

User Guide

MWN-WAPR150N

Wireless-N Broadband Router



Copyright Statement

MEDIALINK is the registered trademark of Medialink Products, LLC. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Medialink Products, LLC. Without the permission of Medialink Products, LLC, any individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages.

All the photos and product specifications mentioned in this manual are for references only. As the upgrade of software and hardware, there will be changes. And if there are changes, Medialink is not responsible for informing in advance. If you want to know more about our product information, please visit our website at www.medialinkproducts.com.

Contents

CHAPTER 1 INTRODUCTION.....	1
1.1 PRODUCT FEATURES.....	2
1.2 PACKAGE CONTENTS.....	3
1.3 LED INDICATOR AND PORT DESCRIPTION	4
CHAPTER 2 HARDWARE INSTALLATION.....	7
2.1 HOW TO INSTALL THE ROUTER.....	7
2.1A DSL MODEM CONFIGURATION.....	11
2.1B NO MODEM ACCESS.....	12
2.2 OPTIMIZING WIRELESS RANGE	113
CHAPTER 3 HOW TO LOGIN TO THE ROUTER.....	14
3.1 HOW TO SET THE NETWORK CONFIGURATIONS	14
3.2 LOGIN TO THE ROUTER	17
CHAPTER 4 QUICK SETUP GUIDE	20
4.1 SETUP WIZARD.....	20
CHAPTER 5 ADVANCED SETTINGS	27
5.1 LAN SETTINGS	27
5.2 WAN SETTINGS.....	28
5.3 MAC ADDRESS CLONE	31
5.4 DNS SETTINGS.....	31
CHAPTER 6 WIRELESS SETTINGS (WLAN).....	32
6.1 BASIC SETTINGS.....	32
6.2 WIRELESS SECURITY SETTING	35
6.3 ADVANCED SETTINGS.....	38
6.4 WPS SETTINGS	40
6.5 WDS SETTINGS – BRIDGE/REPEATER	42
6.6 WIRELESS ACCESS CONTROL	45
6.7 CONNECTION STATUS	45

CHAPTER 7 DHCP SERVER	46
7.1 DHCP SETTINGS	46
7.2 DHCP LIST AND BINDING	47
CHAPTER 8 VIRTUAL SERVER	48
8.1 PORT RANGE FORWARDING	48
8.2 DMZ SETTINGS – GAMING/VIDEOCONFERENCING.....	50
8.3 UPNP SETTINGS	51
CHAPTER 9 TRAFFIC CONTROL.....	52
9.1 TRAFFIC CONTROL	52
CHAPTER 10 SECURITY SETTINGS	54
10.1 CLIENT FILTER SETTINGS	54
10.2 URL FILTER SETTINGS – WEBSITE BLOCKING	55
10.3 MAC ADDRESS FILTER – PARENTAL CONTROL	57
10.4 PREVENT NETWORK ATTACK - FIREWALL	58
10.5 REMOTE WEB MANAGEMENT	59
10.6 WAN PING	60
CHAPTER 11 ROUTING SETTING	61
11.1 ROUTING TABLE	61
CHAPTER 12 SYSTEM TOOLS	62
12.1 TIME SETTINGS	62
12.2 DDNS	63
12.3 BACKUP/RESTORE SETTINGS	64
12.4 RESTORE TO FACTORY DEFAULT SETTING	66
12.5 UPGRADE FIRMWARE	67
12.6 REBOOT THE ROUTER.....	68
12.7 PASSWORD CHANGE.....	68
12.8 SYSTEM LOG	70
12.9 LOGOUT	70
APPENDIX 1: GLOSSARY	71

Chapter 1 Introduction

Thank you for purchasing Medialink's 150Mbps Wireless N Router!

MWN-WAPR150N utilizes advanced technology compatible with IEEE802.11n and IEEE802.11g/b standards, it can provide up to 150Mbps stable transmission rate. Additionally, it includes router, wireless access point, four-port switch and firewall in one, dedicated to SOHOs (Small Office/Home Office) and family networking.

It supports WDS (Wireless Distribution System) function for repeating and amplifying the signals to extend the wireless network coverage. Besides, the Router also supports all of the latest wireless security features, such as 64/128-bit WEP, WPA, WPA2, WPA&WPA and WPS (PBC and PIN) encryption methods, packet filtering and port forwarding, to prevent unauthorized access and protect your network against malicious attack.

In addition, URL and MAC address filtering can make it easy for parents and network administrator to manage network and QoS bandwidth control over specific computer's downloading speed is supported as well. Moreover, UPnP and

WMM support can smooth your MSN voice, and the included Setup Wizard on CD-ROM will be quick and easy for non-savvy users to install the device and access the Internet.

1.1 Product Features

- Includes router, wireless access point, four-port switch and firewall in one
- Provides up to 150Mbps uploading and downloading speed
- Supports two WPS (Wi-Fi Protected Setup) encryption methods: PBC and PIN
- Compliant to IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3 and IEEE802.3u standards
- Supports 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- Supports RTS/CTS protocol and data partitioning function
- Provides one 10/100Mbps Auto-Negotiation Ethernet WAN port
- Provides four 10/100Mbps Auto-Negotiation Ethernet LAN ports
- Supports xDSL/Cable MODEM, static and dynamic IP in community networking
- Supports remote/local Web management

- Supports WMM to better smooth your voice and video
- Supports SSID stealth mode and access control based over MAC address (up to 30 entries)
- Supports Auto MDI/MDIX
- Supports wireless Roaming technology for high-efficient wireless connections
- Supports auto negotiation/manual mode for 802.11b/802.11g/802.11n
- Supports UPnP and DDNS
- Supports Firefox 1.0, IE5.5 or above
- Supports SNMP
- Supports virtual server, DMZ host
- Built-in firewall for hacker's attack prevention
- Supports DHCP server/client
- Supports auto wireless channel selection
- Supports LAN access control to the Internet
- Provides syslog to record the status of the router
- Supports WDS wireless network extension
- Supports QoS function
- Built-in omni-directional antenna

1.2 Package Contents

Please unpack the box and check the following items:

- One MWN-WAPR150N Wireless Broadband Router
- One Quick Installation Guide

- One Power Adapter
- One Network Cable
- One CD-ROM

If any of listed items are missing or damaged, please contact the Medialink reseller from whom you purchased for replacement immediately.

1.3 LED Indicator and Port Description

Front Panel and LED Indicator Show



LED indicator description on front panel (from L to R)

POWER

Solid indicates the power is connected and on.

SYS

Blinking indicates the system running.

WPS

When blinking, it indicates the device is negotiating with

client in WPS mode.

INTERNET (WLAN)

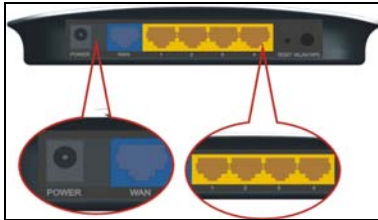
Wireless signal LED indicator. Blinking indicates the wireless function is enabled.

LAN (4, 3, 2, 1)

Wired local network LED indicator. Solid indicates it is connected with Ethernet device and the device is turned on; blinking indicates the device is transmitting and/or receiving data.

WAN

Wide area network indicator. Solid indicates the Router's WAN port is connected and working; blinking indicates the port is being transmitted and received data packets.

Back Panel Show:**Rear Panel: (From L to R)*****POWER***

The jack is for power adapter connection. Please use the included 9V DC power adapter.

WAN

A 100Mbps Ethernet port, can be connected with MODEM, Switch, Router and other Ethernet device for Internet connecting to DSL MODEM, Cable MODEM and ISP.

LAN (1, 2, 3, 4)

4 10/100Mbps Ethernet ports can be connected with Ethernet switch, Ethernet router and NIC card.

RESET

The system reset button (recessed). Use a small non-metallic object to press this button for 7 seconds. The settings configured in this device will be deleted and it will restore the settings to the default.

WLAN/WPS

WPS button. Press it for 1 second, the WPS feature will be enabled and WPS indicator will be shown blinking.

Chapter 2 Hardware Installation

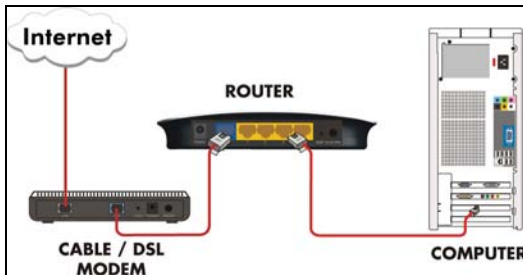
2.1 How to Install the Router

Please follow these instructions BEFORE you insert the CD.

Important Notes:

- The CD contains the EZ-Connect Setup Wizard, which is an alternative means to configure your router but is not required. There are no drivers or files needing to be installed on any computer or device in order to operate this router.
- It is possible to configure this router both with a wired or wireless connection.
- Some DSL modems will require additional configuration prior to using this router. See **“2.1a DSL Modem Configuration”** below.
 1. Shut Down your computer.
 2. If you have an existing Wireless Router, please completely disconnect it from your computer and modem.
 3. RESET and Unplug your modem. To reset your modem:
 - a. Check for a reset button and hold it down for 5 seconds. The reset button will look like a pin-hole and requires a small object to

- depress it. If there is a reset button, it must be used.
- b. Unplug the modem's power cord and remove the battery (if applicable).
 - c. If you do not have access to the modem, continue through these steps until Step 9.
4. Connect you Network Cable(s)
- a. Plug a network cable from your Cable/DSL modem into your Medialink Router Port. (DO NOT connect the included AC/DC Adapter to the router's Power port at this time.)
 - b. Using another network cable, plug one end to your computer's network port. Plug the other end into one of the Medialink Router's ports numbered 1, 2, 3, or 4.



5. Power On your Cable/DSL Modem
 - a. Plug in the power cord for your modem. Reinstall the batteries (if applicable).
 - b. Wait 30 seconds for the modem to fully restart.
6. Power on your Medialink Router and Check the Status Lights.
 - a. Connect the AC/DC Adapter to the router's Power port. Connect the other end into an electrical outlet. Wait 30 seconds to allow the router to fully start.
7. Check the status of your Medialink Router.
 - a. On the front panel of your Medialink Router, the POWER and WAN (Internet). The SYS and WLAN LED's should be blinking. If not, make sure the cables are connected correctly.
8. Power ON your computer
 - a. Turn on your computer
 - b. It is recommended that you temporarily turn off any third party firewalls or networking software during installation of your Medialink

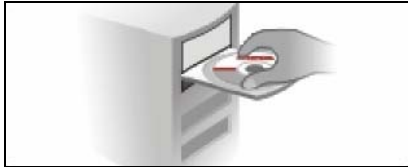
Router.

9. Confirm access to the Internet - Open your internet browser (For example, Internet Explorer, Firefox or Safari) and confirm that you are able to access the internet. If so, proceed to Step 10.
 - If you cannot access the internet. If you have a DSL connection, see **“2.1a DSL Modem Configuration”** below.
 - If you cannot access the internet and you cannot access your Modem, see **“2.1b No Modem Access”**
 - If you do not have DSL, please carefully repeat steps 1 thru 8 as it is important to correctly Reset your modem, Connect the devices and Power On the devices in the precise order as outlined in Steps 1 thru 8.

If you still cannot connect to the internet, please call technical support at 856-216-8222 or download the latest FAQ at www.medialinkproducts.com/support

10. Insert the CD included with your router, double click the “RouterSetupWizard” icon and follow the instructions to complete the installation.

*If you cannot or choose not to use the CD for configuring your router, proceed to “Chapter 3.2 Login to the Router” of this User Guide to complete the configuration of your router.



2.1a DSL Modem Configuration

Some DSL Modems require the PPPoE connection to be handled by the router instead of the modem to be able to successfully create a network using some routers. To configure your DSL modem, first connect your computer directly to the modem using a network cable and proceed with the following steps:

1. Open your internet browser and in the address bar type the IP address of the modem. (Typically the default IP address is 192.168.0.1 or 192.168.1.1. See your modem's manual to be sure.)
2. Click on Advanced Settings
3. The PPP Location must be set to “Bridged” mode
4. You may have to click “WAN IP Address” to see the PPP Location

5. "Bridged Mode" might be called "Transparent Bridge Mode", or "1483 Transparent Bridged Mode".
6. Once the modem is set to Bridged, it will reboot. At this point your computer will no longer have access to the internet.
7. Connect the router between the modem and the computer using network cables.
8. Access the Router's GUI (See Chapter 3.2 Login to the Router)
9. Click Next on the Setup Wizard.
10. Select "ADSL Virtual Dial-up via PPPoE" and click Next.
11. When prompted, enter your DSL username and password, click Next.
12. Restart the computer (See Chapter 3.2 – Step 4 to Configure your Wireless Network)

2.1b No Modem Access

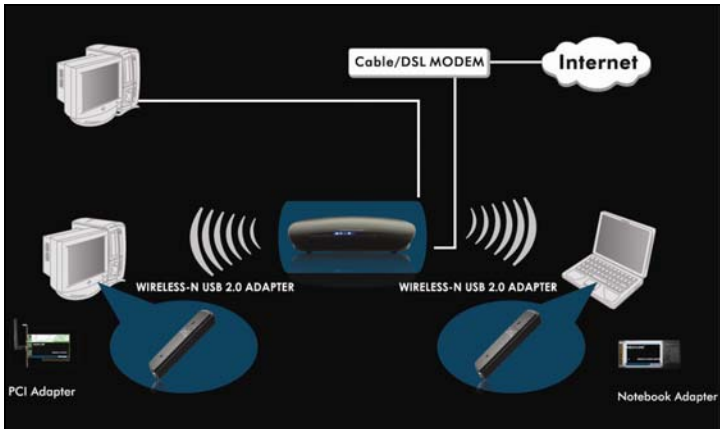
1. Open your internet browser and in the address bar type the IP address of the router (default is 192.168.0.1). Enter the username and password ('admin' for both) when prompted and click "ok".
2. Click on "System Status"
3. Click "Release" then "Renew"
4. Click "System Tools>Reboot". Reboot the router and

try again to confirm access to the internet. If still no access, continue. If you have access, insert the CD and follow the prompts.

5. Click "Advanced Settings>MAC Address Clone". Click "Clone MAC Address".
6. Click "System Tools>Reboot". Reboot the router and try again to confirm access to the internet. If you have access, insert the CD and follow the prompts. If still no access, try restarting the computer then contact Tech Support – support@medialinkproducts.com or 856-216-8222.

2.2 Optimizing Wireless Range

The best possible placement of your wireless router is nearest the center of your wireless devices. The internal antenna is omni-directional. Center the router both vertical and horizontally within the coverage area as much as possible. The router can be wall-mounted to achieve better signal as well.



Chapter 3 How to Login to the Router

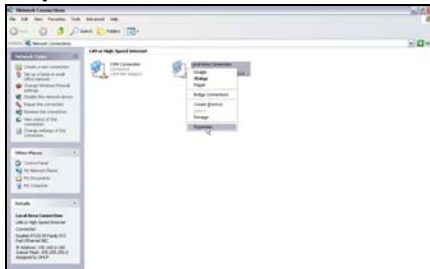
This chapter explains how to enter the Router's Web-based Graphical User Interface or GUI. After you have finished the hardware installation, the following steps will assist you to set the network configurations for you computer.

3.1 How to Set the Network Configurations

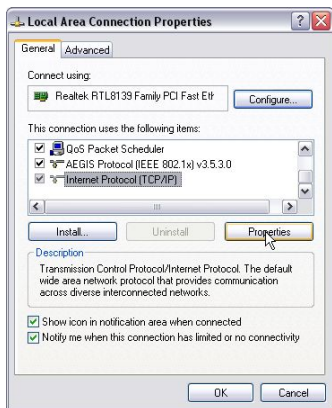
1. On your computer desktop right click **"My Network Places"** and select **"Properties"**.



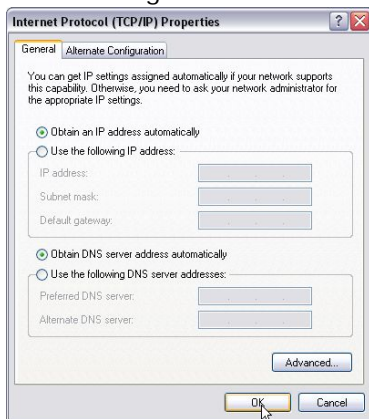
2. Right click **“Local Area Network Connection”** and select **“Properties”**.



3. Select **“Internet Protocol (TCP/IP)”** and click **“Properties”**.



4. Select **“Obtain an IP address automatically”** and **“Obtain DNS server address automatically”**. Click **“OK”** to save the configurations.



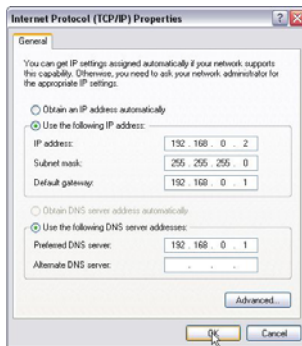
Or select **“Use the following IP address”** and enter the IP address, Subnet mask, Default gateway as follows:

IP Address: 192.168.0.XXX: (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0


Gateway: 192.168.0.1

You need to input the DNS server address provided by your ISP. Otherwise, you can use the Router's default gateway as the Preferred DNS proxy server. Click "**OK**" to save the configurations.



3.2 Login to the Router

1. To access the Router's Web-based Graphical User Interface (GUI) or if you are completing the configuration of your router, you must first login to the router by launching a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, `http://192.168.0.1`. Press "**Enter**".

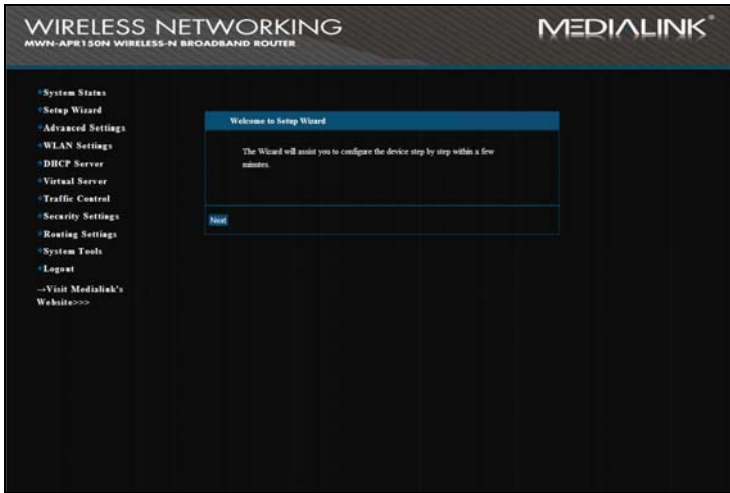
 `http://192.168.0.1/`

2. Input the "**admin**" in both User Name and Password.

Click "OK".



3. If you enter the correct user name and password, you will see the "Welcome to Setup Wizard" screen.
 - a. If you are logging in to the router to change your settings, choose the setting you would like to edit from the options to the left of the browser window.
 - b. **Connect to ISP:** Click Next and the Setup Wizard will guide you through to complete the installation of your router.



4. **Configuring Your Wireless Network:** Once you have completed the setup wizard, you may want to change your SSID (Name of Wireless Network) and Security type to a name and password that you will remember (the router's default SSID is "medialink")

- a. **Naming Your Wireless Network:** Click **WLAN Settings**, then click **Basic Settings**. Change the SSID name to a name that will identify your wireless network (For example: Smith or MyWireless.) Then, Click **Apply**. (Screen will not change)

(For more details on your Basic Settings, open the “Help_BasicWirelessSecuritySettings.pdf” document located in the User Guide folder on the CD.)

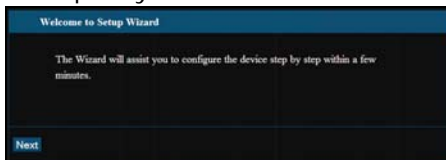
- b. **Change your Security Type:** Click **WLAN Settings**, then click **Security Settings**. (For help in choosing your security type see the “Help_WirelessNetworkSecurity.pdf” or “Help_WEP_WPA_WPA2.pdf” document located in the User Guide folder on the CD.)

Chapter 4 Quick Setup Guide

This chapter deals with how to install and configure your router via the Web-based Graphical User Interface (GUI). After you have completed the hardware installation steps in Chapter 2.1 (pages 7-9), you may proceed to Chapter 4.1 to run the router’s setup wizard through the web-based interface rather than using the installation CD.

4.1 Setup Wizard

1. Here is the “**Welcome to Setup Wizard**” for configuring your Router quickly. Click “**Next**”.



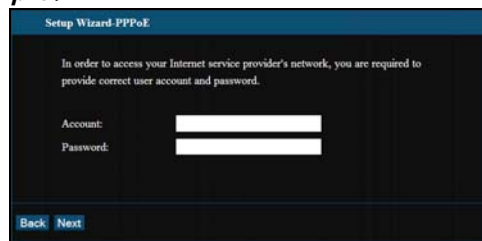
2. In this screen, select the type of Internet connection you use. If you are not sure, press the **“Detect”** button or contact your Internet Service Provider, and click **“Next”**.



ADSL Virtual Dial-up (Via PPPoE)

Enter the Account and Password provided by your ISP, and click **“Next”**.

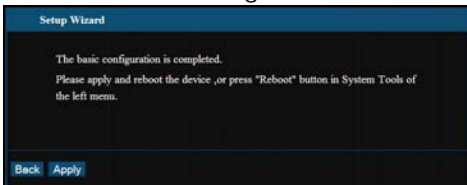
For example:



Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP

address keeps changing every time you connect. You do not need to enter the information like other modes. Click "**Next**" and "**Save**" to finish the settings.



Static IP

In this screen, fill in the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click "**Next**".

For example:

ISP provides the following TCP/IP parameters as follows:

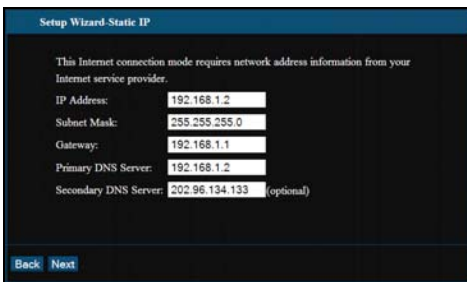
IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS Server: 192.168.1.2

Alternate DNS Server: 202.96.134.133

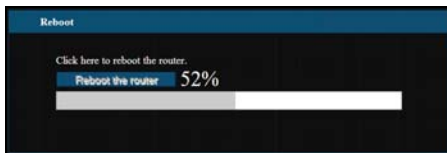


The screenshot shows a web-based configuration page titled "Setup Wizard - Static IP". The page has a dark background with light text. At the top, it says "This Internet connection mode requires network address information from your Internet service provider." Below this, there are five input fields, each with a label and a value:

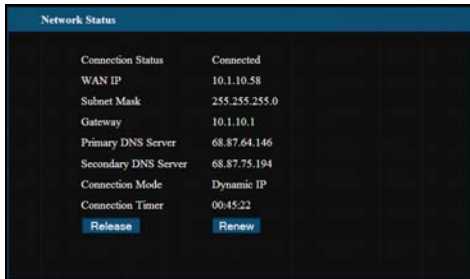
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
Primary DNS Server:	192.168.1.2
Secondary DNS Server:	202.96.134.133 (optional)

At the bottom left, there are two buttons: "Back" and "Next".

Click "**Save**" to complete the setup wizard. The Router will record the settings you made. To activate the settings, it is recommended to select "Reboot the Router" from "System Tools" of the left menu.



Click the "**System Status**" in the left menu of the Web-based Utility to find out the current network and system information. If the "**Connection Status**" is "**Connected**", you have completed the Router's basic settings. Your computer will now have access to the Internet. If you want to configure more, please proceed to the following explanations for Advanced Settings.



The screenshot shows a 'Network Status' window with a dark background and light text. It lists various network parameters and their current values. At the bottom, there are two buttons: 'Release' and 'Renew'.

Network Status	
Connection Status	Connected
WAN IP	10.1.10.58
Subnet Mask	255.255.255.0
Gateway	10.1.10.1
Primary DNS Server	68.87.64.146
Secondary DNS Server	68.87.75.194
Connection Mode	Dynamic IP
Connection Timer	00:45:22
Release	Renew

L2TP

L2TP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter L2TP username.

Password: Enter L2TP password.

MTU: Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1500 is the default MTU. Lowering this number might be ideal.

Address Mode: Select "Static" if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the L2TP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.

Setup Wizard L2TP

L2TP Server: 0.0.0.0 (IP or Domain name)

User Name: medialink

Password: *****

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Back Next

PPTP

PPTP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter PPTP username provided by your ISP.

Password: Enter PPTP password provided by your ISP.

Address Mode: Select "Static" if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the PPTP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.

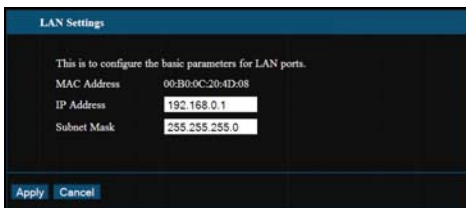
Setup Wizard-PPTP

PPTP Server:	<input type="text" value="pptp_server"/>	(IP or Domain name)
User Name:	<input type="text" value="medialink"/>	
Password:	<input type="password" value="*****"/>	
Address Mode:	<input type="text" value="Static"/>	
IP Address:	<input type="text" value="192.168.1.1"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>	
Default Gateway:	<input type="text" value="192.168.1.254"/>	

Chapter 5 Advanced Settings

5.1 LAN Settings

LAN Settings are for the basic TCP/IP parameters of LAN ports.



LAN Settings	
This is to configure the basic parameters for LAN ports.	
MAC Address	00-B0-0C-20-4D-08
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- ✧ **MAC Address:** The Router's physical MAC address as seen on your local network, which is unchangeable.
- ✧ **IP Address:** The Router's LAN IP addresses (not your PC's IP address). 192.168.0.1 is the default value.
- ✧ **Subnet Mask:** The Router's subnet mask is the measurement of the network size. 255.255.255.0 is the default value.
- ✧ **IMPORTANT:** Once you modify the IP address, you need to remember it for the next time you login to the Web-based Utility.

5.2 WAN Settings

After you have selected the ISP connection type in “Setup Wizard” here is where you can modify the related settings.

Virtual Dial-up (PPPoE)

WAN Settings

WAN connection mode: PPPoE

Account:

Password:

MTU: (Default by 1492. Do NOT Modify Unless Necessary)

Service Name: (Do NOT Modify Unless Necessary)

AC Name: (Do NOT Modify Unless Necessary)

Internet Connection Option

Connect Automatically.

Connect Manually.

Connect on Demand

Max Idle Time: (60—3600 seconds)

Connect on Fixed Time

IMPORTANT: Please set the time in “System Tools” before you select this Internet connection.

Time From: h m T h m

- ✧ **Connection Mode:** Shows your current connection mode.
- ✧ **Account:** Provided by your ISP.
- ✧ **Password:** Provided by your ISP.
- ✧ **MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1500. Do not modify it unless necessary.

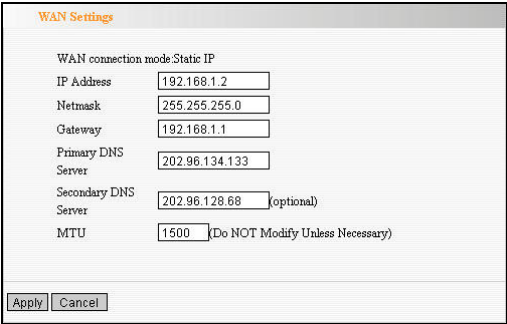
If some websites or web application software can not be open or enabled, try to change the MTU value to a lower value like 1492, 1450, 1400, etc.

- ✧ **Service Name:** Defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- ✧ **AC Name:** Enter it if provided. Do NOT modify it unless necessary.
- ✧ **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- ✧ **Connect Manually:** Connect to the Internet manually.
- ✧ **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet will stay connected at all times. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- ✧ **Connect on Fixed Time:** Connect to the Internet during the time you specify.

Notice:

The “Connect on Fixed Time” can be deployed only when you have set the current time in “Time Settings” from “System Tools”.

Static IP



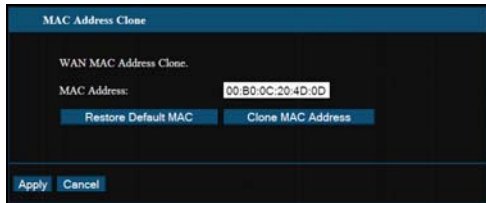
The screenshot shows the 'WAN Settings' configuration page. At the top, it says 'WAN connection mode: Static IP'. Below this are several input fields: 'IP Address' with the value '192.168.1.2', 'Netmask' with '255.255.255.0', 'Gateway' with '192.168.1.1', 'Primary DNS Server' with '202.96.134.133', 'Secondary DNS Server' with '202.96.128.68' and '(optional)' to its right, and 'MTU' with '1500' and '(Do NOT Modify Unless Necessary)' to its right. At the bottom left, there are 'Apply' and 'Cancel' buttons.

If your connection mode is Static IP, you can modify the following addressing information.

- ✧ **IP Address:** Here enter the WAN IP address provided by your ISP.
- ✧ **Subnet Mask:** Enter the WAN Subnet Mask here.
- ✧ **Gateway:** Enter the WAN Gateway here.
- ✧ **Primary DNS Server:** Enter the Primary DNS server provided by your ISP.
- ✧ **Secondary DNS Server:** Enter the secondary DNS.

5.3 MAC Address Clone

This page is for the Router's MAC address to WAN.

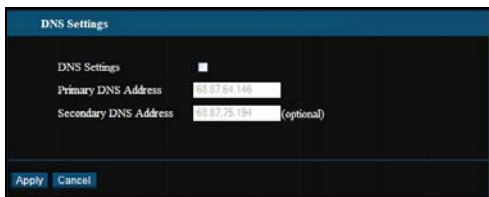


Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

- ✧ **MAC Address:** The MAC address to be registered with your Internet service provider.
- ✧ **Clone MAC Address:** Register your PC's MAC address.
- ✧ **Restore Default MAC Address:** Restore to the default hardware MAC address.

5.4 DNS Settings

DNS is short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.



- ✧ **DNS:** Click the checkbox to enable the DNS server. The Router's DHCP server will answer the client's requests and distribute DNS address.
- ✧ **Primary DNS Address:** Enter the necessary address provided by your ISP.
- ✧ **Secondary DNS Address:** Enter the second address if your ISP provides, which is optional.

Notice:

After the settings are completed, reboot the device to activate the modified settings.

Chapter 6 WLAN (Wireless) Settings

6.1 Basic Settings



- ✧ **Enable Wireless:** Check to enable the Router’s wireless features; uncheck to disable it.
- ✧ **Network Mode:** Select one mode from the list. The default is 11b/g/n mixed mode.
- ✧ **11b mode:** Allow the wireless clients to connect with the device in 11b mode only at the maximum speed of 11Mbps.
- ✧ **11g mode:** Allow the wireless clients to connect with the device in 11g mode only at the maximum speed of 54Mbps.
- ✧ **11b/g mode:** Allow the 11b/g-compliant client devices to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g

speed.

- ✧ **11b/g/n mode (default):** Allow 11b/g/n-compliant client device to connect with the AP with auto-negotiation speed.
- ✧ **SSID:** SSID (Service Set Identifier) is the unique name of the wireless network.
- ✧ **Broadcast (SSID):** Select "Enable" to enable the device's SSID to be visible by wireless clients. The default is enabled.
- ✧ **BSSID:** Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- ✧ **Channel:** Specify the effective channel (from 1 to 11\Auto) of the wireless network.
- ✧ **Extension Channel:** To increase data throughput of wireless network, the extension channel range is used in 11n mode.
- ✧ **Channel Bandwidth:** Select the channel bandwidth to improve the wireless performance. When the network has 11b/g and 11n clients, you can select the 40M; when it is an 11n network, select 20/40M to improve its throughput.

6.2 Wireless Security Setting

Select the encryption method to be used to secure your wireless network and create your password.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window:



❖ **WEP Key1~4:** Set the WEP key with the format of

ASCII or Hex. You can enter either ASCII code (5 or 13 ASCII characters. Illegal characters such as “/” is not allowed but all other case-sensitive letters, numbers and symbols are allowed) Or enter either 10 or 26 Hex characters (not case-sensitive – letters ‘a’ through ‘f’ and numbers only).

- ❖ **Default Key:** Select one key from the four configured keys as the currently active one.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.



- ❖ **WPA Algorithms** : Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is AES mode.
- ❖ **Pass Phrase** : Create a password using 8-63 ASCII characters (case-sensitive letters, numbers and symbols are allowed).
- ❖ **Key Renewal Interval** : Set the key's renewal period. (3600 is the default)

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access) however, can slow your connection.



- ❖ **WPA Algorithms** : Provides TKIP [Temporal Key

Integrity Protocol] or AES [Advanced Encryption Standard]. The default is AES mode.

- ✧ **Pass Phrase:** Create a password using 8-63 ASCII characters (case-sensitive letters, numbers and symbols are allowed).
- ✧ **Key renewal Interval:** Set the key's renewal period. (3600 is the default)

6.3 Advanced Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, etc.

Advanced Settings

BG Protection Mode	Auto
Basic Data Rates	Default(1-2-5.5-11 Mbps)
Beacon Interval	100 ms (range 20 - 999, default 100)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)

WMM Capable Enable Disable

APSD Capable Enable Disable

Apply Cancel

- ✧ **BG protection Mode:** Auto by default. It is for 11b/g wireless client to connect to 11n wireless network

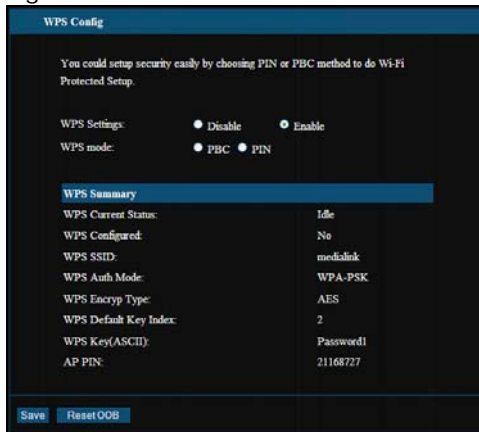
smoothly in a complicated wireless area.

- ✧ **Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Here, default value is (1-2-5.5-11Mbps...). It is recommended not to modify this value.
- ✧ **Beacon Interval:** Set the beacon interval of wireless radio. Default value is 100. It is recommended not to modify this value.
- ✧ **Fragment Threshold:** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes. It is recommended not to modify this value.
- ✧ **RTS Threshold:** RTS stands for "Request to Send". This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2347. It is recommended not to modify this value in SOHO environment.
- ✧ **TX Power:** Set the output power of wireless radio. The default value is 100.
- ✧ **WMM Capable:** This will enhance the data transfer performance of multimedia data when they're being transferred over wireless network. It is recommended to enable this option.
- ✧ **APSD Capable:** It is used for auto power-saved service.

The default is disabled.

6.4 WPS Settings

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the device through encrypted contents. The users only enter PIN code or press WLAN/WPA button on the panel to configure it without selecting encryption method and secret keys by manual. In the “WLAN Settings” menu, click “WPS settings” to enter the next screen.



- ✧ **WPS settings:** To enable or disable WPS function. The default is “enable”.
- ✧ **WPS mode:** Provide two ways: PBC (Push-Button

Configuration) and PIN code.

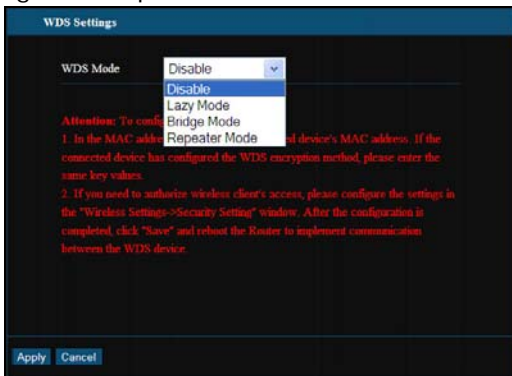
- ✧ **PBC:** Select the PBC or press the WLAN/WPS button on the back of the device for about one second and the WPS indicator will be blinking for 2 minutes. While the light is blinking, you can enable another device to implement the WPS/PBC negotiation between them by pressing the device's WPS button. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports up to 32 clients access.)
- ✧ **PIN:** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client.
- ✧ **WPS Summary:** Shows the current state of Wi-Fi protected setting, including authorized mode, encryption type, default key and other information.
- ✧ **WPS Current Status:** Idle means WPS in idle state. Start MSC process means the process has been started and is waiting to be connected. Configured means the negotiation is successful between server and clients.
- ✧ **WPS Configured:** "Yes" means WPS feature is enabled and active. "No" means it is not active. If a passphrase or key is used with normal security settings, then "No" will display here.
- ✧ **WPS SSID:** Show the main SSID set by WPS.
- ✧ **WPS Auth. Mode:** The authorization mode deployed

by WPS, generally WPA/WPA2-personal mode.

- ✧ **WPS Encrypt Type:** The encryption type used by WPS, generally AES/TKIP.
- ✧ **WPS Key :** The effective key generated by AP automatically.
- ✧ **AP PIN (KEY) :** The PIN code used by default (located on the bottom of the router).
- ✧ **Reset OOB:** When this button is pressed, the WPS client will be idle state, and WPS indicator will be turned off. AP will not respond the WPS client's requests and the security mode will be set as WPA mode.

6.5 WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.



NOTE: Before you enable WDS on a primary or secondary router configure each router as follows:

Primary Router Configuration

- ✧ IP Address: 192.168.0.1
- ✧ Subnet Mask: 255.255.255.0
- ✧ WLAN SSID: Your Choice
- ✧ WLAN Security: Your Choice
- ✧ Broadcast Channel: Your choice (default is 6)
- ✧ Channel Extension: Your choice (default is 10)
- ✧ WDS Mode: Lazy
- ✧ WDS Encrypt: None
- ✧ DHCP Server: Enabled
- ✧ Prevent Network Attack (Firewall): Enabled

Secondary Router Configuration

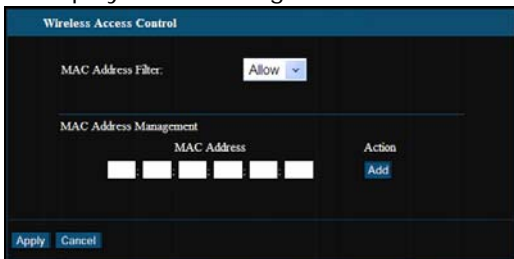
- ✧ IP Address: 192.168.0.X (last digit different than Primary)
 - ✧ Subnet Mask: 255.255.255.0
 - ✧ WLAN SSID: Your Choice (make it different from Primary Router so you can tell the routers apart)
 - ✧ WLAN Security: Your Choice (doesn't have to be the same as Primary Router, but it is recommended so you can remember it easily)
 - ✧ Broadcast Channel: 6 (these channels don't have to be 6 but it has to match Primary Router)
 - ✧ Channel Extension: 10 (Same thing. doesn't have to be 10 but has to match Primary Router)
 - ✧ DHCP Server: Disabled
 - ✧ Prevent Network Attack (Firewall): Disabled
- ✧ **Lazy:** Use this mode on the primary router connected directly to the ISP (modem) when additional routers are

used as additional access points. The secondary routers must be set to "Bridge" or "Repeater" when this option is selected.

- ✧ **Bridge:** Setup a secondary router as a wired or wireless access point. Connect an Ethernet cable to the LAN port of the Primary router and connect the other end to a LAN port of the Secondary router. (Primary router must be set to "Lazy"). Click "Open Scan" and select the MAC address of the Primary router to connect the two devices and establish a wider network.
- ✧ **Repeater Mode :** Setup a secondary router as a Wireless Access Point. (Primary router must be set to "Lazy"). Click "Open Scan" and select the MAC address of the Primary router to connect the two devices and establish a wider network.
- ✧ **Encrypt Type:** Select one from WEP, TKIP, AES for security here. (**Note:** It is recommended to leave this disabled and only use the WLAN Security Settings instead.)
- ✧ **Pass phrase:** Enter the encrypted key for wireless devices. (**Note:** It is recommended to leave this disabled and only use the WLAN Security Settings instead.)
- ✧ **AP MAC:** Input the MAC address of another (opposing) wireless router you want to connect.
- ✧ **Reboot the Router:** Click "System Tools->Reboot" when finished configuring WDS.

6.6 Access Control

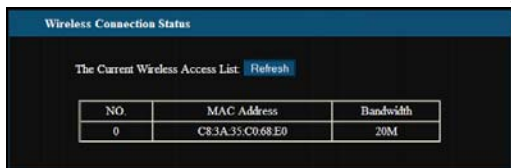
Allow or block specific wireless clients via their MAC Address to the wireless network. Select "WLAN Settings -> Access Control" to display the following screen:



- ✧ **MAC Address Filter :** Enable/disable MAC address filter. Select "Off" to disable MAC address filter; "Block" to prevent the MAC addresses in the list from accessing the wireless network; "Allow" to allow the MAC address in the list to access the wireless network.
- ✧ **MAC Address Management:** Input the MAC address to implement the filter policy. Click "Add" to finish the MAC add operation.
- ✧ **MAC list:** Show the added MAC addresses. You can add or delete them.

6.7 Connection Status

This page shows wireless client's connection status, including MAC address, Channel bandwidth, etc. Select "WLAN Settings->Connection Status" to enter the following screen:



NO.	MAC Address	Bandwidth
0	C8:3A:35:C0:68:E0	20M

- ✧ **MAC Address:** Shows current MAC addresses of the hosts connecting to the Router.
- ✧ **Bandwidth:** Shows current bandwidth of the hosts (wireless client).

Chapter 7 DHCP Server

7.1 DHCP Settings

DHCP (Dynamic Host Control Protocol) assigns an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating "Obtain an IP Address Automatically". Specify the starting and ending address of the IP Address pool to establish the range of your IP addresses. "100" to "200" is set by default.

DHCP Server	
DHCP Server	<input checked="" type="checkbox"/> Enable
IP Address Start	192.168.0. <input type="text" value="100"/>
IP Address End	192.168.0. <input type="text" value="200"/>
Lease Time	<input type="text" value="One day"/>

- ✧ **DHCP Server:** Click the checkbox to enable/disable DHCP server.
- ✧ **IP Address Start/End:** Enter the range of IP address for DHCP server distribution.
- ✧ **Lease Time:** The length of the IP address lease.

For example:

If the lease time is an hour, then DHCP server will reclaim the IP address every hour.

7.2 DHCP List and Binding

Here you can manually control which IP addresses are associated with each device in your network but typing in a "Static IP Address" within the range set. Then specify a MAC address of the device you want to assign the IP address to and click "Add". Repeat as necessary.

DHCP List&Binding

Static IP

IP Address 192.168.0.103

MAC Address C8 3A 35 C0 68 E0 [Add](#)

NO.	IP Address	MAC Address	IP-MAC bind	Delete
Refresh				
Host Name	IP Address	MAC Address	Lease	
Office	192.168.0.100	00:00:00:00:00:00	00:00:00	
Office	192.168.0.101	00:00:00:00:00:00	00:00:00	
Monica's iPhone	192.168.0.102	60FB42E909B9	22:18:38	
mediahdge-jc	192.168.0.103	C83A35C068E0	15:11:37	
WIRELESS	192.168.0.104	00:1C:C4:67:64:5F	22:13:25	

[Apply](#) [Cancel](#)

- ✧ **IP Address:** Enter the IP address which needs to be bound.
- ✧ **MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click "Add" to add the entry in the list.
- ✧ **Hostname:** The name of the computer which is added a new IP address.
- ✧ **Lease Time:** The left time length of the corresponding IP address lease.

Chapter 8 Virtual Server

8.1 Port Range Forwarding

This section deals with the port range forwarding. The Port Range Forwarding allows you to set up a range of public

services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.

Port Range Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port	End Port	To IP Address	Protocol	Enable	Delete
1.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/>	<input type="text"/>	192.168.0.	<input type="text" value="TCP"/>	<input type="checkbox"/>	<input type="checkbox"/>

Well Known Service Port: ID:

- ✧ **Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.
- ✧ **IP Address:** Enter the IP address of the PC where you want to set the applications.
- ✧ **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- ✧ **Delete/Enable:** Click to check it for corresponding operation.

- ✧ **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- ✧ **Add:** Add the selected well-known port to the policy ID.

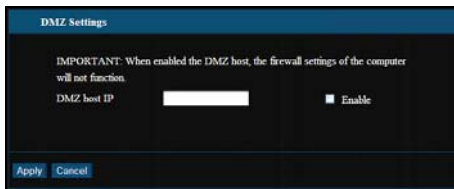
NOTE:

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

8.2 DMZ Settings

(For Gaming Systems/Video Conferencing)

The DMZ function allows one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.



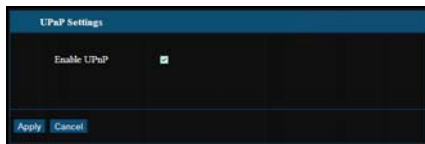
- ✧ **DMZ Host IP Address:** The IP address of the

computer/game system you want to expose.

- ✧ **Enable:** Click the checkbox to enable the DMZ host.
- ✧ **IMPORTANT:** When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

8.3 UPNP Settings

Latest Universal Plug and Play is supported. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.



Enable UPnP: Click the checkbox to enable the UPnP.

Chapter 9 Traffic Control

9.1 Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including IP address range configuration.

Traffic Control Settings

Traffic Control

Interface Upload BW Download BW

WAN: 512 2048 (KByte/s)

Protocol	Port	Service
TCP&UDP	0	All

Services: TCP&UDP 0 All

IP: 192.168.0.

Up/Down: Up

BW Range: (KByte/s)

Apply:

Add

Nam	Port	IP	Up/Down	BW Range	Apply	Edit	Del
-----	------	----	---------	----------	-------	------	-----

Apply Cancel

- ✧ **Enable Traffic Control:** To enable or disable the internal IP bandwidth control. The default is disabled.
- ✧ **Interface:** To limit the uploading and downloading bandwidth in WAN port.
- ✧ **Service:** To select the controlled service type, such as HTTP service.
- ✧ **IP Starting Address:** The first IP address for traffic

control.

- ✧ **IP Ending Address:** The last IP address for traffic control.
- ✧ **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- ✧ **Bandwidth:** To specify the uploading/downloading Min./Max. Traffic speed (KB/s), which can not exceed the WAN speed.
- ✧ **Apply:** To enable the current editing rule. If not, the rule will be disabled.
- ✧ **Add:** After editing the rule, click the “Add” button to add the current rule to rule list.
- ✧ **Apply:** Click “Apply” to activate the current rule.
- ✧ **Cancel:** Click “Cancel” to cancel.

Chapter 10 Security Settings

10.1 Client Filter Settings

Control and limit specific computers and devices on the network from accessing the internet at specific times of the day.

The example below shows a policy that blocks the IP addresses from 192.168.0.100 to 120 from accessing the internet Sunday through Thursday 9pm to 5:30am.

The screenshot shows the 'Client Filter' configuration page. At the top, there is a section for 'Client Filtering Settings' which is checked. Below this, the 'Access Policy' is set to '10'. The 'Enable' checkbox is checked, and there is a 'Delete the Policy: Clear' button. The 'Filtering Mode' is set to 'Enable', with 'Disable' also available. The 'Policy Name' is 'Kids'. The 'Start IP' is '192.168.0.100' and the 'End IP' is '192.168.0.120'. The 'Port' is '1' to '99999'. The 'Type' is 'Both'. The 'Times' are set to '20' to '5' and '30'. The 'Date' is set to 'Everyday', 'Sun', 'Mon', 'Tue', and 'Wen'.

Client Filter

Client Filtering Settings

Access Policy: 10

Enable: Delete the Policy: Clear

Filtering Mode: Disable Enable access the Internet

Policy Name: Kids

Start IP: 192.168.0.100

End IP: 192.168.0.120

Port: 1 ~ 99999

Type: Both

Times: 20 ~ 5 : 30

Date: Everyday Sun Mon Tue Wen Thr Fri Sat

Apply Cancel

- ✧ **Client Filter:** Check to enable client filter.
- ✧ **Access Policy:** Select one number from the drop-down menu. Set up to 10 rules (policies).
- ✧ **Enable:** Check to enable the access policy.
- ✧ **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- ✧ **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- ✧ **Policy Name:** Enter a name for the access policy selected.
- ✧ **IP Start/End:** Enter the starting/ending IP address for the computer/device you want the policy to apply to. You must have manually assigned IP addresses to the clients you wish to control or else the client’s IP address will change when the lease runs out.
- ✧ **Port No.:** Enter the port range based over the protocol for access policy. If you don’t know the specific Ports you want to block, enter 1–99999 to block them all.
- ✧ **Protocol:** Select one protocol (TCP/UDP/Both) from the drop-down menu. If you’re unsure, select “Both”
- ✧ **Times:** Select the time range of client filter.
- ✧ **Days:** Select the day(s) to run the access policy.

10.2 URL Filter Settings

Limit or control the websites that can be accessed by specific computers/devices on the network.

The screenshot shows the 'URL Filter' configuration page. At the top, 'URL Filtering Setting' is checked and labeled 'Enable'. Below this, 'Access Policy' is set to '10'. The 'Enable' checkbox is checked, and there is a 'Delete the Policy' button labeled 'Clear'. The 'Filtering Mode' section has two radio buttons: 'Disable' (selected) and 'Enable', with the text 'access the Internet' next to the 'Enable' option. The 'Policy Name' field contains 'Kids'. The 'Start IP' field is '192.168.0.100' and the 'End IP' field is '192.168.0.200'. The 'URL' field contains 'www.facebook.com'. At the bottom, there are 'Times' dropdowns set to '21:00 ~ 6:00' and a 'Date' section with 'Everyday' checked and other days (Sun, Mon, Tue, Wen, Thr, Fri, Sat) unchecked. 'Apply' and 'Cancel' buttons are at the bottom left.

- ✧ **URL Filter:** Check to enable URL filter.
- ✧ **Access Policy:** Select one number from the drop-down menu.
- ✧ **Enable:** Check to enable the access policy.
- ✧ **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- ✧ **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- ✧ **Policy Name:** Enter a name for the access policy selected.
- ✧ **Start/End IP:** Enter the starting/ending IP address.

- ✧ **URL Strings:** Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.
- ✧ **Times:** Select the time range of client filter.
- ✧ **Days:** Select the day(s) to run the access policy.

10.3 MAC Address Filter (Parental Control)

Limit or Control Access to the internet for specific computers on the network at certain times of the day.

For example: The example below shows “Jack’s PC” will not have internet access from 10:00pm to 6am everyday.

The screenshot shows the 'MAC Filter' configuration page. At the top, 'MAC Filtering Settings' is set to 'Enable'. Below this, 'Access Policy' is set to '10'. There is an 'Enable' checkbox and a 'Delete the Policy: Clear' button. The 'Filtering Mode' section has two radio buttons: 'Disable' (selected) and 'Enable'. The 'Policy Name' is 'Jack's PC'. The 'MAC Address' is 'C8 3A 35 C5 45 C5'. The 'Times' are set to '21:00 - 6:00'. The 'Date' is set to 'Everyday'. At the bottom, there are 'Apply' and 'Cancel' buttons.

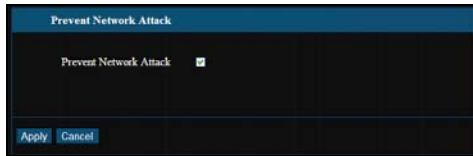
- ✧ **MAC Address Filter:** Check to enable MAC address filter.
- ✧ **Access Policy:** Select one number from the drop-down menu.
- ✧ **Enable:** Check to enable the access policy.
- ✧ **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- ✧ **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- ✧ **Policy Name:** Enter a name for the access policy selected.
- ✧ **MAC Address:** Enter the MAC address you want to run the access policy.
- ✧ **Times:** Select the time range of client filter.
- ✧ **Days:** Select the day(s) to run the access policy.
- ✧ **Apply:** Click to make the settings go into effect.

10.4 Prevent Network Attack (Firewall)

This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically.

The attacker’s IP address can be found from the “System

Log”.



Prevent Network Attack: Check to enable it for attack prevention.

10.5 Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the “Enable”.



- ✧ **Enable:** Check to enable remote web management.
- ✧ **Port:** The management port open to outside access. The default value is 8080.
- ✧ **WAN IP Address:** Specify the range of the WAN IP address for remote management.

Note:

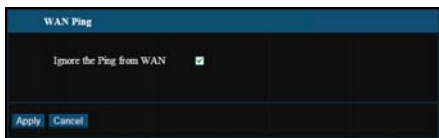
1. If you want to login the device's Web-based interface via port 8080, you need use the format of WAN IP address: port (for example `http://219.134.32.101: 8080`) to implement remote login.
2. If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 218.88.93.33-218.88.93.35, then only the IP addresses as 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the Router.

For example:

If you want to configure the IP address 218.88.93.33 to access the device's web interface, please set it as follows:

10.6 WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.

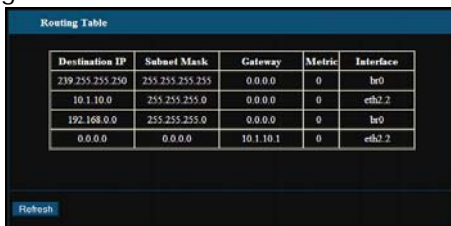


- ✧ **Ignore Ping from WAN:** Check to ignore the ping request and give no reply.

Chapter11 Routing Setting

11.1 Routing Table

The main duty for a router is to look for a best path for every data frame, and transfer this data frame to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.

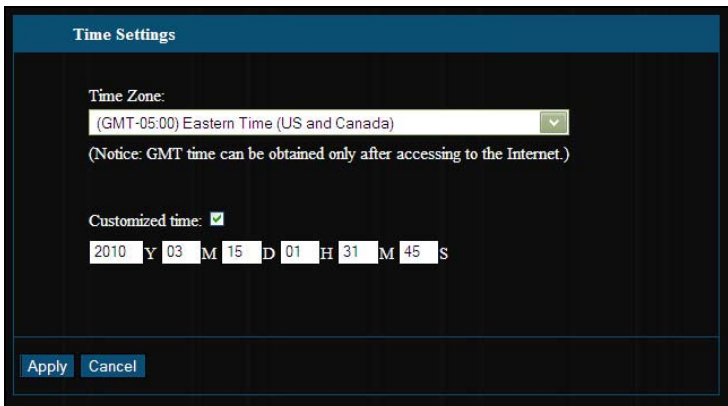


Destination IP	Subnet Mask	Gateway	Metric	Interface
239.255.255.250	255.255.255.255	0.0.0.0	0	br0
10.1.10.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	10.1.10.1	0	eth2.2

Chapter 12 System Tools

12.1 Time Settings

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.



The screenshot shows a web interface titled "Time Settings". It features a "Time Zone:" label above a drop-down menu currently displaying "(GMT-05:00) Eastern Time (US and Canada)". Below this is a notice: "(Notice: GMT time can be obtained only after accessing to the Internet.)". There is a "Customized time:" label with a checked checkbox. Below it are input fields for time: "2010" for Year, "03" for Month, "15" for Day, "01" for Hour, "31" for Minute, and "45" for Second. At the bottom left, there are "Apply" and "Cancel" buttons.

Time Zone: Select your time zone from the drop-down menu.

Customized time: Enter the time you customize.

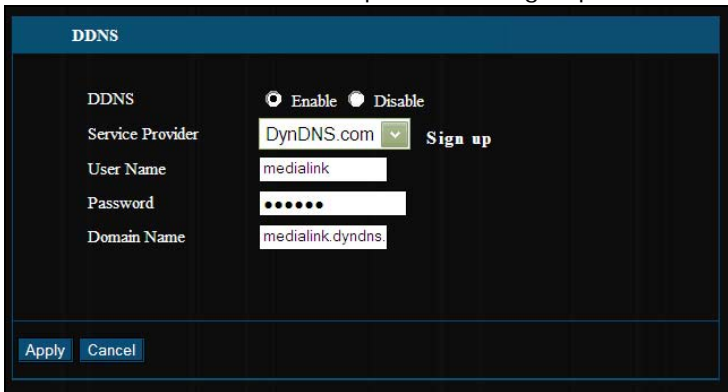
Note:

When the Router is powered off, the time setting

will be lost. Before the Router will obtain GMT time automatically, you need connect with the Internet and obtain the GMT time, or set the time on this page first. Then the time in other features (e.g. firewall) can be activated.

12.2 DDNS

The **DDNS (Dynamic Domain Name System)** is supported in this Router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select “Enable” and a DDNS service provider to sign up.



The screenshot shows the DDNS configuration page. At the top, there is a blue header with the text "DDNS". Below the header, there are several fields and controls:

- DDNS**: A section header.
- Enable/Disable**: Two radio buttons. The "Enable" button is selected (indicated by a filled circle), and the "Disable" button is unselected (indicated by an empty circle).
- Service Provider**: A dropdown menu with "DynDNS.com" selected. To the right of the dropdown is a "Sign up" button.
- User Name**: A text input field containing "medialink".
- Password**: A text input field with masked characters (dots).
- Domain Name**: A text input field containing "medialink.dyndns".

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

- ✧ **Main Features:** Your ISP provides dynamic IP address, DDNS is used to capture the changeable IP address and

match the fixed domain. Then users can have access to the Internet to communicate with others.

DDNS can help you establish virtual host in your home and company.

- ✧ **DDNS:** Click the radio button to enable or disable the DDNS service.
- ✧ **Service Provider:** Select one from the drop-down menu and press “Sign up” for registration.
- ✧ **User Name:** Enter the user name the same as the registration name.
- ✧ **Password:** Enter the password you set.
- ✧ **Domain Name:** Enter the domain name which is optional.

For example:

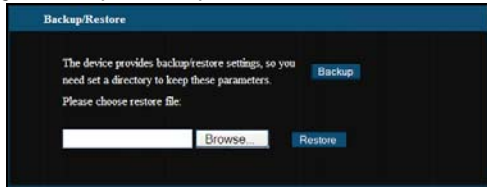
In the local host 192.168.0.10 establish a Web server, and register in 3322.org as follows:

User name	Medialink
Password	123456
Domain Name	Medialink.vicp.net

After mapping the port in the virtual server, setting account information in DDNS server and in the address field entering <http://Medialink.3322.org>, you can access the Web page.

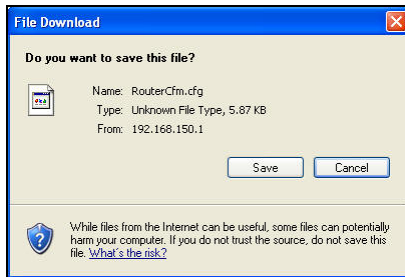
12.3 Backup/Restore Settings

The device provides backup/restore settings, so you need set a directory to keep these parameters.



Backup Setting:

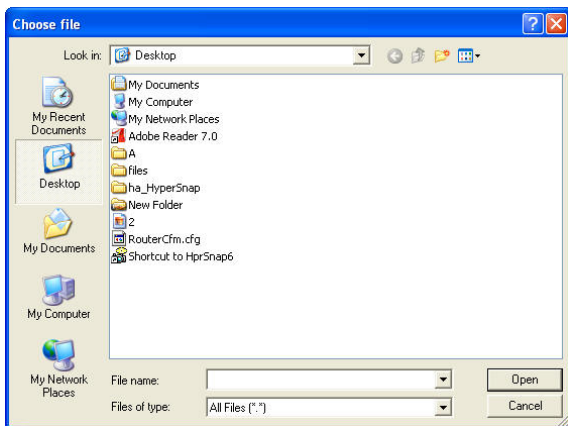
Click “Backup” button to back up the Router’s settings and select the path for save.



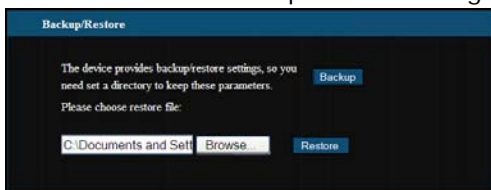
Click “Save” to save the configuration files.

Restore Setting:

Click “Browse” button to select the backup files.

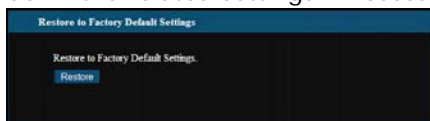


Click "Restore" button to restore previous settings.



12.4 Restore to Factory Default Setting

This button is to reset all settings to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.



✧ **Restore:** Click this button to restore to default settings.

Factory Default Settings:

User Name: admin

Password: admin

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

NOTE:

After restoring to default settings, please restart the device, then the default settings can go into effect.

12.5 Upgrade Firmware

The Router provides the firmware upgrade by clicking the "Upgrade" after browsing the firmware upgrade packet which you can download from www.medialinkproducts.com.



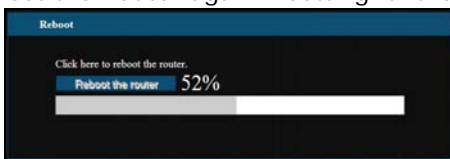
✧ **Browse:** click this button to select the upgrade file.

✧ **Upgrade:** click this button to start the upgrading

process. After the upgrade is completed, the Router will reboot automatically.

12.6 Reboot the Router

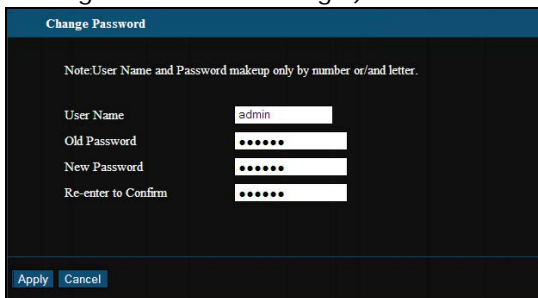
Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.



Reboot the router: Click this button to reboot the device.

12.7 Password Change

This section is to set a new user name and password to better secure your router and network. (This is not necessary unless you want to limit the people already on your network from accessing the router's settings.)

A screenshot of a web interface titled "Change Password". It includes a note: "Note: User Name and Password makeup only by number or/and letter." Below the note are four input fields: "User Name" with the value "admin", "Old Password", "New Password", and "Re-enter to Confirm", all of which are masked with dots. At the bottom of the form are two buttons: "Apply" and "Cancel".

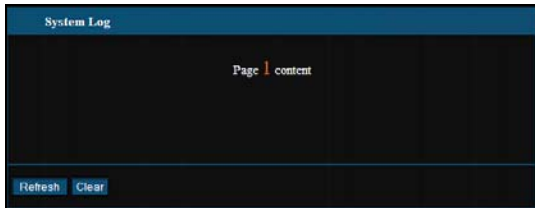
- ✧ **User Name:** Enter a new user name for the device.
- ✧ **Old Password:** Enter the old password.
- ✧ **New Password:** Enter a new password.
- ✧ **Re-enter to Confirm:** Re-enter to confirm the new password.

NOTE:

The only people able to access the router's GUI are the people connected to your network through a wired or wireless connection. Changing the password to the GUI is not necessary unless you want to restrict access to the GUI from devices that are connected to the network. (For example: if Parental Control is enabled, you may want to change this password)

12.8 System Log

This section is to view the system log. Click the “Refresh” to update the log. Click “Clear” to clear all shown information. If the log is over 150 records, it will clear them automatically.



- ✧ **Refresh:** Click this button to update the log.
- ✧ **Clear:** Click this button to clear the current shown log.

12.9 Logout

After you have finished the settings completely, in logout page click “OK” to logout of the router GUI.

Appendix 1: Glossary

Access

Point (AP): Any entity that has station functionality and provides access to the distribution services, via the wireless medium(WM) for associated stations.

Channel: An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID: Service Set identifier. An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP: Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless

network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommended using.

WPA/WPA2: A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network. WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.