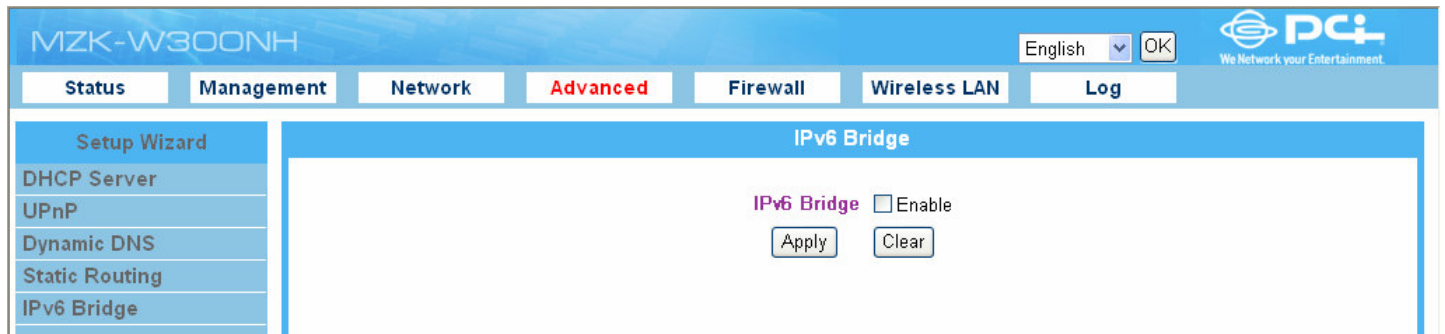


1.5. IPv6 Bridge

MZK-W300NH supports IPv6 Bridge function, which can connect between LAN and WAN in Data. In using this function, you can connect to computers in your network thru PPPoE connection



- **Enable** : Click the check box to enable IPv6 Bridge function.
- **Apply** : Click this button to save the settings.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" to configure the page again.

2. Firewall

MZK-W300NH has three kinds of firewall functions which are Local Server, DMZ, and IP Filtering.

2.1. Local Server

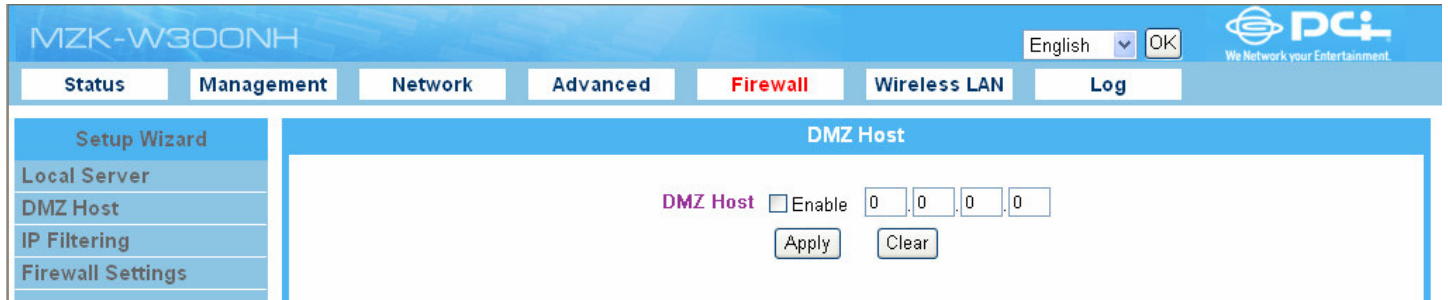
Local Server configuration is used to i) make a server on LAN publicly accessible via the Internet and ii) access applications including online games and chat programs. Some services and applications used on the Internet have been already registered in the product to simplify Local Server configuration. You may set **32** sets of servers.

No.	Protocol	WAN Port Range	Server IP	Server Port Range	Enable
1	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
2	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
3	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
4	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
5	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
6	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
7	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
8	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
9	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
10	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
11	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
12	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>
13	TCP	0 - 0	0 . 0 . 0 . 0	0 - 0	<input type="checkbox"/>

- **Protocol** : Select to use "TCP" or "UDP" protocol.
- **WAN Port Range** : Enter the source port number for the service or application.
- **Server IP** : Enter the IP address of the PC that serves as local server.
- **Server Port Range** : Enter the destination port number for the service or application.
- **Enable** : Put a check in the check box to enable each server.
- **Apply** : Click this button to save the settings.
- **Clear** : If there is anything wrong with the settings you made, you can click "Clear" to configure the page again.

2.2. DMZ

If your computer cannot use Internet applications or cannot provide services to remote users when applying MZK-W300NH 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-W300NH can only correspond to a single DMZ host.



- **Enable DMZ** : Check this box to enable DMZ function, uncheck this box to disable DMZ function.
- **Client PC IP address** : Please enter the private IP address that the Internet IP address will be mapped to.
- **Apply** : Click this button to save the settings.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" 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.

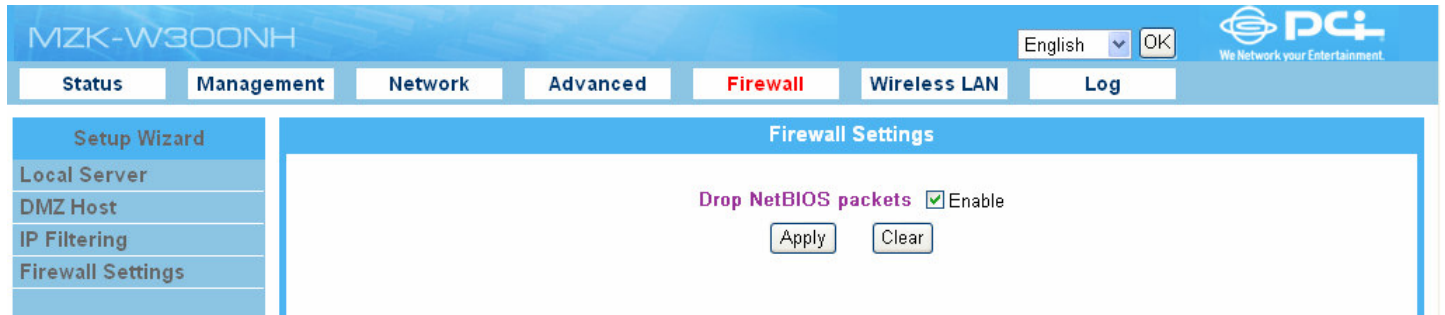
2.3. IP Filtering

The built-in IP filter of MZK-W300NH applies pre-configured filter rules to packets received as well as packets transmitted by the product. Filter rules include IP filtering and Port filtering. You may set **32** sets of filter rules.

No.	Action	Protocol	Source IP/Netmask	Source PORT	Destination IP/Netmask
1	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
2	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
3	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
4	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
5	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
6	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
7	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
8	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
9	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
10	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
11	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0
12	Drop	TCP	0.0.0.0 / 0.0.0.0	0 - 0	0.0.0.0 / 0.0.0.0

- **Action** : "Drop" means drop the packets to filter. "Accept" means accept all packets related to this session.
- **Protocol** : Choose to filter "TCP" or "UDP" protocol.
- **Source IP/Netmask** : Enter the Source IP address which you want to filter and it's Netmask.
- **Source PORT** : Specify the Source PORT which you want to filter.
- **Destination IP/Netmask** : Enter the Destination IP address which you want to filter and it's Netmask
- **Source PORT** : Specify the Destination PORT which you want to filter.
- **Apply** : Click this button to save the settings.
- **Clear** : If there is anything wrong with the settings you made, you can click "Clear" to configure the page again.

2.4. Firewall Settings

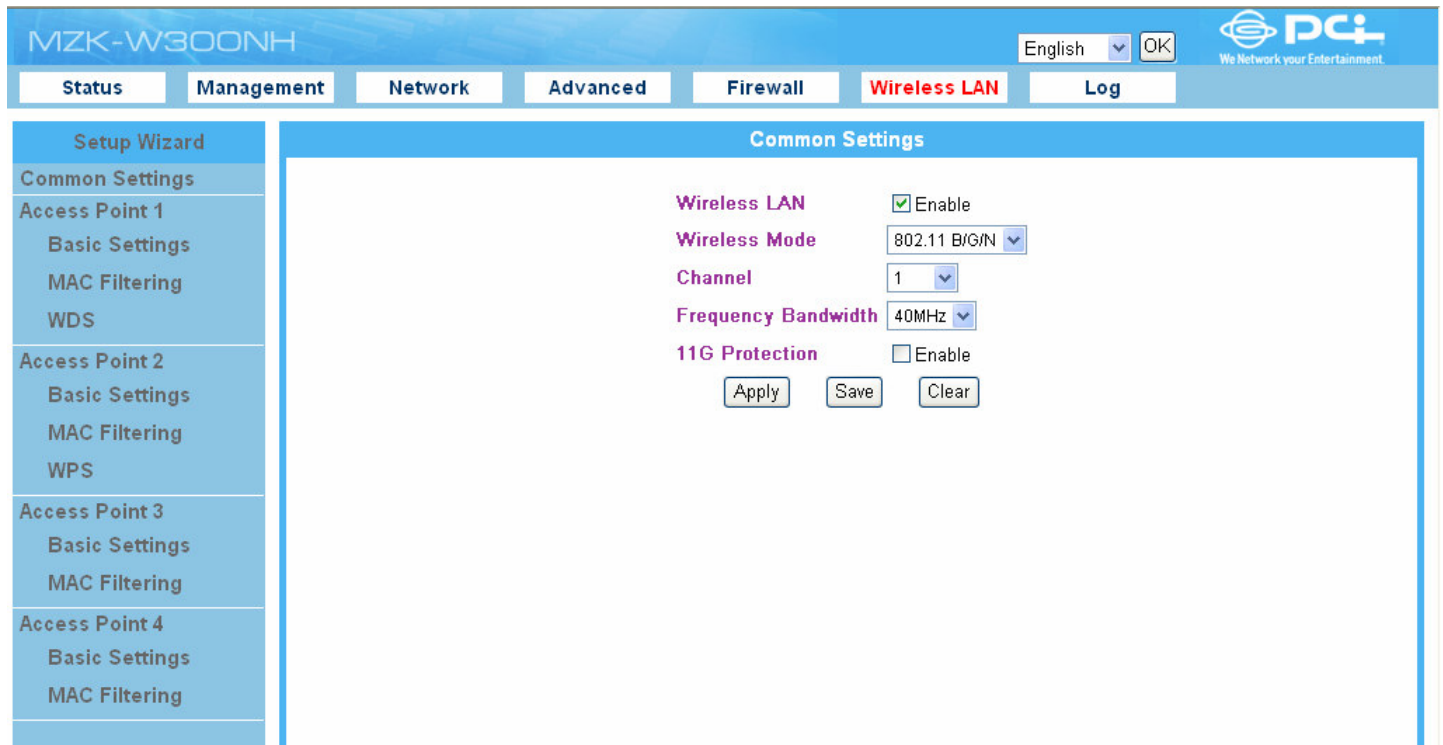


The screenshot displays the web interface for the MZK-W300NH device. At the top, the model number 'MZK-W300NH' is visible on the left, and a language dropdown menu set to 'English' with an 'OK' button is on the right. Below this is a navigation bar with tabs for 'Status', 'Management', 'Network', 'Advanced', 'Firewall' (highlighted in red), 'Wireless LAN', and 'Log'. On the left side, there is a sidebar menu with options: 'Setup Wizard', 'Local Server', 'DMZ Host', 'IP Filtering', and 'Firewall Settings' (highlighted). The main content area is titled 'Firewall Settings' and contains a single configuration option: 'Drop NetBIOS packets' with a checked checkbox and the text 'Enable'. Below this option are two buttons: 'Apply' and 'Clear'.

- **Enable** : Click the check box to enable Drop NetBIOS packets function.
- **Apply** : Click this button to save the settings.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" to configure the page again.

3. Wireless LAN

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.



MZK-W300NH can simulate four different Access Points (APs), so you can have four different APs with different settings. You can configure these four access points by clicking the “**Wireless LAN**” tag on the upper part of the webpage.

Access Point 1 supports WDS (Wireless Distribution System), and Access Point 2 supports WPS (Wi-Fi Protected Setup), while Access Point 3 and Access Point 4 only support MAC Filtering function.

Please configure your wireless LAN by the following steps.

3.1. Common Settings

The screenshot shows a configuration window titled "Common Settings" with a blue header. It contains five settings:

- Wireless LAN**: A checkbox labeled "Enable" which is checked.
- Wireless Mode**: A dropdown menu showing "802.11 B/G/N".
- Channel**: A dropdown menu showing "1".
- Frequency Bandwidth**: A dropdown menu showing "40MHz".
- 11G Protection**: A checkbox labeled "Enable" which is unchecked.

At the bottom of the settings are three buttons: "Apply", "Save", and "Clear".

- **Wireless LAN** : Click the check box to enable the Wireless function. The default value is "Enabled". After modifying the settings, please click "Apply" to save the settings and restart the system.
- **Wireless Mode** : Scroll down the list to choose a band width. There are six kinds of modes: **B/G/N, G/N, B/G, B, G, and N.**
- **Channel** : 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.
- **Frequency Bandwidth** : Choose a kind of frequency bandwidth: **20MHz or 20/40MHz.**
- **11G Protection** : Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points.
- **Apply** : Click this button to save the settings.
- **Save** : Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you made, you can click "Clear" to configure the page again.

3.2. Basic Settings

Basic Settings pages for Access Point 1~4 are slightly different. Here we use Access Point 1's **Basic Settings** page as demonstrating example.

Basic Settings

SSID	<input type="text" value="planexuser"/> <input checked="" type="checkbox"/> Enable
Hide SSID	<input type="checkbox"/> Enable
LAN Blocking	<input type="checkbox"/> Enable
Internet Blocking	<input type="checkbox"/> Enable
SSID Blocking	<input type="checkbox"/> Enable
Wireless Separating	<input type="checkbox"/> Enable
Authentication	<input type="text" value="Shared key"/>
Encryption	<input type="text" value="WEP(64 Bit)"/>
Pass Phrase	<input type="text"/> <small>*8-63 ascii characters or 64 digits Hexadecimal</small>
Default Key	<input type="text" value="KEY 1"/>
WEP Key 1	<input type="text" value="1223334444"/>
WEP Key 2	<input type="text"/>
WEP Key 3	<input type="text"/>
WEP Key 4	<input type="text"/>
RADIUS Server IP	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
RADIUS Port	<input type="text" value="1812"/>
RADIUS Pass Phrase	<input type="text"/>

- **SSID** : Every SSID is unique in the WLAN (SSID can be 16-digit ASCII characters and case-sensitive). SSID can prevent two nearby WLAN from combining to be one. You can give BLW-54MF an SSID, and only whose SSID is the same with it can connect with it. The default SSID is "planexuser". **Notice: When entering your SSID, please don't use special characters such as "@", "#", "\$", "%", "^", "&", "*", "(", and ")". Using special characters or symbols could cause wireless connection difficulties.** You can click "Enable" check box to enable the Access Point.
- **Hide SSID** : If you check the check box of "Hide SSID," SSID of MZK-W300NH will not appear on the other PC's wireless network list. Therefore, the Wireless Router/AP can block the users without authentication.

- **LAN Blocking:** Click the check box to enable LAN Blocking function.
- **Internet Blocking:** Click the check box to enable Internet Blocking function.
- **SSID Blocking:** Click the check box to enable SSID Blocking function.
- **Wireless Separating** : Enable this function to discard the packets between wireless adapters.
- **Authentication:** Please refer to **3.3 Security** below and setup your wireless LAN securities.
- **Apply** : Click this button to save the settings.
- **Save:** Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" to configure the page again.

3.3. Security

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 10 kinds of authentication of MZK-W300NH wireless Router. 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-W300NH.

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

Authentication	<input type="text" value="Shared key"/>
Encryption	<input type="text" value="WEP(64 Bit)"/>
Pass Phrase	<input type="text"/>
	*8-63 ascii characters or 64 digits Hexadecimal
Default Key	<input type="text" value="KEY 1"/>
WEP Key 1	<input type="text" value="1223334444"/>
WEP Key 2	<input type="text"/>
WEP Key 3	<input type="text"/>
WEP Key 4	<input type="text"/>
RADIUS Server IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
RADIUS Port	<input type="text" value="1812"/>
RADIUS Pass Phrase	<input type="text"/>
	<input type="button" value="Apply"/> <input type="button" value="Save"/> <input type="button" value="Clear"/>

- **Authentication** : There are 10 kinds of authentication types : **Open System or Shared Key, Open System, Open System with 802.1x, Shared Key, WPA, WPAPSK, WPA2, WPA2PSK, WPAWPA2, WPAPSK/WPA2PSK.**
- **Encryption** : There are four types of encryption settings, please set the key depending on the real environment. According to the type and length, there are four Key types:
 - **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."
 - **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.
- **Pass Phrase** : It's 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.
- **Default Key** : You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys. Only the key you select

it in the "**Default key**" will take effect.

- **WEP Key 1~4** : The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.
- **RADIUS Server IP** : Please input the IP address of your RADIUS authentication server here.
- **RADIUS Port** : Please input the port number of your RADIUS authentication server here. **Default setting is 1812.**
- **RADIUS Pass Phrase** : Please input the password of your RADIUS authentication server here.
- **Apply** : Click this button to save the settings and restart the router.
- **Save**: Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" to configure the page again.

3.4. MAC Filtering

If you set MAC Filtering, only those whose wireless MAC addresses listed on the Device List **can** or **cannot** connect with MZK-W300NH. The default mode is that all the wireless stations are allowed to access MZK-W300NH. Up to **20** MAC addresses can be assigned by using this function.

MAC Filtering

MAC Filtering

Action

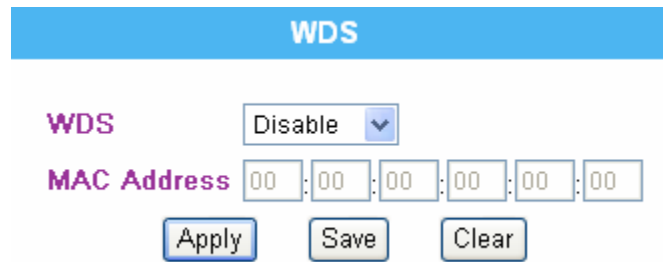
Device List

No.	Comment	MAC Address
1	<input type="text"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

- **Action** : Choose an action from the list. The default value is **Disable**.
 - **Disable** – Choose this function to disable MAC filtering function. This means all the users may connect with MZK-04G without limitation.
 - **Allow** – Choose this function to let users only whose MAC addresses were added to the Device List can connect with MZK-04G and eliminate other users.
 - **Deny** – Choose this function to deny those users whose MAC addresses were added to the Device List cannot connect with MZK-04G, while other users can connect with it.
- **Apply** : Click this button to save the settings and restart the router.
- **Save**: Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you made, you can click "**Clear**" to configure the page again.
- **Comment** : Enter any text to describe the MAC address which you want to allow or deny. It can be 16 alphanumerical characters at most.
- **MAC address** : Enter the MAC address of your wireless devices here.
- **Apply** : Click "**Apply**" button to add the save/apply the settings and then the added MAC address will be listed on the table.
- **Save**: Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you just entered, you can click "**Clear**" to configure the column again.

3.5. WDS

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.



WDS

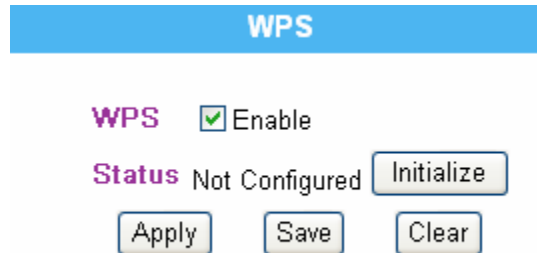
WDS

MAC Address

- **WDS: Mode** : There are three kinds of wireless modes to choose from. Please select the wireless mode according to the real environment.
 - **AP Mode** : Standard wireless AP (access point).
 - **Bridge (WDS)** : Connect MZK-W300NH with another wireless router, to expand the range of the network.
 - **Repeater (WDS)** : Connect MZK-W300NH with up to four other wireless routers, to expand the scope of network.
- **MAC address** : Enter the MAC address of the wireless AP here.
- **Apply** : Click "**Apply**" button to add the save/apply the settings and then the added MAC address will be listed on the table.
- **Save**: Click this button to save the settings you made and return to the current page.
- **Clear** : If there is anything wrong with the settings you just entered, you can click "**Clear**" to configure the column again.

3.6. WPS

Use the unique **WPS (Wi-Fi Protected Setup)** function to cooperate with other wireless network devices 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.



WPS

WPS Enable

Status Not Configured Initialize

Apply Save Clear

- **WPS:** Click this check box to enable the WPS function.
- **Status:** WPS connection status will be shown in this field. You can click "**Initialize**" button to start WPS connection. You have 2 minutes to go to the wireless device you would like to connect. Also, you could press the button on the side panel of MZK-W300NH.
- **Apply :** Click "**Apply**" button to add the save/apply the settings and then the added MAC address will be listed on the table.
- **Save:** Click this button to save the settings you made and return to the current page.
- **Clear :** If there is anything wrong with the settings you just entered, you can click "**Clear**" to configure the column again.

4. Log

After entering the **Log** page of MZK-W300NH, this page shows the general current system log.

4.1. System Log

System Log records every events happened on the MZK-W300NH Wireless Router. These data are useful for troubleshooting.

MZK-W300NH English OK PCI We Network your Entertainment

Status Management Network Advanced Firewall Wireless LAN Log

Setup Wizard System Log

System Log

```
Jan 1 09:00:14 router user.warn kernel: AR7100 GPIOC major 0
Jan 1 09:00:14 router user.info kernel: JFFS2 version 2.2. (C) 2001-2003 Red Hat, Inc.
Jan 1 09:00:14 router user.info kernel: Initializing Cryptographic API
Jan 1 09:00:14 router user.info kernel: io scheduler noop registered
Jan 1 09:00:14 router user.info kernel: io scheduler deadline registered
Jan 1 09:00:14 router user.info kernel: Serial: 8250/16550 driver $Revision: #1 $ 1 ports, IRQ sharing disabled
Jan 1 09:00:14 router user.info kernel: serial8250.0: ttyS0 at MMIO 0x0 (irq = 19) is a 16550A
Jan 1 09:00:14 router user.info kernel: PPP generic driver version 2.4.2
Jan 1 09:00:14 router user.info kernel: PPP Deflate Compression module registered
Jan 1 09:00:14 router user.info kernel: PPP BSD Compression module registered
Jan 1 09:00:14 router user.info kernel: NET: Registered protocol family 24
Jan 1 09:00:14 router user.notice kernel: Creating 6 MTD partitions on 'ar7100-nor0':
Jan 1 09:00:14 router user.notice kernel: 0x00000000-0x00040000 : 'u-boot'
Jan 1 09:00:14 router user.notice kernel: 0x00040000-0x00050000 : 'u-boot-env'
Jan 1 09:00:14 router user.notice kernel: 0x00050000-0x001b0000 : 'uImage'
Jan 1 09:00:14 router user.notice kernel: 0x001b0000-0x007c0000 : 'rootfs'
Jan 1 09:00:14 router user.notice kernel: 0x007c0000-0x007e0000 : 'config'
Jan 1 09:00:14 router user.notice kernel: 0x007e0000-0x00800000 : 'ART'
Jan 1 09:00:14 router user.warn kernel: Netfilter messages via NETLINK v0.30.
Jan 1 09:00:14 router user.info kernel: NET: Registered protocol family 2
Jan 1 09:00:14 router user.warn kernel: IP route cache hash table entries: 512 (order: -1, 2048 bytes)
Jan 1 09:00:14 router user.warn kernel: TCP established hash table entries: 2048 (order: 1, 8192 bytes)
Jan 1 09:00:14 router user.warn kernel: TCP bind hash table entries: 2048 (order: 1, 8192 bytes)
Jan 1 09:00:14 router user.info kernel: TCP: Hash tables configured (established 2048 bind 2048)
Jan 1 09:00:14 router user.info kernel: TCP reno registered
Jan 1 09:00:14 router user.warn kernel: ip_conntrack version 2.4 (256 buckets, 2048 max) - 232 bytes per
conntrack
Jan 1 09:00:14 router user.warn kernel: ip_tables: (C) 2000-2002 Netfilter core team
```

- **Refresh** : Refresh the System Log to get the latest status.

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:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 60 950-1: 2001 +A11: 2004

Safety of Information Technology Equipment

EN50385 : (2002-08)

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1: (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.6.1: (2005-09)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.2.1 (2002-08)




Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.



In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE0560!

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in

[German]	Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
[et] Eesti [Estonian]	Käesolevaga kinnitab [<i>tootja nimi = name of manufacturer</i>] seadme [<i>seadme tüüp = type of equipment</i>] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
[en] English	Hereby, [<i>name of manufacturer</i>], declares that this [<i>type of equipment</i>] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[es] Español [Spanish]	Por medio de la presente [<i>nombre del fabricante</i>] declara que el [<i>clase de equipo</i>] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[el] Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [<i>name of manufacturer</i>] ΔΗΛΩΝΕΙ ΟΤΙ [<i>type of equipment</i>] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
[fr] Français [French]	Par la présente [<i>nom du fabricant</i>] déclare que l'appareil [<i>type d'appareil</i>] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
[it] Italiano [Italian]	Con la presente [<i>nome del costruttore</i>] dichiara che questo [<i>tipo di apparecchio</i>] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [<i>name of manufacturer / izgatavotāja nosaukums</i>] deklarē, ka [<i>type of equipment / iekārtas tips</i>] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [<i>manufacturer name</i>] deklaruoja, kad šis [<i>equipment type</i>] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart [<i>naam van de fabrikant</i>] dat het toestel [<i>type van toestel</i>] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
[mt] Malti [Maltese]	Hawnhekk, [<i>isem tal-manifattur</i>], jiddikjara li dan [<i>il-mudell tal-prodott</i>] jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[hu] Magyar [Hungarian]	Alulírott, [<i>gyártó neve</i>] nyilatkozom, hogy a [<i>... típus</i>] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
[pl] Polski [Polish]	Niniejszym [<i>nazwa producenta</i>] oświadcza, że [<i>nazwa wyrobu</i>] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[pt] Português [Portuguese]	[<i>Nome do fabricante</i>] declara que este [<i>tipo de equipamento</i>] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
[sl] Slovensko [Slovenian]	[<i>Ime proizvajalca</i>] izjavlja, da je ta [<i>tip opreme</i>] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.