

NEXXT
SOLUTIONS



Viking 150 / Polaris 150
Wireless-N 3G Router | User Manual

Copyright Statement

Nexxt Solutions™ is a registered trademark. Other trademarks or brand names contained herein are the trademarks or registered brand names of their respective owners. Copyright of the whole product as integration, including its accessories and software, belongs to Nexxt Solutions Ltd. No individual or third party is allowed to copy, plagiarize, reproduce, or translate it into other languages, without express consent from Nexxt Solutions, Ltd. All of the photos and product specifications mentioned in this manual are used as reference only. Upgrades of software and hardware may occur, and should there be any changes, Nexxt Solutions shall not be responsible for notifying about any such modifications in advance. If you would like to know more about our products, please visit our website at www.NexxtSolutions.com.

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.

CONTENTS

Package Contents

Chapter 1 Introduction

- 1.1 Overview of the router
- 1.2 Main features
- 1.3 Panel layout
- 1.3.1 Polaris 150
- 1.3.2 Viking 150
- 1.4 LED indicator description
- 1.4.1 Polaris 150
- 1.4.2 Viking 150
- 1.5 System requirements
- 1.6 Installation environment requirements

Chapter 2 Quick Installation Guide

- 2.1 Preliminary steps
- 2.1.1 Polaris 150 hardware connection
- 2.1.2 Viking 150 hardware connection
- 2.2 Quick setup
- 2.2.1 Network configuration
- 2.2.2 Router configuration using 3G router mode

Chapter 3 Router configuration

- 3.1 Login
- 3.2 Status
- 3.3 Operation modes
- 3.3.1 3G router mode
- 3.3.2 Wireless router mode
- 3.3.3 Standard AP mode
- 3.4 PC configuration
- 3.5 WPS
- 3.6 Network
 - 3.6.1 Internet access
 - 3.6.2 3G Preferred
 - 3.6.3 3G only
 - 3.6.4 WAN Preferred
 - 3.6.5 WAN only

4 MAC clone

5. LAN

6. Wireless

- 6.1 Wireless settings
- 6.2 Wireless security
- 6.3 Wireless MAC filtering
- 6.4 Wireless advanced settings
- 6.5 Wireless statistics

7. DHCP

- 7.1 DHCP settings
- 7.2 DHCP Clients list
- 7.3 Address reservation

8. Forwarding

- 8.1 Virtual servers
- 8.2 Port triggering
- 8.3 DMZ
- 8.4 UPnP

9. Security

- 9.1 Basic security
- 9.2 Advanced security
- 9.3 Local management
- 9.4 Remote management
- 9.5 Parental control
- 9.6 Access control

10. Rule

- 10.1 Host
- 10.2 Target
- 10.3 Schedule

11. Advanced routing

- 11.1 Static routing list
- 11.2 System routing table

12. Bandwidth control

- 12.1 Control settings
- 12.2. Rules list

13. IP & MAC Binding

- 13.1 Binding settings
- 13.2 ARP List

14. Dynamic DNS

- 14.1 Comexe.cn DDNS
- 14.2 Dyndns.org DDNS
- 14.3 No-ip.com DDNS

15. System tools

- 15.1 Time settings
- 15.2 Diagnostic
- 15.3 Firmware upgrade
- 15.4 Factory defaults
- 15.5 Backup & Restore
- 15.6 Reboot
- 15.7 Password
- 15.8 System log
- 15.9 Statistics table

Appendix A: General specifications

Appendix B: Glossary

Package contents

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

- One wireless-N 3G Router
- One DC Power adapter
- One USB cable (for Polaris 150 only)
- One network cable
- One Quick Installation Guide

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

Chapter 1.

Thank you for purchasing our Wireless-N 3G Router, the Viking 150 or the Polaris 150 model, from Nexxt Solutions.

1.1 Product overview

The Viking 150/Polaris 150 gives you the freedom to quickly set up a stable and high speed wireless network, up to 150Mbps, on-the-go and share a 3G connection. By connecting a UMTS/HSPA/EVDO USB Card to the router, a Wi-Fi hotspot is instantly established allowing users to share an Internet connection anywhere 3G coverage is available. So whether you're on the train, camping, or at a construction site, you'll have a reliable wireless connection to accommodate your networking needs.

Incredible speed

The Viking 150/Polaris 150 provides up to 150Mbps, faster than that of traditional 11g products, surpasses 11g performance enabling the use of high bandwidth-consuming applications such as HD Videos. It provides 150Mbps wireless connectivity for the network share on the go.

Multi-level security

The Viking 150/Polaris 150 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 Viking 150/Polaris 150 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.

1.2 Main features

- The Polaris 150 is a travel size design, small enough to take on the road
- The Polaris 150 provides a one 10/100M Auto-Negotiation RJ45 Ethernet WAN/LAN port, one 3G/3.75G USB port and one Micro USB port for power
- The Viking 150 provides four 10/100M Auto-negotiation Ethernet LAN ports, one 3G/3.75 USB port and one 10/100M WAN port
- Compatible with IEEE 802.11b/g/n, IEEE802.3/3u
- Compatible with UMTS/HSPA/EVDO USB 3G/3.75G Modem
- Compatible with Apple products, Android devices, Kindle and majority of portable Wi-Fi devices
- Wireless N speed up to 150Mbps
- Supports WPS security setup
- Provides WEP, WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security
- Polaris 150 can be powered by laptop or power adapter with low power consumption
- Supports 3G router Mode, WISP Client router mode, and AP Mode
- Supports 3G/PPPoE/Dynamic IP/Static IP/PPTP/L2TP Cable Internet access
- Supports VPN Pass-through, Virtual Server and DMZ Host
- Supports UPnP, Dynamic DNS, Static Routing
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Built-in NAT and DHCP server supporting automatic and dynamic IP address distribution
- 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

1.3 Panel layout

1.3.1 Polaris 150

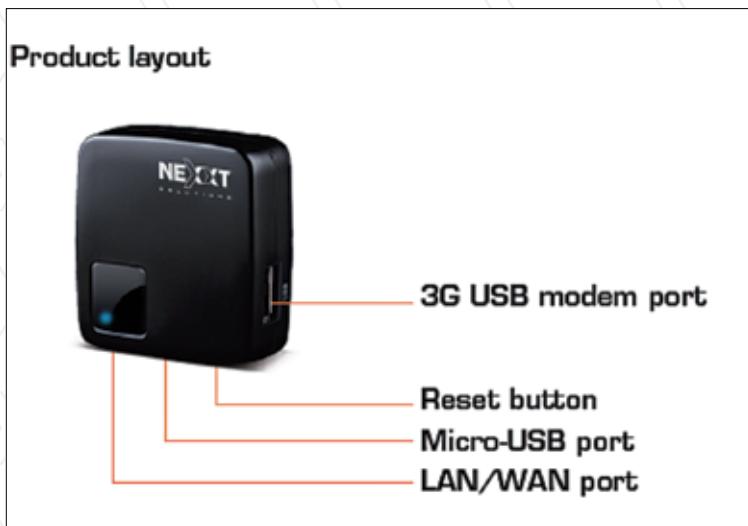


Figure 1-1

- **3G USB modem port:** This port is used to plug a 3G modem/card.
- **Reset button:** Use it to reset the router to its factory default values.
- **Micro USB port:** This port is used to connect the supplied power adapter.
- **LAN/WAN port:** This RJ45 Ethernet port can be LAN or WAN port depending on the operation mode selected.

1.3.2 Viking 150

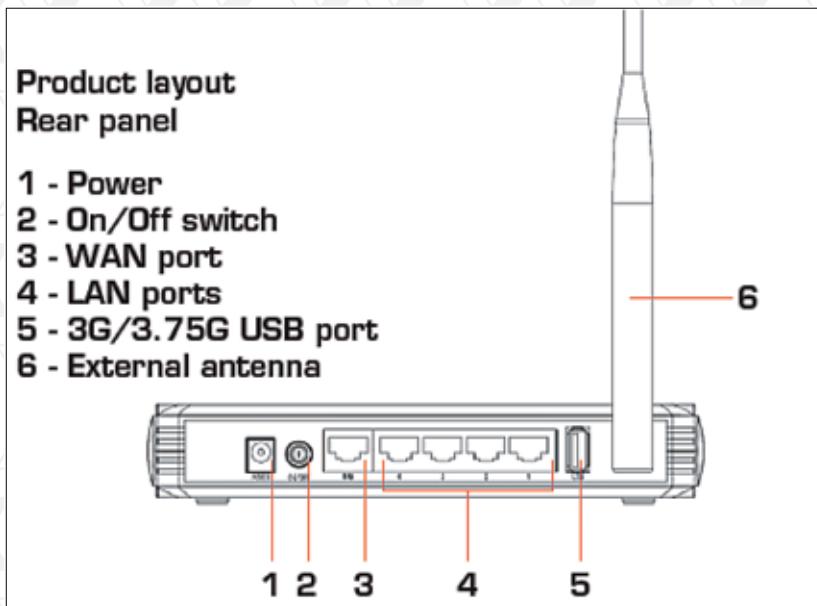


Figure 1-2

Nexxt Solutions – Wireless-N 3G router

1. Power: Connect the supplied power adapter to this jack.
2. On/Off switch: Use this switch to power the unit on and off.
3. WAN port: This RJ45 port is where you will connect the DSL/cable modem, or Ethernet line.
4. LAN ports (1-4): Connect your laptop or desktop computers in your network to any of these 5. RJ45 Ethernet ports.
6. USB: This port is used to plug a 3G/3.75G USB modem/card.
- External antenna: Wirelessly broadcasts your signal throughout your home or office.

1.4 LED indicator description

1.4.1 Polaris 150

Status	Description
On	The router is working properly
Flashing	The router is receiving and transferring data
Off	The router is not working or connected properly

1.4.2 Viking 150

Name	Status	Indication
PWR	Off	Power is off.
	On	Power is on.
SYS	On	The router is initializing.
	Flashing	The router is working properly.
	Off	The router has a system error.
WLAN/LAN1-4	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port, but no activity is being detected.
	Flashing	There is an active device linked to the corresponding port.
3G	On	The USB 3G dongle is connected.
	Flashing	Data is being received or sent through the 3G dongle.
	Off	No device is linked to the USB port.
WPS/Reset	Flashing slowly	A wireless device is connecting to the network by WPS function. This process takes around 2 minutes to complete.
	On	A wireless device has been successfully added to the network by WPS function. The LED will remain lit for about 5 minutes.
	Flashing quickly	A wireless device failed to be added to the network by WPS function.
	Button	Press and hold for 7-10 seconds to reset the router to its factory default values.

Note: After a device is successfully added to the network by the WPS function on the Viking 150, the corresponding LED will remain on for about 5 minutes before going off.

1.5 System requirements

- 3G Mobile Broadband Internet Access Service (With a UMTS/HSPA/EVDO USB dongle) or Wired Broadband Internet Connection from ISP.
- PCs with a working Ethernet adapter or wireless adapter.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer 5.0, Netscape Navigator 6.0 or above.

1.6 Installation environment requirements

- Place the router in a well ventilated place, far away from any heat generating device, heater or heating vents.
- Avoid 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

Chapter 2.

Installation guide

2.1 Preliminary steps

There are a total of three operation modes supported by the Polaris 150: 3G Router, Wireless router, Standard AP (including Access Point, Repeater, Bridge with AP, and Client). Set up the router according to the mode you are going to apply.

2.1.1 Polaris hardware connection

Note: By default, the Polaris 150 operates as a 3G router

1. First, connect one end of the supplied USB cable into micro USB port on the router, and the other end into the power adapter, before plugging the power adapter to a standard electrical wall socket.
2. Insert the user-supplied 3G modem into the USB port on the device.
3. Then, open the web-based management page of the router in order to configure all applicable parameters and to quickly establish a connection to the internet.
4. In this mode, the LAN/WAN port is used as LAN port for wired connection with your computer while all other devices can share the Internet wirelessly.

2.1.2 Viking 150 hardware connection

Note: By default, the Viking 150 operates as a 3G router

1. First, connect one end of the supplied power adapter to the AC input jack located on the rear panel of the router, before plugging the other end to a standard electrical wall outlet.
2. Insert the user-supplied 3G/3.75G modem into the USB port on the device.
3. Then, open the web-based management page of the router in order to configure all applicable parameters and to quickly establish a connection to the internet.
4. In this mode, the LAN ports are used for linking your network devices to your computer using wired connection, while all other devices can share the Internet wirelessly.

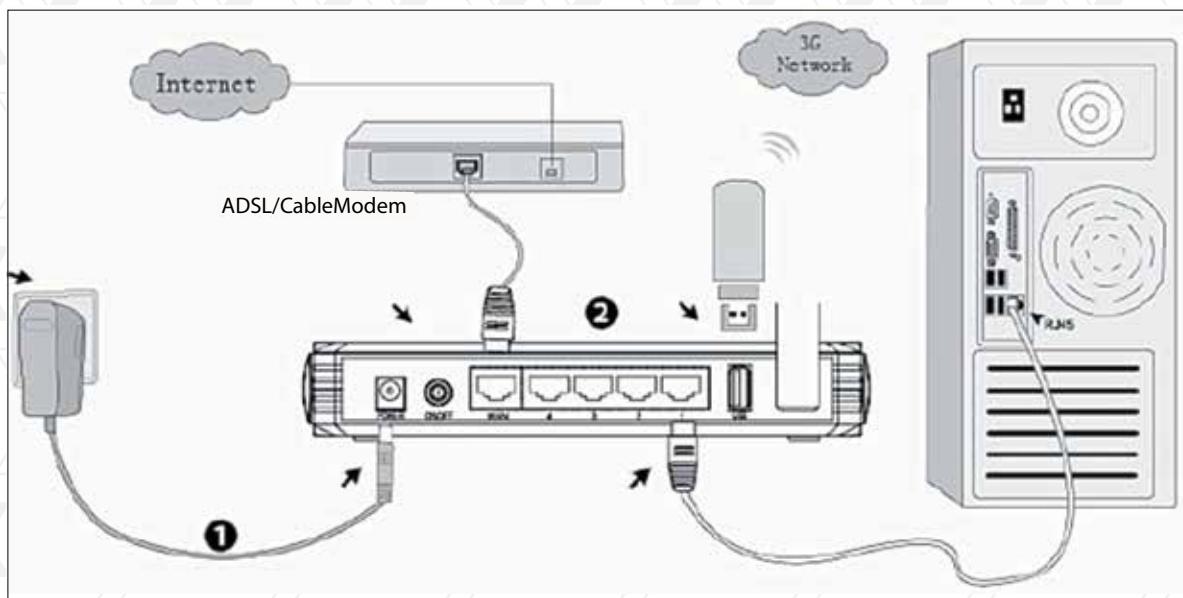


Figure 1-3

2.2 Quick setup

2.2.1 Network configuration

We recommend connecting your mobile router to your PC wirelessly. Therefore, you must make sure that your PC is equipped with a wireless adapter before proceeding. (We recommend using our Nexxt Solutions wireless adapters. Check our website for further information).

Please note that in this quick installation guide, we use Windows 7 to illustrate the setup process.

1. Go to **Start → Control Panel → Network and Internet → Network and Sharing Center → Change adapter settings**. Right click on **Wireless Network Connection**, and select **Properties**.



Figure 2-1

2. On the item list, click on **Internet Protocol Version (TCP/IPv4)**



Figure 2-2

3. Select both options: **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to finish and exit the PC configuration.



Figure 2 -3

4. Next, click on the wireless connection icon in the lower right corner of the computer's desktop. Then, click on the refresh button, select the default SSID of the router and check the **Connect automatically** box to enable the connection.



Figure 2-4

- Click the **Connect** button. When **Connect** appears on the screen, it means that you have successfully connected to your wireless router.

Note: The default SSID of the network is Nexxt_xxxxxx (whereby xxxxxx represents the last unique six characters of each router's MAC address). No default wireless password is required at this point.

2.2.2 Router configuration

- Open a web browser and enter **192.168.0.1** on the address field, and press the **Enter** key. When prompted, enter **admin** as the default user name and password, both in lower case. Click **OK** to continue



Figure 2-6 Polaris 150



Figure 2-7 Viking 150

2. After successfully logging in, configure the router according to the mode selected. In this guide, the 3G Only (Viking 150) or 3G Router Mode (Polaris 150) is used to illustrate the process.
3. Select **Quick Setup** from the list on the left column, in order to configure your router. Then click Next.

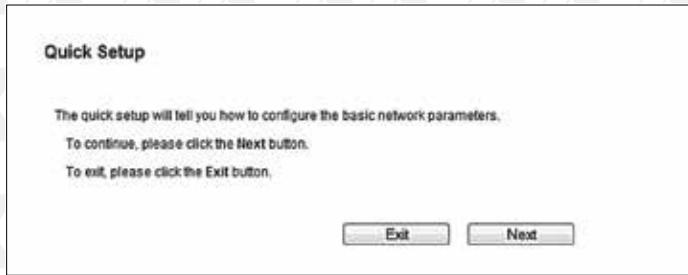


Figure 2-8

4. Choose the 3G Router mode (for Polaris 150) or the 3G Only mode (for Viking 150) in the Quick Setup- Internet Access window. Click **Next** to move on to the next step.



Figure 2-9 - Polaris 150



Figure 2-10 - Viking 150

5. Select your **Location** and **Mobile ISP** from the preset drop down list. Please note that the user can set these parameters manually if the preset options are not found in the list. That can be done by checking the Set the **Dial Number, APN, User Name and Password manually** box. Click **Next** when done.

Nexxt Solutions – Wireless-N 3G router



Figure 2-11

6. Use the **Quick Setup-Wireless** dialog box to configure your wireless parameters of the router. We recommend selecting a unique and easy to remember wireless network name (SSID), your Region, in addition to setting up a WPA-Personal/WPA2-Personal wireless security password to prevent unauthorized access to your network. Click **Next** to continue.



Figure 2-12

7. On the **Quick Setup - Finish** dialog box, click the **Reboot** button to complete the Quick Setup procedure.

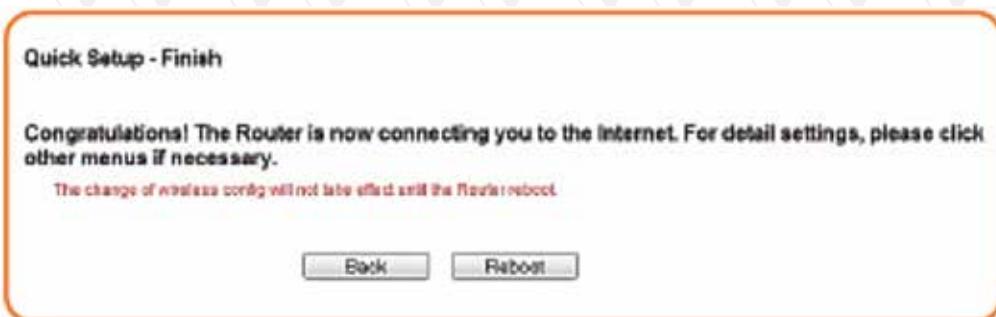


Figure 2-13

Note: Once the device reboots, reconnect to your wireless network using the newly programmed SSID and Password, if you have set them up in the steps described above. Now, you are ready to start enjoying your connection to the internet.

3.1 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.

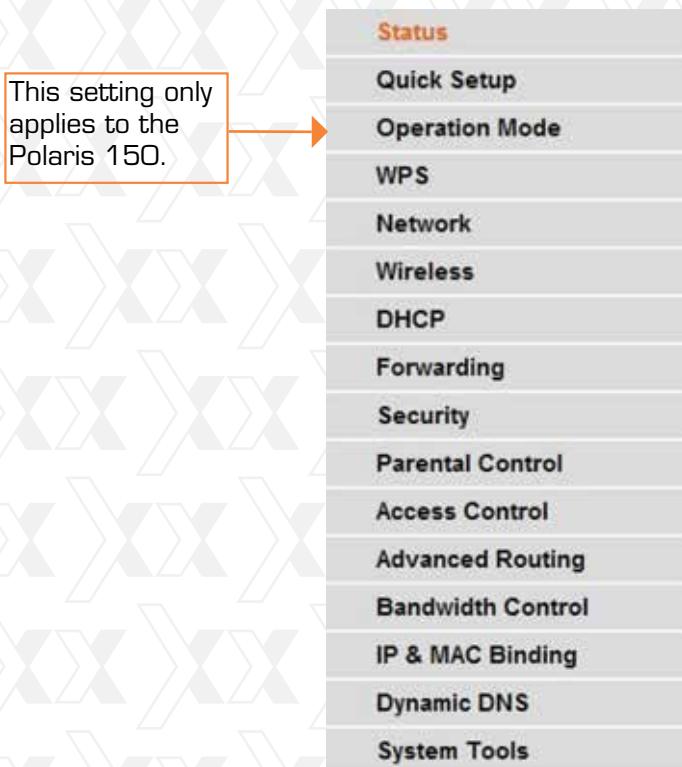


Figure 3-1

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

3.2 Status

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

Nexxt Solutions – Wireless-N 3G router

Status	
Firmware Version:	3.15.1 Build 130403 Rel.38084n
Hardware Version:	ARNPRI54U1 v1 00000000
LAN	
MAC Address:	14-E6-E4-E3-40-8A
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Wireless Radio:	Enable
Name (SSID):	Nextt_E340BA
Channel:	Auto (Current channel 11)
Mode:	11sgn mixed
Channel Width:	Automatic
MAC Address:	14-E6-E4-E3-40-8A
WDS Status:	Disable
3G	
3G USB Modem:	Unplugged.
Signal Strength:	0%
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
DNS Server:	0.0.0.0 , 0.0.0.0
Traffic Statistics	
Received	0
Bytes:	0
Packets:	0
0	0
System Up Time:	0 days 00:07:41
<input type="button" value="Refresh"/>	

Figure 3-2 Router Status

3.3 Operation modes (Polaris 150 only)

Go to **Operation mode**, and you will be able to see the different modes the router is able to operate in, as explained below.

3.3 Operation modes (Polaris 150 only)

In this mode, the device enables multiple users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at 3G Router mode.

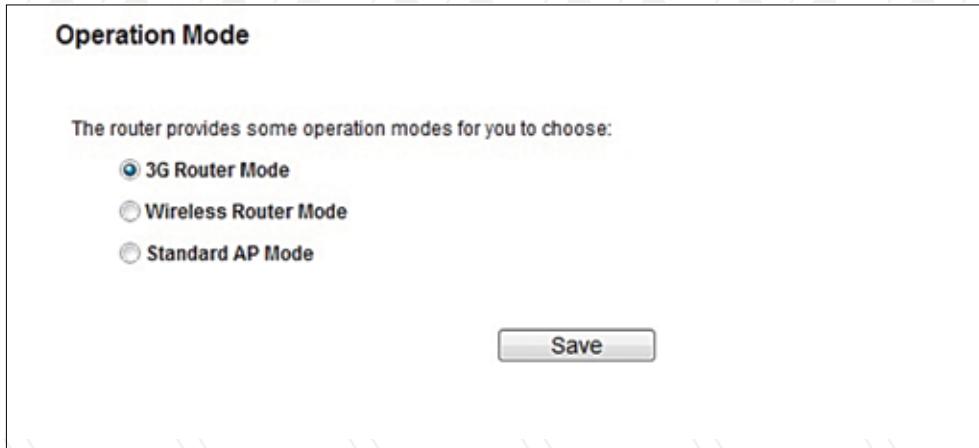


Figure 3-3

3.3.2 Wireless router mode

In this mode, the device enables multiple users to share the Internet. The LAN devices share the same IP from the ISP through a wireless port. While connecting to ISP, the Ethernet port works as a WAN port at Wireless Router mode.

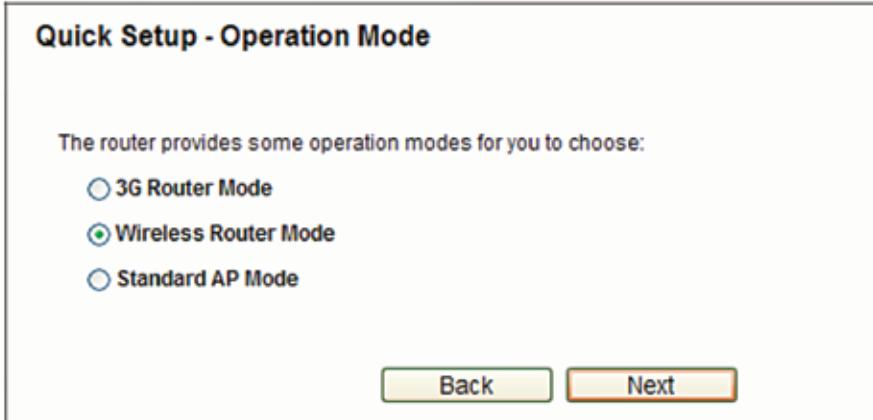


Figure 3-4

3.3.3 Standard AP mode

In this mode, the device enables multiple users to access and provides several wireless modes, such as AP, Client, Repeater and so on.

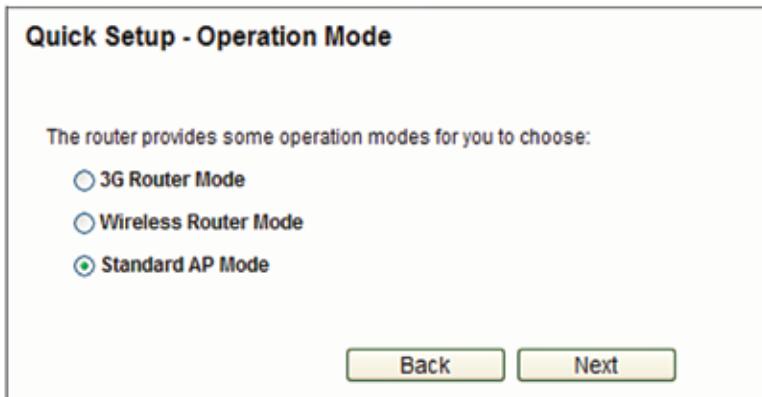


Figure 3-5

Note: The router will reboot automatically after you click the **Save** button.

3.4 PC configuration

Go to **Start → Control Panel → Network and Internet → Network and Sharing Center → Change adapter settings**. Right click on **Wireless Network Connection**, and select **Properties**.

Follow the same steps **3G Router mode**, **Wireless router mode** and **Standard AP mode**

3.5 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.

Note: WPS function is disabled by default. To do the below steps, you must enable this option.

a. Open the **WPS** menu. The following screen (shown in Figure 3-7) will appear.

- 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.
- Disable PIN of this device - WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- Add device - You can add a new device to the existing network manually by clicking this button.

a. **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: Click the **Enable WPS** button to trigger the WPS function in Figure 3-7, and click the **Add device** button in Figure 3-7, then the following screen will appear.

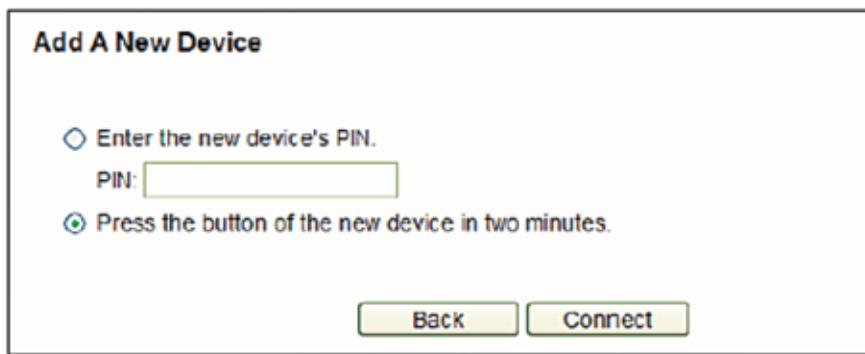


Figure 3-7 Add a new device

Step 2: Choose **Press the button of the new device in two minutes** and click **Connect**.

Step 3: For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the WPS as below, and click **Next**.



Figure 3-8 The WPS Configuration Screen of Wireless Adapter

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



Figure 3-9 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: Configure the wireless adapter. Please choose **Enter a PIN into my access point or a registrar** in the configuration utility of the WPS as below, and click **Next**.



Figure 3 -10 WPS Configuration Screen of wireless adapter

Note: In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Step 2: Configure the router. Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 3-11, then the following screen will appear.

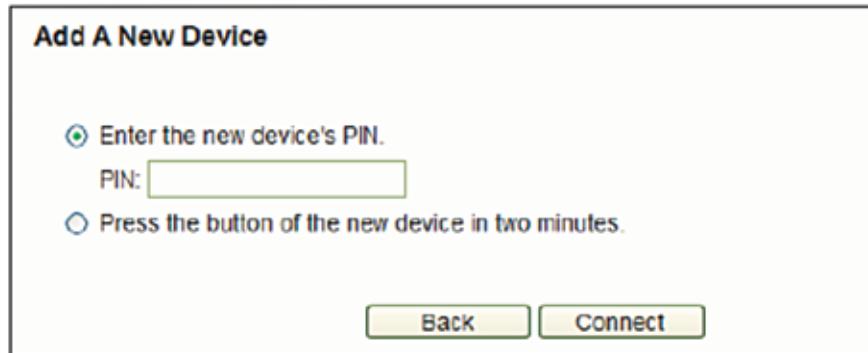


Figure 3-11

Step 3: Choose **Enter the new device's PIN** and enter the **PIN** code of the wireless adapter in the field behind **PIN** in the previous figure. Then click **Connect**.

Note: The PIN code of the wireless adapter is always displayed on the WPS or WPS configuration screen.

Method Two: Enter the PIN from my router

Step 1: Get the current PIN code of the router in Figure 3-12 (each router has its unique PIN code. Take the PIN code 12345670 of this router, for example).

Step 2: For the configuration of the wireless adapter, please choose **Enter a PIN from my access point** in the configuration utility of the WPS as below, and enter the PIN code of the Router into the field **Access Point PIN**. Then click **Next**.



Figure 3-12

- c. You will see the following screen when the new device successfully connected to the network.



Figure 3-13 Add a new device

Note:

- 1.The status LED on the router will remain orange all the time if the device has been successfully added to the network (Viking 150 only).
- 2.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.

3.6 Network

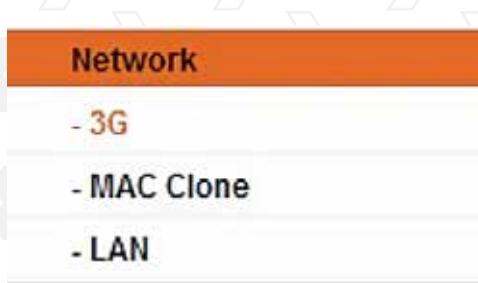


Figure 3-14 Polaris 150



Figure 3-15 Viking 150

As shown in Figure 3-14, there are several submenus under the Network setting (depending on the operation mode). **Internet Access** (Viking 150 ONLY), **3G**, **MAC Clone**, **WAN** (seen in **Wireless Router Mode**), **MAC Clone** (Viking 150 ONLY) and **LAN**. Click on any of these items in order to configure the corresponding function.

3.6.1 Internet access (Viking 150 only)

Go to **Network→Internet Access** in the menu in order to configure the 3G access mode as shown on the screen below. The router is designed to work with either WAN port or 3G USB modem, and supports automatic 3G switching if Ethernet WAN failover.

Quick Setup - Internet Access

The router provides some Internet access mode for you to choose:

- 3G Preferred** - Use 3G as the primary access, WAN as a backup. (RJ45 Ethernet Port as WAN)
- WAN Preferred** - Use WAN as the primary access, 3G as a backup. (RJ45 Ethernet Port as WAN)
- WAN Only** - Only use WAN as the access to the Internet. (RJ45 Ethernet Port as WAN)
- 3G Only** - Only use 3G as the access to the Internet. (RJ45 Ethernet Port as LAN)

[Back](#)

[Next](#)

Figure 3-16 Internet access mode

3.6.2. 3G Preferred

If you opt to use 3G as your primary connection, the device will try 3G access first. When 3G access fails and WAN access is available, or when no 3G USB modem is inserted, the device will switch to WAN access automatically. When the device is successfully connected to the 3G network, it will immediately cancel the WAN connection to switch back to 3G access.

3.6.3. 3G Only

The device will only attempt to connect to 3G. WAN access is disabled in this mode.

3.6.4 WAN Preferred

If you opt to use broadband as your primary connection, the device will try WAN access first. When WAN access fails, and 3G access is available, the device will switch to 3G access automatically. When the device is successfully connected to the WAN network, it will immediately cancel the 3G connection to switch back to WAN access.

3.6.5 WAN Only

The device will only attempt to access the broadband connection. 3G access is disabled in this mode.

Note:

1. When the **3G Preferred** or **WAN Preferred** is selected, the device will connect, disconnect or switch the access type being used automatically. Please note that the Connect/Disconnect button (on 3G, PPPoE, PPTP, L2TP) and other related parameters cannot be manually set.
2. The device is able to support the switch between 3G and WAN modes as long as the WAN connection is set to Dynamic IP, Static IP or PPPoE.

4.6.2 3G

Go to **Network → 3G** in the menu to configure the parameters of the 3G mode on the screen, as shown below. To use the 3G mode, you should first insert your USB modem on the USB port of the router. The USB modem parameters will be set automatically if the card is supported by the router. Take MA180 for example. If the USB modem that you have inserted is supported by the router, click **Advanced Settings**.



Figure 3-17

Note (Viking 150 only): 3G settings are unavailable when the Internet Access mode is set to **WAN Only**. If you want to use the 3G mode, you will have to change the settings explained on 4.6.1 Internet Access.

This screenshot shows the "3G" configuration page. At the top, it says "3G USB Modem: Identifying...". Below that is a note: "If your location or ISP is not listed, or the default Dial number / APN is not the latest one, or your ISP requires you to enter a new username and password, please click Advanced Settings to set them manually." It has dropdown menus for "Location: USA" and "Mobile ISP: AT&T". A note below says, "You have set the Dial Number and APN manually, if you want to modify, please enter the advance page." Under "Connection Mode:", there are three radio buttons: "Connect on Demand" (unchecked), "Connect Automatically" (checked), and "Connect Manually" (unchecked). A "Max Idle Time: 15 minutes (0 means it remains active all the time times)" input field is shown. Under "Authentication Type:", there are three radio buttons: "Auto" (checked), "PAP", and "CHAP". A note below says, "Notice: The default is Auto, do not change unless necessary." At the bottom are "Connect" and "Disconnect" buttons, and status indicators: "Connected" (grayed out), "Save" (blue), and "Modem Settings".

Figure 3-18 3G

- **Location** - Select the location where you're enjoying the 3G card.
- **Mobile ISP** - Select the ISP (Internet Service Provider) you apply to for 3G service. The router will show the default Dial Number and APN of that ISP.
- **Connect on Demand** - You can configure the device to disconnect your Internet service after a specified period of Internet inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, check the corresponding radio button. If you want your Internet connection to remain active all the time, 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.

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

- **Connect Automatically** - The connection can be re-established automatically after being disabled. Check the radio button to enable this option.
- **Connect Manually** - The device can be configured to be manually connected or disconnected. After a specified period of inactivity (Max Idle Time), the device will disable your Internet connection, without re-establishing your connection automatically once you attempt to access the Internet again. To use this option, check the corresponding radio button. If you want your Internet connection to remain active all the time, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you wish to keep the Internet active, unless a new link requested.

Note: Sometimes the connection cannot be terminated despite your setting a Max Idle Time. This is because some applications are continually linked to the internet in the background.

- **Authentication type** - Some ISPs require a specific authentication type. Confirm this information with your ISP or keep it in Auto mode. Three options are provided in this case.
 - **Auto:** The device automatically negotiates with the dialing server, so the type does not need to be specified. Auto is the default type setting.
 - **PAP:** Password Authentication Protocol. This protocol allows the device to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.
 - **CHAP:** Challenge Handshake Authentication Protocol. This protocol allows the router to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

Click the **Advanced settings** button to set up the advanced options in the screen as shown in Figure 3-19.

3G Advanced Settings

Location:	USA
Mobile ISP:	AT&T
<input type="checkbox"/> Set the Dial Number, APN, Username and Password manually	
Dial Number:	*99#
APN:	broadband
Username:	WAP@CINGULAR.COM (optional)
Password:	***** (optional)
MTU Size (in bytes):	1480 (The default is 1480, do not change unless it is necessary)
<input type="checkbox"/> Use the following DNS Servers	
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0 (Optional)

Save **Back**

Figure 3-19 3G Advanced settings

- **Location / Mobile ISP** – These two fields will display the location and the ISP you have selected in the previous page (shown in Figure 4-7). While you tick the below option Set the Dial Number and APN manually, there will be no specific information in these two fields.
- **Set the Dial Number and APN manually** - Tick the checkbox and then you are able to fill in the Dial Number and APN blanks below, if your ISP is not listed in the Mobile ISP field in the previous page (Figure 4-7).
- **Dial Number** - Enter the Dial Number provided by your ISP.
- **APN** - Enter the APN (Access Point Name) provided by your ISP.
- **Username/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **MTU Size** - The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Use the following DNS Servers** - If your ISP specifies a DNS server IP address for you, click the checkbox, and fill the Primary DNS and Secondary DNS blanks below. The Secondary DNS is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
- **Primary DNS** - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

Click the **Save** button to save your settings.

Click the **Back** button to return the previous page.

Click the **Modem settings** button (in Figure 3-20) if your 3G USB Modem is not supported by the Router, and then you will see the screen as shown in Figure 3-21. Parameters of your USB modem can be configured on this page.



Figure 3-20 3G USB Modem settings

There is already much 3G USB modem information embedded in the router. The USB modem parameters will be set automatically if the card is supported by the router. But when the router finds the card you just insert “unknown” to it, it will prompt you to set these parameters. The router can identify your “unknown” card if the correct parameters are in the list. We suggest you to do the “3G USB Modem Setting” only in such circumstance.

To add 3G USB Modem entries, follow the steps below.

1. Download a most recent 3G USB modem configuration file from our website.
2. Click the **Add New...** button in Figure 3-20, and then you will see Figure 3-21.
3. Click **Browse...** to select the path name where you save the downloaded file on the computer into the File blank.
4. Click the **Upload** button to upload the configuration.

Upload 3G USB Modem Configuration File

File:

Please Note: If you restore the Device's factory setting, the bin file will be lost. In the event that you do lose the bin file, you will need to re-upload it, or download our latest firmware from www.nexxtsolutions.com. The updated firmware will be installed into your 3G Device and restore all of its functions.

Figure 3-21 Add or Modify a 3G USB Modem entry

4.6.3 WAN

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

Note: WAN settings are unavailable when the Internet Access mode is set to 3G Only mode. Please change settings on 4.6.1 Internet Access if you want to use WAN.

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 3-22):

WAN

WAN Connection Type:	Dynamic IP	<input type="button" value="Detect"/>
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	
	<input type="button" value="Renew"/>	<input type="button" value="Release"/> Obtaining network parameters...
MTU Size (in bytes):	1500	(The default is 1500, do not change unless necessary.)
<input type="checkbox"/> Use These DNS Servers		
Primary DNS:	0.0.0.0	
Secondary DNS:	0.0.0.0 (Optional)	
Host Name:	ARNPR154U1	
<input type="checkbox"/> Get IP with Unicast DHCP (It is usually not required.)		
<input type="button" value="Save"/>		

Figure 3-22 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.)

WAN

WAN Connection Type:	<input type="button" value="Static IP"/> <input type="button" value="Detect"/>
IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/> (Optional)
MTU Size (in bytes):	<input type="text" value="1500"/> (The default is 1500, do not change unless necessary.)
Primary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
<input type="button" value="Save"/>	

Figure 3-23 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 3-24):

WAN

WAN Connection Type:

PPPoE Connection:

User Name:	<input type="text" value="username"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>

Secondary Connection: Disabled Dynamic IP Static IP (For Dual Access/Russia PPPoE)

The current Internet Access is 3G preferred. The Connection Mode and Max Idle Time could not be set manually.

Connection Mode:

- Connect on Demand
Max Idle Time: minutes (0 means remain active at all times.)
- Connect Automatically
- Time-based Connecting
Period of Time: from : (HH:MM) to : (HH:MM)
- Connect Manually
Max Idle Time: minutes (0 means remain active at all times.)

Disconnected!

Figure 3-24 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.
- **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 3-25 will be displayed:

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

ISP Specified IP Address: Use IP address specified by ISP
0.0.0.0

Detect Online Interval: Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)

Primary DNS: Use the following DNS Servers
0.0.0.0

Secondary DNS: (Optional)

Save **Back**

Figure 3-25 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 3-26):

WAN

WAN Connection Type: **BigPond Cable**

User Name: Password:

Auth Server: Auth Domain:

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

The current Internet Access is 3G preferred. The Connection Mode and Max Idle Time could not be set manually.

Connection Mode:

- Connect on Demand
- Connect Automatically
- Connect Manually

Max Idle Time: minutes (0 means remain active at all times.)

Save

Figure 3-26 WAN –BogPond cable

- **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.
e.g.

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 3-27):

WAN

WAN Connection Type: L2TP

User Name: username

Password: *****

Connection Mode: Connect on Demand Connect Automatically Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

Save

Figure 3-27 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 3-28):

WAN

WAN Connection Type: **PPTP**

User Name: **username**
Password: *********

Connection Mode: Connected on Demand Connect Automatically Connect Manually

Max Idle Time: **15** minutes (0 means remain active at all times.)

Save

Figure 3-28 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 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 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. 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 4-1below.

MAC Clone

WAN MAC Address:	<input type="text" value="38-83-45-65-BC-7B"/>	Restore Factory MAC
Your PC's MAC Address:	<input type="text" value="50-E5-49-C7-64-4F"/>	Clone MAC Address
Save		

Figure 4 -1 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 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.

5. LAN

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

LAN

MAC Address:	<input type="text" value="14-E6-E4-E3-40-8A"/>
IP Address:	<input type="text" value="192.168.0.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Save	

Figure 5-1 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.

6. Wireless



Figure 6-1 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 6-1): **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.

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.

Wireless Settings

Wireless Network Name: (Also called SSID)

Region:

Warning: Make sure to select the correct country to conform to local laws. Incorrect settings may cause interference.

Channel:

Mode:

Channel Width:

Enable Wireless Radio
 Enable SSID Broadcast
 Enable WDS Bridging

Figure 6-2 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 represents 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.

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.
- **Enable WDS Bridging** – Check this box to enable WDS Bridging. With this function, the router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown below. Make sure the following settings are correct.

The screenshot shows a configuration interface for enabling WDS Bridging. At the top, there is a checked checkbox labeled "Enable WDS Bridging". Below it, there are several input fields and dropdown menus:

- SSID(to be bridged):** An empty text input field.
- BSSID(to be bridged):** An empty text input field with a placeholder "Example:00-1D-0F-11-22-33".
- Survey**: A yellow button with the word "Survey" in blue text.
- Key type:** A dropdown menu with "None" selected.
- WEP Index:** A dropdown menu with "1" selected.
- Auth type:** A dropdown menu with "open" selected.
- Password:** An empty text input field.

At the bottom right of the form is a green "Save" button.

Figure 6-3

- **SSID (to be bridged)** - The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID (to be bridged)** - The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.

- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth Type** - This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
- **Password** - If the AP your router is going to connect needs password, you need to fill the password in this blank.

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).

The screenshot shows a configuration window for wireless security. At the top is a checked checkbox labeled "Enable WDS Bridging". Below it are two input fields: "SSID(to be bridged)" and "BSSID(to be bridged)", with a note "Example:00-1D-0F-11-22-33" next to the second field. A "Survey" button is located between them. Below these are dropdown menus for "Key type" (set to "None"), "WEP Index" (set to "1"), "Auth type" (set to "open"), and a "Password" field. At the bottom is a green "Save" button.

Figure 6-4

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.

WPA/WPA2 – Personal (Recommended) - It's the WPA/WPA2 authentication type based on pre-shared passphrase.

Version - you can choose the version of the WPA-PSK security on the drop-down list. The default setting is Automatic, which can select **WPA-PSK** (Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.

Encryption - When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

Note: If you check the **WPA/WPA2 – Personal (Recommended)** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 6-5.

WPA/WPA2 - Personal(Recommended)

Version: Automatic|Recommended

Encryption: TKIP

Password: 456EDC7A

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30.0 means no update)

We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

Figure 6-5

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

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

- WPA /WPA2** - 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 6-6

WPA/WPA2 - Enterprise

Version: Automatic

Encryption: TKIP

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

Figure 6-6

- 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.

WEP - It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in Figure 6-7

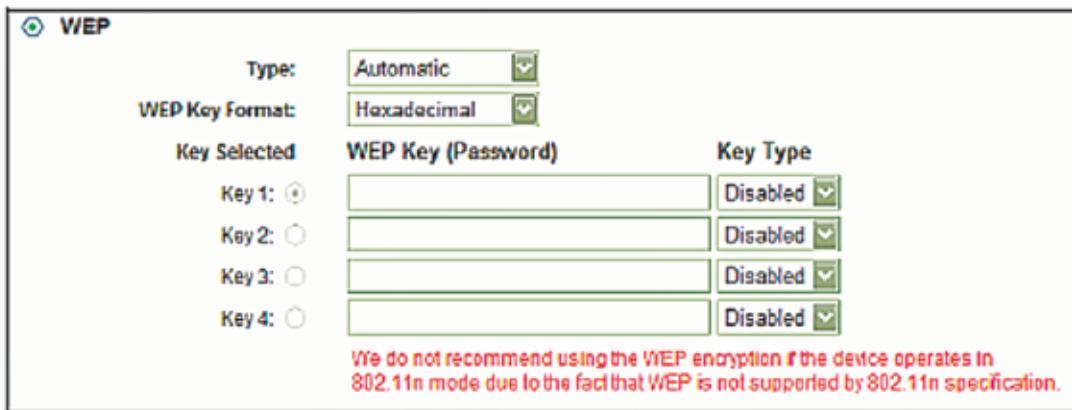


Figure 6-7

- **Type** - you can choose the type for the WEP security on the pull-down list. The default setting is Automatic, which can select Open system or Shared key authentication type 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 promoted) 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 promoted) 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 promoted) or 16 ASCII characters.

Note: If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

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 6-8.

Wireless MAC Filtering

Wireless MAC Filtering: **Disabled**

Filtering Rules

Deny the stations specified by any enabled entries in the list to access.
 Allow the stations specified by any enabled entries in the list to access.

ID	MAC Address	Status	Description	Modify

Figure 6-8 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 6-9 below:

Add or Modify Wireless MAC Address Filtering entry

MAC Address:	<input type="text"/>
Description:	<input type="text"/>
Status:	<input type="button" value="Enabled"/>

Figure 6-9 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:

Filtering Rules				
<input type="radio"/> Deny the stations specified by any enabled entries in the list to access. <input checked="" type="radio"/> Allow the stations specified by any enabled entries in the list to access.				
ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-8A	Enabled	Wireless station A	Modify Delete
2	00-0A-EB-00-23-11	Enabled	Wireless Station B	Modify Delete

Figure 6-10

6.4 Wireless advanced settings

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

Wireless Advanced

Beacon Interval :	<input type="text" value="100"/> (40-1000)
RTS Threshold:	<input type="text" value="2346"/> (256-2346)
Fragmentation Threshold:	<input type="text" value="2346"/> (256-2346)
DTIM Interval:	<input type="text" value="1"/> (1-255)
<input checked="" type="checkbox"/> Enable WMM	
<input checked="" type="checkbox"/> Enable Short GI	
<input type="checkbox"/> Enable AP Isolation	

Save

Figure 6-11 Wireless Advanced

- **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.

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.

Wireless Statistics				
Current Connected Wireless Stations numbers: 1 Refresh				
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	70-73-CB-08-FB-E1	STA-ASSOC	70	29
Previous Next				

Figure 6-12 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.

7. DHCP



Figure 7-1 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.

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.

DHCP Settings	
DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Address Lease Time:	120 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.1 (Optional)
Default Domain:	(Optional)
Primary DNS:	0.0.0.0 (Optional)
Secondary DNS:	0.0.0.0 (Optional)
Save	

Figure 7-2 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.

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 7-3).

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	GenericCase-PC	C8-3A-35-CF-E4-8A	192.168.0.100	01:31:14
Refresh				

Figure 7-3 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.

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 7-4). 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.

Address Reservation					
ID	MAC Address	Reserved IP Address	Status	Modify	
				Add New...	Enable All
Previous Next					

Figure 7-4 Address Reservation

- **MAC Address** – The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address** - The IP address that the device reserved.
- **Status** – It shows whether the entry is enabled or not
- **Modify** – Use this link to modify or delete an existing entry.

To reserve IP addresses:

- 1.Click the **Add new** button. (The dialog box as shown in Figure 7-5 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 computer you wish to add.
- 3.Click the **Save** button when finished.

The dialog box has a title bar 'Add or Modify an Address Reservation Entry'. It contains three input fields: 'MAC Address' (with a placeholder box), 'Reserved IP Address' (with a placeholder box), and 'Status' (set to 'Enabled' with a checked checkbox). At the bottom are 'Save' and 'Back' buttons.

Figure 7-5 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.

8. Forwarding



Figure 8-1 Forwarding menu

There are four submenus under **Forwarding** (shown in Figure 4-33): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click on any of these items in order to configure the corresponding function.

8.1 Virtual servers

Go to **Forwarding** → **Virtual servers** in the menu, in order to visualize and add virtual servers, as shown in the following screen (Figure 8-2). Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

Virtual Servers							
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify	
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>							
						<input type="button" value="Previous"/>	<input type="button" value="Next"/>

Figure 8-2 Virtual servers

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYYY format, XXX is the start port number, YYYY is the end port number).
- **IP Address** - The IP Address of the PC providing the service application.
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the Internal Port is the same as the Service Port, or enter a specific port number when Service Port is a single one.
- **Protocol** - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the router).
- **Status** - This field displays either Enabled or Disabled, as the current status for the device.

To setup a virtual server entry:

1. Click the **Add New...** button. (as in Figure 8-3).
2. Select the service you want to use from the **Common Service Port list**. If the **Common Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **IP Address** box.
4. Select the protocol used for this application, either TCP or UDP, or All.
5. Click on the check box to **Enable** the virtual server.
6. Click the **Save** button.

Add or Modify a Virtual Server Entry

Service Port:	(00000 or 00)
Internal Port:	(00, Only valid for single Service Port or leave a blank)
IP Address:	
Protocol:	ALL
Status:	Enabled
Common Service Port:	—Select One—
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 8-3 Add or Modify a Virtual Server Entry

Note: If your computer or server has more than one type of service available, please select a different service, and enter the same IP Address for that computer or server.

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.

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.

Note: If you set the service port of the virtual server as 80, you must set the Web management port on **System Tools -> Remote Management** page to be any other value except 80, such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.2 Port triggering

Go to **Forwarding -> Port triggering** in the menu, in order to visualize and add port triggering, as shown in the next screen (Figure 8-4). Some applications require multiple connections, like Internet games, video conferencing, Internet calling, and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications to let them work with a NAT router.

Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify

Figure 8-4 Port Triggering

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger port field.
 2. The router records this connection, opens the incoming port or ports associated with this entry in the **Port triggering** table, and associates them with the local host.
 3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.
- **Trigger port** - The port for outgoing traffic. An outgoing connection using this port will “Trigger” this rule.
 - **Trigger protocol** - The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the router).
 - **Incoming ports range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with “,”. For example, 2000-2038, 2050-2051, 2085, 3010-3030.
 - **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).
 - **Status** - It displays the current status of this entry, either Enabled or Disabled.

To add a new rule, follow the steps below.

1. Click the Add New... button. The following screen will be displayed, as shown in Figure 8-5.
2. Select a common application from the Common applications drop-down list, then the Trigger Port field and the Incoming ports field will be automatically filled. If the Common applications do not have the application you need, enter the Trigger port and the Incoming Ports manually.
3. Select the protocol used for Trigger Port from the Trigger protocol drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the Incoming protocol drop-down list, either **TCP** or **UDP**, or **All**.
5. Select **Enable** in Status field.
6. Click the **Save** button to store the new rule.

Add or Modify a Port Triggering Entry

Trigger Port:	<input type="text"/>
Trigger Protocol:	<input checked="" type="checkbox"/> ALL
Incoming Ports:	<input type="text"/>
Incoming Protocol:	<input checked="" type="checkbox"/> ALL
Status:	<input checked="" type="checkbox"/> Enabled
Common Applications:	<input type="button" value="--Select One--"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 8-5 Add or Modify a Triggering 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.

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

Note:

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule allows only to be used by a single host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

8.3 DMZ

Go to **Forwarding → DMZ**, in order to visualize and configure the DMZ host, as shown in the screen below (Figure 8-6). The DMZ host feature allows one local host to be exposed to the Internet so as to gain access to certain applications, such as Internet gaming or video-conferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled, and should also have a new static IP Address assigned to it, because its IP Address may be changed when using the DHCP function.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address: 0.0.0.0

Save

Figure 8-6 DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field.
3. Click the **Save** button.

Note: Once you set the DMZ host, the firewall protection for that host will be disabled.

8.4 UPnP

Go to **Forwarding** → **UPnP** in the menu, in order to visualize the information related to the **UPnP** (Universal Plug and Play) feature, as shown in the screen below (Figure 8-7). The UPnP architecture allows any compatible device, such as Internet computers, to access the local host resources or other networking equipment, as needed. UPnP devices on the LAN can be automatically discovered using the UPnP application.

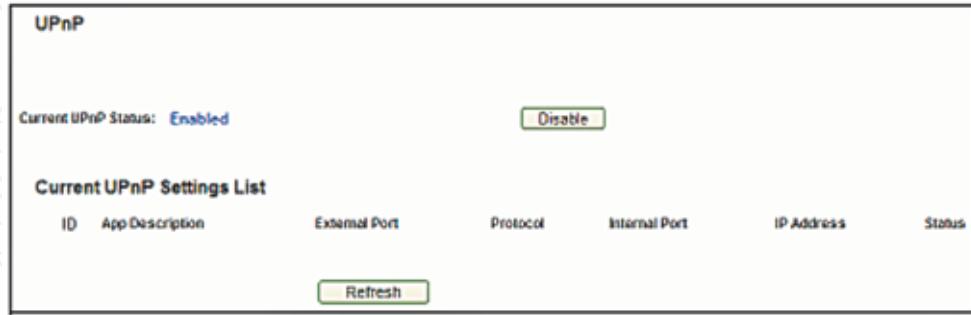


Figure 8-7 UPnP Setting

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the Enable or Disable button. Please note that since this feature is enabled by default, it may present a risk to security.
- **Current UPnP Settings List** - This table displays the current UPnP information.
- **App Description** - The description provided by the application in the UPnP request.
- **External Port** - External port, which the router opened for the application.
- **Protocol** - Shows which type of protocol is opened.
- **Internal Port** - Internal port, which the router opened for local host.
- **IP Address** - The UPnP device that is currently accessing the router.
- **Status** - The port status is displayed in this field. “Enabled” means that the port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

9. Security



Figure 9-1 Security menu

There are four submenus under the Security (shown in Figure 9-1): **Basic security**, **Advanced security**, **Local management** and **Remote management**. Click on any of these items in order to configure the corresponding function.

9.1 Basic security

Go to **Security → Basic security**, in order to configure the basic security settings, as shown in the screen below (Figure 9-2).

The screenshot displays the 'Basic Security' configuration interface. It is organized into three main sections: Firewall, VPN, and ALG. Each section contains several configuration options with enable/disable radio buttons. A 'Save' button is located at the bottom right of the form.

Firewall	
SPI Firewall:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

VPN	
PPTP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

ALG	
FTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
TFTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
H323 ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RTSP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Save

Figure 9-2 Basic Security

- **Firewall** - A firewall protects your network from the outside world. In this page, the user can enable or disable the router firewall.
- **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable this option.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the device.
- **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the device, click on Enabled.
- **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the device, click on Enable.
- **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the device, click on Enable.

ALG - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway, so as to support address and port translation for certain application layer “control/data” protocols, such as FTP, TFTP, H323 etc.

- **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click on Enable.
- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click on Enable.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click on Enable.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click on Enable.

Click the **Save** button to store your settings.

9.2 Advanced Security

Go to **Security → Advanced Security** in the menu, in order to protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood, as shown in the following screen (Figure 9-3).

Figure 9-3 Advanced security

- **Packets Statistics Interval (5~60)** - The default value is 10. Select the desired setting between 5 and 60 seconds from the drop-down list. This value determines the time interval between packets. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection** - Denial of Service protection. Check the corresponding box to Enable or Disable this function. Only when DoS is enabled, flood filters will be effective.

Note: You must first enable Traffic Statistics in "System Tool → Traffic Statistics" for the DoS Protection feature to work.

- **Enable ICMP-FLOOD Attack Filtering** – Check this box to **Enable or Disable** the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Select the desired setting 5 ~ 3600. When the current ICMP-FLOOD Packets number exceeds the set value, the router will immediately startup the blocking feature.
- **Enable UDP-FLOOD Filtering** - **Enable or Disable** the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. . Select the desired setting between 5 ~ 3600. When the current UPD-FLOOD Packets number exceeds the set value, the router will immediately startup the blocking feature.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Check this box to Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Select the desired setting between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets number exceeds the set value, the router will immediate startup the blocking feature.
- **Ignore Ping Packet from WAN Port** – Check this box to Enable or Disable this option. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet From LAN Port** - Check this box to **Enable or Disable** this option. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend the network against some viruses.

Click the **Save** button to store the settings.

Click the **DoS Host Block List** button to display the DoS host table with the items excluded.

9.3 Local Management

Go to **Security → Local Management** in the menu, in order to configure the management rule as shown in the screen below (Figure 4 43). The management feature allows you to deny computers in LAN from accessing the router.

Local Management

Management Rules

All the PCs on the LAN are allowed to access the Device's Web-Based Utility

Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:	
MAC 2:	
MAC 3:	
MAC 4:	

Your PC's MAC Address:

Figure 9-4 Local management

By default, the radio button “**All the PCs on the LAN are allowed to access the router’s Web-Based Utility**” is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the router’s Web-Based Utility locally from inside the network, check the radio button “**Only the PCs listed can browse the built-in web pages to perform Administrator tasks**”, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (where X is any hexadecimal digit). Only the PCs with a MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After clicking the **Add** button, your PC’s MAC Address will be placed in the above list.

Click the **Save** button to store your settings.

Note: If your PC is blocked but you want to access the router again, use a pin to press and hold the Reset Button (hole) on the back panel for about 5 seconds, to reset the router to its factory default values on the Web-Based Utility.

9.4 Remote Management

Go to **Security → Remote Management** in the menu, in order to configure the Remote Management feature, as shown in the screen below (Figure 9-5). This feature allows you to manage your router from a remote location via the Internet.

Remote Management	
Web Management Port:	80
Remote Management IP Address:	0.0.0.0 (Enter 255.255.255.255 for all)
Save	

Figure 9-5 Remote management

- **Web Management Port** - Web browser normally uses the standard HTTP port 80 for access. This router’s default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the router from internet.

Note:

1. To access the router, you should type your Router’s WAN IP address into your browser’s address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router’s WAN address is 202.96.12.8, and the port number used is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked to type the router’s password. After successfully entering the username and password, you will be able to access the router’s web-based utility.
2. Be sure to change the router’s default password to a more secure password.

9.5 Parental Control

Go to **Parental Control** in order to configure this monitoring feature, as shown in the screen below. (Figure 9-10). Parental control can be used to monitor the internet activities of a child, limit his/her access to certain websites and to restrict the amount of time they spend surfing.

ID	MAC address	Website Description	Schedule	Status	Modify
	50-E5-49-C7-61-4F				
Add New...	Enable All	Disable All	Delete All		
Previous Next Current No. 1 Page					

Figure 9-10 Parental control settings

- **Parental Control** - Check Enable if you want to activate this function; otherwise, check Disable.
- **MAC Address of Parental PC** - In this field, enter the MAC address of the monitoring PC, or you can make use of the Copy To Above button below.
- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to enter this address into the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the monitored PC.
- **Schedule** - The time period allowed for the monitored PC to have access to the Internet. For detailed information, please go to “**Access Control → Schedule**”.
- **Modify** – Use this link to edit or delete an existing entry.

To add a new entry, please follow the steps below.

- 1.Click the **Add New** button. The screen shown in figure 9-11 below will appear.
- 2.In the MAC Address of Child PC field, enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you want to control. Or you can choose the MAC address from the All Address in Current LAN drop-down list.
- 3.Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.
- 4.Enter the allowed domain name of the website, either the full name or the keywords (e.g. Google) in the Allowed Domain Name field. Any domain name with keywords in it (www.google.com.cn) will be allowed.
- 5.Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the **Schedule in red** below to open the Advanced **Schedule Settings** page, and create the schedule you need.
- 6.In the Status field, select the **Enabled** or **Disabled** condition for that entry.
- 7.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.

Add or Modify Parental Control Entry

The Schedule is based on the time of the Device. The time can be set in "System Tools -> [Time settings](#)".

MAC Address of Child PC:	<input type="text"/>
All MAC Address In Current LAN:	<input type="button" value="please select-"/>
Website Description:	<input type="text"/>
Allowed Domain Name:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Effective Time:	<input type="button" value="Anytime"/>
The time schedule can be set in "Access Control -> Schedule "	
Status:	<input type="button" value="Enabled"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 9-11 Add or Modify Parental Control Entry

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the steps as described below.

- 1.1.Click the **Parental Control** menu on the left to enter the Parental Control Settings page. Check **Enable** and enter the MAC address **00-11-22-33-44-BB** in the MAC Address of Parental PC field.
- 2.2.Click **Access Control Schedule** on the left to enter the Schedule Settings page. Click the **Add New** button to create a new schedule, being identified as Schedule_1. The day is Sat, and the Time is all day-24 hours.
- 3.3.Click the **Parental Control** menu on the left to go back to the Add or Modify Parental Control Entry page:

- Click the **Add New** button.
 - Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
 - Enter Allow Google in the **Website Description** field.
 - Enter www.google.com in the **Allowed Domain Name** field.
 - Select the Schedule_1 you just created from the **Effective Time** drop-down list.
 - In **Status** field, select **Enable**.
4. Click **Save** to complete your settings.

Return to the **Parental Control Settings** page to open the following list, as shown in figure 9-12.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow Google	Schedule_1	<input checked="" type="checkbox"/>	Edit Delete

[Add New...](#) [Enable All](#) [Disable All](#) [Delete All](#)

[Previous](#) [Next](#) CurrentNo. [Page](#)

Figure 9-12 Parental control settings

9.6 Access control

Access Control

- Rule
- Host
- Target
- Schedule

Figure 9-13 Access control

There are four submenus under **Access Control** (Figure 9-13): **Rule**, **Host**, **Target** and **Schedule**. Click on any of these items in order to configure the corresponding function.

10. Rule

Go to **Access Control** → **Rule**, in order to visualize and set Access Control rules in the screen below, as shown in Figure 10-1.

Access Control Rule Management

Enable Internet Access Control

Default Filter Policy

Allow the packets specified by any enabled access control policy to pass through the Device

Deny the packets specified by any enabled access control policy to pass through the Device

Save

ID	Rule Name	Host	Target	Schedule	Status	Modify
Setup Wizard						
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/> <input type="button" value="Move"/>						
ID <input type="text"/> ToID <input type="text"/>						
<input type="button" value="Previous"/> <input type="button" value="Next"/> Current No. 1 <input type="button" value="Page"/>						

Figure 10-1 Access control rule management

- **Enable Internet Access Control** - Check this box to enable the Internet Access Control feature, so that the Default Filter Policy can take effect.
- **Rule Name**- The name of the rule is displayed here, which is unique.
- **Host** - The host selected with the corresponding rule is displayed in this field.
- **Target** - The target selected with the corresponding rule is displayed in this field.
- **Schedule** - The schedule selected with the corresponding rule is displayed in this field.
- **Action** - The action taken by the router to deal with the packets is displayed here. It could be Allow or Deny. Allow means that the router permits the packets to pass through. Deny means that the router is configured to reject the packets.
- **Status** - This field displays the current status of the rule. Enabled means the rule will be applied. Disabled means the rule will not take effect.
- **Modify** – Use this link to edit or delete an existing rule.

To add a new rule, please follow the steps below.

- 1.Click the **Add New** button. The screen shown in figure 10-2 below will appear.
- 2.Assign a name (e.g. Rule_1) to the rule in the **Rule Name** field.
- 3.Select a **host** from the Host drop-down list, or choose **Click here to add a new host list**.
- 4.Select a target from the **Target** drop-down list, or choose **Click here to add new target list**.
- 5.Select a schedule from the **Schedule** drop-down list, or choose **Click here to add new schedule**.
- 6.In the **Action** field, select **Deny** or **Allow**.
- 7.In the **Status** field, select the **Enabled** or **Disabled** condition for that entry.
- 8.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.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to go to the following page, or click the **Previous** button to return to the last page.

Add or Modify Internet Access Control Entry

Rule Name:	<input type="text"/>
Host:	<input type="button" value="Click Here To Add New Host List."/>
Target:	<input type="button" value="Any Target"/> Click Here To Add New Target List.
Schedule:	<input type="button" value="Anytime"/> Click Here To Add New Schedule.
Action:	<input type="button" value="Deny"/>
Status:	<input type="button" value="Enabled"/>

Figure 10-2 Add or Modify Internet Access Control Entry

For example: If you wish to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from **18:00 to 20:00** on **Saturdays and Sundays**, and forbid other hosts in the LAN from accessing the Internet, you should follow the steps as described below:

1. Click **Access Control → Host** on the left to open the **Host Settings** page. Add a new entry identified as Host_1, using 00-11-22-33-44-AA as the MAC Address.
2. Click **Access Control → Target** on the left to enter the **Target Settings** page. Add a new entry identified as Target_1, using www.google.com as the Domain Name.
3. Click **Access Control → Schedule** on the left to open the **Schedule Settings** page. Add a new entry identified as Schedule_1. The days are Sat. and Sun. Start Time is 1800 and Stop Time is 2000.
4. Click **Access Control → Rule** on the left to return to the **Access Control Rule Management** page. Select **Enable Internet Access Control** and choose **Deny the packets not specified by any access control policy to pass through the router**.
5. Click the **Add New** button to insert a new rule as follows:
 - In the **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - In the **Host** field, select Host_1.
 - In the **Target** field, select Target_1.
 - In the **Schedule** field, select Schedule_1.
 - In the **Action** field, select Allow.
 - In the **Status** field, select Enable.
 - Click **Save** to complete your settings.

Then you will go back to the Access Control Rule Management page where the list below will be displayed.

ID	Rule Name	Host	Target	Schedule	Action	Status	Modify
1	1	Host_1	Target_1	Schedule_1	Deny	Enabled	Edit Delete

Figure 10-3

10.1 Host

Go to menu **Access Control → Host**, in order to visualize and set a Host list in the screen, as shown in figure 10-4 below. The host list is necessary for the Access Control Rule.

Host Settings			
ID	Host Description	Information	Modify
			Add New... Delete All
Previous Next Current No. <input type="text" value="1"/> Page			

Figure 10-4 Host settings

- **Host Description** - The description of the host, which is unique, is displayed here.
- **Information** - The data about the host is displayed in this field. It can be IP or MAC.
- **Modify** – Use this link edit or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
 2. In the **Mode** field, select IP Address or MAC Address.
 - If you select an IP Address, the screen shown in figure 10-5 will be opened.
 1. In the **Host Description** field, create a unique description for the host (e.g. Host_1).
 2. In the **MAC Address** field, enter the corresponding address.
 3. Click the **Save** button to complete your settings.
- Click the **Delete All** button to erase all the entries in the table.
 Click the **Next** button to go to the following page, or click the **Previous** button to return to the last page.

Add or Modify a Host Entry

Mode:	<input type="button" value="IP Address"/>
Host Description:	<input type="text"/>
LAN IP Address:	<input type="text"/> - <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 10-5 Add or Modify a Host Entry

Add or Modify a Host Entry

Mode:	<input type="button" value="MAC Address"/>
Host Description:	<input type="text"/>
MAC Address:	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 10-6 Add or Modify a Host Entry

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA, first you must complete the steps as described below:

- 1.1.Click the **Add New** button in figure 10-7 to open the Add or Modify a Host Entry page.
- 2.2.In the Mode field, select **MAC Address** from the drop-down list.
- 3.3.In the Host Description field, create a unique description for the host (e.g. Host_1).
- 4.4.In the MAC Address field, enter **00-11-22-33-44-AA**.
- 5.5.Click **Save** to complete your settings.

When done, you will return to the Host Settings page, where the following list will be displayed.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Details

Figure 10-7

10.2 Target

Go to menu **Access Control → Target**, in order to visualize and set a Target list, as shown in the screen below (figure 10-8). The target list is necessary for the Access Control Rule.

ID	Target Description	Information	Modify
			Modify

Add New... Delete All

Previous Next Current No. 1 Page

Figure 10-8 Target settings

- **Target Description** - The target name, which is unique, is displayed in this field.
- **Information** - The target can be an IP address, port, or domain name.
- **Modify** – Use this link to edit or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In the **Mode** field, select IP Address or Domain Name.
 - If you select IP Address, the screen shown in figure 10.9 will be displayed
 1. In the **Target Description** field, create a unique description for the target (e.g. Target_1).
 2. In the **IP Address** field, enter the corresponding address for the target.
 3. Select a common service from the **Common Service Port** from the drop-down list, so that the **Target Port** will be automatically filled out. If the **Common Service Port** drop-down list does not have the service you want, specify the **Target Port** manually.
 4. In the **Protocol** field, select TCP, UDP, ICMP or ALL.
 - If you select Domain name, the screen shown in figure 10-10 will be displayed.
 1. In the **Target description field**, create a unique name for the target (e.g. Target_1).
 2. Enter the **domain name**, either the full name or the keywords (for example google) in the Domain name blank field. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter up to 4 domain names.
3. Click the **Save** button.

Click the **Delete all** button to erase all the entries in the table.

Click the **Next** button to go to the following page, or click the **Previous** button return to the last page.

Add or Modify an Access Target Entry

Mode:	IP Address
Target Description:	<input type="text"/>
IP Address:	<input type="text"/> - <input type="text"/>
Target Port:	<input type="text"/> - <input type="text"/>
Protocol:	ALL
Common Service Port:	--please select--

Save **Back**

Figure 10-9 Add or Modify an Access Target Entry

Add or Modify an Access Target Entry

Mode:	Domain Name
Target Description:	<input type="text"/>
Domain Name:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

Save **Back**

Figure 10-10 Add or Modify an Access Target Entry

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA in the LAN, so that it is able to access **www.google.com** only, first you must complete the steps as described below.

1. Click the **Add New** button in figure 10-11 to open the Add or Modify an Access Target Entry page.
2. In the **Mode** field, select **Domain name** from the drop-down list.
3. In the **Target description** field, create a unique description to identify the target (e.g. Target_1).
4. In the **Domain name** field, enter **www.google.com**.
5. Click **Save** to complete your settings.

When done, you will return to the Target Settings page, where following list will be displayed.

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete
Add New... Delete All			

Figure 10-11

Go to **Access control** → **Schedule** in the menu, in order to visualize and set a Schedule list in the next screen, as shown in figure 10-12. The Schedule list is necessary to establish the Access Control Rule.

Schedule Settings				
ID	Schedule Description	Day	Time	Modify
				Add New... Delete All
				Previous Next Current No. <input checked="" type="checkbox"/> Page

Figure 10-12 Schedule Settings

- **Schedule description** - The name assigned to the schedule, which is unique, is displayed in this field.
- **Day** - The day(s) of the week is shown in this field.
- **Time** - The 24-hour period of the day is displayed in this field.
- **Modify** – Use this link to edit or delete an existing schedule.

To add a new schedule, follow the steps below.

1. Click the **Add new** button, as shown in figure 10-13. The screen displayed in figure 4 58 will open in this step.
2. In the **Schedule description** field, create a unique name to identify the schedule (e.g. Schedule_1).
3. In the **Day** field, select the day or days you want to include.
4. In the **Time** field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click **Save** to complete your settings.

Click the **Delete** all button to erase all the entries in the table.

Click the **Next** button to go to the following page, or click the **Previous** button return to the last page.

Advance Schedule Settings

Note: The Schedule is based on the time of the Device.

Schedule Description:	<input type="text"/>
Day:	<input checked="" type="radio"/> Everyday <input type="radio"/> Select Days
	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time:	all day-24 hours: <input checked="" type="checkbox"/>
Start Time:	<input type="text"/> (HHMM)
Stop Time:	<input type="text"/> (HHMM)
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 10-13 Advanced Schedule Settings

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA, so that it is able to access www.google.com only from **18:00 to 20:00** on **Saturdays** and **Sundays**, you must first complete the steps as described below:

1. Click the **Add New** button shown in figure 10-13 to enter to the **Advanced Schedule Settings** page.
2. In the **Schedule description** field, create a unique name to identify the schedule (e.g. Schedule_1).
3. In the **Day** field, check the **Select days** radio button, and choose Sat and Sun next.
4. In the **Time** field, enter 1800 in the **Start time** field and 2000 in the **Stop time** field.
5. Click **Save** to complete your settings.

When done, you will return to the Schedule Settings page, where following list will be displayed.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete
Add New...		Delete All		

Figure 10-13 Advanced Schedule Settings

11. Advanced routing

Advanced Routing

- **Static Routing List**
- **System Routing Table**

Figure 11-1 Advanced routing

There are two submenus under the Advanced routing menu as shown in Figure 11-1: Static Routing List and System Routing Table. Click any of them, and you will be able to configure the corresponding function.

11.1 Static Routing

Go to **Advanced routing → Static routing list**, in order to configure the static route as shown in the next screen (Figure 11-2). A static route is a pre-determined path that network information must travel to reach a specific host or network.

ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify

Add New... **Enable All** **Disable All** **Delete All**

Previous **Next**

Figure 11-2 Static Routing

To add static routing entries:

1. Click the **Add new** button as shown in figure 11-3. The following screen will open.

Add or Modify a Static Route Entry

Destination Network: [Text Input]

Subnet Mask: [Text Input]

Default Gateway: [Text Input]

Status: Enabled

Save **Back**

Figure 11-3 Add or Modify a Static route entry

2. Enter the following data:

- **Destination IP Address** - The Destination IP address is the address of the network or host that you want to assign a static route to.
- **Subnet mask** - The Subnet mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP Address of the gateway device that allows for contact between the router and the network or host.

3. Select **Enabled** or **Disabled** for this entry from the **Status** pull-down list.

4. Click the **Save** button to make the entry take effect.

Other configurations for the entries:

Click the **Delete all** button to erase all entries.

Click the **Enable all** button to activate all entries

Click the **Disabled all** button to cancel all entries.

Click the **Previous** button to view the information in the last screen, click the **Next** button to view the information in the following screen.

11.2 System routing table

Choose menu **Advanced routing** → **System routing table**, you can configure the system routing table in the next screen (shown in Figure 11-4). System routing table views all of the valid route entries in use.

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
Refresh				

Figure 11-4 System routing table

System Routing Table **Destination network** - The **Destination network** is the address of the network or host to which the static route is assigned.

Subnet mask - The **Subnet mask** determines which portion of an IP address is the network portion, and which portion is the host portion.

Gateway - This is the IP address of the gateway device that allows for contact between the Router and the network or host.

Interface - This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet).

12. Bandwidth control



Figure 12-1 Bandwidth control

There are two submenus under the Bandwidth control menu as shown in Figure 12-1. Click on any of these items in order to configure the corresponding function. Below you will find detailed descriptions for each of these items.

12.1 Control settings

Go to **Bandwidth control** → **Control settings** in the menu, in order to configure the Egress and Ingress Bandwidth using the screen shown below. Enter the appropriate values in kbps, with settings below 100000. For optimal control of the bandwidth, please select the correct Line Type and ask your ISP what is the maximum egress and ingress bandwidth that can be set.

Bandwidth Control Settings	
Enable Bandwidth Control:	<input type="checkbox"/>
Line Type:	<input checked="" type="radio"/> ADSL <input type="radio"/> Other
Egress Bandwidth:	512 Kbps
Ingress Bandwidth:	2048 Kbps
Save	

Figure 12-1 Bandwidth control settings

- **Enable bandwidth control** - Check this box so that the Bandwidth Control settings can take effect.
- **Line type** - Select the right type for you network connection. If you are unsure about the type you should choose, please contact your ISP directly to find out.
- **Egress bandwidth** - The upload speed through the WAN port.
- **Ingress bandwidth** - The download speed through the WAN port.

12.2 Rules list

Go to **Bandwidth control** → **Rules list** in the menu, in order to visualize and configure the Bandwidth Control rules in the screen below.

Bandwidth Control Rules List							
ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							
Add New...	Delete All						
Previous	Next	Now is the 1 page					

Figure 12-2 Bandwidth control rules list

To add/modify a Bandwidth control rule, follow the steps below.

Step 1: Click the **Add New** button as shown in figure 12-2. A new screen will open, just like the one included in figure 12-3.

Step 2: Enter the information in the corresponding fields.

Bandwidth Control Rule Settings

Enable:	<input checked="" type="checkbox"/>
IP Range:	<input type="text"/> - <input type="text"/>
Port Range:	<input type="text"/> - <input type="text"/>
Protocol:	ALL <input checked="" type="checkbox"/>
Egress Bandwidth:	Min Bandwidth(Kbps) <input type="text"/> Max Bandwidth(Kbps) <input type="text"/>
Ingress Bandwidth:	<input type="text"/> <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Figure 12-3 Bandwidth control rule settings

Step 3: Click the **Save** button.

Figure 12-3 Bandwidth control rule settings

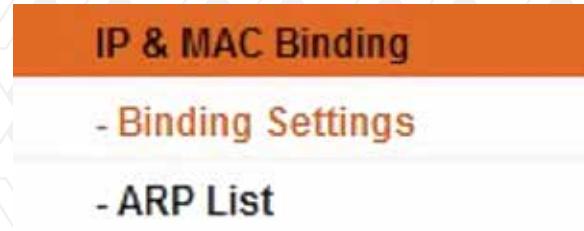


Figure 13-1 IP & MAC Binding menu

There are two submenus under **IP & MAC Binding** (shown in Figure 13-1): **Binding setting** and **ARP List**. Click on any of these items in order to scan or configure the corresponding function. Detailed descriptions of each of these items are provided below.

13.1 Binding setting

This page displays the **IP & MAC Binding setting** table; which you can set up based on your individual preferences (figure 13-2).

The screenshot shows a web-based configuration interface titled "Binding Settings". At the top, there is a radio button group for "ARP Binding" with "Disable" selected. Below it is a table header with columns: "ID", "MAC Address", "IP Address", "Bind", and "Modify". A message "The list is empty" is displayed above the table body. At the bottom of the page are several buttons: "Add New...", "Enable All", "Disable All", "Delete All", "Find", "Previous", "Next", "Current No. 1", and "Page".

Figure 13-2 Binding setting

- **MAC Address** - The MAC address of the monitored computer in the LAN.
- **IP Address** - The assigned IP address of the monitored computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** – Use this link to edit or delete an existing entry.

When you want to add or edit an IP & MAC Binding entry, click the **Add New** button or **Modify** button, and then you will be directed to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 13-3).

The screenshot shows a form titled "IP & MAC Binding Settings". It contains three input fields: "Bind" (checkbox checked), "MAC Address" (text input field), and "IP Address" (text input field). At the bottom are "Save" and "Back" buttons.

Figure 13-3 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New** button, as shown in figure 13-2.
2. Enter the **MAC Address** and **IP Address**.
3. Select the **Bind** checkbox.
4. Click the **Save** button to accept your changes.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry, follow the steps below.

1. Click the **Find** button, as shown in figure 13-4.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page.

ID	MAC Address	IP Address	Bind	Link
1	00-11-22-33-44-AA	192.168.0.50	<input checked="" type="checkbox"/>	To page

Find **Back**

Figure 13-4 Find IP & MAC Binding Entry

Click the **Enable All** button to activate all entries.

Click the **Delete All** button to erase all entries.

13.2 ARP List

You can see IP addresses on the LAN and their associated MAC addresses by viewing the ARP list. Also, you can use the Load and Delete buttons to manage the list. The user can use this list to visualize all the existing IP & MAC binding entries (shown in figure 13-5).

ID	MAC Address	IP Address	Status	Configure
1	C8-3A-35-CF-E4-8A	192.168.0.100	Unbound	Load Delete

Bind All **Load All** **Refresh**

Figure 13-5 ARP List

- **MAC Address** - The MAC address of the monitored computer in the LAN.
- **IP Address** - The assigned IP address of the monitored computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** – To load or delete an item.
 - **Load** – To load the item into the IP & MAC Binding list.
 - **Delete** – To erase the item.

Click the **Bind all** button to bind all the current items. This option is only available when the ARP binding is enabled.

Click the **Load all** button to include all items to the IP & MAC Binding list.

Click the **Refresh** button to update all items.

Note: An item cannot be entered to the IP & MAC Binding list if the IP address of the item has been loaded before. An error warning will be displayed as well. Likewise, the “Load All” command will only load the items without interfering with the IP & MAC Binding list.

4.16 Dynamic DNS

Go to Dynamic DNS in order to configure the Dynamic DNS feature.

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (defined by the user) and a dynamic IP address. Your friends can then connect to your server by entering the domain name you provide, no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers, such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

14.1 Comexe.cn DDNS

If the dynamic DNS Service provider you select is www.comexe.cn, the page will appear as shown in figure 14-1.

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name: username

Password: *****

Enable DDNS

Connection Status: DDNS not launching!

Figure 14-1 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **Domain name** received from your dynamic DNS service provider.
2. Type the **User name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to log into the DDNS service.

Connection status -The status of the DDNS service connection is displayed here.
Click **Logout** to exit the DDNS service.

If the dynamic DNS **Service provider** you select is www.dyndns.org, the page will appear as shown in figure 4 71.

The screenshot shows a web-based configuration interface for a DDNS service. At the top, it says "DDNS". Below that, "Service Provider:" is set to "Comexe (www.comexe.cn)" with a checked checkbox and a link to "Go to register...". There are five input fields for "Domain Name", each with a green border. Underneath these are "User Name:" (set to "username") and "Password:" (set to "*****"). A checkbox labeled "Enable DDNS" is unchecked. The "Connection Status:" section shows "DDNS not launching!". At the bottom are three buttons: "Login" (green), "Logout" (light gray), and "Save" (green).

Figure 14-2 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain name** you received from dynamic DNS service provider here.
4. Click the **Login** button to log into the DDNS service.

Connection status -The status of the DDNS service connection is displayed here.
Click **Logout** to exit the DDNS service.

14.3 No-ip.com DDNS

If the dynamic DNS **Service provider** you select is www.no-ip.com, the page will appear as shown in figure 14-3.

The screenshot shows a web-based configuration interface for a DDNS service. At the top, it says "DDNS". Below that, under "Service Provider", "Dyndns (www.dyndns.org)" is selected with a checked checkbox, and there is a link "Go to register...". There are three input fields: "User Name" containing "username", "Password" containing a masked password, and "Domain Name" containing an empty field. Below these is a checkbox "Enable DDNS" which is unchecked. Under "Connection Status", it says "DDNS not launching!" and has two buttons: "Login" and "Logout". At the bottom is a "Save" button.

Figure 14-3 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

- 1.1. Type the **User name** for your DDNS account.
- 2.2. Type the **Password** for your DDNS account.
- 3.3. Type the **Domain name** you received from dynamic DNS service provider.
- 4.4. Click the **Login** button to log into the DDNS service.

Connection status - The status of the DDNS service connection is displayed here.
Click **Logout** to exit the DDNS service.

15. System Tools



Figure 15-1 System Tools menu

Go to **System Tools** in order to display the submenus under the main menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System Log** and **Statistics**. Click on any of these items in order to configure the corresponding function. You will find detailed descriptions for each of these items below.

15.1 Time settings

Go to menu **System tools** → **Time setting**, in order to configure the time on the following screen.

Time zone:	(GMT-05:00) Eastern Time (US Canada)		
Date:	1	1	1970 (MM/DD/YY)
Time:	1	52	48 (HH/MM/SS)
NTP Server 1:	0.0.0.0 (Optional)		
NTP Server 2:	0.0.0.0 (Optional)		
<input type="button" value="Get GMT"/>			
<input type="checkbox"/> Enable Daylight Saving Start: Mar 3rd Sun 2am End: Nov 2nd Sun 3am			
Daylight Saving Status: daylight saving is down.			
Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server(IP Address or Domain Name) in the above frames.			
<input type="button" value="Save"/>			

Figure 15-2 Time settings

- **Time zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the corresponding blank fields.
- **Time** - Enter your local time in HH/MM/SS into the corresponding blank fields.
- **NTP Server prior** - Enter the address for the NTP Server, then the router will preferentially obtain the time from the NTP Server. In addition, the router can automatically update the time from any enabled NTP server once it connects to the Internet.

To set time manually:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
2. Click the **Get GMT** button to obtain the system time from the Internet

To enable Daylight Saving:

1. Check the **Enable Daylight Saving** box to enable this function.
2. Define the span of time during which you want this feature to work. For example, if you want this feature to be effective from 0 o'clock (am) on the 1st Sunday of April until at 6 o'clock (pm) on the 2nd Saturday of September, enter "Apr", "1st", "Sun", "0am" in the **Start** field, followed by "Sep", "2nd", "Sat", "6pm" in the **End** field.
3. Click the **Save** button for the new settings to take effect.

<input checked="" type="checkbox"/> Enable Daylight Saving			
Start:	Mar	3rd	Sun 2am
End:	Nov	2nd	Sun 3am
Daylight Saving Status: daylight saving is down.			

Figure 15-3 System routing table

Note:

1. This setting will be used for some time-based functions, such as firewall. You must specify your time zone once you successfully login to the router; otherwise, time dependent functions will fail to work.
2. The time will be lost if the device is turned off.
3. The device will obtain the GMT automatically from the Internet if it is configured accordingly.
4. In daylight saving configuration, the start and end times shall be within the same year, in which the start time should be earlier than the end time.
5. The daylight saving function starts working one minute after being enabled.

15.2 Diagnostic

Go to **System tools** → **Diagnostic** in the menu, in order to start the Ping or Traceroute functions, which are designed to check the connectivity status of your network, as shown in the screen below.

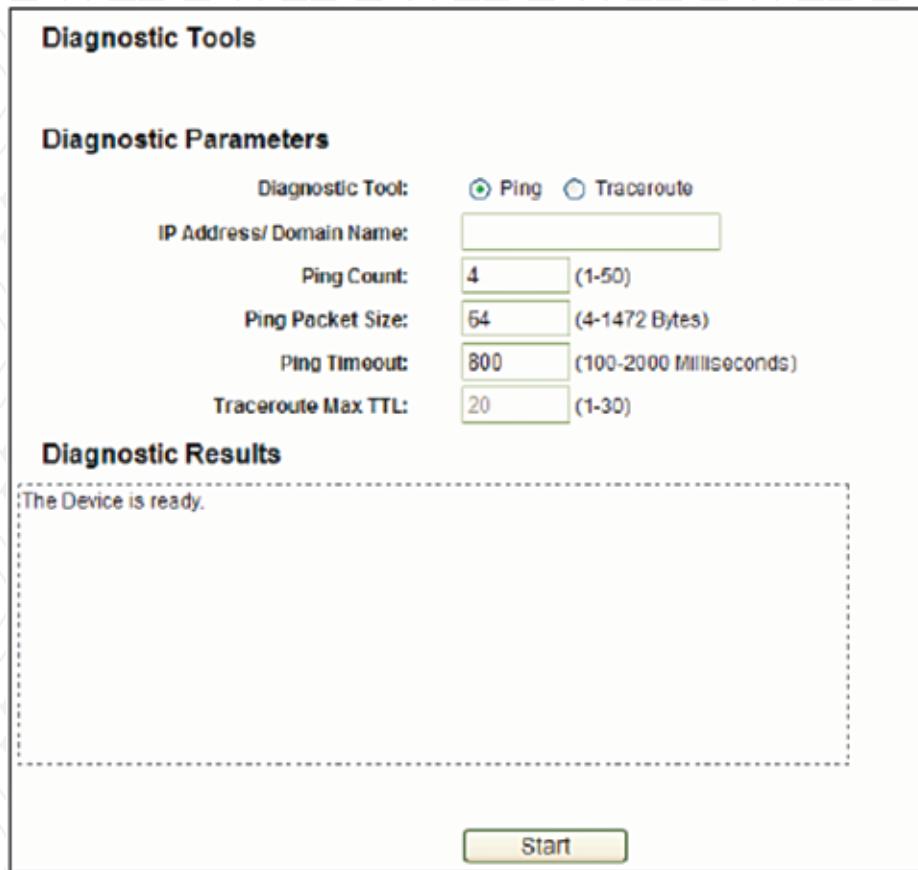


Figure 15-4 Diagnostic Tools

- **Diagnostic tool** - Check the radio button to select one of the diagnostic tools.
 - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - **Traceroute** - This diagnostic tool tests the performance of a connection.

Note: You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, make sure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

IP Address/Domain name - Type the destination IP address (such as 202.108.22.5) or Domain name of the PC whose connection you wish to diagnose.

- **Pings count** – Specifies the number of Echo Request messages sent. The default is 4.
- **Ping packet size** – Specifies the number of data bytes to be sent. 64 is the default value.
- **Ping timeout** - Sets the maximum time that the application will wait for a reply, in milliseconds. When time exceeds the timeout limit, the session will expire. 800 is the default value
- **Traceroute Max TTL** - Sets the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20

Click **Start** to check the connectivity of the Internet.

The **Diagnostic results** page displays the outcome of the diagnosis.

If the results you obtained are similar to the values that appear in the screen below, it means that the connectivity to the Internet is fine.

Diagnostic Results

```
Pinging 192.168.0.1 with 64 bytes of data:

Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4

Ping statistics for 192.168.0.1
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1
```

Figure 15-5 Diagnostic Results

Note: Only one user can use this tool at a time. “Number of Pings”, “Ping Size” and “Ping Timeout” are Ping parameters. “Tracert Hops” is a Traceroute parameter.

15.4 Factory Defaults

Go to **System Tools → Firmware Upgrade** in the menu, in order to update the latest firmware version available for the router. The following screen will be displayed.

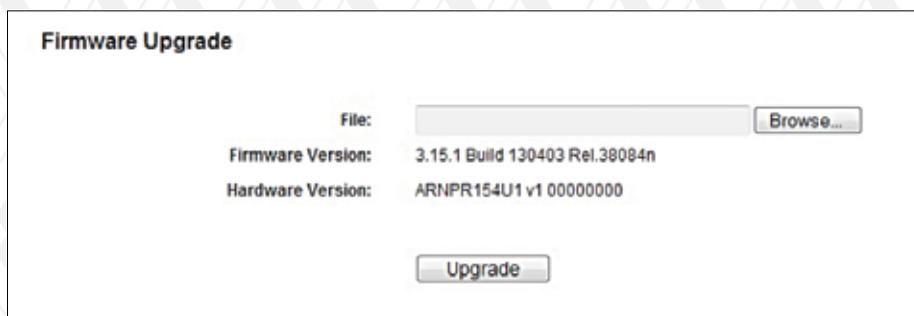


Figure 15-6 Firmware Upgrade

- **Firmware version** - The current firmware version is displayed here.
- **Hardware version** – The current hardware version is displayed here. The hardware version of the upgrade file must match the router's current hardware version.

15.5 Backup & Restore

- 1.Download the latest firmware upgrade file from our website (<http://www.nexxtsolutions.com>).
- 2.Type or select the path and file name of the update file into the File field. Or click the Browse button to locate the update file.
- 3.Click the Upgrade button.

Note:

- 1.New firmware versions are posted at <http://www.nexxtsolutions.com> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the router rather than the configuration, you can try to upgrade the firmware.
- 2.When you upgrade the router's firmware, you may lose its current configuration. Therefore, before upgrading the firmware, please write down your customized parameters to avoid losing important settings.
- 3.Do not turn off power or press the reset button while the firmware is being upgraded; doing so might cause serious damage to the router.
- 4.The router will reboot after the upgrading has been finished.

15.4 Factory Defaults

Go to **System Tools → Factory Defaults** in the menu, in order to restore the router configuration to its factory default values, as seen on the following screen



Figure 15-4 Diagnostic Tools

Click the **Restore** button to reset all settings to their factory default values.

- **Default User Name:** admin
- **Default Password:** admin
- **Default IP Address:** 192.168.0.1
- **Default Subnet Mask:** 255.255.255.0

Note: Any settings you have saved will be lost after the default settings are restored.

15.5 Backup & Restore

Go to **System Tools → Backup & Restore** in the menu, in order to save the current configuration of the router as a backup file and restore the original settings using a backup file as shown in Figure 15-8.



Figure 15-8 Backup & Restore Configuration

- Click the **Backup** button to save all the configuration settings to your local computer as a file.
- To upgrade the router's configuration, follow the instructions below.
 - Click the **Browse...** button to locate the update file for the router, or enter the exact path to the Setting file in the text box.
 - Click the **Restore** button.

Note: The current configuration will be covered by the uploading configuration file. If the process fails, it will render the device unmanageable. The restoring process lasts 20 seconds and the device will restart automatically. Keep the power of the device on during the entire process to avoid any potential damage to the unit.

15.6 Reboot

Go to **System Tools → Reboot**, and press the Reboot button in order to reset the device, as shown in the screen below.



Figure 15-9 Reboot the router

Some settings of the router will only take effect after rebooting, which include:

- LAN IP Address change (system will reboot automatically).
- DHCP Settings change.
- Wireless configuration change.
- Web Management Port change.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

15.7 Password

Go to **System Tools → Password**, in order to change the router's factory default user name and password, using the screen shown in figure 15-10.

The username and password must not exceed 14 characters in length and must not include any spaces!

Old User Name:	<input type="text"/>
Old Password:	<input type="password"/>
New User Name:	<input type="text"/>
New Password:	<input type="password"/>
Confirm New Password:	<input type="password"/>

Save **Clear All**

Figure 15- 10 Password

It is strongly recommended that you change the factory default user name and password of the device. All users who try to access the device web-based utility will be prompted to type the device default user name and password.

Note: The new user name and password must not exceed 14 characters in length, and must not include any spaces.

Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to delete all existing entries.

15.8 System Log

Go to **System tools → System log**, in order to view the logs of the router.

System Log

Log Type: All	Log Level: ALL
Log is Empty.	
Time = 1970-01-01 2:04:11 7452s H.Ver = ARNPR154U1 v1 00000000 : S.Ver = 3.15.1 Build 130403 Rel.38084n L = 192.168.0.1 : M = 255.255.255.0 W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0	

Refresh **Save Log** **Clear Log**

Previous Next Current No. 1 Page

Figure 15-11 System log

- **Log type** - By selecting the log type, only logs of this type will be shown.
- **Log level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save log** - Click to save all the logs in a txt file.
- **Mail log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Clear log** - All the logs will be deleted from the router permanently, not just from the page.

Click the **Next** button to go to the following page, or click the **Previous** button return to the last page.

15.9 Statistics

Go to **System Tools→Statistics** in the menu, in order to visualize the router statistics, including the total traffic and current traffic of the last Packets Statistic Interval.

IP Address/ MAC Address	Total		Current			Modify
	Packets	Bytes	Packets	Bytes	ICMP Tx	
The current list is empty.						

Figure 15-12 Statistics

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To activate it, click the Enable button.
- **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds from the pull-down list. This statistics interval defines the time between each transmission of data packets.

Select the **Auto-refresh** checkbox to update data automatically.

Click the **Refresh** button to update data immediately.

- **Sorted Rules** - Select a rule from the pull-down list to display the corresponding statistics.

Click **Reset All** to restore the values of all the entries to zero.

Click **Delete All** to erase all entries in the table.

15.9 Statistics Table:

IP/MAC Address		The IP/MAC Address displayed with statistics
Total	Packets	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval expressed in seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval expressed in seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval expressed in seconds
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval expressed in seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval expressed in seconds
Modify	Reset	Reset the value of the entry to zero
	Delete	Delete the existing entry in the table

15.9 Statistics Table:

General	Polaris 150	Viking 150
Standards	IEEE 802.11g, 802.11b, 802.11i, 802.1X, 802.3, 802.3u, 802.3X and 802.11n	
Protocols	CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP	
Ports	One 10/100M-Auto Negotiation WAN RJ45 port	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M -Auto Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100 Ω STP (maximum 100m)	
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100 Ω STP (maximum 100m)	
LEDs	System	PWR, SYS, WLAN, LAN (1-4), WAN, 3G, WPS
Safety & Emissions	FCC	
Wireless		
Frequency Band	2.4 - 2.4835GHz	
Radio Data Rate	11n: up to 150Mbps (Automatic)	
	11g: 54/48/36/24/18/12/9/6Mbps (Automatic)	
	11b: 11/5.5/2/1Mbps (Automatic)	
Channels	1-11	
Frequency expansion	DSSS (Direct Sequence Spread Spectrum)	
Modulation	DBPSK, DQPSK, QPSK, CCK and OFDM (BPSK/QPSK/16-QAM/64-QAM)	
Security	WPA/WPA2, WPA-PSK/WPA2-PSK (TKIP/AES) and 64/128/152-bit WEP	
Sensitivity	130M: -68dBm@10% PER; 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER	
RF Power	11b: 18dBm 11g: 15dBm 11n: 12dBm	
Antenna gain	0dBi	5dBi
Environmental and Physical		
Temperature	Operating : 0°C~40°C (32°C ~104°C) Storage: -40°C~70°C (-40°C ~158°C)	
Humidity	Operating: 10% - 90% RH, Non-condensing Storage: 5% - 90% RH, Non-condensing	

Appendix B: Glossary

- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configures the TCP/IP parameters for all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** - An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID** - A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, in which network serving users are limited in a local area.