



USER'S MANUAL

English Version: 1.0

MZK-W04N
Draft IEEE 802.11n Wireless Broadband Router

Draft IEEE 802.11n Wireless Broadband Router

MZK-W04N

Foreword

Explanation of the signals

In order to let you set up and use this product correctly, please pay attention when reading or browsing the manual as you see these signals listed below.



Warning/ Danger

Users should read the explanation carefully and understand it completely, otherwise users might be in danger or even be injured.



Caution/ Be Careful

Remind users to be careful when setting up the product and to avoid damaging the product or its system programs.

Seeking for service or searching for an agent or a distributor

Thank you for purchasing products from Planex Communications Inc. If you have any operational problems while configuring or setting up the product, you may contact with our Customer Service Department or ask the agent or the distributor from which you bought the product for help. Moreover, during warranty, if you find any defect or breakdown of the product, you may bring the product, assembly, and its warranty card to our company or to where you bought the product to ask for repair.

★Every product has different warranty period and contract; please refer to our company for further information or consult the agent or the distributor.

Planex Communications Inc.

Support Phone : **+65-6338-1704 (Singapore)**

+886-2-8218-7114 or +886-2-2219-7454 (Taiwan)

Customer Service E-Mail : techsupport@planex.com.tw

Contact Us

Tel : **+886-2-2219-1816**

Fax : **+886-2-2219-0655**

Agents & Distributors : <http://www.planex.net/where/index.htm>

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.



Trademarks:

All trade names and trademarks are the properties of their respective companies.

Copyright © 2007 All Rights Reserved.

Contents

Foreword

Chapter1 Introduction to MZK-W04N	1
1. Contents of Package	5
2. Product Functions	6
3. How to Set Up MZK-W04N	8
Chapter2 Setup & Configuration	11
1. Client's Computer Setup	11
2. Web Configuration	13
3. Quick Setup	16
3.1 Time Zone	17
3.2 Broadband Type & IP Address Info	18
4. System	23
4.1 Time Zone	23
4.2 Password Settings	24
4.3 Remote Management	25
4.4 RIP	26
4.5 SNMP	27
5. WAN	28
5.1 Dynamic IP	28
5.2 Static IP	29
5.3 PPPoE	30
5.4 PPTP	32

5.5 L2TP	35
5.6 Telstra Big Pond	37
5.7 DNS	38
5.8 DDNS.....	39
6. LAN	40
6.1 LAN Settings	40
Chapter3 Advanced Setup & Configuration	43
1. Wireless	43
1.1 Basic Settings	44
1.2 Advance Settings.....	45
1.3 Security Settings	48
1.3.1 Disabled.....	51
1.3.2 WEP	52
1.3.3 WPA pre-shared key	53
1.3.4 WPA RADIUS.....	54
1.4 Access Control.....	55
1.5 WPS	56
2. QoS	61
3. NAT	62
3.1 Port Forwarding	63
3.2 Virtual Server	64
3.3 Special Applications	67

Contents

3.4 UPnP Setting	69
3.5 ALG Settings	70
4. Firewall	71
4.1 Access Control	72
4.2 URL Blocking	74
4.3 DoS	75
4.4 DMZ	77
5. Status	79
5.1 Internet Connection	79
5.2 Device Status	80
5.3 System Log	80
5.4 Security Log	81
5.5 Active DHCP Client	81
5.6 Statistics	82
6. Tool	82
6.1 Configuration Tool	83
6.2 Firmware Upgrade	86
6.3 Restart	88

1

Introduction to MZK-W04N

Introduction

Thank you for purchasing **Draft IEEE 802.11n Wireless Broadband Router MZK-W04N**. This 802.11n wireless router is a multi-function device which provides **shared broadband Internet access for all LAN users** and **4-Ports switching hub for 10/100 Base-T connections**.

MZK-W04N Wireless Router incorporates many advanced features, and it was designed to provide sophisticated but easy to use functions. MZK-W04N has a built-in Web server, thus you can access its settings through Web browsers, such as IE, Netscape, Firefox, and so on. You can set up and configure the settings easily and completely and enjoy the convenience instantly.

MZK-W04N has embedded with IEEE802.11b/g and Draft-N wireless communication standard. All the PCs and network devices, including PDA, mobile phone, game console and other digital appliances, with wireless functions can surf online wirelessly through MZK-W04N wireless broadband router. Cooperate with Draft-N wireless adapter, MZK-W04N can let data transmission rate up to 300Mbps! With all these features, MZK-W04N Wireless Router must be the best solution for both beginners and advanced users. The following chapters will introduce you the configuration steps and fantastic functions of MZK-W04N.

Special Features

→Internet Access Features

- **4-Port Switching Hub:**The Wireless Router incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support:**Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Router can act as a DHCP Server for devices on your local LAN and WLAN.
- **Shared Internet Access:**All users on the LAN or WLAN can access the Internet through the Wireless Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation). MZK-W04N can let at most 253 users connect online.
- **xDSL, Static IP & Cable Modem Support:**The Wireless Router has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- **PPPoE Support:**The Internet (WAN port) connection supports PPPoE (PPP over Ethernet).
- **Dynamic IP Address:**On the Internet (WAN port) connection, the Wireless Router support Dynamic IP Address (IP Address is allocated on connection).

→Configuration & Management

- **Easy Setup:**Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Remote Management:**The Wireless Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

- **UPnP Support:**UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later.
- **AP/Router Switch:**There is a switch on the back panel of MZK-W04N. You may use AP/Router switch to choose the function you want to use.
- **Built-in WPS (Wi-Fi protected setup) Function:**All you need to do is to press a button and then you can easily setup up wireless Internet and security settings. (Only Windows XP and 2000 OS support WPS function.)

→Wireless Features

- **Standards Compliance:**The Wireless Router complies with the IEEE802.11b/g and Draft-N (DSSS) specifications for Wireless LANs.
- **Support IEEE 802.11g Wireless Stations:**The IEEE 802.11g standard provides for backward compatibility with the standard 802.11g Wireless stations.
- **3dBi Antennas:**3dBi PR-SMA antennas can make data transmission rate faster and the radio coverage can be larger and have less dead spots.
- **Speeds to 300Mbps:**All speeds up to the 802.11n maximum of 300Mbps (theoretical value) are supported.
- **Wireless LAN Security:(WEP, WPA, WPA-PSK Support)** Supports for WEP (Wired Equivalent Privacy) and WPA-PSK, as well as Wireless access control to prevent unknown wireless stations from accessing your LAN. Key sizes of 64 Bit and 128 Bit are supported.
- **WDS support.**
- **Wireless MAC Access Control:**The Wireless Access Control feature can check the the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.

→Advanced Functions

- **Communication Applications:**Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- **WMM Support:**MZK-W04N can let you have better video/audio data transmission quality.
- **Special Internet Applications:**Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **DDNS Support:**DDNS (Dynamic DNS) allows Internet users to connect to Virtual Servers on your LAN using a domain name, even if your IP address is not fixed.
- **DMZ:**One PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet.
- **URL Filter:**Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Internet Access Log:**See which Internet connections have been made.
- **QoS Support.**

→Security Features

- **Password - protected Configuration:**Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **NAT Protection:**An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the Wireless Router.

- **Protection against DoS attacks:** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks.

1. Contents of Package

After purchasing MZK-W04N Wireless Router from a distributor or an agency, please open the package and check that all the components listed below are included. If there is any item missing or damaged, please contact with the distributor or the agency at once.

- MZK-W04N Wireless Broadband Router x 1
- 3dBi Antenna x 3
- AC Adapter x 1
- UTP Cable x 1
- Short Cord x 2
- User's Manual x 1
- Warranty Card x 1



If plug the AC adapter which includes in the product package into a socket with different voltage power supply, it will cause damage and that is not included in warranty.

2. Product Functions

Front Panel—LEDs



LEDs	Status	Meaning
Power	On/Off	When starting up MZK-W04N, the Power LED will be on.
WLAN	On/Blinking	When MZK-W04N finds any available wireless connection, the WLAN LED will be on. And the WLAN LED will be blinking when transmitting or receiving data via WLAN port.
WAN Link/Act	On/Blinking	When the connection is established between MZK-W04N and a modem, the WAN LED will be on. And the WAN LED will be blinking when transmitting or receiving data via WAN port.
WAN 10/100	On/Off	When the data transmission rate reaches 100Mbps, the WAN LED will be on. If the rate is only 10Mbps, the LED will be off.
LAN Link/Act	On/Blinking	When the connection is established between MZK-W04N and a modem, the LAN LED will be on. And the LAN LED will be blinking when transmitting or receiving data via LAN port.
LAN 10/100	On/Off	When the data transmission rate reaches 100Mbps, the LAN LED will be on. If the rate is only 10Mbps, the LED will be off.

Antenna & Ports



Ports	Function	
WAN	Connect a DSL or Cable Modem to the WAN port and link to the internet. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.	
LAN	Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports. Any LAN port can be connected with another hub, if required.	
Power	Plug the power cord into this port and the other side of the adaptor should be plugged into the socket.	
Button	Function	Usage
WPS	Wi-Fi Protected Setup	Please refer to WPS configuration chapter.
Reset	Reset to Default	Press the button for 3-5 seconds, and then unplug the power cord, but do not release the Reset button and wait for 3 seconds before plugging the power cord back. Release the Reset button and MZK-W04N will automatically restart and back to the default settings.
AP/Router	AP/Router Switching	Turn up or turn down the switch and then restart the system to choose the function you want to use.

3.How to Set Up MZK-W04N

1.Unwrap the package of MZK-W04N Wireless Router and check if the components are complete and without missing anything.

2.Choose an Installation Site.

Select a suitable place on the network to install MZK-W04N Wireless Router. And make sure that the wireless router and the DSL/Cable modem are not powered on yet.



For best Wireless reception and performance, the Wireless Router should be positioned in a central location with minimum obstructions between the Wireless Router and the PCs. Also, if using multiple Access Points, adjacent Access Points should use different Channels.

3.Connect LAN Cables.

Use standard LAN cables to connect PCs to the switching hub ports on MZK-W04N. Both 10 Base-T and 100 Base-T connections can be used simultaneously.

4.Connect WAN Cable.

Connect the DSL or Cable modem to the WAN port on MZK-W04N.

5.Power On.

Power the DSL or Cable modem on. At last, connect the adapter with MZK-W04N and plug the other side of the power cord into the power socket. Power MZK-W04N Wireless Router on. While detecting, the Power LED and WAN LED will be on, and LAN LED and WLAN LED will be blinking for a while and then the MZK-W04N will be ready in a short time.



Plug the AC Adapter which comes with MZK-W04N in a different voltage power supply will cause damage on MZK-W04N, and it is not included in warranty.

System Requirements

- Windows, Macintosh, or Linux-based Operating System with an installed Ethernet adapter
- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage)
- To use the Wireless Router, all Wireless devices must be compliant with the IEEE802.11b/g/n specifications.

2

Setup & Configuration

1. Client's Computer Setup

The computers on your LAN need to be set up to cooperate with MZK-W04N Wireless Router.

Please make sure that your operating system already enabled your interface card on the host and connected to one of the LAN ports on MZK-W04N through Cat.5 cable. Be sure that LEDs on MZK-W04N are already on and the LED corresponds with the port which you connected. If you switch on MZK-W04N for the first time, owing to the default status, it will automatically enable the embedded DHCP server and start to distribute IP to your host. In addition, the default IP address of MZK-W04N is “**192.168.1.1**.” If your operating system is Windows 98/2000/XP, you may be able to use command of “**ipconfig**” to inquire whether you have the correct IP address or not. If you are using Linux/Unix-Like system, you can use “**ifconfig**” to check your NIC (Network Interface Card) address. The instructions are as follows:

● Windows98

1. Click “**Start**→**Programs**→**MS-DOS**” or “**Start**→**Run**” and type in “**command.exe**” and then press enter.
2. “**MS-DOS**” window will appear.
3. Type “**ipconfig**” after the command of “**c:>**” and then press enter.
4. MS-DOS will appear your NIC address in the window, please take notice of the value of “**IP Address**” and “**Default Gateway**.”
5. The value of “**Default Gateway**” is the IP address of MZK-W04N.

● Windows 2000/XP

1. Please make sure that you do have the authority to access as an “**Administrator**” or you are already one of the “**System Administrators.**”
2. Click “**Start→Programs→Accessories→Command Prompt**” or “**Start→Run,**” and then type in “**cmd.exe**” and press enter.
3. It will appear a “**MS-DOS**” window.
4. Type “**ipconfig**” after the command of “**c:>**” and then press enter.
5. MS-DOS will appear your NIC address in the window, please take notice of the value of “**IP Address**” and “**Default Gateway.**”
6. The value of “**Default Gateway**” is the IP address of MZK-W04N.

● Linux / Unix-Like

1. At first please make sure that your NIC are already enabled and works properly.
2. And be sure you have “**root**” number or your already are one of the members of a “**root**” group.
3. Please type “**ifconfig**” of “**ifconfig -a**” after “**#**” and then press enter.
4. It will appear your present NIC address in the window, please take notice of the value of “**IP Address**” and “**Gateway.**”
5. The value of “**Gateway**” is the IP address of MZK-W04N.

If you can get “**IP Address**” and “**Gateway,**” normally, it means that you may use web browser to configure MZK-W04N. Type your destination — “**http://192.168.1.1**” (default IP Address of MZK-W04N) on the Address Bar in the web browser. If you have changed the default IP Address of MZK-W04N, please type in the new address on the address bar.

2. Web Configuration

The MZK-W04N Wireless Router contains an HTTP server. This enables you to connect the router, and configure it by using your web browser.

Before attempting to configure MZK-W04N Wireless Router, please ensure that your PC can establish a physical connection to the Wireless Router. The PC and the MZK-W04N Wireless Router must be directly connected with each other (using the LAN ports on MZK-W04N) or on the same LAN segment. Besides, the MZK-W04N Wireless Router must be set up and powered on.

The MZK-W04N Wireless Router's default IP Address is "192.168.1.1." If the IP address has already used by another device, the other device must be turned OFF until MZK-W04N is allocated a new IP Address.

Using UPnP

After set up and powered on the MZK-W04N Wireless Router, if your Windows system supports UPnP, an icon for the Wireless Router will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut for the newly-discovered device. Unless you intend to change the IP Address of the MZK-W04N Wireless Router, you can accept the desktop shortcut. Whether you accept the desktop shortcut or not, you can always find UPnP devices in Network Neighborhood. Double click the icon of the MZK-W04N Wireless Router (either on the Desktop, or in Network Neighborhood) to start the configuration.

Using Web Browser

To establish a connection between your PC and the MZK-W04N Wireless Router:

1. Start the WEB browser.
2. In the Address box, enter “http://192.168.1.1” which is the default IP Address of the MZK-W04N Wireless Router. Press “**Enter**” on your keyboard, and the pop-up will ask you to enter the **User Name** and **Password** to get into the program.



3. Enter the default User Name “**Admin**” and Password “**0000**” and then click “**OK**” to enter the system. You can also put a check in the “**Remember my password**” check box, and next time you do not need to enter password to enter the system.



4. After entering the system, MZK-W04N will show you the homepage. During configuration, you can use the links on the top of the page to navigate. Besides, it is necessary that, after configuring, you should click “Apply” to enable the settings you’ve made.



If your MZK-W04N Wireless Router does not response, and you cannot enter the web configuration page, please follow the steps below to check if there is any problem:

1. Make sure that MZK-W04N Wireless Router is properly installed and powered on, and LAN connection is O.K. You can test the connection by using “Ping” command:



- ◆ Open MS-DOS window or click “Start→Run” on the desktop to show the command prompt window.
- ◆ Enter the command: ping 192.168.1.1
- ◆ If it shows the message of “Request time out,” the problem can be either disorder of connection, or the conflict between your PC’s IP address and the router’s IP address.

2.If your PC uses static IP address, the IP address must be in the range of 192.168.1.2~192.168.1.254, in order not to occupy the MZK-W04N's default IP address “**192.168.1.1.**” In addition, the subnet mask must be “**255.255.255.0.**” To know more details of your PC and Internet connection, please check the TCP/IP settings on your PC.



3.You have to make sure that your PC and MZK-W04N are on the same segment. Besides, you have to use the wired LAN interface when first accessing the web configuration page, the wireless interface only works when the settings of MZK-W04N matches your PC's wireless settings.

3.Quick Setup

After you login the configuration utility, you can click “**Quick Setup**” on the left upper page to start setting up MZK-W04N Wireless Broadband Router. You can finish setting up the router and begin to connect Internet just through a few simple and easy steps. Please follow the instructions below to set up MZK-W04N.



3.1. Time Zone

You can set the system time according to the time zone where you locate now.



- **Set Time Zone** : Scroll the list to choose the time zone for MZK-W04N.
- **Time Server Address** : You can enter the Internet address of an NTP(Network Time Protocol) Server for your system to synchronize with.
- **Daylight Savings** : If you want to set up Daylight Savings, please click “**Enable Function**” check box first, and then set up the time period.
- **Next** : After finishing choosing the time zone, please click “**Next**” to continue setting up.

3.2. Broadband Type & IP Address Info

The followings are the most common used connection types: **Cable Modem**, **Fixed-IP xDSL**, and **PPPoE xDSL**. If you want to know more about the other types of WAN configurations, please refer to “WAN” configuration page.

- ✓ 1. Time Zone
- ✓ 2. Broadband Type
- 3. IP Address Info

Broadband Type
Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed IP xDSL, PPPoE xDSL or PPPoE xDSL connection.

Cable Modem
A connection through a cable modem requires manual configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.

Fixed-IP xDSL
Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.

PPPoE xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.

PPoP xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPoP to establish a connection. You must choose this option and enter the required information.

L2TP xDSL
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

Telstra Big Pond
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below. This information is provided by Telstra BigPond.

→ Cable Modem

1. If you use cable modem, you may choose this entry and use the wizard to configure. Click “**Cable Modem**” to proceed.

- ✓ 1. Time Zone
- ✓ 2. Broadband Type
- 3. IP Address Info

Broadband Type
Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed IP xDSL, PPPoE xDSL or PPPoE xDSL connection.

Cable Modem
A connection through a cable modem requires manual configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.

Fixed-IP xDSL
Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.

PPPoE xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.

PPoP xDSL
If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPoP to establish a connection. You must choose this option and enter the required information.

L2TP xDSL
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

Telstra Big Pond
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below. This information is provided by Telstra BigPond.

2.The following are the WAN settings; please configure the settings according to the real environment.



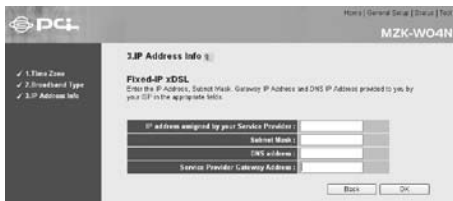
- **Host Name** : Enter the host name of your PC and this is optional. It is only required when your service provider asks you to do so.
- **MAC address** : The default MAC address of MZK-W04N is the Network Interface Card's (NIC) MAC address on the WAN side. If you were asked to use the NIC provided by the ISP, you may click “**Clone Mac address**” and enter the MAC address of NIC provided by the ISP. We do not suggest you to change the default MAC address, if your ISP does not ask you to change it.
- **Back** : If you want to go back to the previous step, please click this button.
- **OK** : After finishing setting up, you may click here.

→Fixed-IP xDSL

1.If you have already had a Static IP address, you can choose this entry and use the wizard to configure. Click **“Fixed-IP xDSL”** to proceed.



2.The following are the WAN settings; please configure the settings according to the real environment.



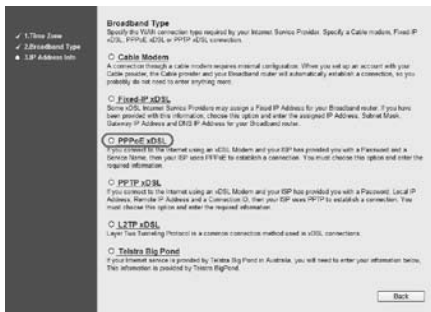
- **ISP address assigned by your Service Provider** : Enter the IP address provided by your ISP.
- **Subnet Mask** : Enter the Subnet Mask address provided by your ISP.
- **DNS address** : Enter the DNS IP address provided by your ISP.
- **Service Provider Gateway Address** : Enter the Default Gateway address provided by your ISP.

● **Back** : If you want to go back to the previous step, please click this button.

● **OK** : After finishing setting up, you may click here.

→ PPPoE

1.If you use PPPoE, you may choose this entry and use the wizard to configure. Click “**PPPoE xDSL**” to proceed.



2.The following are the WAN settings; please configure the settings according to the real environment.



● **User Name** : Enter the User Name provided by your ISP. (The ID must be alphanumeric characters and case sensitive.)

- **Password** : Enter the Password provided by your ISP. (The password must be alphanumeric characters and case sensitive.)
- **Service Name** : If your ISP provided the Service Name, please enter the name according to the provided information. (The name must be alphanumeric characters and case sensitive.)
- **MTU** : MTU means **Maximum Transmission Unit**, the largest physical packet size, measured in bytes, that a network can transmit. The default value is 1454. Please set up the MTU according to your system environment. Only enter a new MTU when your ISP requires, otherwise, please leave it as the default setting. When using PPPoE connection, you may need to change MTU settings to maintain the connection with your ISP, however, if the incorrect value was entered, you may be unable to access certain websites. Reducing the packet size can help connecting to certain websites or speeding up the transmission rate.
- **Connection Type** : There are three connection type—**Continuous** 、 **Connect On Demand** 、 **Manual** 。 Select “**Continuous**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will automatically reconnect to your ISP. Select “**Connect On Demand**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will reconnect to your ISP when there's a connecting request. Select “**Manual**” and whenever you restart the system or the connection is stopped, you have to manually set up to reconnect to your ISP.
- **Idle Time Out** : Idle Timeout means a period of idle time before you go offline. Enter a maximum period of time (seconds) to define the maximum idle time. If the idle time is above the defined maximum idle time, it will go offline immediately. You can set the value to be 0 or Auto Reconnect to disable this function.
- **Back** : If you want to go back to the previous step, please click this button.
- **OK** : After finishing setting up, you may click here.

3. Click **“Apply”** to save those previous settings. Please do not close the window or unplug the power cord when restarting the system. The system will automatically go back to the homepage after restarting.



4. System

On the System configuration page, you can configure many things, such as

- ◆ Time Zone and NTP (Network Time Protocol)
- ◆ Password
- ◆ Remote Management
- ◆ RIP
- ◆ SNMP

4.1. Time Zone

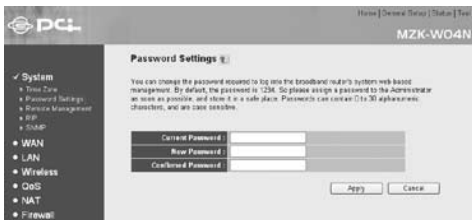
You can set the system time according to the time zone where you locate now.



- **Set Time Zone** : Scroll the list to choose the time zone for MKZ-W04N.
- **Time Server Address** : You can enter the Internet address of an NTP(Network Time Protocol) Server for your system to synchronize with.
- **Daylight Savings** : If you want to set up Daylight Savings, please click “**Enable Function**” check box first, and then set up the time period.
- **Apply** : Click this button, the system will save the settings and synchronize with NTP Server.
- **Cancel** : If there is anything wrong with the configuration, you can click “**Cancel**” to configure the page again.

4.2.Password Settings

The default User Name of MKZ-W04N Wireless Router is “**admin**” and Password is “**0000.**” It is recommended that you should change the default password to have better protection over the router and the LAN. You must memorize the password set by you to enter the system; otherwise, you have to restore the whole systems and then configure the settings again.

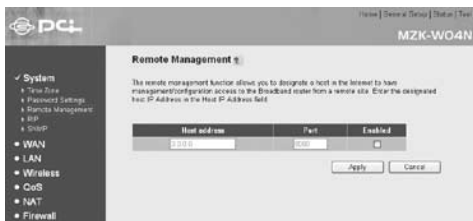


- **Current Password** : Enter the current Password of the administration.
(Enter 30 alphanumeric characters at most.)

- **New Password** : Enter a new Password of the administration. (Enter 30 alphanumeric characters at most.)
- **Confirmed Password** : Please enter the password again for confirmation.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

4.3.Remote Management

MZK-W04N Wireless Router can be managed by any PC from your LAN. If the router has connected to the Internet, the administrator can also configure it via the Internet. Owing to the security, however, you must have a static IP before performing remote management.



- **Host address** : Enter the IP address of the remote management interface.
- **Port** : Enter the port number of the remote management port.
- **Enabled** : Click the check box to enable remote management function.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

4.4.RIP

Routing Information Protocol is abbreviated as **RIP**, an interior gateway protocol defined by RFC 1058 that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables.



● **Enable/Disable** : Choose to “**Enable**” or “**Disable**” RIP function. The default setting is disabled.

● **Apply** : Click this button to save the settings and restart the router.

● **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again..

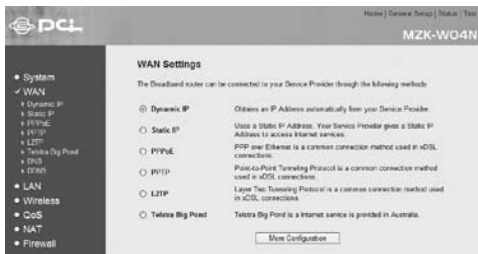
Simple Network Management Protocol is abbreviated as **SNMP**. It is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.



- **Enable/Disable** : Choose to “**Enable**” or “**Disable**” SNMP function. The default setting is disabled.
- **Community** : Only the effective Community can access data on the agent program. “**Public**” is the most common Community.
- **Trap Receiver** : Please enter the IP address of the Trap Receiver.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

5. WAN

In the WAN settings, MZK-W04N Wireless Router provides many kinds of access. You can configure the WAN side according to the real environment. Click “**More Configuration**” to proceed.



5.1. Dynamic IP

If you automatically get the IP address from your ISP or use the Cable Modem, please choose “**Dynamic IP**” from the above page.



- **Host Name** : Enter the host name of your PC and this is optional. It is only required when your service provider asks you to do so.
- **MAC address** : The default MAC address of MZK-W04N is the Network Interface Card's (NIC) MAC address on the WAN side. If you were asked to use the NIC provided by the ISP, you may click “**Clone Mac address**” and enter the MAC address of NIC provided by the ISP. We do not suggest you to change the default MAC address, if your ISP does not ask you to change it.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

5.2.Static IP

If you do not need to make a dial-up connection, and your ISP provides you a static IP address, please choose “**Static IP**” from the above page.



- **ISP address assigned by your Service Provider** : Enter the IP address provided by your ISP.
- **Subnet Mask** : Enter the Subnet Mask address provided by your ISP.

- **Service Provider Gateway Address** : Enter the Gateway address provided by your ISP.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

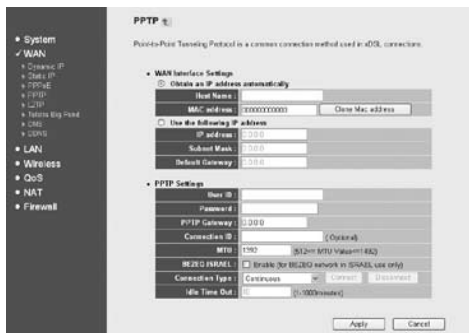
5.3.PPPoE

If your ISP assigns a new IP address for you whenever you login, please choose “**PPPoE (Point to Point Protocol over Ethernet)**” from the above page.

- **User Name** : Enter the User Name provided by your ISP. (The ID must be alphanumeric characters and case sensitive.)
- **Password** : Enter the Password provided by your ISP. (The password must be alphanumeric characters and case sensitive.)
- **Service Name** : If your ISP provided the Service Name, please enter the name according to the provided information. (The name must be alphanumeric characters and case sensitive.)

- **MTU** : MTU means **Maximum Transmission Unit**, the largest physical packet size, measured in bytes, that a network can transmit. The default value is 1454. Please set up the MTU according to your system environment. Only enter a new MTU when your ISP requires, otherwise, please leave it as the default setting. When using PPPoE connection, you may need to change MTU settings to maintain the connection with your ISP, however, if the incorrect value was entered, you may be unable to access certain websites. Reducing the packet size can help connecting to certain websites or speeding up the transmission rate.
- **Connection Type** : There are three connection type—**Continuous** 、 **Connect On Demand** 、 **Manual** 。 Select “**Continuous**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will automatically reconnect to your ISP. Select “**Connect On Demand**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will reconnect to your ISP when there's a connecting request. Select “**Manual**” and whenever you restart the system or the connection is stopped, you have to manually set up to reconnect to your ISP.
- **Idle Time Out** : Idle Timeout means a period of idle time before you go offline. Enter a maximum period of time (seconds) to define the maximum idle time. If the idle time is above the defined maximum idle time, it will go offline immediately. You can set the value to be 0 or Auto Reconnect to disable this function.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

Point-to-Point Tunneling Protocol (PPTP), a protocol that allows corporations to extend their own corporate network through private “tunnels” over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).



WAN Interface Settings

- **Obtain an IP address automatically/Use the following IP address** : Select the type of how you obtain IP address from your service provider. You can choose “**Obtain and IP address automatically**” (equal to DHCP, please refer to “**Cable Modem**” section above), or “**Use the following IP address**” (it means static IP address). WAN interface settings must be correctly set, or the Internet connection will fail even those settings of PPTP settings are correct.

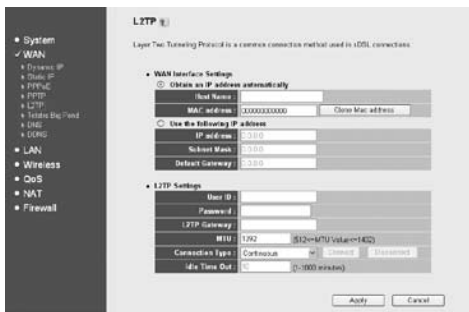
PPTP Settings

- **User ID** : Enter the User ID provided by your ISP. (The ID must be alphanumeric characters and case sensitive.)
- **Password** : Enter the Password provided by your ISP. (The password must be alphanumeric characters and case sensitive.)
- **PPTP Gateway** : Enter the IP address of PPTP gateway assigned by your ISP.
- **Connection ID** : Please enter the connection ID here, however, this is option and you can leave it blank.
- **MTU** : MTU means **Maximum Transmission Unit**, the largest physical packet size, measured in bytes, that a network can transmit. The default value is 1454. Please set up the MTU according to your system environment. Only enter a new MTU when your ISP requires, otherwise, please leave it as the default setting. When using PPPoE connection, you may need to change MTU settings to maintain the connection with your ISP, however, if the incorrect value was entered, you may be unable to access certain websites. Reducing the packet size can help connecting to certain websites or speeding up the transmission rate.
- **BEZEQ-ISRAEL** : “**BEZEQ-ISRAEL**” is only required when you're using the service provided by BEZEQ network in Israel.
- **Connection Type** : There are three connection type—**Continuous** \ **Connect On Demand** \ **Manual** . Select “**Continuous**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will automatically reconnect to your ISP. Select “**Connect On Demand**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will reconnect to your ISP when there's a connecting request. Select “**Manual**” and whenever you restart the system or the connection is stopped, you have to manually set up to reconnect to your ISP.

- **Idle Time Out** : Idle Timeout means a period of idle time before you go offline. Enter a maximum period of time (seconds) to define the maximum idle time. If the idle time is above the defined maximum idle time, it will go offline immediately. You can set the value to be 0 or Auto Reconnect to disable this function.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

5.5.L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private network. L2TP is original from Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP provides additional security features other than PPTP. L2TP acts as data link layer protocol for tunneling network traffic between clients and VPN server over an Internet. It builds up Point-to-Point Protocol (PPP) sessions within an L2TP tunnel.



WAN Interface Settings

- **Obtain an IP address automatically/Use the following IP address** : Select the type of how you obtain IP address from your service provider. You can choose “**Obtain and IP address automatically**” (equal to DHCP, please refer to “**Cable Modem**” section above), or “**Use the following IP address**” (it means static IP address). WAN interface settings must be correctly set, or the Internet connection will fail even those settings of L2TP settings are correct.

L2TP Settings

- **User ID** : Enter the User ID provided by your ISP. (The ID must be alphanumeric characters and case sensitive.)
- **Password** : Enter the Password provided by your ISP. (The password must be alphanumeric characters and case sensitive.)
- **L2TP Gateway** : Enter the IP address of L2TP gateway assigned by your ISP.
- **MTU** : MTU means **Maximum Transmission Unit**, the largest physical packet size, measured in bytes, that a network can transmit. The default value is 1454. Please set up the MTU according to your system environment. Only enter a new MTU when your ISP requires, otherwise, please leave it as the default setting. When using PPPoE connection, you may need to change MTU settings to maintain the connection with your ISP, however, if the incorrect value was entered, you may be unable to access certain websites. Reducing the packet size can help connecting to certain websites or speeding up the transmission rate.
- **Connection Type** : There are three connection type—**Continuous** 、 **Connect On Demand** 、 **Manual** 。 Select “**Continuous**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will automatically reconnect to your ISP. Select “**Connect On Demand**” and whenever you restart the system or the connection is stopped, MZK-W04N Wireless Router will reconnect to your ISP when there's a connecting request. Select “**Manual**” and whenever you restart the system or the connection is stopped, you have to manually set up to reconnect to your ISP.
- **Idle Time Out** : Idle Timeout means a period of idle time before you go offline. Enter a maximum period of time (seconds) to define the maximum idle time. If the idle time is above the defined maximum idle time, it will go offline immediately. You can set the value to be 0 or Auto Reconnect to disable this function.
- **Apply** : Click this button to save the settings and restart the router.

- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

5.6. Telstra Big Pond

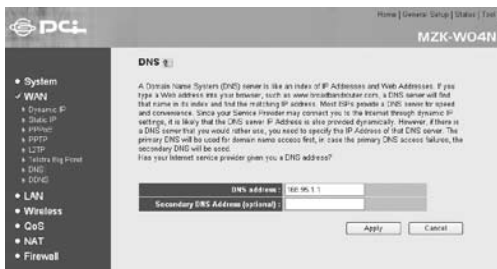
If you're using the Internet service provided by Telstra Big Pond in Australia. You may need to do the following settings according to the information provided by your ISP.

The screenshot shows the PCL router's configuration interface. The top right corner displays 'Menu [General Setup | Status | Test]' and the router model 'MZK-WO4N'. The left sidebar has a tree view with 'WAN' selected. The main content area is titled 'Telstra Big Pond' and contains the following text: 'If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below. This information is provided by Telstra BigPond'. Below this text are four input fields: 'User Name', 'Password', a checkbox labeled 'User decide login server manually', and 'Login Server'. At the bottom right of the form are two buttons: 'Apply' and 'Cancel'.

- **User Name** : Enter the User Name provided by your ISP. (The ID must be alphanumeric characters and case sensitive.)
- **Password** : Enter the Password provided by your ISP. (The password must be alphanumeric characters and case sensitive.)
- **User decide login server manually** : Check this check box to manually enter the login server by yourself.
- **Login Server** : Enter the IP address of the login server.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

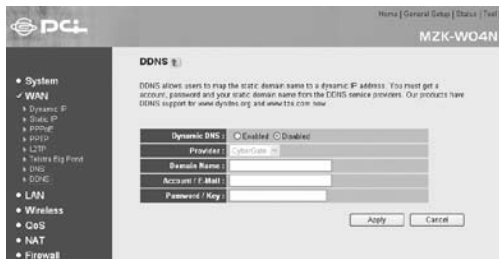
5.7.DNS

If you choose “Dynamic IP” or “PPPoE” as WAN settings, and there's at least one DNS will be assigned automatically. If you have other preferred DNS server, or your ISP do not give you an IP address of DNS server, you can configure the DNS settings on this page.



- **DNS address** : Enter the DNS address provided by your ISP.
- **Secondary DNS Address (optional)** : Enter another DNS address provided by your ISP, however, this is option and you may leave it blank.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

Dynamic DNS can let you connect with one or more DDNS services to update your current dynamic IP address.



- **Dynamic DNS** : You may **Enabled** DDNS function and then choose a DDNS provider from the list. The default status is **Disabled**.
- **Provider** : Scroll down the list to choose a service provider.
- **Domain Name** : Enter the Domain Name which you registered.
- **Account / E-Mail** : Enter the Account or E-Mail which you use to login the service.
- **Password / Key** : Enter the Password or Key which you use to login the service.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click "**Cancel**" to configure the page again.

6. LAN

Here you can do LAN IP, DHCP Server, and Static DHCP Lease settings.

6.1.LAN Settings

On the LAN Settings page, you can set up LAN IP address and so on; moreover, you can enable DHCP function to assign IP addresses to users on the LAN.

DHCP stands for **Dynamic Host Control Protocol**. MZK-W04N Wireless Router has a built-in DHCP server which can automatically assign an IP address to those computers/devices on the LAN/private network. If you enable DHCP server, the client host will obtain an IP address automatically. Whenever you turn on the computer, it will automatically load the proper TCP/IP settings from MZK-W04N. The DHCP server will allocate an unused IP address from the IP address pool to the requesting computer, but you must specify the beginning and ending address of the IP address pool.

- System
- WAN
- ✓ LAN
- Wireless
- QoS
- NAT
- Firewall

LAN Settings

You can enable the Directlead router's DHCP server to dynamically allocate IP Address to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

- LAN IP

IP address	192.168.1.1
Subnet Mask	255.255.255.0
IGMP-14 Snooping Time	Disabled <input type="checkbox"/>
DHCP Server	Enabled <input checked="" type="checkbox"/>
- DHCP Server

Lease Time	Forever <input type="checkbox"/>
Start IP	192.168.1.20
End IP	192.168.1.60
Default Name	
- Static DHCP Leases Table
It allows to entry 16 sets address only.

NO.	MAC address	IP address	Select
<input type="button" value="Create Database"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable Static DHCP Leases

No.	MAC address	IP address	Act
1			<input type="button" value="Add"/> <input type="button" value="Del"/>

LAN IP

- **IP address** : Here is the IP address of the LAN side of MZK-W04N. It is usually the default gateway of the client's PC. The default IP address is “192.168.1.1” .
- **Subnet Mask** : The Subnet Mask of the LAN side of MZK-W04N is “255.255.255.0” .
- **802.1d Spanning Tree** : If you want to use 802.1d Spanning Tree function, please scroll down the list to “**Enabled**” it. The default setting is “**Disabled**” .
- **DHCP Server** : Scroll down the list to “**Enabled**” or “**Disabled**” the DHCP server of MZK-W04N. The default setting is “**Disabled**” .

DHCP Server

- **Lease Time** : Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this router from dropdown menu.
- **Start IP/End IP** : Please enter the first and the last IP addresses which MZK-W04N distribute IP addresses to. The IP addresses in this range can get assigned IP addresses from MZK-W04N. (However, all the PCs on the same LAN should use the same subnet mask.)
- **Domain Name** : If you have already registered a domain name, you can enter your domain name here. It is optional.

Static DHCP Lease Table

- **Static DHCP Lease Table** : If you already set a range of IP addresses for the DHCP server to distribute, the clients who get the IP addresses will be listed here.
- **Enable Static DHCP Leases** : DHCP server can let a PC get the same IP address whenever it starts up on the LAN. You can distribute an appointed IP address to a specific computer according to the PC's MAC address. MZK-W04N provides 16 sets of static IP addresses for the DHCP server. The added DHCP clients will be listed on "**Static DHCP Leases Table**" on the bottom of the page. If you want to remove a single DHCP client, you may choose the item and click "**Delete Selected**"; or if you want to delete all the clients, you can click "**Delete All**". If you want to cancel the check you just made, you may click "**Reset**".
- **MAC address** : Enter the MAC address of the PC or network device.
- **IP address** : Enter the IP address you want to assign to the PC or network device.
- **Add** : After entering the MAC address and IP address, click this button to add the settings to Static DHCP Leases Table.
- **Clear** : If you want to clear the just entered but not added MAC address or IP address, click this button.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click "**Cancel**" to configure the page again.

3 *Advanced Setup & Configuration*

1. Wireless

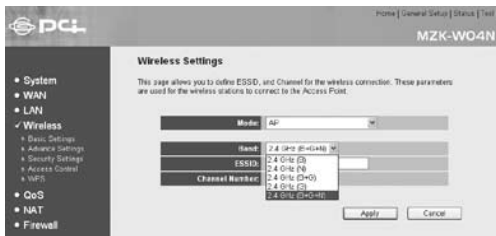
If your computer, PDA, game console, or other network devices which is equipped with wireless network interface, you can use the wireless function of this router to let them connect to Internet and share resources with other computers with wired-LAN connection. You can also use the built-in security functions to protect your network from being intruded by malicious intruders.

Choose **“Enabled”** or **“Disabled”** the Wireless function. The default value is **“Enabled”**. After modifying the settings, please click **“Apply”** to save the settings and restart the system.



1.1. Basic Settings

This page includes all the fundamental and basic parameters. After changing any parameters, you have to apply and restart the device and then the new settings can be effective.



● **Mode** : There are four kinds of wireless modes to choose from. Please select the wireless mode according to the real environment.

■ **AP** : Standard wireless AP (access point).

■ **AP Bridge-Point to Point** : Connect MZK-W04N with another wireless router, to expand the range of the network.

■ **AP Bridge-Point to Multi-Point** : Connect MZK-W04N with up to four other wireless routers, to expand the scope of network.

■ **AP Bridge-WDS** : Connect MZK-W04N with up to four WDS-capable wireless routers, to expand the range of network.

- **Band** : Scroll down the list to choose a band width. There are five kinds of modes: **B, N, B+G, G,** and **B+G+N**.
- **ESSID** : You can give MZK-W04N a unique name and let it be easily distinguished from other APs. It can be 32 alphanumeric characters.
- **Channel Number** : Here shows the channels provided by the local wireless connection. The setting of the channels of the wireless network should be the same as the wireless APs.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.2. Advance Settings

It is recommended that you should not arbitrarily change the default value on this page; otherwise, the performance of the wireless connection might be declined. If you want to configure this page to have better wireless performance, you can still modify the settings to comply with your environment.

Advance Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your D-Link router.

Fragment Threshold:	2346	(355-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20-1024 ms)
DTIM Period:	3	(1-10)
Data Rate:	Auto	
B Data Rate:	Auto	
Channel Width:	<input type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
Preamble Type:	<input type="radio"/> Short Preamble <input type="radio"/> Long Preamble	
Broadcast Cast:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
CTS Protect:	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power:	100 %	
Radio Mode:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
WMM:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
No Forwarding:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Apply Cancel

- **Fragment Threshold** : This value can define the maximum packet sized, so the packets bigger than this size will be segmented. If you set the lower value, and found there is higher packets error value, you can set the value higher, however, that may decrease the whole performance of MZK-W04N. The default value is **2346**, and you can set a value between **256~2346**.
- **RTS Threshold** : Here you can define the minimum value of RTS (Request to Send) packets and prevent “**Hidden Nodes**” problems. Please enter a value between 0~2347, and when the packets are bigger than the RTS value the function will start to work.
- **Beacon Interval** : Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to start up again and receive the beacon.
- **DTIM Period** : Set the DTIM period of wireless radio. Do not modify default value if you don't know what it is, and the default value is **3**.
- **Data Rate/N Data Rate** : The transmission rate can be: Auto/1/2/5.5/11/6/9/12/ 18/24/36Mbps. When you choose “**Auto**,” MZK-W04N will automatically find the proper transmission rate for you. If you choose higher transmission rate, the distance between the AP and the Wireless NIC must be closer. Besides, when the Wireless NIC is 802.11b type, the maximum transmission rate is 11Mbps. **N Data Rate** setting is the same as above, but it only works for 802.11n clients.
- **Channel Width** : Set channel width of wireless radio. Do not modify default value if you don't know what it is, default setting is “**Auto 20/40 MHz**” .
- **Preamble Type** : A preamble is a signal used in wireless environment to synchronize the transmitting timing including synchronization and

start frame delimiter. It can also define the length of CRC (cyclic redundancy check) blocking. There are two Preambles: Short and Long. When the traffic is heavier, the shorter preamble should be used.

- **Broadcast Essid** : If you choose “**Disabled**,” the ESSID of MZK-W04N will not appear on the other PC's wireless network list. It also means that only whose ESSID is the same with MZK-W04N can connect with MZK-W04N. Therefore, the Wireless Router/AP can block the users without authentication.
- **CTS Protect** : You can choose: **Auto**, **Always** or **None** protection mode. Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It's recommended to set this option to “**Auto**” or “**Always**” . However, if you set to “**None**” , your wireless router should be able to work fine, too.
- **Tx Power** : Please manual choose the transmitting power for MZK-W04N. There are several levels to choose. The system default is **100%** which means MZK-W04N has the maximum Tx Power on wireless network.
- **Turbo Mode** : Click the check box to accelerate the transmission rate of MZK-W04N. The default value is enabled.
- **WMM** : The short of Wi-Fi MultiMedia, it will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is or not sure if you need it, it's safe to set this option to be “**Enable**” , however, default value is “**Disable**” .
- **Not Forwarding** : Enable this function to discard the packets between wireless adapters.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.3.Security Settings

3

In this page, you can configure the security of your wireless network. Selecting different method can make different levels of security. However, no matter what kind of authentication or encryption you use to prevent data packets from being eavesdropped by people without authentication, it may cause decrease of the data throughput of the wireless connection.

Authentication and Encryption

There are 4 kinds of authentication of MZK-W04N wireless Router: **Disabled/Open System**, **WEP**, **WPA pre-shared Key**, and **WPA RADIUS**. After selecting the authentication mode, it has to cooperate with the encryption type. The settings of authentication on the destination network must be the same with MZK-W04N.

- **Disabled/Open System** –If enabling this mode, there is no need authentication to access AP or wireless NIC.
- **Pre-Shared Key** –Only those who are sharing the same key with the AP can connect with it.
- **WEP** –WEP is short for Wired Equivalent Privacy, a security protocol for WLANs defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it transmitted from one end point to another. There are two kinds of WEP encryption: 64 bit and 128 bit. 64 bit needs 10 hex characters to be the key and 128 bit needs 26 hex characters.
- **WPA** – is short for Wi-Fi Protected Access. It was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. Through the data encryption, access control and authentication, it provides better protection over data transmission. WPA uses 128-digit keys to ensure the wireless network privacy and security.

- **WPA2** – is short for Wi-Fi Protected Access 2. It is the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. There are two versions of WPA2: WPA2-Personal, and WPA2- Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.
- **WPA-PSK** – is short for Wi-Fi Protected Access-Pre-Shared Key. WPA-PSK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.
- **TKIP** – is short for **Temporal Key Integrity Protocol**. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- **AES** – is short for **Advanced Encryption Standard**. AES is a symmetric 128-bit block data encryption technique. It has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits.
- **Pass Phrase** – Pass Phrase also named Shared Secret which is used only when enabling WPA-PSK authentication. A passphrase is a string of characters longer than the usual password (which is typically from four to 16 characters long) that is used in creating a digital signature (an encoded signature that proves to someone that it was really you who sent a message) or in an encryption or a decryption of a message. It is applicable only when you select WPA-PSK authentication. You will need to enter an 8~63 characters password to start the encryption process, which will generate four WEP keys automatically.

- **RADIUS** – is short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). RADIUS setup is used to set up additional parameters for authorizing wireless clients through RADIUS server. The RADIUS setup is required when you select to use Open System with 802.1x or WPA authentication.

Encryption	WEP Key 1~4	Passphrase
Open System or Shared Key		
WEP64 (bit)	10 hex characters	Null
WEP128 (bit)	26 hex characters	Null
Open System		
WEP64 (bit)	10 hex characters	Null
WEP128 (bit)	26 hex characters	Null
Open System with 802.1x		
WEP64 (bit)	Null	Null
WEP128 (bit)	Null	Null
Shared Key		
WEP64 (bit)	10 hex characters	Null
WEP128 (bit)	26 hex characters	Null
WPA		
TKIP	Null	Null
AES	Null	Null
WEP64 (bit)	Null	Null
WEP128 (bit)	Null	Null
WPA-PSK		
TKIP	Null	8-63 characters
AES	Null	8-63 characters
WEP64 (bit)	Null	8-63 characters
WEP128 (bit)	Null	8-63 characters

1.3.1.Disabled

If the security settings is disabled, there is no need authentication to access AP or wireless NIC.



The 802.1x authentication is mainly focus on “WPA” and “WPA2” encryption.

- **RADIUS Server IP address** : Please input the IP address of your RADIUS authentication server here.
- **RADIUS Server Port** : Please input the port number of your RADIUS authentication server here. **Default setting is 1812.**
- **RADIUS Server Password** : Please input the password of your RADIUS authentication server here.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.3.2.WEP

WEP is short for Wired Equivalent Privacy, a security protocol for WLANs defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it transmitted from one end point to another. There are two kinds of WEP encryption: 64 bit and 128 bit. 64 bit needs 10 hex characters to be the key and 128 bit needs 26 hex characters.



● **Key Length** : There are four types of WEP key settings, please set the key depending on the real environment. According to the type and length, there are four WEP Key types:

- **Hexadecimal** – Only “A~F,” “a~f,” and “0~9” are allowed to be set in a WEP key.
- **ASCII** – Numerical values, characters or signs are all allowed to be arranged into a WEP key. It is more recognizable for user.
- **64-bit** – Enter 10-digit Hex values or 5-digit ASCII values as the encryption keys. For example: “0123456aef” or “Guest.”
- **128-bit** – Enter 26-digit Hex values or 13-digit ASCII values as the encryption keys. For example: “01234567890123456789abcdef” or “administrator.”

- **Default Tx Key** : Choose a default key from 1 to 4 keys.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.3.3. WPA pre-shared key

WPA-PSK is short for Wi-Fi Protected Access-Pre-Shared Key. WPA-PSK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.

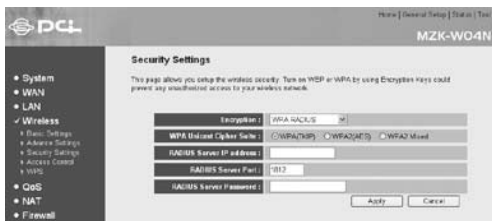


- **WPA Unicast Cipher Suite** : There are three kinds of encryption:
 - **TKIP** – It is short for **Temporal Key Integrity Protocol**. TKIP scrambles the key using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
 - **AES** – Short for **Advanced Encryption Standard**, a symmetric 128-bit block data encryption technique. It works at multiple network layers simultaneously and has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits.
 - **Mixed** – Mixed encryption type.

- **Pre-shared Key Format/Pre-shared Key** : Passphrase also named Shared Secret which is used only when enabling WPA-PSK authentication. A passphrase is a string of characters longer than the usual password (which is typically from four to 16 characters long) that is used in creating a digital signature (an encoded signature that proves to someone that it was really you who sent a message) or in an encryption or a decryption of a message. It is applicable only when you select WPA-PSK authentication. You will need to enter an 8~63 characters password to start the encryption process, which will generate four WEP keys automatically.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.3.4. WPA RADIUS

WPA is short for Wi-Fi Protected Access. It was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. Through the data encryption, access control and authentication, it provides better protection over data transmission. WPA uses 128-digit keys to ensure the wireless network privacy and security.



- **WPA Unicast Cipher Suite** : There are three kinds of encryption:
 - **TKIP** – It is short for **Temporal Key Integrity Protocol**. TKIP scrambles the key using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
 - **AES** – Short for **Advanced Encryption Standard**, a symmetric 128-bit block data encryption technique. It works at multiple network layers simultaneously and has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits.
 - **Mixed** – Mixed encryption type.
- **RADIUS Server IP address** : Please input the IP address of your RADIUS authentication server here.
- **RADIUS Server Port** : Please input the port number of your RADIUS authentication server here. Default setting is 1812.
- **RADIUS Server Password** : Please input the password of your RADIUS authentication server here.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

1.4. Access Control

If you set the wireless access control list, only those whose wireless MAC addresses listed on the Wireless Access Control table **can** connect with MZK-W04N. The default mode is that all the wireless stations are allowed to access MZK-W04N. Up to **20** MAC addresses can be assigned by using this function.



- **Enable Wireless Access Control** : To use MAC address filtering, you have to check “Enable Wireless Access Control” . When this item is unchecked, wireless router will not perform MAC address filtering on wireless clients.
- **MAC address** : Enter the MAC address of your wireless devices here, dash (-) or colon (:) are not required.
- **Comment** : Enter any text to describe the MAC address which you want to allow. It can be 16 alphanumerical characters at most.
- **Add** : Click “Add” button to add the save/apply the settings and then the added MAC address will be listed on the table.
- **Clear** : If you want to delete the MAC address and the comment just entered, you may click this button.

- **Delete Selected/Delete All/Reset** : If you want to remove a single MAC address, you may choose the item and click **“Delete Selected”** ; or if you want to delete all the clients, you can click **“Delete All”** . If you want to cancel the check you just made, you may click **“Reset”** .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click **“Cancel”** to configure the page again.

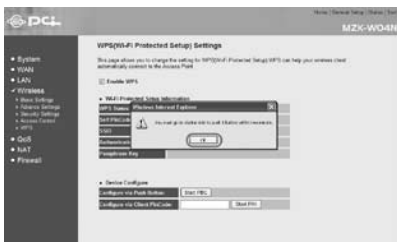
1.5. WPS

Use the unique **WPS (Wi-Fi Protected Setup)** function to cooperate with PCI wireless adapter — **GW-US300MiniW** and you may complete the setup of wireless configuration and encryption within a simple click on a button. However, this function only works on **Windows 2000** and **XP OS**. There are two ways to set up WPS.

I. Start PBC

1. Enter the configuration page of MZK-W04N and click **“LAN→Wireless→WPS”** . Click the **“Start PBC”** button and then there pops up a warning dialog box to tell you that you should go to the station side (GW-US300MiniW) within 2 minutes to click **“PBC”** button.

※ **You can also click the button on the rear panel of MZK-W04N to start PBC connection. However, you should also go to the configuration page of GW-US300MiniW to click “PBC” to make the connection.**



2. Open the utility of GW-US300MiniW. Click the button of **“PBC”** and then GW-US300Mini will automatically start to make a connection with MZK-W04N and use the same wireless settings and encryption configuration with it. If they successfully make a connection, GW-US300MiniW will show a green check before the AP’s SSID.



2.QoS

By configuring the **QoS (Quality of Service)**, you can control the traffic through MZK-W04N, and make good use of the bandwidth. The administrator should configure the bandwidth of the WAN according to the information that ISP provided.

3

PC-L Home | General Setup | Status | (Tab)

MZK-W04N

QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority (including dedicated bandwidth, controlled jitter and latency) required by some real-time and interactive traffic, and engineered user characteristics. Also important is making sure that pending priority for one or more flows does not cause other flows fail.

Enable QoS

Total Download Bandwidth: 0 kbits

Total Upload Bandwidth: 0 kbits

Current QoS Table

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
----------	-----------	------------------	--------------------	--------

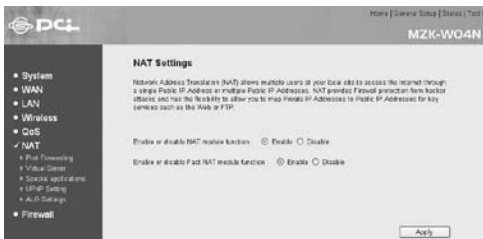
Buttons: Add, Edit, Save Selector, Cancel All, Move Up, Move Down, Reset, Apply, Cancel

- **Enable QoS** : Check the check box to enable the QoS function. Enable this function can limit the maximum bandwidth, or give the specific user guaranteed bandwidth.
- **Total Download Bandwidth** : You can set the limit of total download bandwidth in kbits. To disable download bandwidth limitation, input '0' here.
- **Total Upload Bandwidth** : You can set the limit of total upload bandwidth in kbits. To disable download bandwidth limitation, input '0' here.
- **Current QoS Table** : All the added QoS rules will be listed here.
- **Add** : Click this button to add a new QoS rule.
- **Edit** : If you want to modify the content of a specific rule, please check the "select" box of the rule you want to edit, then click 'Edit' button. Only one rule should be selected a time! If you didn't select a rule before clicking 'Edit' button, you'll be prompted to add a new rule.

- **Delete Selected/Delete All/Reset** : If you want to remove a single QoS rule, you may choose the item and click **“Delete Selected”** ; or if you want to delete all the clients, you can click **“Delete All”** . If you want to cancel the check you just made, you may click **“Reset”** .
- **Move Up/Move Down** : Select the QoS rule which you want to move. If you want to make the rule prior, just click **“Move Up”** ; if you want to make the rule posterior, just click **“Move Down”** .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click **“Cancel”** to configure the page again.

3.NAT

NAT, Network Address Translation, can let a single IP address be shared with multiple computers. Without NAT, all computers must be assigned with a valid Internet IP address to get connected to Internet, but Internet service providers only provide very few IP addresses to each user. Therefore it's necessary to use NAT technology to share a single Internet IP address to multiple computers on local network, so everyone can get connected to Internet. Click **“Enable”** to start using this nice function. The default setting is **“Enable”** .



3.1. Port Forwarding

This function allows you to redirect a single port or consecutive ports of Internet IP address to the same port of the IP address on local network. The port number(s) of Internet IP address and private IP address (the IP address on local network) must be the same. If the port number of Internet IP address and private IP address are different, please use “**Virtual Server**” function.

Port Forwarding

Enable Port Forwarding

Private IP	Type	Port Range	Comment
<input type="text"/>	Both	<input type="text"/>	<input type="text"/>

Add Reset

Current Port Forwarding Table

ID	Private IP	Type	Port Range	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Uncheck Selected Uncheck All Reset

Apply Cancel

- **Enable Port Forwarding** : Check this box to enable port mapping, or uncheck this box to disable port mapping.
- **Private IP** : Enter the IP address of the computer on local network which provides internet service.
- **Type** : Select the type of connection, TCP or UDP. If you're not sure, please select “**Both**” .
- **Port Range** : Enter the starting port number in the left field, and input the ending port number in the right field. If you only want to redirect a single port number, just fill the port number in the left field.
- **Comment** : Enter any text to describe the port forwarding. It can be 16 alphanumerical characters at most.
- **Add** : Click “**Add**” button to add the mapping to port forwarding table.
- **Reset** : Delete the just entered but not added value.

- **Current Port Forwarding Table** : All the entered port forwarding rule will be listed here.
- **Delete Selected/Delete All/Reset** : If you want to remove a single port forwarding, you may choose the item and click “**Delete Selected**” ; or if you want to delete all the clients, you can click “**Delete All**” . If you want to cancel the check you just made, you may click “**Reset**” .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

3.2. Virtual Server

MZK-W04N can enable Virtual Server function, and remote hosts can use public IP address to connect with the Internet and FTP and then enter the LAN, but all the PCs on the LAN will not be seen from the outside. Virtual Server function can let users set a local server with specific port number which stands for the specific port, such as Web (80), FTP (21), and Telnet (23). When MZK-W04N receives an incoming access request to the specific port, it will forward the request to the corresponding internal server which means the external request for accessing a specific port will be reassigned to a different port.



To enable Server Port is like to open the firewall, which exposes your LAN to users on the Internet. It is to say that the NAT function of MZK-W04N will not be able to provide protection and prevent hackers.



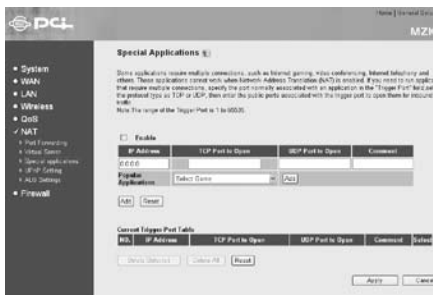
- **Enable Virtual Server** : Check this box to enable virtual server, or uncheck this box to disable virtual server.
- **Private IP** : Please enter the IP address of the server on the LAN side which provides virtual server service.
- **Private Port** : Enter the port number that you want to set for virtual server port which might be different from the external port number. It can be a single port number or a range of ports. When receiving an incoming packet corresponding with the specific port number, the packet will be transferred to the appointed port.
- **Type** : Select the type of connection, TCP or UDP. If you're not sure, please select **"Both"** .
- **Public Port** : Enter the port number used for Internet application, for example, port 20 which is usually used for FTP, and port 80 for WWW, and so on. If applications require multiple ports, you should assign a range of port for it.
- **Comment** : Enter any text to describe this virtual server. It can be 16 alphanumerical characters at most.
- **Add** : Click **"Add"** button to add the virtual server rule to the Current Virtual Server Table.
- **Reset** : Delete the just entered but not added value.

- **Current Virtual Server Table** : All the entered triggering port will be listed here.
- **Delete Selected/Delete All/Reset** : If you want to remove a single virtual server, you may choose the item and click “**Delete Selected**” ; or if you want to delete all the clients, you can click “**Delete All**” . If you want to cancel the check you just made, you may click “**Reset**” .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

3.3.Special Applications

If the Internet applications do not use standard connections or port numbers, it might be unable to work because the connections of the applications could probably be blocked by the firewall of MZK-W04N Wireless Router. In this case, you can define these kinds of Internet applications as “**Special Applications**” to make them work properly.

You can define the special applications by your own, but you need detailed information about the applications such as port number, which normally can be available from the application providers. Moreover, you have to check “**Enable**” before add or edit an application.



- **Enable** : Check this box to enable virtual server or uncheck this box to disable virtual server.
- **IP Address** : Enter the IP address of the computer which provides Internet service.
- **TCP Port to Open/UDP Port to Open** : Enter a port or a range of port to be the incoming port. Once the trigger port is detected, the incoming packets are allowed to pass the firewall to the specified incoming ports.
- **Comment** : Enter any text to describe this special application. It can be 16 alphanumerical characters at most.

- **Popular Applications** : Scroll down the list to choose a popular application which can be either TCP or UDP type.
- **Add** : Click “**Add**” button to add the special application rule to the Current Trigger-Port Table.
- **Reset** : Delete the just entered but not added value.
- **Current Trigger-Port Table** : All the entered triggering port will be listed here.
- **Delete Selected/Delete All/Reset** : If you want to remove a single special application rule, you may choose the item and click “**Delete Selected**” ; or if you want to delete all the clients, you can click “**Delete All**” . If you want to cancel the check you just made, you may click “**Reset**” .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

3.4. UPnP Setting

If your Windows Operating System supports UPnP service, when you enable the UPnP service and the MZK-W04N Wireless Router is connecting with the computer, the task bar will show the icon of MZK-W04N to inform you that a new device is found and inquire you whether if you want to set a shortcut on the desktop.



- **Enable/Disable** : If your operating system supports this function, you may enable it.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

3.5.ALG Settings

The Application Layer is like a rule to access the Internet. It can let local programs communicate with the remote programs, and sending information to each other in the open environment.

To use the Application Layer Gateway, the appropriate Application Layer Gateway definition must be selected in the service configuration item. (You can refer to the Special Application settings by click the link under the page) Network traffic that matches the service definition (service must be enabled as well) will be managed by the selected Application Layer Gateway.



- **Enable** : Click the check boxes which you want to apply with the Special Applications. Enable the ALG can let specific two-way applications be used in the open environment.
- **Name/Comment** : There are many applications listed here. Please check the check box of the special support for applications you need, and then click “**Apply**” button.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

4.Firewall

Firewall is an advanced function which can be used to allow or deny TCP/IP data packets passing through MZK-W04N Wireless Router. It works like an IP filter, but has some additional settings; therefore, you can create more detailed regulations of accessing to MZk-W04N.

3



- **Enable or disable Firewall module function** : Please select “**Enable**” or “**Disable**” to enable or disable firewall function of this router, the click “**Apply**” button. The following page will show you that settings have been saved. Please click “**Continue**” to back to previous setup menu and continue on other setup procedures; or click “**Apply**” to reboot the router so the settings will take effect (Please wait for about 50 seconds while router is rebooting).

4.1. Access Control

This function allows or denies computers with specific MAC address from connecting to the network; it can also allow or deny computers with specific IP address, protocol, or port.



- **Enable MAC Filtering** : Check this box to enable MAC address filtering, and please select “Deny” or “Allow” to decide the behavior of MAC filtering table. If you select deny, all MAC addresses listed in filtering table will be denied from connecting to the network; if you select allow, only MAC addresses listed in filtering table will be able to connect to the network, and rejecting all the other network devices.
- **Client PC MAC address** : Please enter the MAC address of computer or network device here, dash (-) or colon (:) are not required.
- **Comment** : You can enter any text here as the comment of this MAC address. You can enter up to 16 alphanumeric characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.
- **Add** : Click “Add” button to add the MAC address which needs to be filtered to the MAC filtering table.

- **Reset** : Delete the just entered but not added value.
- **MAC Filtering Table** : All the entered MAC address will be listed here.
- **Delete Selected/Delete All/Reset** : If you want to remove a single filtering rule, you may choose the item and click “**Delete Selected**” ; or if you want to delete all the clients, you can click “**Delete All**” . If you want to cancel the check you just made, you may click “**Reset**” .
- **Enable IP Filtering Table** : Check this box to enable IP address filtering, and please select “**Deny**” or “**Allow**” to decide the behavior of IP filtering table. If you select deny, all IP addresses listed in filtering table will be denied from connecting to the network; if you select allow, only IP addresses listed in filtering table will be able to connect to the network, and rejecting all the other network devices.
- **IP Filtering Table** : All the entered IP address will be listed here.
- **Delete Selected/Delete All/Reset** : If you want to remove a single filtering rule, you may choose the item and click “**Delete Selected**” ; or if you want to delete all the clients, you can click “**Delete All**” . If you want to cancel the check you just made, you may click “**Reset**” .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

4.2.URL Blocking

Use URL Filter to prevent PCs from accessing websites including the following URL strings. Users can enter some key words such as adult, hacker or other related words to prevent PCs on the LAN from connecting with these websites.



- **Enable URL Blocking** : Check the check box to start using URL Blocking; uncheck it to disable URL Blocking.
- **URL/Keyword** : Enter the strings/key words which you want to filter. Click “Add” and then the website related to these strings will be blocked and cannot be connected with.
- **Add** : Click “Add” button to add the URL/keyword to the URL/Keyword filtering table.
- **Reset** : Delete the just entered but not added value.
- **Delete Selected/Delete All/Reset** : If you want to remove a single blocking rule, you may choose the item and click “Delete Selected” ; or if you want to delete all the clients, you can click “Delete All” . If you want to cancel the check you just made, you may click “Reset” .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “Cancel” to configure the page again.

4.3.DoS

A **DoS (Denial of Service)** attack does not attempt to steal data or damage your PCs, but overloads your Internet connections and paralyzes the service. If Anti-DoS function is enabled, DoS attack will be detected and blocked. The default status is disabled. It is recommended that you should use the function to block all the possible DoS attacks.

You can click the check box to enable the Anti-DoS and choose the items which you need to use. Too many Anti-DoS functions are enabled can also affect the efficiency of the Internet connection via MZK-W04N. We suggest you to set the appropriate amount of Anti-DoS functions according to your real needs as to meet the balance between the efficiency and the security.



- **Ping of Death** : Ping of Death is a special packet, and it will cause certain computer to stop responding. Check this box and the router will filter this kind of packet out.

- **Discard Ping From WAN** : Ping is a common and useful tool to know the connection status of a specified remote network device, but some malicious intruder will try to fill your network bandwidth with a lot of PING request data packet, to make your internet connection become very slow, even unusable. Check this box and the router will ignore all inbound PING request, but when you activate this function, you will not be able to ping your own router from internet, too.
- **Port Scan** : Some malicious intruder will try to use a “**port scanner**” to know how many ports of your Internet IP address are open, and they can collect a lot of valuable information by doing so. Check this box and the router will block all traffics which are trying to scan your Internet IP address.
- **Sync Flood** : This is another kind of attack, which uses a lot of fake connection request to consume the memory of your server, and try to make your server become unusable. Check this box and the router will filter this kind of traffic out.
- **Advanced Settings** : Click this button and you can set advanced settings of the DoS prevention method listed above.
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click “**Cancel**” to configure the page again.

4.4.DMZ

If your computer cannot use Internet applications or cannot provide services to remote users when applying MZK-W04N at the same time, you can let the host which wants to access to the Internet using DMZ function. Enter the host's LAN IP address to enable this function, but be aware that one MZK-W04N can only correspond to a single DMZ host.

3



- **Enable DMZ** : Check this box to enable DMZ function, uncheck this box to disable DMZ function.
- **Public IP** : Select “**Dynamic IP**” or “**Static IP**” . If you select “**Dynamic IP**” , you have to select an Internet connection session from dropdown menu; if you select “**Static IP**” , please input the IP address that you want to map to a specific private IP address.
- **Client PC IP address** : Please enter the private IP address that the Internet IP address will be mapped to.
- **Add** : Click “**Add**” button to add the public IP address and associated private IP address to the DMZ table.
- **Reset** : Click to delete the values you just entered but not added yet.
- **Current DMZ Table** : All existing public IP addresses and mapped private IP addresses will be displayed here.

- **Delete Selected/Delete All/Reset** : If you want to remove a single DMZ entry, you may choose the item and click **“Delete Selected”** ; or if you want to delete all the clients, you can click **“Delete All”** . If you want to cancel the check you just made, you may click **“Reset”** .
- **Apply** : Click this button to save the settings and restart the router.
- **Cancel** : If there is anything wrong with the settings you made, you can click **“Cancel”** to configure the page again.



Adding a client host to DMZ might expose it to a variety of danger such as virus or worm attacks because of unrestricted Internet access; therefore, only use this option as the last means. Besides, before using DMZ function, you should update the up-to-date settings of security system and virus signatures on the host.

5. Status

After entering the configuration homepage of MZK-W04N, please click **“Status”** on the right upper corner of the page. This page shows the general current system status.

3

The screenshot shows the 'Status and Information' page of the MZK-W04N device. The left sidebar contains a 'Status' menu with options: Internet Connection, Device Status, System Log, Security Log, Active DHCP Client, and Statistics. The main content area is titled 'Status and Information' and includes a description: 'You can use the Status page to monitor the connection status for the broadband router, WLAN/LAN interfaces, firmware and hardware version numbers, set legal strength to access your network, and information on all DHCP client PCs currently connected to your network.' Below this is a 'System' table:

System	Mode	Wireless Router
Up time	04h 01m 54s	
Hardware Version	Rev. A	
Boot Code Version	1.0	
Runtime Code Version	1.03	

5.1. Internet Connection

Click the link of **“Internet Connection”** on the left side of the page to check the current Internet connection status of MZK-W04N.

The screenshot shows the 'Internet Connection' page of the MZK-W04N device. The left sidebar contains a 'Status' menu with options: Internet Connection, Device Status, System Log, Security Log, Active DHCP Client, and Statistics. The main content area is titled 'Internet Connection' and includes a description: 'View the current internet connection status and related information.' Below this is a table showing connection details:

Active IP Protocol	Fixed IP connect
IP Address	218.64.186.2
Subnet Mask	255.255.255.248
Default Gateway	218.64.188.14
MAC Address	00:0E:2C:44:60:F2
Primary DNS	148.96.1.1
Secondary DNS	0.0.0.0

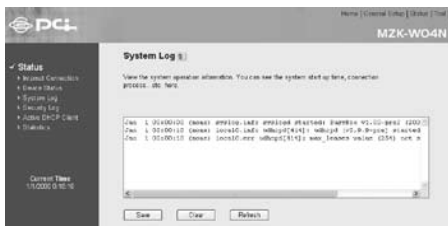
5.2. Device Status

Click the link of “**Device Status**” on the left side of the page, it will show you the current settings of WLAN and LAN.



5.3. System Log

System Log records every events happened on the MZK-W04N Wireless Router. These data are useful for troubleshooting, but enabling all logs will generate a large amount of data and affect the performance.



- **Save** : Save current event log to a text file.
- **Clear** : Delete all event logs displayed here.
- **Refresh** : Refresh the event log to get the latest status.

5.4. Security Log

All the information about network and system security is kept here, and you can use this function to check the security event log of your router.

3



- **Save** : Save current event log to a text file.
- **Clear** : Delete all event logs displayed here.
- **Refresh** : Refresh the event log to get the latest status.

5.5. Active DHCP Client

If you're using the DHCP server function of MZK-W04N, you can use this function to check all the active DHCP leases issued by this router.

Please click “**Active DHCP client**” link on the left of web management interface, and the following message will be displayed on your web browser.



- **Refresh** : All information about active DHCP leases issued by this router will be displayed here. You can click “**Refresh**” button to display latest information.

5.6. Statistics

You may click this page to check the packet counters for data transmission status of WLAN, LAN, and WAN.

The screenshot shows the 'Statistics' page in the PC4 management interface. The page title is 'Statistics' and the device ID is 'MZK-W04N'. A 'Refresh' button is located above a table of statistics. The table lists statistics for Wireless LAN, Ethernet LAN, and Ethernet WAN, including Sent and Received Packets.

Network Type	Stat Type	Value
Wireless LAN	Sent Packets	547
	Received Packets	14,091
Ethernet LAN	Sent Packets	204
	Received Packets	1,112
Ethernet WAN	Sent Packets	141
	Received Packets	2,406

- **Refresh** : Click this button to refresh the statistics of the packet counters.

6. Tool

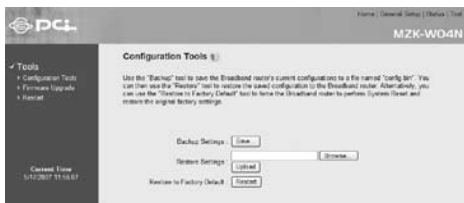
After entering the configuration homepage, click “**Tool**” link on the upper right of the page to use the backup, restore, and upgrade functions.

The screenshot shows the 'Tools Setting' page in the PC4 management interface. The page title is 'Tools Setting' and the device ID is 'MZK-W04N'. The page contains a description of the Tools Settings area, which includes basic configuration tools like Save, Restore, Configuration Settings, and Upgrade System Firmware.

6.1. Configuration Tool

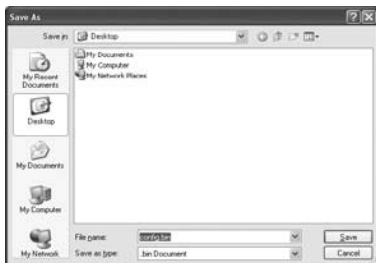
Before upgrading, you can use this function to save current system settings or upload the previous settings after upgrading the firmware.

3



→ Backup Settings

You may click “Save” button to save current system settings to your local disk. (The format will be “*.bin” file)



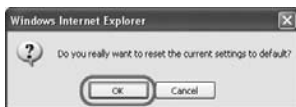
→Restore Settings

Make sure the saved system setting file is in the local host disk and then click **“Browse”** to search for the saved system setting file. Click **“Open”** to select the system setting file that you want and then click **“Upload”** to start restore the settings. After restoring the settings, please click **“OK”** to go back to the homepage.



→Restart

Click **“Restart”** and then click **“OK”** on the pop-up dialog box, the system will restart to the factory default value afterward. After successfully restoring to default, please click **“OK”** to go back to the homepage.



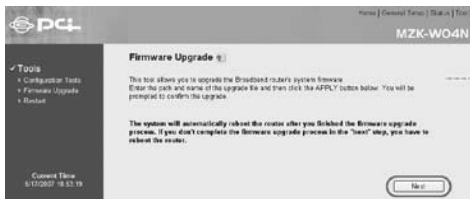
6.2. Firmware Upgrade

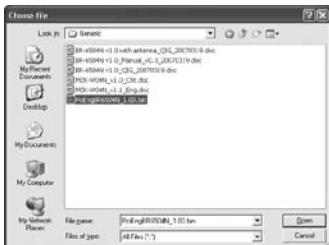
You can upgrade the firmware of MZK-W04N via Web Browser.

First, please go to the website: <http://www.planex.com.tw/download/index.htm> to download the latest firmware of MZK-W04N. Be sure that the firmware is stored in your PC's disk and then click **“Browse”** to search for the firmware file which you just downloaded. Click **“Open”** to use the firmware and click **“Apply.”** After the dialog box pops up and ask you if you want to continue upgrading the firmware, you can click **“OK”** to start upgrading immediately. Upgrading firmware will not change any settings, but it is recommended that you should save the settings before upgrading the firmware.



It takes about 2~3 minutes to upgrade the firmware. When upgrading, please do not turn off the power of MZK-W04N. After finishing upgrading, MZK-W04N will restart automatically.





6.3.Restart

3

Go to the “**Restart**” configuration page, and then click “**Apply**” to restart the system.

