LB-LINK®

150Mbps MINI WIRELESS ROUTER
User Manual

Product Features

◆Supports multiple operating modes (Gateway, Ethernet conversion etc)
◆Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
◆MIMO technology utilizes reflection signal to increase eight times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
◆Provides 150Mbps transmission rates
◆Supports AP/WIFI change by manual
◆Supports WMM to make your voice and video transmit more smooth
◆Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
◆Use WPS (PBC and PIN) encryption method to keep you from remembering long passwords
◆Supports remote/local Web management
◆Supports wireless Roaming technology and ensures high-efficient wireless connections
◆Supports wireless SSID stealth mode and MAC address access control
◆Supports Auto MDI/MDIX
◆Provides system log to record the status of the router
◆Supports MAC address filtering, NAT, NAPT
◆Supports UPnP and DDNS
◆Supports the access control, it can control multiple MAC addresses
◆Supports DHCP server/client
◆Supports SNTP
◆Supports auto wireless channel selection
◆Supports WDS function (wireless distribution system)

Software Specification	
Standards	IEEE 802.11n(Draft 2.0), IEEE 802.11g, IEEE 802.11b
Wireless Signal Rates With Automatic Fallback	11n: 270/243/216/162/108/81/54/27Mbps 135/121.5/108/81/54/40.5/27/13.5Mbps 130/117/104/78/52/39/26/13Mbps 65/58.5/52/39/26/19.5/13/6.5Mbps 11g: 54/48/36/24/18/12/9/6M(dynamic) 11b: 11/5.5/2/1M(dynamic)
Frequency Range	2.4-2.4835GHz
Wireless Transmit Power (MAX)	16dBm
Modulation Technology	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

	270M: −72dBm@10% PER
	130M: −72dBm@10% PER
	108M: −72dBm@10% PER
Receiver Sensitivity	54M: −72dBm@10% PER
	11M: −85dBm@8% PER
	6M: −88dBm@10% PER
	1M: −90dBm@8% PER

1.Package Contents
* 150Mbps MINI wireless router
* Power Adapter 5V=500MA
* User Manual
* One Ethernet Network Cable
* Quick Install Guide

2.Rear Panel
Power: Special Power Adapter.
WAN: WAN PORT(RJ-45) Connect to XDSL/Cable Modem or Ethernet.

3.Notices
1. Please use the special power with this router, otherwise it will be damaged.
2. WAN: WAN port (RJ-45)connects to XDSL or Ethernet
3. WPS/Reset:
  Reset: Press this button for 5 seconds, the LED indicators of SYS will blink fast, Loosen the button, router will restore default setting and restart automatically.
  WPS: Press this button for 1 second, the LED indicators of WPS will blink fast ,Loosen the button the router will start working with WPS model.

4. Front Panel
LED Indicators

Power	Power Indicator	LED will consistently light when power is on
WIFI	Wireless indicator	Indicator light glint slowly indicates no signal transmitted Indicator light glint quickly indicates signal transmitted
WLAN	WLAN status indicator	The light will consistently light or glint when plug the Network Cable

5 Hardware Install Process
5.1 Establish Wireless LAN Connection
First make sure the PC is equipped with Wireless LAN Card.
5.2 Establish WAN Connection
Connect the WAN port of router to XDSL/Cable Modem by a line.
5.3 Power Link
Connect the power and the router will start automatically.

6. How to Check the Network Connection

Appendix 1: TCP/IP address setup methods (Take Win XP as an example, and turn the manual switch to AP mode)

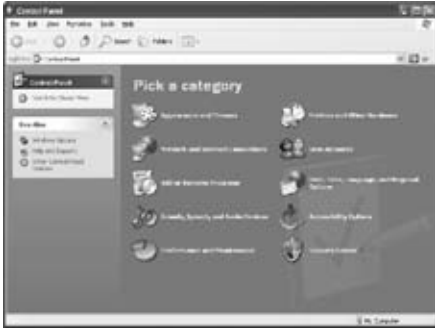Click "Start - Control Panel", open the Control Panel (As indicated in figure1)

Figure1

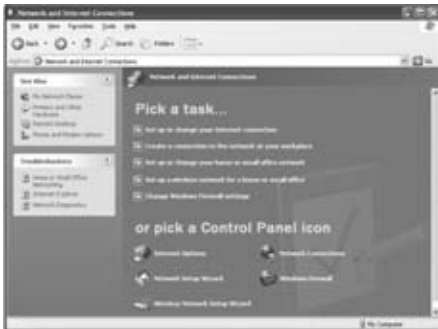Click "Network and Internet Connections", enter the corresponding page(As indicated in figure2)

Figure2

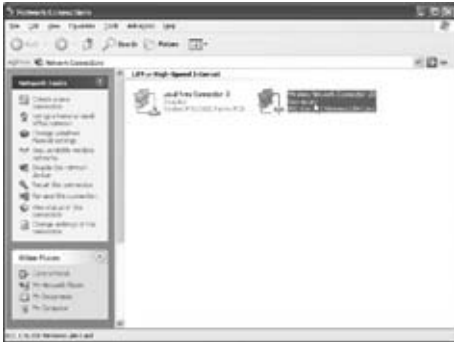Click "Network Connections" enter the corresponding page
(As indicated in figure3)

Figure3

Select "wireless network connection", click the right button of mouse,
select "Properties", then it will popup a "nature of WLAN network connection"
dialog box, Choosing "Internet protocol(TCP/IP) "in "this connection use
the following items" ,then click "properties" (As indicated in figure4)


Figure4

Select "Use the following IP address", Fill 192.168.16.xxx. (xxx is any number
from 2 to 254) in IP address. Subnet mask is 255.255.255.0 , default gateway
is 192.168.16.1(As indicated in figure5),Click"OK"come back to"properties"
dialog box, Click"OK"again to exit the setting interface.
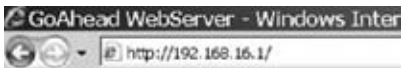

Figure5

Select "wireless network connection",then click right button of mouse,
select"View Avalable Wireless Networks", enter the network connection
interface
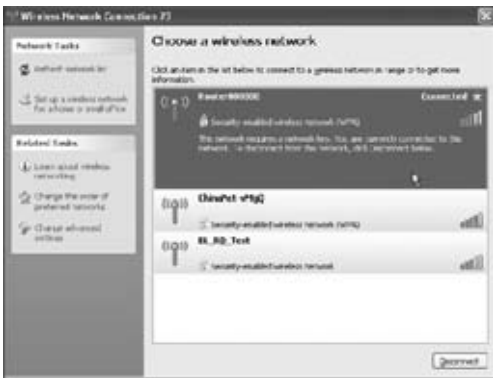
7. Basic Configurations

7.1 To access the router's web-based utility, launch a web browser and input the Router's default IP address(http://192.168.16.1). Press "Enter".

7.2 Please input the "admin" in both User Name and Password. Click "OK".

8. Internet settings
8.1 WAN Connection Mode:
8.1.1 Connection Mode 1: Static mode
In this screen, fill the network address information provided by your ISP in IP Address, Subnet Mask, Gateway and Primary DNS server fields.

IP Address: Enter the WAN IP address provided by your ISP here.
Subnet Mask: Enter the WAN Subnet Mask here.
Default 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
8.1.2 Connection Mode 2: Dynamic IP DHCP (Auto config)
If your connection mode is DHCP Mode, it means your IP address keeps changing each time you connect.

8.1.3 Connection Mode 3: ADSL Virtual Dial-up PPPoE(XDSL)

Enter the User Name and Password provided by your ISP

8.1.4 Connection Mode 4: L2TP Mode

Select L2TP (Layer 2 Tunneling Protocol) if your ISP use the L2TP connection, your ISP will provide you with a username and password , please fill in the parameters.

L2TP provides two access modes.

If the L2TP offered by your ISP is Dynamic IP , Please select Dynamic.

If the L2TP offered by your ISP is Static IP , Please fill in the parameters provided by your ISP.

Server IP: Enter the Server IP provided by your ISP.
User Name: Enter L2TP user name.
Password: Enter L2TP password.
Address Mode: Select "Static" if IP address , subnet mask, and gateway are provided by your ISP In most cases, select "Dynamic".
IP Address: Enter the L2TP IP address provided by your ISP.
Subnet Mask: Enter the Subnet Mask provided by your ISP.
Default Gatway: Enter the Default Gateway supplied by your ISP.

8.1.5 Connection Mode 5: PPTP
If the connection is "PPP Tunneling Protocol", please input the following parameters provided by your ISP: Server IP Address, User Name, and Password.
PPTP provides two access modes.
If the PPTP provided by your ISP is Dynamic IP, Please select Dynamic.
If the PPTP provided by your ISP is Static IP, Please fill in the parameters provided by your ISP.Click "**Apply**", Router will reboot.

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 IP address , subnet mask, and gateway are provided by your IP.In most cases, select"Dynamic".
IP Address: Enter the PPTP IP address provided by your ISP.
Subnet Mask: Enter the Subnet Mask provided by your ISP.
Default Gateway: Enter the default gateway provided by your ISP.

8.2 LAN Connection Mode

MAC Address: The router's physical MAC address unchangeable on your local network, which is fixed.
IP Address: The router's LAN IP address (not is your PC IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. Default value is 192.168.16.1
Subnet Mask: It's shown the router's subnet mask for measurement of the network size. Default value is 255.255.255.0
DHCP Type: Activate the checkbox to enable DHCP server
Start/End IP Address: Enter the range of IP address for DHCP server distribution.

8.3 DHCP Clients

You could monitor DHCP clients here
Expires in: The length of the IP address lease

8.4. Advanced Routing

You may add and remote custom Internet routing rules, disable/enable dynamic routing exchange protocol here

9.Wireless Settings
9.1 Basic Wireless Settings

Network Mode: Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.
Network Mode(SSID): Main Service Set Identifier. It's the "name" of your wireless network.
Multiple SSID: Minor Service Set Identifier. It is optional.

9.2 Advanced Wireless Settings

BG protection Mode: Auto by default. You can select on or off.
Beacon Interval: Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.
Fragment Threshold: Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold: Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.
TX Power: You can set the output power of wireless radio. you don't need to set output power to 100 unless under the environment of large space, setting output power can enhance security (malicious / unknown users in distance will not be able to reach your wireless router)

9.3 Security Settings
9.3.1 WEP Settings
WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). 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.

SSID Choice: Select SSID to be configured security. The device supports to configure different security classes between the main SSID and the subordinate SSID.

Security Mode: There are several different security modes, you can choose one from mixed WEP, WPA-Personal, WPA-Enterprise, etc.

Default Key: Select a valid encryption key.

WEP Key1, 2, 3, 4: Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be ASCII Characters or Hexadecimal Digits.

9.3.2 WPA-PSK (WIFI Protected Access), a WIFI standard is a relatively new wireless encryption scheme, designed to improve the security features of WEP. It can be applied to more powerful encryption types (such as TKIP Temporal Key Integrity Protocol or AES Advanced Encryption Standards) and can change the keys dynamically on every authorized wireless device.

WPA Algorithms: Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

Pass Phrase: Enter the key which must have 8-63 ASCII characters

Key Renewal Interval: Enter the key renewal period. It is to tell the Router how often to change the keys.

9.3.3 WPA2-PSK (Wi-Fi Protected Access version 2), It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.
WPA Algorithms: Select key Algorithms such as TKIP, AES and TKIP&AES.
Pass Phrase: Enter the key which must have 8-63 ASCII characters.
Key Renewal Interval: Enter the key renewal period. It is to tell the router how often to change the keys.

9.3.4 WPA
The authentication protocol is based on RADIUS servers. This security mode is used when a RADIUS server is connected to the router.
IP Address: Please input IP address of the radius server here.
Port: Please input the port number of the radius server here.
Shared Secret: The encryption key that the router is authenticated through RADIUS server
Key Renewal Interval: The recertification time interval between the router and the server. The default value is 3600s.

9.3.5 WPA2
This security mode is also used when a RADIUS server is connected to the router.
WPA Algorithms: Select key Algorithms such as TKIP and AES.
IP Address: Please input IP address of the radius server here.
Port: Please input the port number of the radius server here.
Shared Secret: The encryption key that the router is authenticated through RADIUS server
Key Renewal Interval: The recertification time interval between the router and the server. The default value is 3600s.

9.3.6 802.1x
This security mode is used when a RADIUS server is connected to the Router. 802.1x, it is a kind of Port-based authentication protocol, authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass.

WEP: Select "enable/disable" WEP encryption which indicates the authentication process between wireless adapter and wireless router.
IP Address: Please input IP address of the radius server here.
Port: Please input the port number of the radius server here.
Shared Secret: The encryption key that the router is authenticated through RADIUS server.

  Key Renewal Interval: The recertification time interval between the router and the server. The default value is 3600s.
⚠ NOTE: To improve security level, Please don't use simple letters or those figures are easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it's worth to use complicated WEP key to improve security level.

9.4 WPS Settings

WPS (WIFI Protected Setting) It can be easy and quick to establish the connection between the wireless network clients and the router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

WPS Mode: Supports two ways to configure WPS settings: PBC (push configuration button) and PIN code

PBC: Select the PBC or press the WPS button on the panel of the Router (Press the button for one second and wait for 2 minutes, then the WPS is enabled. you can enable another router to implement the WPS/PBC negotiation with it. The WPS mode only supports one client 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 client.

9.5 Ethernet conversion setting (make sure the manual switch turn to WIFI mode)

In Ethernet conversion Mode, WAN port is the wireless network port, and LAN port is the Ethernet port. Around the workstation, you can connect PC to the router. Open "wireless setting"->Click "Search for wireless radio station"->select SSID->Click "connection"

SSID: SSID is the unique ID name of access point. The wireless work station must keep the same SSID name with the AP's for connections. By enabling Open Scanning button, the device can search available APS.

BSSID: To connect certain AP, you need to know the AP's MAC address. By enabling open scanning button to find out the available AP's MAC address.

Security Mode: router provides the following security authentication methods:

(1) WEP: selects ASCII format (5-13 ASCII characters except illegal characters.) or Hex format (10-26 Hex characters).

(2) WPA/WPA2-personal (PSK) is safer than other encryption methods because the key is subject to change all the time. WPA-PSK/WPA2-PSK utilizes the TKIP or AES encryption algorithm.

WEP Mode: The shared key requires the same WEP keys between the access point and work station.

Default KEY: After entering the WEP keys, select one key as the default one, for example, Key 1

KEY Format: ASCII: Enter 13 characters with case sensitive ("a-z", "A-Z" and "0-9"). Hex: enter 26 Hex characters ("A-F", "a-f" and "0~9").

  KEY 1: If the KEY 1 is selected as default key, the key will be enabled.
  KEY 2: If the KEY 2 is selected as default key, the key will be enabled.
  KEY 3: If the KEY 3 is selected as default key, the key will be enabled.
  KEY 4: If the KEY 4 is selected as default key, the key will be enabled.

WPA/WPA2 Algorithm: When the WPA-PSK /WPA2-PSK authentication is selected, you can select one from two: TKIP and AES. For example, if the wireless provider selects TKIP, the wireless receiver (client) also needs to select TKIP for this authentication way.
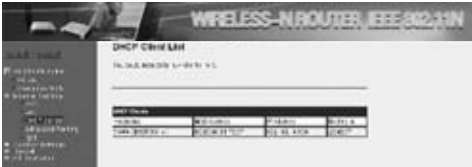
Password: When WPA-PSK /WPA2-PSK authentication type is selected, enter the access password provided by AP users here.

Apply: Click "Apply" to make the settings go into effect.

Cancel: Click "Cancel" to throw all setting saved last time.

9.6 Station List

You could monitor stations which associated to this AP here

MAC Address: Shows the connecting PC MAC address

10. Firewall settings

10.1 MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus worm and malicious activity on the Internet

MAC/IP/Port Filtering: If you want to access the Router from any external IP Address, please select the "Disable".

MAC Address: To specify an external IP address, please add the MAC address manually and click "Apply".

10.2 Port Forwarding Settings

You may setup Virtual Servers to provide services on Internet

Virtual Server Settings: Setting enable and disable the virtual server, the default is disabled.
IP address: Enter the IP address of the PC where you want to set the applications.
Port Range: Enter the start/end port number which ranges the External ports used to set the server or Internet applications, Range from 1to 9999.
Protocol: Select the protocol (TCP/UDP/TCP&UDP) for the application.

10.3 DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet

The DMZ function allows one computer in LAN to be exposed to the Internet for a special-purpose service such as Internet gaming or video conferencing.
DMZ Settings: select checkbox to enable the DMZ host
DMZ IP Address: The IP address of the computer you want to expose
IMPORTANT: When enable the DMZ host, the firewall settings of the DMZ host will not function.

11. Administration settings

11. 1 System Management Settings
You may configure administrator account and password, NTP settings, and Dynamic DNS settings here

Select Language: set language
Account: Enter a new user name for the device.
Password: Enter a new password then Click "Apply"

11.2 Upload Firmware Settings
Upgrade the WiFi-150M Router firmware to obtain new functionality.
It takes about 1 minute upload to upgrade flash, please wait patiently
Caution! A corrupted image will hang up the system.

The Router provides the firmware upgrade by clicking the "Upgrade" after browsing for the firmware upgrade packet.

Browse: Click this button to browse the directory where you download the firmware upgrade files.

Apply: Click this button to start upgrade.

IMPORTANT: Do not turn off the system during the firmware upgrade to avoid damaging the device. The router will reboot after upgrade.

11.3 Settings Management

You can save system settings by exporting them to a configuration file, restore them by importing the file, and reset them to factory default

Load Defaults: Click this button to reset all configurations to the default values. It means router will lose all settings you set before. So please note down the related settings if necessary.

Factory Default Settings:

User Name: admin

Password: admin

IP Address: 192.168.16.1

Subnet Mask: 255.255.255.0

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

LB-LINK