

# TABLE OF CONTENT

<b>1. ABOUT THIS GUIDE</b> .....	<b>3</b>
1.1 Navigation of the User's Guide .....	3
<b>2. PRODUCT OVERVIEW</b> .....	<b>3</b>
2.1 Introduction .....	3
2.2 Features .....	3
2.3 Panel Layout.....	4
2.3.1 Front Panel .....	4
2.3.2 Rear Panel.....	5
<b>3. HARDWARE INSTALLATION</b> .....	<b>6</b>
3.1 Hardware Installation .....	6
3.2 Check the Installation .....	6
3.3 Set up the Computer .....	6
<b>4. CONNECTING TO INTERNET</b> .....	<b>8</b>
4.1 Accessing Web page .....	8
4.2 Changing Password.....	9
4.3 Setup Wizard.....	10
4.3.1 WAN Type .....	10
4.3.1.1 Dynamic IP Address .....	11
4.3.1.2 Static IP Address .....	11
4.3.1.3 PPPoE .....	12
4.3.2 Wireless Setting.....	12
<b>5. ADVANCED SETTINGS</b> .....	<b>14</b>
5.1 System Status.....	14
5.2 Network Settings .....	15
5.2.1 WAN Interface .....	15
5.2.2 LAN Interface.....	16
5.2.3 DHCP Server .....	16
5.2.4 TCP/IP Status .....	18
5.3 Wireless.....	18
5.3.1 Wireless Status.....	18
5.3.2 Wireless Basic Settings .....	19
5.3.3 Wireless Security Settings .....	20
5.3.3.1 WEP .....	20
5.3.3.2 802.1x .....	21
5.3.3.3 WPA/WPA2.....	21
5.3.4 WDS Settings .....	23
5.3.5 WPS Configuration Setup.....	23

5.3.6 Repeater Settings .....	25
5.3.7 Advanced Settings .....	26
<b>5.4 Firewall .....</b>	<b>28</b>
5.4.1 Access Control .....	29
5.4.2 IP/Port Filtering .....	29
5.4.3 MAC Filtering .....	30
5.4.4 URL Filtering .....	31
5.4.5 Port Trigger .....	31
5.4.6 Virtual Server .....	32
5.4.7 DMZ .....	33
<b>5.5 Management .....</b>	<b>33</b>
5.5.1 Traffic Statistics .....	33
5.5.2 DDNS .....	34
5.5.3 Time Zone Settings .....	35
5.5.4 System Log .....	36
5.5.5 Upgrade Firmware .....	37
5.5.6 Save/Reload Settings .....	37
5.5.7 Password .....	38
5.5.8 Reboot .....	38

# ***1. ABOUT THIS GUIDE***

---

Thank you very much for purchasing this N01-R15DC Wireless Router. This guide will introduce the features of this device and tell you how to connect, use and configure the Router to connect with Internet. Please follow the instructions in this guide to avoid affecting the Router's performance by improper operation.

## **1.1 Navigation of the User's Guide**

**Product Overview.** Describes the router, its features and appearance.

**Hardware Installation.** Describes the hardware installation and settings on computer.

**Connecting to Internet.** Tells how you can connect your computer to Internet successfully using the Router.

**Advanced Settings.** Lists all technical functions including Wireless, Network Settings, Firewall and Management of the Router.

# ***2. PRODUCT OVERVIEW***

---

## **2.1 Introduction**

N01-R15DC is a combined wired/wireless network connection device that integrates with internet-sharing router and 4-port switch. It allows users to access Internet by DHCP/PPPoE/Static IP and can expand the wireless coverage. N01-R15DC can be also used as a repeater and a Wireless AP. Generally, it is a high performance and cost-effective solution for home and small offices.

## **2.2 Features**

- Complies with IEEE 802.11n and IEEE 802.11g/b standards for 2.4GHz Wireless LAN.
- Up to 150Mbps wireless speed.
- Supports PPPoE, Dynamic IP and static IP broadband functions.
- Supports 64/128-bit WEP, WPA/WPA2 and 802.1x encryption.
- IP/MAC/URL filtering makes access and time control more flexibly.
- WDS mode makes it simple for WLAN expansion.
- Supports WMM for improved audio and video streaming.
- Multi-SSID allows you to create multiple SSIDs for different purpose.
- Connects to secure network easily and fast using WPS.
- Repeater function allows more PCs to surf Internet.
- Supports port bandwidth control.
- Easy to install and configure.

## 2.3 Panel Layout

### 2.3.1 Front Panel

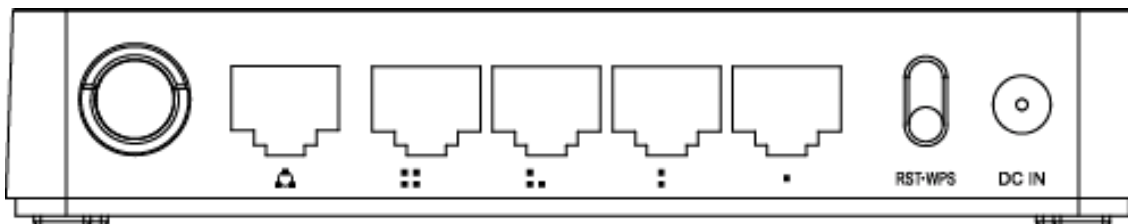
The front panel of Router N01-R15DC consists of 8 LEDs, which is designed to indicate connection status.



<b>POWER</b>	This indicator lights blue when the hub is receives power, otherwise it is off.
<b>CPU</b>	This indicator blinks blue when Router powered on.
<b>WLAN</b>	This indicator lights blue when there are wireless devices connected and transmitting data to WLAN Router.
<b>WAN</b>	When the WAN port is connected successfully the indicator lights blue.
	During transmitting or receiving data through the WAN port the indicator blinks blue.
<b>1/2/3/4 LAN</b>	When one of the LAN ports has a successful connection, the corresponding indicator lights blue.
	During transmitting or receiving data through the LAN port the indicator blinks blue.

## 2.3.2 Rear Panel

The figure below shows the rear panel of the router.



<b>DC IN</b>	The Power socket is where you will connect the power adapter.
<b>RST/WPS</b>	<b>RST:</b> With the router powered on, press and hold the button until the CPU LED becomes quick-flash from slow-flash. And then release the button and wait the router to reboot to its factory default settings.
	<b>WPS:</b> If you have client devices you can press this button to quickly establish a router and client devices and automatically configure wireless security for your wireless network.
<b>WAN</b>	This port is where you will connect the DSL/cable Modem, or Ethernet.
<b>1/2/3/4 LAN</b>	This port connects the router to local PC.

**Note:** Press and hold RST/WPS button for about less than 5 seconds and the CPU LED indicator changes its lighting, it is WPS working. If more than 5 seconds and the CPU LED not response, the router will reboot to default factory settings.

# 3. **HARDWARE INSTALLATION**

---

## 3.1 Hardware Installation

For those computers you wish to connect with Internet by this router, each of the computers must be properly connected with the router through provided UTP LAN Cables.

1. Connect the provided UTP LAN cable to one of the router's LAN port.
2. Connect the other end of the UTP LAN cable to your computer's LAN port.
3. Connect the second UTP LAN cable to router's WAN port.
4. Connect the other end of the UTP LAN cable to ADSL or Modem port.
5. Plug the Power Adapter into the Router and then into an outlet.
6. Turn on your computer.
7. Check and confirm that the Power LED and LAN LED on the router are ON.

## 3.2 Check the Installation

The control LEDs of the WLAN Router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, CPU, LAN, WLAN and WAN port LEDs of the WLAN Router will blink for one second indicating a normal status.
2. When the WAN Port is connected to the ADSL/Cable modem, the WAN LED will light up.
3. When the LAN Port is connected to the computer system, the LAN LED will light up.

## 3.3 Set up the Computer

The default IP address of the Router is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description.

Connect the local PC to the LAN port on the Router. There are then two ways to configure the IP address for your PC.

### ◆ **Configure the IP address manually**

Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (Router's default IP address).

### ◆ **Obtain an IP address automatically**

Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the Router. Open a command prompt, and type in **ping 192.168.1.1**, then press **Enter**.

```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

If the result displayed is similar to that shown in above figure, it means that the connection between your PC and the Router has been established.

```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>_
```

If the result displayed is similar to that shown in the above figure, it means that your PC has not connected to the Router successfully. Please check it following below steps:

**1. Is the connection between your PC and the Router correct?**

If correct, the LAN port on the Router and LED on your PC's adapter should be lit.

**2. Is the TCP/IP configuration for your PC correct?**

Since the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

## 4. CONNECTING TO INTERNET

---

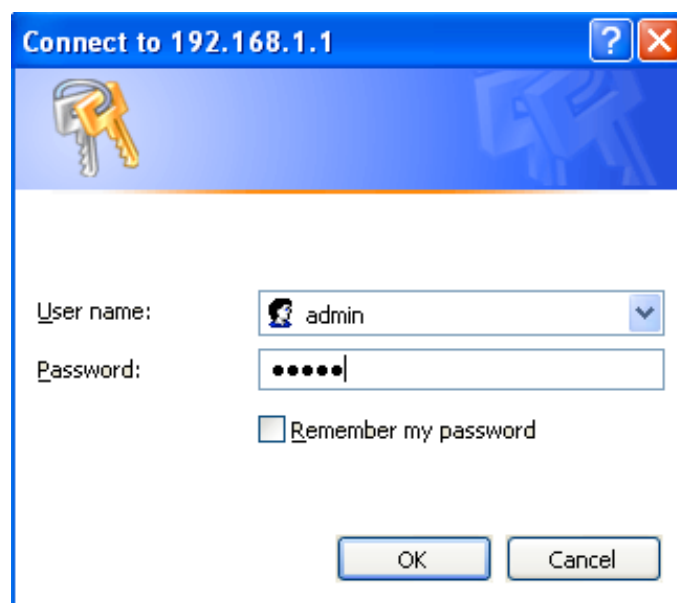
This chapter introduces how to configure the basic functions of your router to access Internet.

### 4.1 Accessing Web page

Connect to the Router by typing 192.168.1.1 in the address field of Web Browser. Then press **Enter** key.



It will show up the following page that requires you to enter valid User Name and Password:



Enter **admin** for User Name and Password, both in lower case letters. Then click **OK** button or press **Enter** key.

**Note:** If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the **Using Proxy checkbox**, and click **OK** to finish it.  
If the User Name and Password are correct, you can configure the router using the web browser.

Now you have logged into the web interface of the router.



Model no.N01-R151DC firmware Version: V3.1

**System Status**

**System Information**

system run time:	0 Day, 01:19:52
Firmware Version:	V3.1, 2012 Year 10 Month 25 Day Thursday

**LAN**

MAC Address	78:44:76:F9:7C:A2
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
DHCP IP Pool	192.168.1.2-192.168.1.254

**WAN**

MAC Address	78:44:76:F9:7C:A1
Connection	Dynamic IP Disconnect
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	0.0.0.0 0.0.0.0

**Wireless**

Access Point Name	NETPRO
Wireless Mode	11b/g/n Mixed

© 2013 Netpro Technologies, CO., LTD. All Rights Reserved

## 4.2 Changing Password

First, we recommend that you change the password to protect the security of your router. Please go to **Management—Password** change the password required to log into your Router.

**Administrator Settings**

**Administrator (The Login Name is "admin")**

New Password	*****
Comfirm Password	*****

**Remote Management**

Enable  Disable

IP Address	
Port	80

**New Password:** new password is used for administrator authentication.

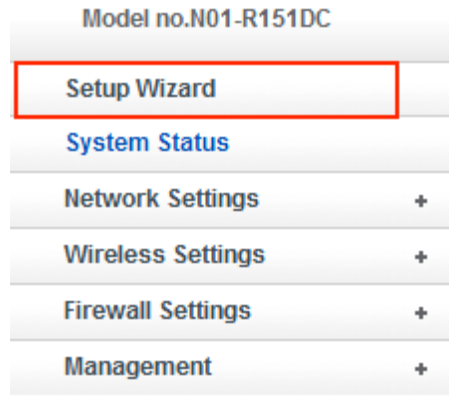
**Confirm Password:** new password should be re-entered to verify its accuracy.

**Note:** password length is 8 characters maximum, characters after the 8<sup>th</sup> position will be truncated.

The **Remote Management** part we will discuss later. Now just keep the setting not change and click **apply**.

## 4.3 Setup Wizard

**Setup Wizard** is provided as part of the web configuration utility. Users can simply follow the step-by-step process to get the Wireless Router configuration ready to run in 3 easy steps by clicking on the **Setup Wizard** on the left navigation menu.



Then the following screen will appear. Please click **Next** to continue.

### Setup Wizard

Welcome to the Network Setup Wizard.

The Network Setup will guide the four quick steps to networking. Please click "Next".

**Step 1. Select Internet connection type**

**Step 2. Setup Internet connection**

**Step 3. Setup wireless setting and Finish**

**Next**

### 4.3.1 WAN Type

This interface is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. There are three methods provided to allow you to access Internet. Please choose the appropriate one according to the information provided by your ISP (Internet Service Provider).

### Select WAN Type

Select the connection method to connect to your ISP. Click "Next" to continue.

<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from your ISP.
<input type="radio"/> Static IP Address	Set static IP information provided to you by your ISP.
<input type="radio"/> PPPoE	Choose this option if your ISP uses PPPoE.

#### 4.3.1.1 Dynamic IP Address

If you choose Dynamic IP Address, you will get a dynamic IP address from your ISP automatically. Click **Next** button, you will see the following page:

##### Set dynamic IP address

Please enter a particular host name or host-specific MAC addresses. Use the button to copy the MAC address of the Ethernet Card and replace the WAN MAC address with the MAC address of the router. Click "Next" to continue.

Host Name	<input type="text" value="NETPRO"/> (Optional)
MAC Address	<input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/> - <input type="text" value=""/> (Optional) <input type="button" value="Clone MAC Address"/>

**Host Name:** defines the DNS host name. By default, it is NETPRO.

**MAC Address:** MAC address is the physical address of your computer's network card. Generally, every network card has one unique MAC address.

**Clone MAC Address:** Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

The settings above is not required, you can just keep them not change.

#### 4.3.1.2 Static IP Address

If your ISP has provided the fixed IP that enable you to access Internet, please choose this option and click **Next** button.

##### Set static IP address

Set static IP information provided to you by your ISP. Click "Next" to continue.

WAN IP Address	<input type="text" value="0.0.0.0"/>
WAN Subnet Mask	<input type="text" value="0.0.0.0"/>
WAN Gateway	<input type="text" value="0.0.0.0"/>
Primary DNS Address	<input type="text"/>
Secondary DNS Address	<input type="text"/> (Optional)

**WAN IP Address:** the IP address provided by your ISP.

**WAN Subnet Mask:** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it

is provided by your ISP.

**WAN Gateway:** This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

**Primary DNS Address:** The Domain Name System (DNS) is an Internet “phone book”, which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requested are forwarded by this router.

**Secondary DNS Address:** this is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

#### 4.3.1.3 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as wireless device or cable modem. All the users over the Ethernet can share a common connection. If you use ADSL virtual dial-up to connect Internet, please choose this option.

##### PPPoE Settings

The service name is optional, but if your ISP requires this information, please enter the appropriate value. Click "Next" to continue.

User Account	<input type="text"/>
User Password	<input type="password"/>
Confirm Password	<input type="password"/>
Service Name	<input type="text"/> (Optional)

**User Account:** a specific valid ADSL user name provided by your ISP.

**User Password:** the corresponding valid password provided by your ISP.

**Confirm Password:** re-enter the password you typed in to ensure the accuracy of the password.

**Service Name:** this is optional. It describes your ISP's service name.

#### 4.3.2 Wireless Setting

Click **Next** to go to the Wireless Setting page, on this page, you can only change the SSID name and set the Pass Phrase (wireless password).

### Wireless Setting

Click "**Back**" to back to previous steps to change the settings after the completion of the Connection Wizard. Click "**Finish**" to save the current settings and will reboot PROLiNK Wireless Access Point.

Network Name(SSID)	<input type="text" value="NETPRO"/>
Pass Phrase	<input type="text"/>

<input type="button" value="Back"/>	<input type="button" value="Finish"/>	<input type="button" value="Exit"/>
-------------------------------------	---------------------------------------	-------------------------------------

Click **Finish** to complete the Setup Wizard. Now you can surf Internet and enjoy the best wireless experience brought by this router.

**Note:** After you set the Pass Phrase, please remember your Network Name (SSID). Then search for the SSID on your PC to build a wireless connection with the device. So you can enjoy the wireless function of this Router.

# 5. ADVANCED SETTINGS

This chapter allows users to configure advanced settings includes Wireless, Network Settings, Firewall and Management. These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Also they should not be changed unless you know what effect the changes will have on your wireless router.

## 5.1 System Status

The System Status provides basic network settings of this Router, including LAN and WAN interface information, and Wireless settings. Also, you could get the current running firmware version or firmware related information from this presentation.

### System Status

#### System Information

system run time:	0 Day, 01:39:32
Firmware Version:	V3.1, 2012 Year 10 Month 25 Day Thursday

#### LAN

MAC Address	78:44:76:F9:7C:A2
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
DHCP IP Pool	192.168.1.2-192.168.1.254

#### WAN

MAC Address	78:44:76:F9:7C:A1
Connection	Dynamic IP Disconnect
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	0.0.0.0 0.0.0.0

#### Wireless

Access Point Name	NETPRO
Wireless Mode	11b/g/n Mixed

### System Information

**System run time:** shows how long the system has run.

**Firmware Version:** displays the current firmware version of the Router.

### LAN

**MAC Address:** shows the MAC address of the LAN interface.

**IP Address:** displays the IP address of the LAN interface.

**Subnet Mask:** shows the subnet mask address of the LAN interface.

**DHCP Server:** displays the current status of DHCP server of the LAN interface.

**DHCP IP Pool:** the IP address range that the DHCP server can assign to every PC connected to this device.

### WAN

**MAC Address:** displays the MAC address of the WAN interface.

**Connection:** displays the connection type of the WAN port.

**IP Address:** shows the IP address of the WAN interface.

**Subnet Mask:** displays the subnet mask of the WAN interface.

**Default Gateway:** displays the assigned IP address of the default gateway.

**DNS:** shows the DNS address.

## Wireless

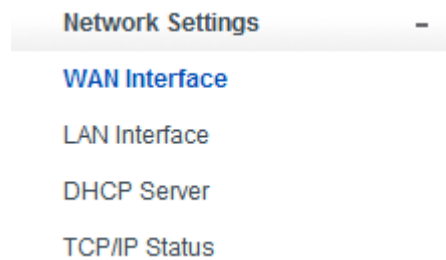
**Access Point Name:** displays the name of the Router.

**Wireless Mode:** shows the IEEE standards it complies with.

**Frequency (Channel):** shows the frequency/Channel it works in.

**Network Name (SSID):** displays the SSID of the Router.

## 5.2 Network Settings



### 5.2.1 WAN Interface

This page is used to configure the parameters for the WAN port of your Access Point. Since we have discussed this setting on **Setup Wizard**, here we introduce the **MTU** value.

**WAN Settings**

<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address automatically from your ISP.
<input type="radio"/> Static IP Address	Set static IP information provided to you by your ISP.
<input type="radio"/> PPPoE	Choose this option if your ISP uses PPPoE.

**Dynamic IP Address**

Host Name	<input type="text" value="NETPRO"/> (Optional)
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> (Optional) <input type="button" value="Clone MAC Address"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/> (Optional)
MTU	<input type="text" value="1500"/>
Auto Reconnection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**MTU:** It means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency. The default value is 1500.

**Auto Reconnection:** this function is enabled by default.

## 5.2.2 LAN Interface

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP. This page allows you to configure the parameters for LAN which connects to the LAN port of your Access Point.

LAN Settings	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Domain Name	<input type="text" value="NETPRO"/> (Optional)
DNS Relay	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LAN SPEED	<input type="radio"/> 10M <input type="radio"/> 100M <input checked="" type="radio"/> AUTO

**IP Address:** This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

**Subnet Mask:** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

**Domain Name:** this is optional, by default, it is NETPRO.

**DNS Relay:** you can choose to enable or disable this function. By default, it is Enable selected.

**LAN SPEED:** choose the LAN data rate. This router supports 10M/100M/AUTO.

## 5.2.3 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically. DHCP server means that all the computers connected to this router will get the IP address dynamically.

DHCP Server	
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Starting IP Address	192.168.1. <input type="text" value="2"/>
Ending IP Address	192.168.1. <input type="text" value="254"/>
Lease Time	<input type="text" value="86400"/> second

**Starting IP Address:** displays the start IP Address of the range that will be assigned to each computer connected with the router.

**Ending IP Address:** displays the ending IP Address of the range that will be assigned to



each computer connected with the router.

**Lease Time:** the IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

**Static DHCP**

Enable  Disable

Host Name	<input type="text"/>
IP Address	192.168.1. <input type="text"/>
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
DHCP Client	SN-201203131531,192.168.1.2,50:E5:49:E <input type="button" value="Clone"/>

Static DHCP function allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server. You can enable or disable this function.

**Host Name:** this represents the name of your IP address.

**IP Address:** displays the IP Address that you want to assign to network device.

**MAC Address:** the MAC Address of the computer that reserves the IP address.

**DHCP Client:** it displays the detailed computer information in the LAN.

The following table shows information about Static/Dynamic DHCP Clients.

Static DHCP Client Table			0/32
Host Name	IP Address	MAC Address	
<b>Dynamic DHCP Client Table</b> <span style="float: right;">1/253</span>			
Host Name	IP Address	MAC Address	Expired Time
SN-201203131531	192.168.1.2	50:E5:49:BB:44:96	Mar/21/2038 14:50:11

## 5.2.4 TCP/IP Status

This page displays the LAN and WAN interface settings of this router. Please see below:

### LAN

MAC Address	78:44:76:F9:7C:A2
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable

### WAN

MAC Address	78:44:76:F9:7C:A1
Connection	Dynamic IP Disconnect
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	0.0.0.0 0.0.0.0

## 5.3 Wireless

<a href="#">Wireless Settings</a>	-
<a href="#">Wireless Status</a>	
<a href="#">Wireless Basic Settings</a>	
<a href="#">Wireless Security Settings</a>	
<a href="#">WDS Settings</a>	
<a href="#">WPS Configuration Setup</a>	
<a href="#">Repeater Settings</a>	
<a href="#">Advanced Settings</a>	

### 5.3.1 Wireless Status

This page displays the current wireless status of the router.

#### Wireless

Access Point Name	NETPRO
Wireless Mode	11b/g/n Mixed
Frequency (Channel)	2462 MHz(Channel 11)
Broadcast Network Name (SSID)	Enable

#### Station Associate List

AID	MAC Address	802.11 PhyMode	BandWidth	Link Rate	Signal Power
-----	-------------	----------------	-----------	-----------	--------------

#### apclient status

Repeater	disable
----------	---------

## 5.3.2 Wireless Basic Settings

On this page, you could configure the parameters for Wireless LAN clients that may connect to your Access Point.

Wireless Network	
Network Mode	11b/g/n Mixed Mode ▾
Network Name(SSID)	NETPRO
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	78:44:76:F9:7C:A0
Country Code	USA,Canada ▾
Frequency (Channel)	2462MHz (Channel 11) ▾
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Extension Channel	2442MHz (Channel 7) ▾

Apply

**Network Mode:** This option allows you to choose the radio standard for operation of your Router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. Here, by default, the 11b/g/n Mixed Mode is selected, this mode offers better compatibility.

**Network Name (SSID):** The name of the wireless network.

**Multiple SSID:** this router supports three SSID settings for wireless connections.

**BSSID:** the basic SSID number.

**Country Code:** this device supports 4 country codes: USA, Canada, China and Japan. You can choose one based on your position.

**Frequency (Channel):** This option provides selectable channel numbers.

**Channel Bandwidth:** This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

**20MHz** is the standard channel spectrum width.

**40MHz** is the channel spectrum with the width of 40MHz.

**Extension Channel:** It indicates the use of channel bonding that allows the network to use two channels at once. Using two channels improves the performance of the Wi-Fi connection. By default, it is Channel 9 selected.

### 5.3.3 Wireless Security Settings

This page enables you to set wireless security method that control how the subscriber station associates to a wireless device and encrypts/decrypts data.

Select SSID	NETPRO
<b>Security Policy</b>	
Security Mode	Disable
<b>Wireless Network Access</b>	
MAC Access Control	<input checked="" type="radio"/> Disabled <input type="radio"/> Allow <input type="radio"/> Deny
Access List	<input type="button" value="Add MAC address"/>

**Select SSID:** if you have defined many SSIDs, please choose the one that you want to set security for. By default, it is NETPRO.

#### Security Policy

##### 5.3.3.1 WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.

<b>Wire Equivalence Protection (WEP)</b>	
Authentication Type	Open System
WEP Key Length	64 bit (10 hex digits/ 5 ascii keys)
WEP Key Entry Method	Hexadecimal
WEP Keys	WEP Key 1 : 11111
	WEP Key 2 : 11111
	WEP Key 3 : 11111
	WEP Key 4 : 11111
Default Key	Key 1

**Authentication Type:** filed relates only to the WEP security option. One of the following authentication modes should be selected if WEP security method is used:

- Open System—station is authenticated automatically by AP (selected by default).
- Shared Key—station is authenticated after the challenge, generated by AP.

**WEP Key Length:** 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The 128-bit option will provide a bit higher level of wireless security.

**WEP Key Entry Method:** Hexadecimal (selected by default) or ASCII option specifies the character format for the WEP key if WEP security method is used.

**WEP Keys:** WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used:

For 64-bit—specify WEP key as 10 Hex (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.

For 128-bit—specify WEP key as 26 Hex (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

**Default Key:** if you set many keys, you could set one to be the default key.

### 5.3.3.2 802.1x

You could choose to enable or disable WEP here. For RADIUS parameters, you need to provide the following information:

Security Policy					
Security Mode	802.1X				
802.1X					
WEP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
RADIUS					
RADIUS Server	IP Address	Port	Shared Secret	Session Time Out	Idle Time Out
		1812	12345	0	0

**IP Address:** enter the IP address of RADIUS server.

**Port:** the UDP port number that the RADIUS server that is used to authenticate the messages sent between them.

**Shared Secret:** it works like a password.

**RADIUS:** Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet Service Provides. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

### 5.3.3.3 WPA/WPA2

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry. It is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

Security Policy	
Security Mode	WPA
<b>WPA</b>	
Authentication Mode	WPA-Personal
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Pass Phrase	12345678
Key Renewal Method	Disable
Key Renewal Interval	3600

**Authentication Mode:** you could choose one from the following options.

A dropdown menu showing the following options: WPA-Personal, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WPA/WPA2-Personal(Mixed Mode), and WPA/WPA2-Enterprise(Mixed Mode).

**WPA2:** it means Wi-Fi Protected Access 2, it is the current most secure method of wireless security and required for 802.11n performance. This mode allows you to choose **TKIP+AES** Algorithm. If you choose Enterprise related modes, you are required to enter **RADIUS Server**.

### WPA Algorithms

**TKIP**--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA.

**AES**--also know as CCMP, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, which uses the Advanced Encryption Standards (AES) algorithm.

**Pass Phrase:** This is a pre-defined key used for encryption during data transmission. It has two formats: Passphrase and Hex (64 characters). Then you need to enter the Pre-Shared Key, either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**Key Renewal Method:** you can choose to disable this function or choose to renew by time or packet.

**Key Renewal Interval:** please set the renewal interval.

***Note:** Since WEP has been proved vulnerable, you may consider using WPA2 for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and/or privacy on your wireless network.*

**MAC Access Control:** you could choose to disable this function, or allow/deny.

**Access List:** click **Add MAC address** button, it will show you the following page:

### Access Control List

MAC Address must be entered with colon (:) as follows Example: 00:11:56:CC:01:C3

MAC Address		MAC Address	
MAC 1:	<input type="text" value="00:00:00:00:00:00"/>	MAC 8:	<input type="text" value="00:00:00:00:00:00"/>
MAC 2:	<input type="text" value="00:00:00:00:00:00"/>	MAC 9:	<input type="text" value="00:00:00:00:00:00"/>
MAC 3:	<input type="text" value="00:00:00:00:00:00"/>	MAC 10:	<input type="text" value="00:00:00:00:00:00"/>
MAC 4:	<input type="text" value="00:00:00:00:00:00"/>	MAC 11:	<input type="text" value="00:00:00:00:00:00"/>
MAC 5:	<input type="text" value="00:00:00:00:00:00"/>	MAC 12:	<input type="text" value="00:00:00:00:00:00"/>
MAC 6:	<input type="text" value="00:00:00:00:00:00"/>	MAC 13:	<input type="text" value="00:00:00:00:00:00"/>
MAC 7:	<input type="text" value="00:00:00:00:00:00"/>	MAC 14:	<input type="text" value="00:00:00:00:00:00"/>

If you choose **allow**, then type in the MAC address that you want to allow to access your wireless network. If you choose **deny**, then enter the MAC address that you deny to access your wireless network. Click **Apply** button to make the change work.

### 5.3.4 WDS Settings

Wireless Distribution System means connecting multiple wireless networks to one. It will use two or more wireless bandwidth Router/AP connecting with each other to expand wireless signal to longer distance. This mode is suitable for medium-size networks like school and enterprise network.

AP's BSSID	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="button" value="search AP"/>
Phy Mode	<input type="text" value="CCK"/> <input type="button" value="v"/>	
Max number of AP is 4.		<input type="button" value="Add"/>
AP's BSSID	Phy Mode	<input type="button" value="Del"/>

**AP'S BSSID:** you need to enter the SSID of other AP that this device can search for. Click **search AP** button to search for AP's SSID.

**Phy Mode:** the device supports 4 modes: CCK, OFDM, HIMIX and GREENFIELD.

### 5.3.5 WPS Configuration Setup

**WPS** (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2. It is enabled by default.

WiFi Protected Setup	Enable ▾	
<b>WPS Current Status :</b>	<b>Unconfigure</b>	<b>PinCode : 63503685</b>
UUID	28802880-2880-1880-a880-784476f97ca0	
Enable Proxy	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
Use Internal Registrar	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled

**UUID:** Universally Unique Identifier.

**Enable Proxy:** you can choose to enable Proxy or disable this function. By default, it is enabled.

**Use Internal Registrar:** you can choose to use Internal Registrar function. By default, it is enabled.

**WPS MODE**

Configure Option	Configure Device via PIN ▾
	Configure Device via PIN
	Configure Device via push-button

**Write Pin Code**

Pin Number	63503685
------------	----------

---

**Wi-Fi Protected Setup Information**

SSID	NETPRO_WPS_XXXX
Authentication Mode	OPEN
Encryption Type	NONE

---

**WPS Reset Configuration**

Reset	<input type="radio"/> Yes	<input checked="" type="radio"/> No
-------	---------------------------	-------------------------------------

**Configure Option:** this router allow you to configure WPS function by PIN or via push button. Choose one you like.

**Pin Number:** if you choose to configure WPS by PIN, then set the Pin number here.

**Reset:** you can choose to reset or not.



## 5.3.6 Repeater Settings

Repeater Function	<input type="text" value="Enable"/>
<b>Wireless Network</b>	
Network Name(SSID)	<input type="text" value="NETPRO"/> <input type="button" value="search AP"/>
BSSID	<input type="text"/>
Channel	<input type="text" value="2462MHz (Channel 11)"/>
EXT Channel	<input type="text" value="lower"/>
Security Mode	<input type="text" value="Disable"/>

**Network Name (SSID):** if you enable the Repeater function, you need to enter the wireless SSID or search for it by clicking **search AP**.

**BSSID:** Basic SSID. This is optional.

**Channel:** this option provides selectable channel numbers.

**EXT Channel:** you could choose Low or Upper.

**Security Mode:** this device supports two security Modes: WEP and WPA. You can refer to wireless security settings to configure this parameter.

## 5.3.7 Advanced Settings

Advanced Wireless	
BG Protection Mode	Auto ▾
Basic Data Rates	Default(1-2-5.5-11 Mbps) ▾
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input type="radio"/> Disable (only in A band)
20/40 BssCoexSupport	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wi-Fi Multimedia	
WMM Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	WMM Configuration

**BG Protection Mode:** Background Protection Mode, by default, it is Auto selected.

**Basic Data Rates:** you can choose the wireless data rate. This router provides three options. By default, it is Default (1-2-5.5-11Mbps).

**Beacon Interval:** By default, it is set to 100ms. Higher Beacon interval will improve the device's wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

**Data Beacon Rate (DTIM):** by default, its value is 1.

**Fragment Threshold:** specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

**RTS Threshold:** determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347 bytes. The default value is 2347, which means that RTS is disabled.

**RTS/CTS** (Request to Send / Clear to send) are the mechanism used by the 802.11 wireless networking protocols to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the

node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses Request to Send/Clear to send frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provide clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

**TX Power:** display the data transmission rate power.

**Short Preamble:** this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field. By default, it is disabled.

**Short Slot:** by default, this is enabled.

**Tx Burst:** enable this function will make it easy for you to enhance the performance in data transmission.

**Pkt\_Aggregate:** by default, this is disabled.

**IEEE 802.11H Support:** you can't change this option.

**20/40 BssCoexSupport:** by default, it is enabled. Support 20/40 at the same time.

**IGMP Snooping:** if you enable this function, multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.

**WMM Capable:** by default, it is disabled.

**WMM** is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.

**WMM Parameters:** you could click **WMM Configuration** button to configure WMM Parameters. See below:

### WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

### WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

## 5.4 Firewall

<b>Firewall Settings</b>	-
<a href="#">Access Control</a>	
<a href="#">IP/Port Filtering</a>	
MAC Filtering	
URL Filtering	
Port Trigger	
Virtual Server	
DMZ	

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of this router helps to protect you local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

## 5.4.1 Access Control

**Access Control**

Enable  Disable

Name

Action  Allow  Deny

	Interface	IP Range	Protocol	Port Range
Source	* <input type="text"/>	<input type="text"/> - <input type="text"/>		
Destination	* <input type="text"/>	<input type="text"/> - <input type="text"/>	TCP <input type="text"/>	<input type="text"/> - <input type="text"/>
Schedule	<input checked="" type="radio"/> Always <input type="radio"/> From time <input type="text"/> : <input type="text"/> <input type="text"/> AM to <input type="text"/> : <input type="text"/> <input type="text"/> <input type="text"/> AM day <input type="text"/> to <input type="text"/>			

Firewall List

0/32 (Lots/Total Lots)

Action	Name	Source	Destination	Protocol
--------	------	--------	-------------	----------

First, you can choose to enable or disable this function according to your needs.

**Name:** Enter the name of the router.

**Action:** you could choose to allow or deny the following addresses entered by you.

**Source:** select the interface of the address, and enter the starting IP address that you want to deny or allow.

**Destination:** select the interface of the address, and enter the ending IP address that you want to deny or allow. About the Port Range, choose the protocol and enter IP range.

**Schedule:** this router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocol (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions. You have to set your time before set schedule.

## 5.4.2 IP/Port Filtering

Depending on whether there is an existing Internet connection, or in other words “the WAN link status is up or down”. You can restrict certain types of data packets from your local network to Internet through the Gateway on this page.

### IP Filters

Enable  Disable

IP Address  -

Port  -

Protocol Type

Schedule

Always

From time  :  AM to  :  AM

day  to

Apply

### IP Filter List

0/32 (Lots/Total Lots)

IP Range	Protocol	Schedule
----------	----------	----------

You can select to enable or disable IP/Port Filtering function. By default, it is disabled.

**IP Address:** the IP address range that you want to filter.

**Port:** the Port address that you want to filter.

**Protocol Type:** choose which particular protocol type should be filtered. Here you can choose UDP/TCP.

**Schedule:** you can choose to always enable this filter function or create a schedule.

**IP Filter List:** this table will list the detailed information about the IP addresses that you want to filter.

### 5.4.3 MAC Filtering

On this page, you can add some MAC addresses to be filtered to isolate users' access from wired LAN.

Use MAC address to allow or deny computers access to the network.

Disable MAC Filters

Only allow computers with MAC address listed below to access the network

Only deny computers with MAC address listed below to access the network

MAC Name

MAC Address  -  -  -  -  -

DHCP Client

apply

### MAC Filter List

0/32 (Lots/Total Lots)

MAC Name	MAC Address
----------	-------------

This router allows you to disable MAC Filtering function or allow/deny MAC address listed.

**MAC Name:** the name of the computer with the MAC you entered.

**MAC Address:** you can enter the MAC addresses that you want to deny or allow.

**DHCP Client:** display the information about one DHCP client.

**MAC Filter List:** this table will list the detailed information about the MAC addresses that will be filtered.

### 5.4.4 URL Filtering

This page is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed.

**Block those URLs which contain keywords listed below.**

Enable  Disable

URL string

0/32  
(Lots/Total Lots)

You can choose to enable or disable URL filtering function.

**URL string:** type in the string contained in URLs that you don't allow LAN users to access.

Enter the URLs that you don't allow LAN users to access. And you can also click **Delete** button to delete the URLs you entered.

### 5.4.5 Port Trigger

This page allows you to trigger port for the traffic of special applications. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Enable  Disable

Name	<input type="text"/>
Trigger Port	<input type="text"/> - <input type="text"/>
Trigger Type	TCP <input type="button" value="v"/>
Public Port	<input type="text"/>
Public Type	TCP <input type="button" value="v"/>

Special Applications List 0/32 (Lots/Total Lots)

Name	Trigger	Public Port
------	---------	-------------

**Enable/Disable:** you can choose to enable or disable this function.

**Name:** please enter the name of the defined network application/service.

**Trigger Port:** type in the starting & ending ports number of the service.

**Trigger type:** Specify the transport layer protocol. It could be TCP, UDP or both.

**Public Port:** type in the public port number.

**Public Type:** choose one transport layer protocol.

**Special Application List:** this table will list the detailed information about the ports that you set before.

## 5.4.6 Virtual Server

Enable  Disable

Name	<input type="text"/>
Private IP Address	<input type="text"/>
Protocol Type	TCP <input type="button" value="v"/>
Public Port	<input type="text"/> ~ <input type="text"/>
Private Port	<input type="text"/>
Schedule	<input checked="" type="radio"/> Always <input type="radio"/> From time <input type="text" value="00"/> : <input type="text" value="00"/> AM <input type="button" value="v"/> to <input type="text" value="00"/> : <input type="text" value="00"/> AM <input type="button" value="v"/> day <input type="text" value="Sunday"/> <input type="button" value="v"/> to <input type="text" value="Sunday"/> <input type="button" value="v"/>

Virtual Server List

0/32 (Lots/Total Lots)

Name	Private IP Address	Protocol	Schedule
------	--------------------	----------	----------

You could choose to enable or disable this function according to your requirement.

**Name:** defines the name for this virtual server.

**Private IP Address:** the IP of the host that is connected to the internal network and needs to be accessible from external network.

**Protocol Type:** the L3 protocol type of the IP Address.

**Public Port:** range of the public port number.

**Private Port:** range of the private port number. It is the TCP/UDP port of the application running on the host that is connected to the internal network.

**Schedule:** you can set the schedule for this virtual server.

**Virtual Server List:** the virtual server list will show you the detailed information about the server computers.



### 5.4.7 DMZ

DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible form the external network side.

Enable  Disable

IP Address 192.168.1.

You can choose to enable or disable DMZ function.

**IP Address:** types in the IP address of the DMZ host

## 5.5 Management

- Management -
- Traffic Statistics
- DDNS
- Time Zone Setting
- System Log
- Upgrade Firmware
- Save/Reload Settings
- Password
- Reboot

### 5.5.1 Traffic Statistics

This page displays the packet counters for transmission and reception regarding to wireless and Ethernet networks.

#### Traffic Statistics

	Receive	Transmit
WAN	0 Packets	0 Packets
LAN	3985 Packets	4855 Packets
WIRELESS	524556 Packets	14517 Packets

## 5.5.2 DDNS

DDNS means Dynamic Domain Name System. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. This router supports three service providers: DynDns, no-ip and 3322. Please log in the websites to register for free DDNS service.

DDNS	
DDNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Provider	<input type="text"/>
Host Name	<input type="text"/>
User Name / E-Mail Address	<input type="text"/>
Password	<input type="text"/>

Apply

You could choose to enable or disable DDNS function.

**Service Provider:** choose one service provider where you have applied for free DDNS service.

**Host Name:** type in the host name you registered from the DDNS provider.

**User Name/Email Address:** enter the User Name or Email you registered from the DDNS provider.

**Password:** enter the Password or Key you set for the User Name.

### 5.5.3 Time Zone Settings

This page allows you to maintain the system time by synchronizing with a public time server over the Internet.

**Time**

Local Time : January 1, 1970 3:21:18

---

**Set the system time :**

Enable NTP  
 Your Computer  
 Manual Setting

Time Zone : (GMT-05:00) Bogota, Lima, Quito

Daylight Saving :  Enable  Disable

---

**Set the Time automatically from NTP Server**

Default NTP Server : 0.pool.ntp.org (Optional)

Set the Time:Year 2012 Month Nove Day 5 Hour 17 Minute 8 Second 22

Apply

**Local Time:** it shows the current time by default.

**Enable NTP:** NTP means Network Time Protocol which is used to make the computer time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.

**Time Zone:** Select the Time Zone where the router is located.

**Daylight Saving:** If the Time Zone you choose implements daylight saving time, please select this option. By default, it is disabled.

**Default NTP Server:** Please choose the corresponding NTP server to get right time. This is optional.

**Set the Time:** please set the right time according to your location.

## 5.5.4 System Log

This page can be used to set remote log server and show the system log.

View Log displays the activities. Click on Log Settings for advance features.

First Page Last Page Previous Next Clear Log Settings

Refresh

page 1 of 3

Time	Message
Jan/1/1970 02:57:35	[WLAN] Main bssid = 78:44:76:f9:7c:a0
Jan/1/1970 02:57:35	[WLAN] MCS Set = ff 00 00 00 01
Jan/1/1970 02:57:35	[WLAN] pAd->TxPowerCtrl.bInternalTxALC == FALSE !
Jan/1/1970 02:57:35	[WLAN] 3. Phy Mode = 9
Jan/1/1970 02:57:35	[WLAN] 2. Phy Mode = 9
Jan/1/1970 02:57:35	[WLAN] 1. Phy Mode = 9
Jan/1/1970 02:57:35	[WLAN] Key4Str is Invalid key length(5) or Type(0)
Jan/1/1970 02:57:35	[WLAN] Key3Str is Invalid key length(5) or Type(0)
Jan/1/1970 02:57:35	[WLAN] Key2Str is Invalid key length(5) or Type(0)

Click **Log Settings** button, it will display the page below:

Logs can be saved by sending it to an admin email address or a storage server.

Remote Syslog Server

Remote Syslog Server / IP Address   Enable  Disable

E-Mail Notification

SMTP Server / IP Address

E-mail Address

Save Logs To Local Hard Drive

Log Type

System Activity

Debug Information

Attacks

Dropped Packets

Notice

**Remote Syslog Server/IP Address:** enter an IP address that allows syslog remote sending function while System log messages are sent to a remote server.

**SMTP Server/IP:** enter a SMTP Server address.

**Email Address:** enter an Email address.

**Log Type:** you can choose one type for log.

### 5.5.5 Upgrade Firmware

This page allows you to upgrade the Access Point firmware to new version. Please note, DO NOT power off the device during the upload because it may crash the system.

Firmware Upgrade	
Firmware Version	3.1
Build Date	Fri Oct 26 18:39:20 KST 2012

To upgrade manually

1. Download a firmware at [ [www.netpro.asia](http://www.netpro.asia) ].
2. Click [Browse] and choose a downloaded firmware
3. Click [Upgrade] button.

No file chosen

**Note.**

- Internet will be unavailable for upgrading firmware.
- Power down for updating firmware can be the cause of system halt.

**Current Firmware Version:** shows the current firmware version.

**Firmware Date:** the date that you upgrade the current firmware.

**Firmware Upgrade:** select the firmware version on your computer then click **Apply** to upgrade the firmware version.

### 5.5.6 Save/Reload Settings

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. Besides, you can reset the current configuration to factory default.

<b>Load Settings From Local Hard Drive</b>	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Load"/>
<b>Restore To Factory Default Settings</b>	<input type="button" value="Restore"/>
	<input type="button" value="Save Settings To Local Hard Drive"/>

**Load Settings From Local Hard Drive:** if you want to reload the settings from the file saved before, you could click **Choose File** button to choose the right file then click **Load** button.

**Restore To Factory Default Settings:** this **Restore** button is provided to allow you to restore the router settings to the default factory settings.

Click **Save Settings To Local Hard Drive** can save the settings to your computer.

## 5.5.7 Password

This page allows you to change the password to login web interface of this router. Also you can enable or disable the Remote Management function here.

**Administrator (The Login Name is "admin")**

New Password	<input type="password"/>
Comfirm Password	<input type="password"/>

**Remote Management**

Enable  Disable

IP Address	<input type="text"/>
Port	<input type="text" value="80"/>

**Remote Management:** if you enable this function, you can manage the router remotely.

**IP Address:** Enter the IP Address that you allow to manage the router remotely.

**Port:** choose the Port number.

## 5.5.8 Reboot

### Reboot

Reboot Device	<input type="button" value="Reboot"/>
---------------	---------------------------------------

Click this **Reboot** button to reboot your router quickly.

## 5.5.9 Warranty

NETPRO provides a limited 1 year warranty to all NETPRO products purchased. The warranty covers the main device, antenna and external power supply failures due to defects in material or workmanship. Packaging, various cables, software products, technical data and other accessories are not covered here. The maximum liability of NETPRO is equal to or no higher than the product's purchased price.