Interval** - Set the desired beacon interval in this field, ranging from 20-1000 milliseconds. Beacons are packets broadcast by the router to synchronize a wireless network. The beacon Interval value indicates the frequency of the beacon. The default value is set to "100".
* **RTS Threshold** - You can specify the RTS (Request to Send) Threshold in this field. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
* **Fragmentation Threshold** - It specifies the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation Threshold too low may result in poor network performance due to the generation of an excessive number of packets. 2346 is the default setting, which is also the value recommended.

* **DTIM Interval** - This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
* **Enable WMM** - WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended to have this feature enabled.
* **Enable Short GI** - This function is enabled by default and used to set the time the receiver waits for RF reflections to settle out before sampling data. Using a short Guard Interval can increase throughput.
* **Enabled AP Isolation** - This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

Note:
If you are not really familiar with the setting of the items in this page, it is strongly recommended to keep the default values unchanged; otherwise, it may result in lower wireless network performance.

4.6.5 Wireless Statistics

Go to "**Wireless → Wireless Statistics**" in the menu, so you can visualize the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

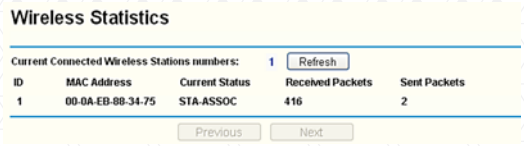


Figure 4-23 Wireless stations linked to the router

* **MAC Address** - The connected wireless station's MAC address.
* **Current Status** - The connected wireless station's operation status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
* **Received Packets** - Packets received by the station.
* **Sent Packets** - Packets broadcast by the station.

No values on this page can be changed. Click on the **Refresh** button to update this page and to show the wireless stations currently connected to the router. If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the following page and click the **Previous** button to return the last page.

Note:

This page will be refreshed automatically every 5 seconds.

4.7 DHCP

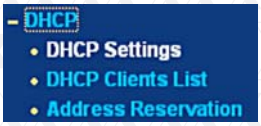


Figure 4-24 The DHCP menu

There are three submenus under **DHCP** (shown in Figure 4-24): **DHCP Settings, DHCP Clients List** and **Address Reservation**. Click on any of these items in order to configure the corresponding function.

4.7.1 DHCP Settings

Go to "**DHCP → DHCP Settings**" in the menu, in order to configure the DHCP Server in this page (shown in Figure 4-25).The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN.

Figure 4-25 DHCP Settings

* **DHCP Server** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network. Otherwise, you must configure the computer manually.
* **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
* **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168. 0.199 is the default end address.
* **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount of time in minutes that this dynamic IP Address will be "leased" to the user. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
* **Default Gateway** - (Optional) This field is used to enter the IP address of the LAN port of the router, default value is 192.168. 0.1
* **Default Domain** - (Optional) This field is used to enter the domain name of your network.
* **Primary DNS** - (Optional) This field is used to enter the DNS IP address provided by your ISP. Consult your ISP if you do not have this value.
* **Secondary DNS** - (Optional) This field is used to enter the IP address of another DNS server if your ISP provides two DNS servers.

Note:
To use the DHCP server function of the router, you must configure all computers on the LAN in the "**Obtain an IP Address automatically**" mode.

4.7.2 DHCP Clients List

Go to "**DHCP → DHCP Clients List**" in the menu, in order to visualize the information about the clients linked to the router, as displayed in the following screen (Figure 4-26).

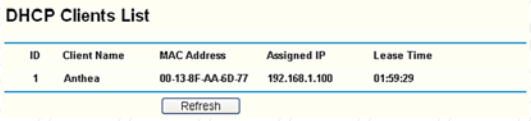


Figure 4-26 DHCP Clients List

* **ID** - The index of the DHCP Client.
* **Client Name** - The name used to identify the DHCP client.
* **MAC Address** - The MAC address of the DHCP client.
* **Assigned IP** - The IP address that the router has allocated to the DHCP client.
* **Lease Time** - The lease granted to the DHCP client. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

No values on this page can be changed. Click the Refresh button to update this page and to show the devices currently linked to the router.

4.7.3 Address Reservation

Go to "**DHCP → Address Reservation**" in the menu, in order to visualize and add reserved addresses for clients, using the screen displayed below (Figure 4-27). When you specify a reserved IP address for a PC on the LAN, that PC will consistently receive the same IP address every time it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

Figure 4-27 Address Reservation

* **MAC Address** - The MAC address of the PC that you want to reserve IP address for.
* **Assigned IP Address** - The IP address reserved for the router.
* **Status** - This field displays either Enabled or Disabled, as the current status for the device.

To Reserve IP addresses:

1. Click the **Add New** button. (The dialog box as shown in figure 4-28 will appear).
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format) and the IP address in dotted-decimal notation belonging to the the computer you wish to add.
3. Click the **Save** button when finished.

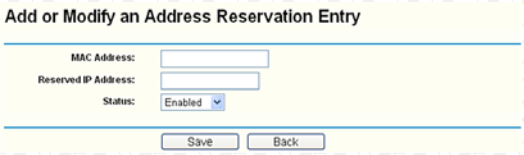


Figure 4-28 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** button next to the entry you want to change. If you want to erase this entry, click on **Delete**.
2. Proceed with the changes you want to make.
3. Click the **Save** button.

Click the **Enable All** button to activate all entries
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries.
Click the **Next** button to go to the following page.
Click the **Previous** button to return to the last page.

4.8 USB Settings

Figure 4-29 USB Settings menu

There are four submenus under USB Settings (shown in Figure 4-29): **Storage Sharing**, **FTP Server, Media Server** and **User Accounts**. Click on any of these items in order to configure the corresponding function.

4.8.1 Storage Sharing

Go to "**USB Settings → Storage Sharing**" in the menu, in order to configure a USB disk drive linked to the router, as shown below in Figure 4-30.

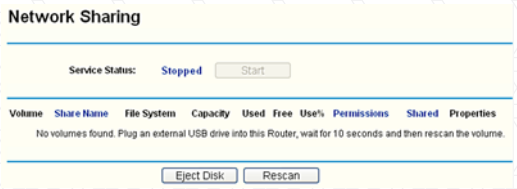
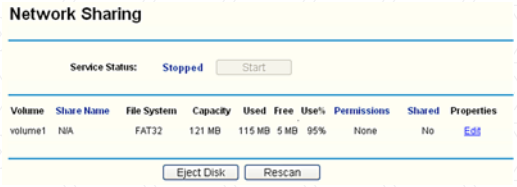


Figure 4-30 Network Sharing

* **Service Status** - Indicates the Network Sharing service's current status.
* **Volume** - The volume name of the USB drive users have access to.
* **Share Name** - The specified share name of the volume.
* **File System** - The file system on the partition can be FAT32 or NTFS.
* **Capacity** - The storage capacity of the USB driver.
* **Used** - The used space of the USB driver.
* **Free** - The available space of the USB driver.
* **Use%** - The percentage of the used space.
* **Permissions** - Read-Only or Read/Write access to the volume designated as the share.
* **Shared** - Indicates the shared or non-shared status of the volume.
* **Properties** - Displays the **Edit** link to specify a volume that the Network Sharing users can access.

Click the **Start** button to initiate the Network Sharing service.
Click the **Stop** button to cancel the Network Sharing service.
Click the **Eject Disk** button to safely remove the USB storage device that is connected to the USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.
Click the **Rescan** button to start a new scan.
Follow the instructions below to set up your router as a file server:

1. Plug an external USB hard disk drive or USB flash drive into this router.
2. Click the **Rescan** button to find the USB drive that has been attached to the Router. The following screen will appear, as shown below.



3. To specify a volume that the Network Sharing users can access, click the **Edit** link in the **Properties** column and configure the corresponding settings in figure 4-31.
4. Set the Network Sharing user's username and password on the **User Accounts** page.
5. Click the Start button to initiate the Network Sharing service.
6. Network Sharing users within your local network

can now access files on the USB drive from Internet Explorer at its Share Name followed by the Router's LAN IP address, for example: \\192.168.0.1\MyShare.

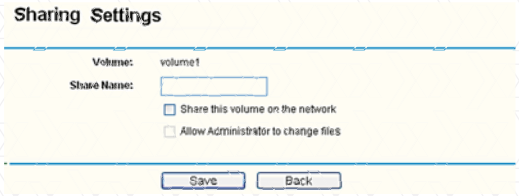


Figure 4-31 Sharing Settings

Note:

1. The router cannot automatically locate the new USB drive. You have to click the **Rescan** button manually to display the list of volumes and information about them.
2. The new settings will not take effect until you restart the service.
3. To unplug the USB drive, click **Eject Disk** button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.
4. Mounted volumes are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.
5. NTFS is the recommended file system for Network Sharing because it supports several features that the other file systems do not, such as large files and large volume support.