

# Zonnet<sup>®</sup>

**ZSR4134WE**

802.11n

**Wireless Broadband Router**

USER MANUAL

## Copyright Statement

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

# Table of Contents

<b>Chapter 1 Introduction</b> .....	1
Welcome .....	1
Contents of Package .....	1
System Requirement .....	1
Getting to Know Your ZSR4134WE .....	2
<b>Chapter 2 Hardware Installation</b> .....	4
<b>Chapter 3 Connect Your ZSR4134WE</b> .....	6
How to Check the Network Connection.....	9
<b>Chapter 4 Basic Configurations</b> .....	10
How to Access the Web-based Configuration Utility .....	10
Setup Wizard .....	11
<b>Chapter 5 Advanced Settings</b> .....	15
LAN Settings .....	15
WAN Settings .....	16
MAC Address Clone .....	19
DNS Settings .....	19
<b>Chapter 6 Wireless Settings</b> .....	20
Wireless Mode .....	20
Basic Settings.....	22
Wireless Security Settings .....	23
WPS Settings.....	28
WDS Settings .....	29
Advanced Wireless Settings.....	30
Wireless Access Control .....	31
Wireless Connection Status .....	31
<b>Chapter 7 DHCP Server</b> .....	32
DHCP Server List.....	33
<b>Chapter 8 Virtual Server</b> .....	34
Single Port Forwarding.....	34
Port Range Forwarding.....	35
Port Trigger Settings.....	36
ALG Service Settings .....	37
DMZ Settings.....	38
UPnP Settings.....	38

<b>Chapter 9 Traffic Control</b> .....	39
<b>Chapter 10 Security Settings</b> .....	40
Client Filter .....	40
URL Filter.....	41
MAC Filter .....	42
Prevent Network Attack .....	42
Remote Web Management.....	43
Local Web Management .....	43
Wan Ping .....	44
<b>Chapter 11 Routing Settings</b> .....	45
Routing Table .....	45
Static Routing .....	45
<b>Chapter 12 System Tools</b> .....	46
Time Settings .....	46
DDNS .....	46
Backup/Restore .....	47
Firmware Upgrade.....	47
Restore to Factory Default Settings .....	48
Reboot.....	48
Change Password.....	49
System Log .....	49
<b>Appendix 1 Product Features &amp; Specifications</b> .....	50
<b>Appendix 2 Troubleshooting</b> .....	52

# Chapter 1 Introduction

## Welcome

Thank you for purchasing Zonet ZSR4134WE – 802.11n wireless broadband router! This high cost-efficiency router is the best choice for Small office / Home office users, all computers and network devices can share a single xDSL / cable modem internet connection at high speed. Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced. When the number of your computers and network-enabled devices grow, you can also expand the number of network slot by simple attach a hub or switch, to extend the scope of your network!

All computers and IEEE 802.11b/g/n(Draft 2.0) wireless-enabled network devices (including PDA, cellular phone, game console, and more!) can connect to ZSR4134WE without additional cabling. The MIMO technology also gives you the highest speed of wireless experience ever! With a compatible wireless card installed in your PC, you can transfer file for up to 300Mbps! The radio coverage is also doubled, so don't worry if your office or house is really big!

Moreover, the user-friendly Setup Wizard on the installation CD can assist you to set up ZSR4134WE easily. It also can be managed or configured through Local/Remote easy-to-use Web-based utility.

## Contents of Package

- One ZSR4134WE
- One CD w/User Manual
- One Quick Installation Guide
- Two 3dBi Antennas
- One Ethernet Network Cable
- One Cradle
- One Power Adapter

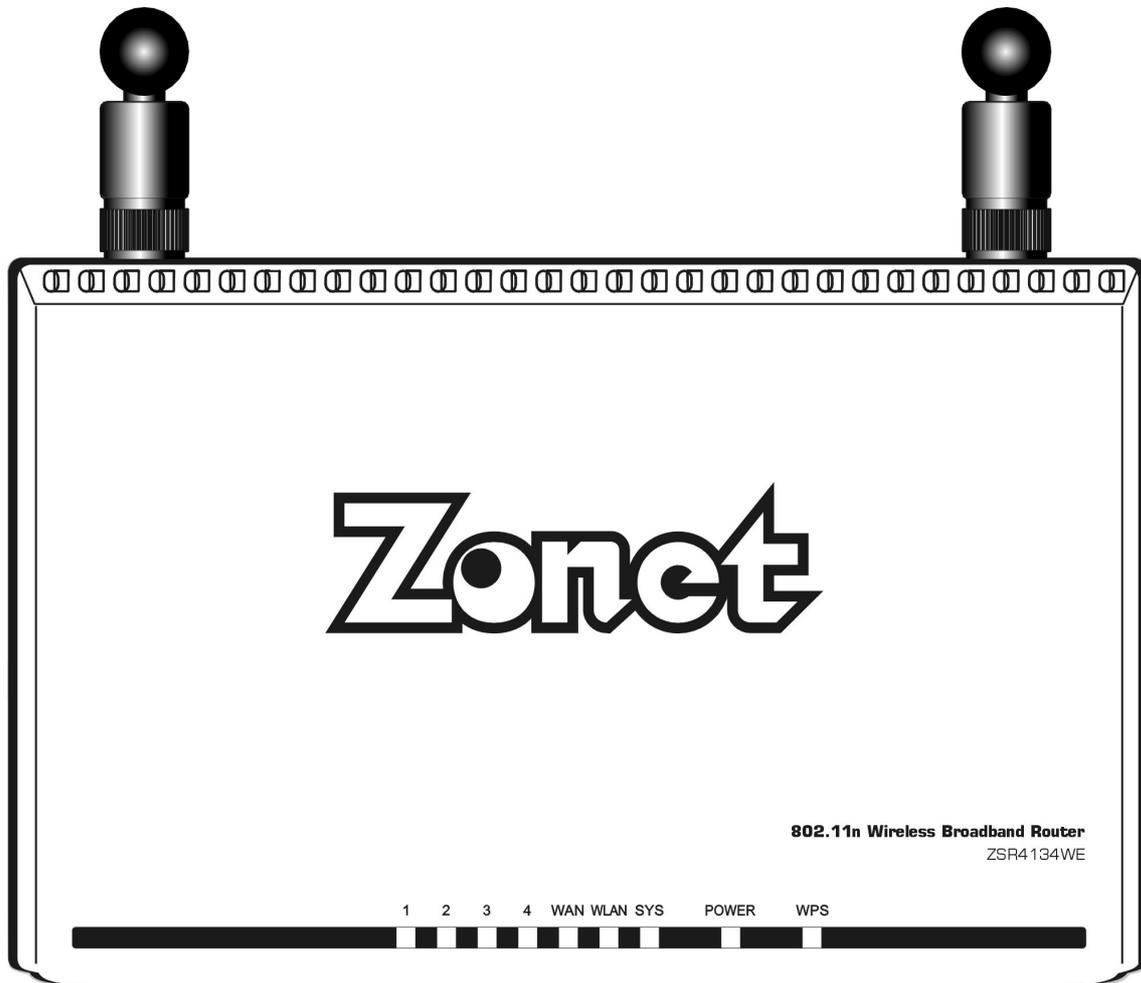
Contact your local authorized reseller or the store purchased from for any items damaged and/or missing.

## System Requirements

- Internet connection, provided by xDSL or cable modem with a RJ-45 Ethernet port.
- Computer or network devices with wired or wireless network interface card.
- Web browser (Microsoft Internet Explorer 5.5 or above, Firefox 1.0 or above).
- An available power socket (100–240V, 50/60Hz)

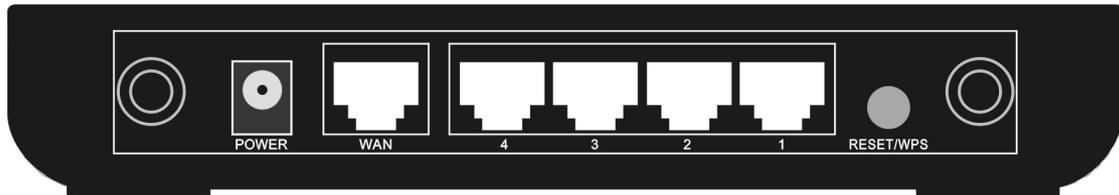
# Getting to Know Your ZSR4134WE

## Top Panel



LED Indicator	Status	Description
POWER	ON	ZSR4134WE is switched on and correctly powered
SYS	Flashing	Indicates the system works normally.
WAN	ON	Indicates WAN port is connected
	Flashing	Indicates WAN activity (transferring or receiving data)
WLAN	Flashing	Indicates the wireless signal is OK.
LAN(1/2/3/4)	ON	Indicates LAN port is connected
	Flashing	Indicates LAN activity (transferring or receiving data)
WPS	Flashing	Indicates ZSR4134WE is negotiating with WPS clients in WPS Mode (PBC or PIN).

## Rear Panel

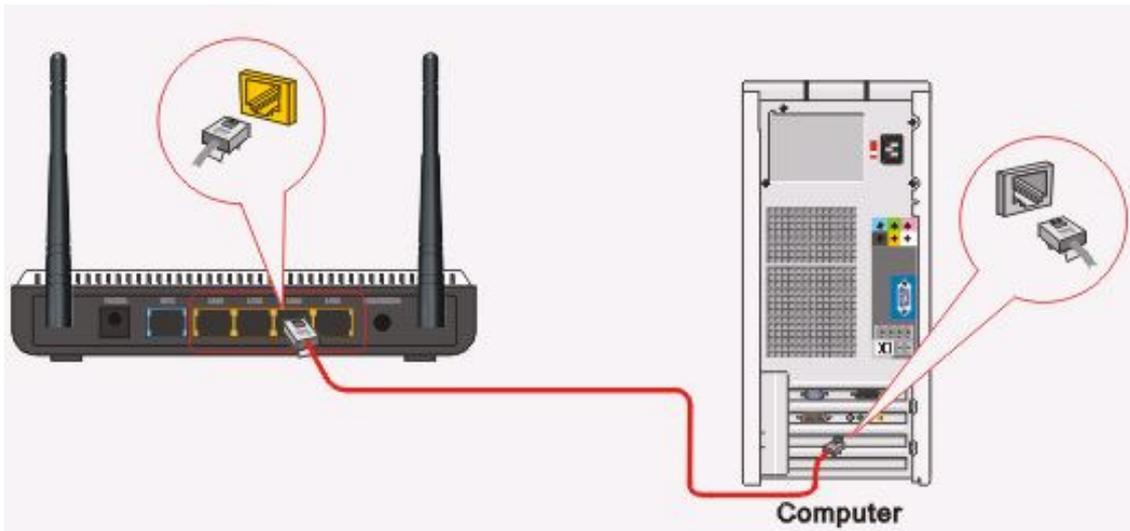


Item Name	Description
Antenna	These antennas are 3dBi dipole antennas.
POWER	Power connector, connects to power adapter
WAN	Wide Area Network (WAN / Internet) port.
1-4 (LAN Ports)	Local Area Network (LAN) ports 1 to 4
RESET/WPS	Reset ZSR4134WE to factory default settings (clear all settings) or start WPS function. Press this button and hold for 7 seconds to restore all settings to factory defaults, and press this button for 1 second to start WPS function.

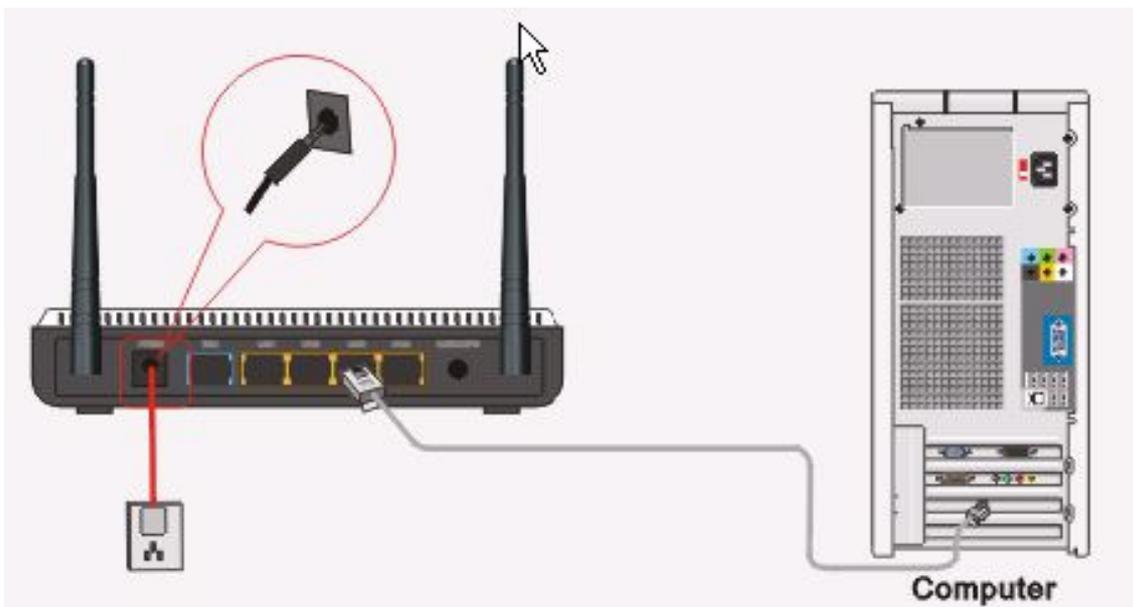
# Chapter 2 Hardware Installation

Please follow the following instruction to build the network connection between your ZSR4134WE and your computers, network devices:

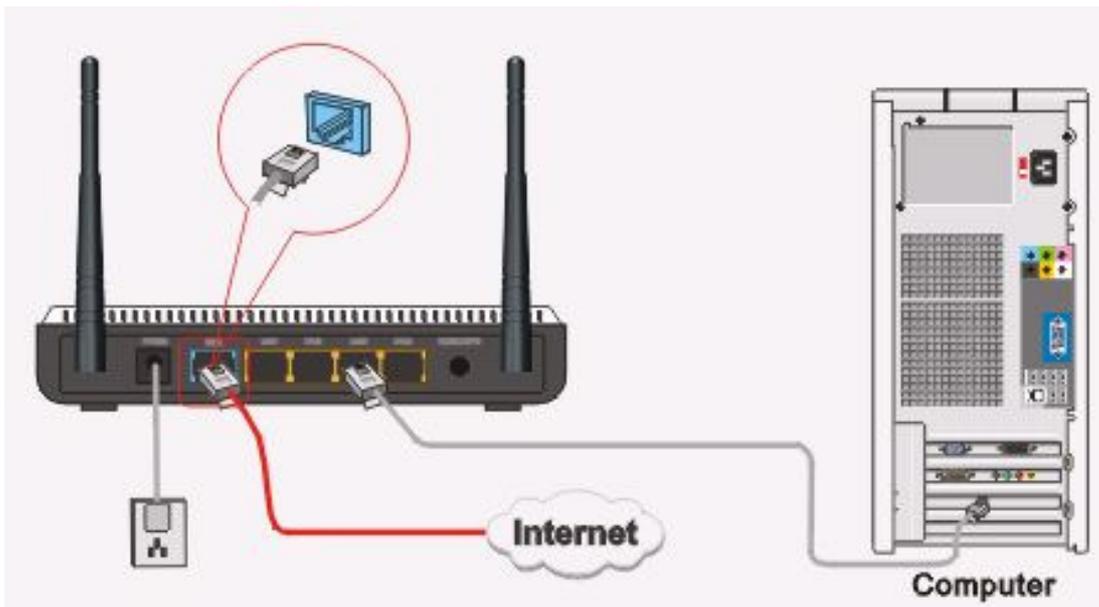
1. Connect all your computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub) to the LAN port of ZSR4134WE.



2. Connect the power adapter to the wall socket, and then connect it to the "Power" socket of ZSR4134WE.



3. Connect your xDSL / cable modem to the WAN port of ZSR4134WE by Ethernet cable.

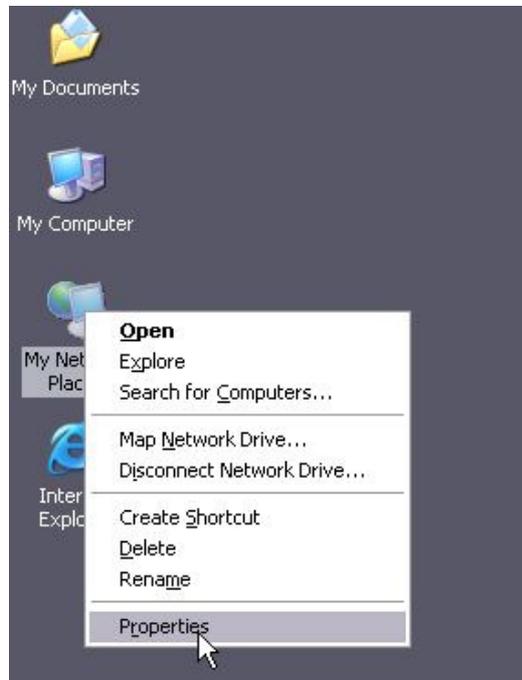


4. Please check all LEDs on the top panel. POWER LED should be steadily on, WAN and LAN LEDs should be on if the computer / network device connected to the respective port of ZSR4134WE is powered on and correctly connected. If any LED you expected is not on, please recheck the cabling, or jump to **“Troubleshooting”** for possible reasons and solution.

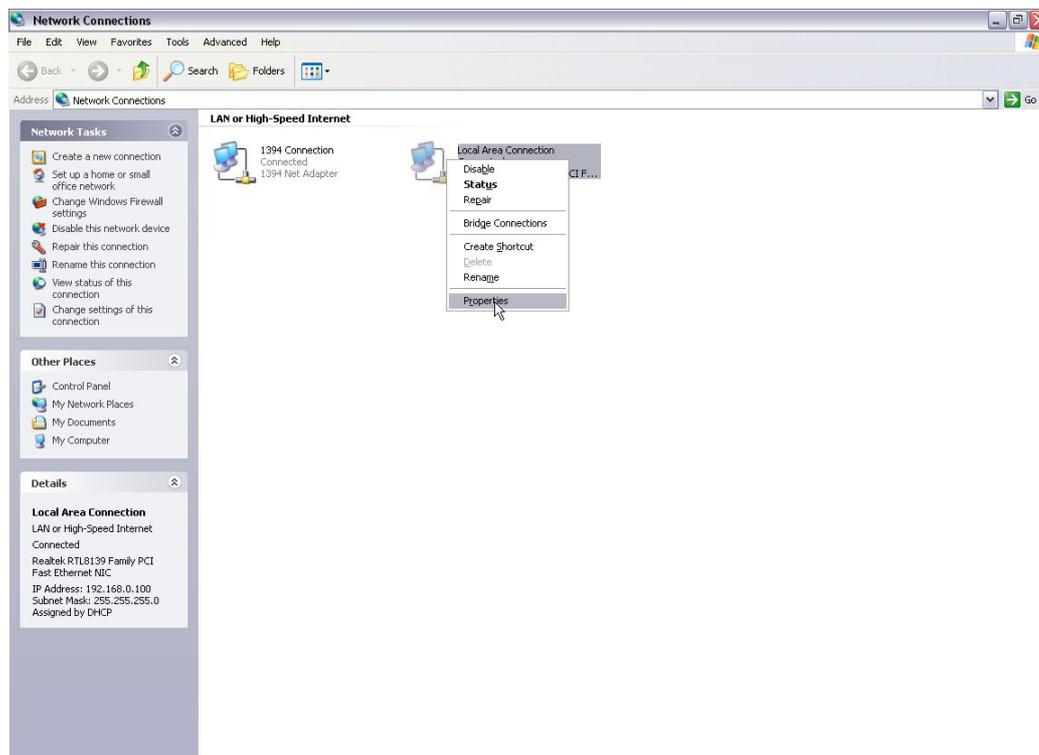
# Chapter 3 Connect Your ZSR4134WE

## How to Set the Network Configurations for My Computer

1. Right click **My Network Places** and select **Properties**



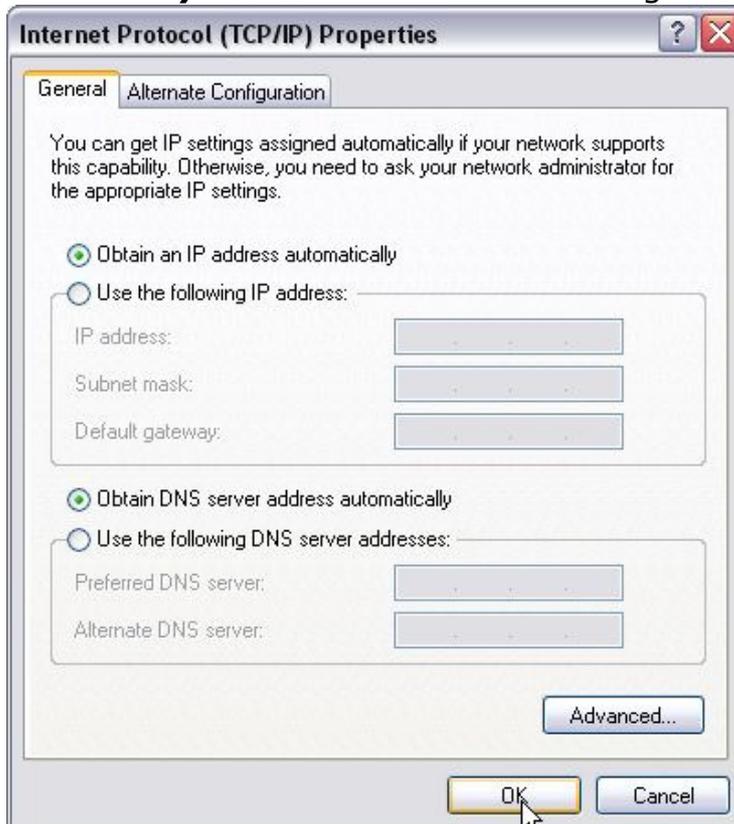
2. Right click **Local Area Network Connection** and select **Properties**.



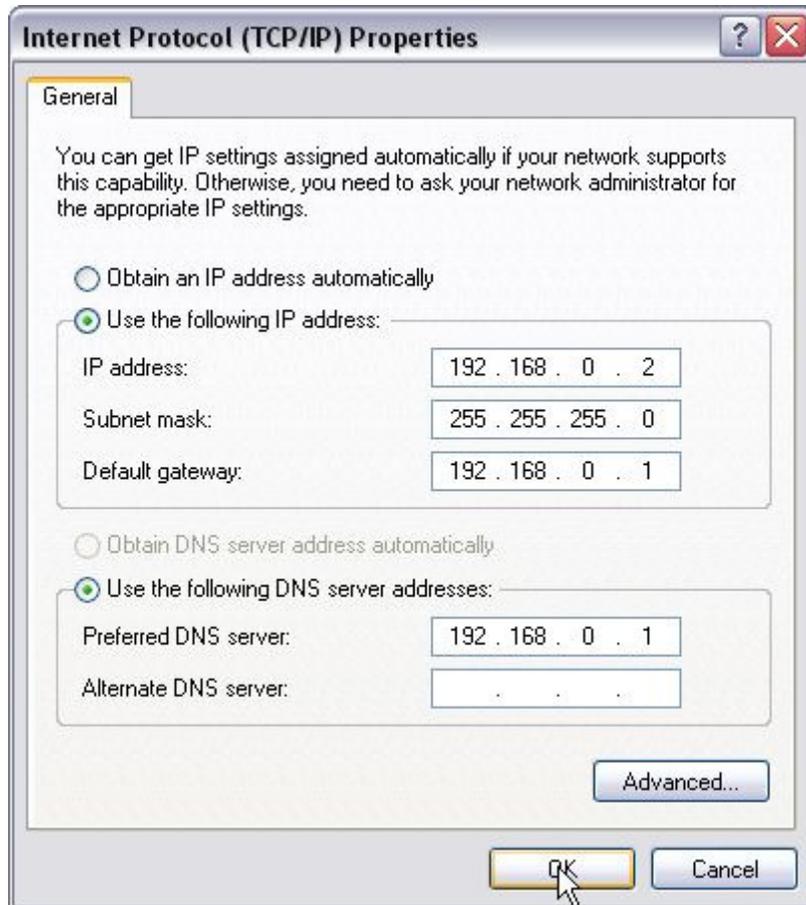
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



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

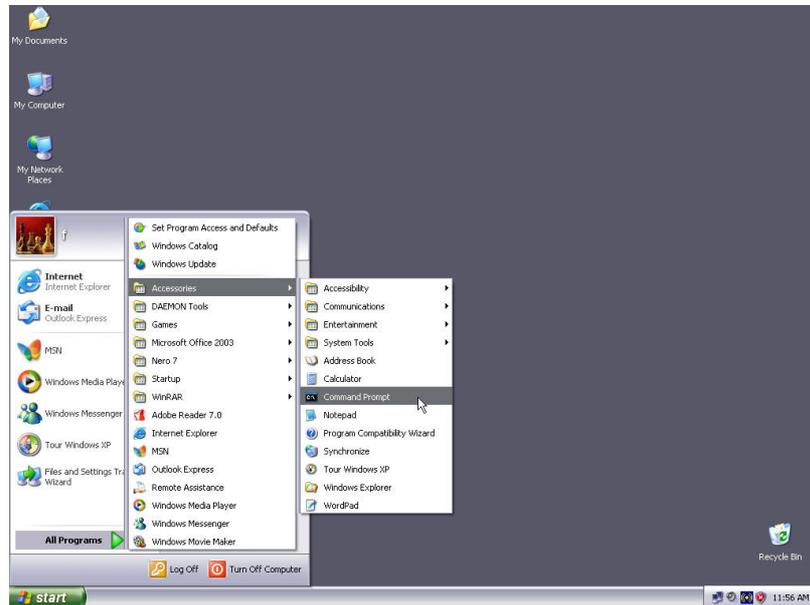


5. Or select **Use the following IP address** and enter the IP address, Subnet mask, Default gateway. Of course, you need to input the DNS server address provided by your ISP. Otherwise, you can use the ZSR4134WE's default gateway as the DNS proxy server. Click **OK** to save the configurations.



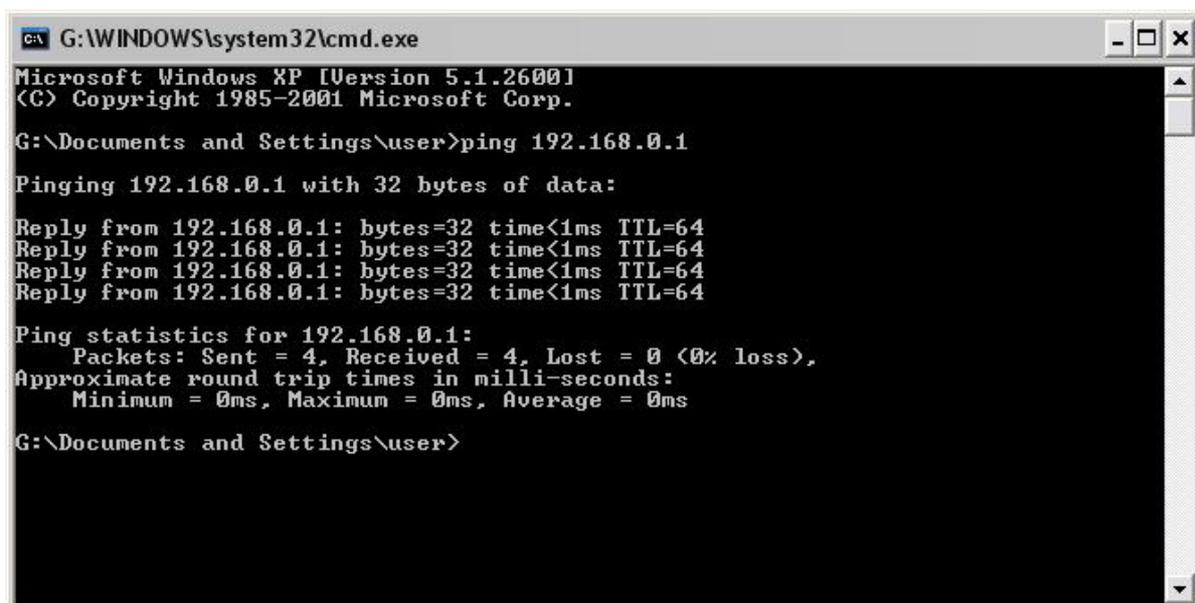
# How to Check the Network Connection

1. Select **Start** → **Programs** → **Accessories** → **Command Prompt**.



2. Input **ping 192.168.0.1** and press **Enter**. If the screen displays as below, it means your PC is connected to your router successfully.

If not, please make sure the hardware installation and network adapter are OK.

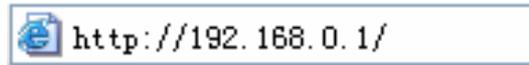


# Chapter 4 Basic Configurations

This section is to show you how to configure your new ZSR4134WE through the Web-based Configuration Utility.

## How to Access the Web-based Configuration Utility

1. After your computer obtained an IP address from ZSR4134WE, please start your web browser, and input the default IP address of ZSR4134WE <http://192.168.0.1> in address bar.

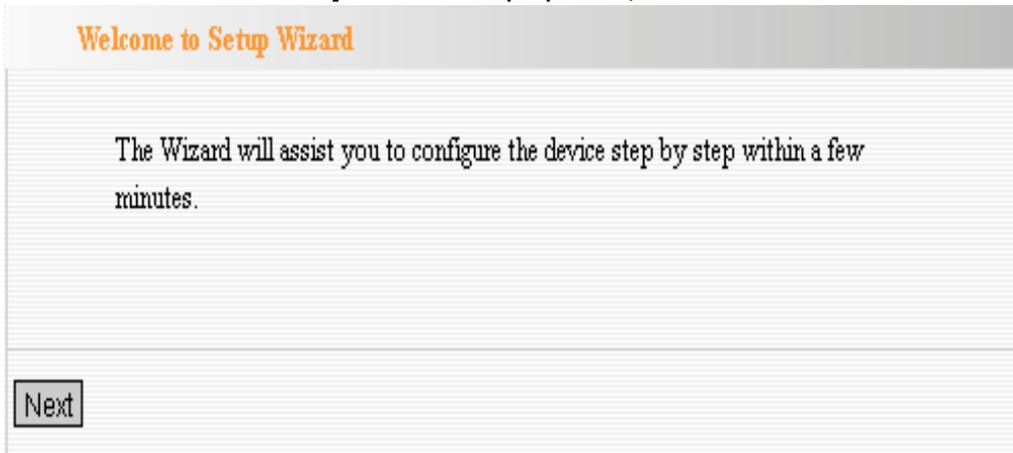


2. Please input user name and password and then click **OK**. Both default user name and password is **admin**.

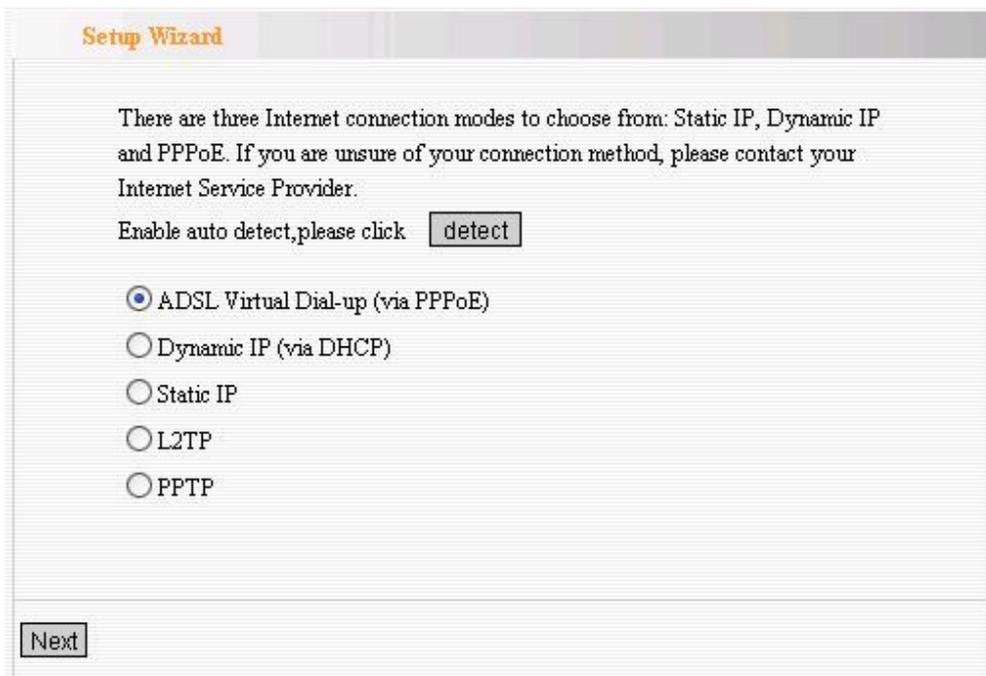


## Setup Wizard

1. When **Welcome to Setup Wizard** pop out, Click **Next** to continue.



2. Select one Internet connection type you're using. If you're not sure, click **Detect** or contact your Internet Service Provider. Click **Next**.



### a. ADSL Virtual Dial-up (Via PPPoE)

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

**Setup Wizard-ADSL**

In order to access your Internet service provider's network, you are required to provide correct user account and password.

Account:

Password:

**b. Dynamic IP (Via DHCP)**

If your connection type is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information.

**c. Static IP**

Fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click **Next**.

**Setup Wizard-Static IP**

This Internet connection mode requires network address information from your Internet service provider.

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:  (optional)

**d. L2TP**

Enter the Account and Password provided by your ISP.

**L2TP**(Layer 2 Tunneling Protocol) **provides two address modes.**

- **Dynamic IP:** If the L2TP offered by your ISP is Dynamic IP, please select Dynamic IP.
- **Static IP:** Please fill in the parameters provided by your ISP.

After configuration, please click **Next**.

**Setup Wizard-L2TP**

L2TP Server IP Address: 192.168.2.55

User Name: default

Password: ●●●●●●

Address Mode: Static

Address Mode: 192.168.2.115

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.55

Back Next

**e. PPTP**

Enter the Server IP Address, User Name, and Password provided by your ISP

**PPTP**(PP Tunneling Protocol) **provides two address modes.**

- **Dynamic IP:** If the PPTP offered by your ISP is Dynamic IP, please select Dynamic IP.
- **Static IP:** Please fill in the parameters provided by your ISP.

After configuration, please click **Next**.

**Setup Wizard-PPTP**

PPTP Server IP Address: 192.168.55.1

User Name: default

Password: ●●●●●●

Address Mode: Static

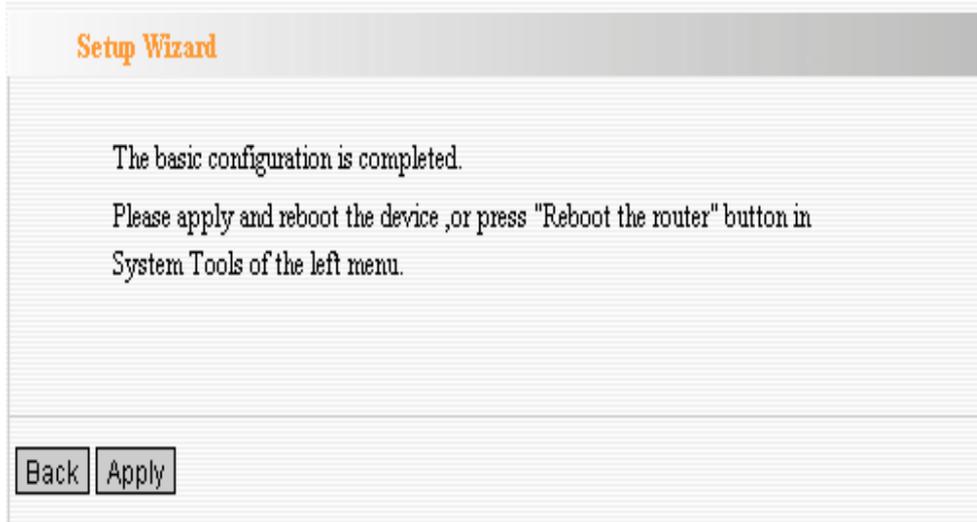
IP Address: 192.168.55.89

Subnet Mask: 255.255.255.0

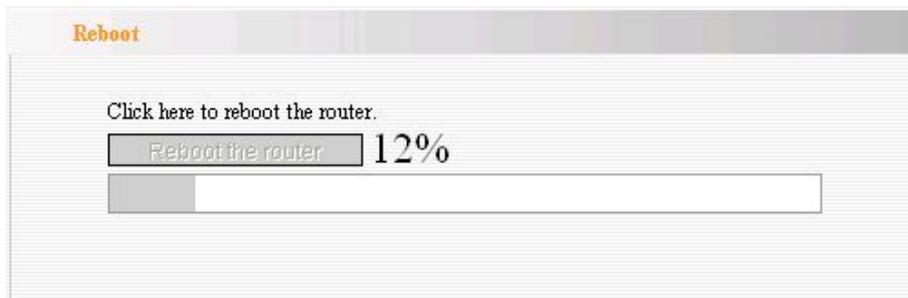
Default Gateway: 192.168.55.1

Back Next

3. Click **Apply** and reboot ZSR4134WE, or select **Reboot** in **System Tools** of the left menu and click **Reboot the router** button.



4. While rebooting, please wait for few minutes and **DO NOT** power off.



5. Select **Network Status** of the left menu to find out the current network and system information.



# Chapter 5 Advanced Settings

## LAN Settings

**LAN Settings**

This is to configure the basic parameters for LAN ports.

MAC Address      00:0C:41:86:0A:B2

IP Address     

Subnet Mask     

- **MAC Address:** ZSR4134WE's physical MAC address on your local network is unchangeable.
- **IP Address:** ZSR4134WE's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. Default value is 192.168.0.1
- **Subnet Mask:** ZSR4134WE's subnet mask for measurement of the network size. Default value is 255.255.255.0.

# WAN Settings

## a. PPPoE

WAN Settings

WAN connection mode: PPPoE

Account

Password

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

Service Name  (Do NOT Modify Unless Necessary)

AC Name  (Do NOT Modify Unless Necessary)

Internet Connection Option

Connect Automatically.

Connect Manually.

Connect on Demand

Max Idle Time:  (60—3600 seconds)

Connect on Fixed Time

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

Time: From  h  m T  h  m

- **Connection Mode:** Show your current connection mode.
- **Account:** Provided by your ISP.
- **Password:** Provided by your ISP.
- **MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1492. Do NOT modify it unless necessary.
- **Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- **AC Name:** Enter it if provided. Do NOT modify it unless necessary.

### Internet Connection Option:

- **Connect Automatically:** Connect automatically to the Internet after rebooting system or connection failure.
- **Connect Manually:** Connect to the Internet by the user manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix.

## b. Static IP

The screenshot shows a 'WAN Settings' dialog box with the following fields and values:

Field	Value
WAN connection mode	Static IP
IP Address	192.168.1.2
Netmask	255.255.255.0
Gateway	192.168.1.1
Primary DNS Server	192.168.0.1
Secondary DNS Server	(option)

Buttons: Apply, Cancel

- **IP Address:** Enter the WAN IP address provided by your ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask.
- **Gateway:** Enter the WAN Gateway.
- **Primary DNS Server:** Enter the Primary DNS server provided by your ISP.
- **Secondary DNS Server:** Enter the second address if your ISP provides, which is optional.

## c. L2TP

The screenshot shows a 'WAN Settings' dialog box with the following fields and values:

Field	Value
WAN connection mode	L2TP
L2TP Server IP:	192.168.2.55
User Name:	default
Password:	••••••••
MTU:	1400
Address Mode:	Static
IP Address:	192.168.2.115
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.2.55

Buttons: Apply, Cancel

- **L2TP Server IP:** Enter the Server IP provided by your ISP.
- **User Name:** Enter L2TP username.
- **Password:** Enter L2TP password.
- **MTU:** Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1400 is the default MTU.
- **Address Mode:** Select **Static** if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select **Dynamic**.
- **IP Address:** Enter the L2TP IP address supplied by your ISP.
- **Subnet Mask:** Enter the Subnet Mask supplied by your ISP.
- **Default Gateway:** Enter the Default Gateway supplied by your ISP.

#### d. PPTP

The screenshot shows a 'WAN Settings' dialog box with the following fields and values:

Field	Value
WAN connection mode:	PPTP
PPTP Server IP Address:	192.168.55.1
User Name:	default
Password:	••••••••
MTU:	1396
Address Mode:	Static
IP Address:	192.168.55.89
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.55.1
MPPE:	<input checked="" type="checkbox"/>

Buttons: Apply, Cancel

- **PPTP Server IP:** Enter the Server IP provided by your ISP.
- **User Name:** Enter PPTP username provided by your ISP.
- **Password:** Enter PPTP password provided by your ISP.
- **Address Mode:** Select **Static** if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select **Dynamic**.
- **IP Address:** Enter the PPTP IP address supplied by your ISP.
- **Subnet Mask:** Enter the Subnet Mask supplied by your ISP.
- **Default Gateway:** Enter the Default Gateway supplied by your ISP.

## MAC Address Clone

The screenshot shows a window titled "MAC Address Clone". Inside, there is a section labeled "WAN MAC Address Clone." followed by a "MAC Address:" label and a text input field containing "02:10:17:F2:AB:12". Below this are two buttons: "Restore Default MAC" and "Clone MAC Address". At the bottom of the window are "Apply" and "Cancel" buttons.

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

## DNS Settings

The screenshot shows a window titled "DNS Settings". It features a "DNS Settings" checkbox which is currently unchecked. Below it are two text input fields: "Primary DNS Address" containing "192.168.0.1" and "Secondary DNS Address" which is empty and followed by "(option)". At the bottom are "Apply" and "Cancel" buttons.

- **DNS:** Choose the checkbox to enable the DNS server.
- **Primary DNS Address:** Enter the necessary address provided by your ISP.
- **Secondary DNS Address:** Enter the second address if your ISP provides, which is optional.

# Chapter 6 Wireless Settings

## Wireless Mode

### a. AP Mode

The screenshot shows a configuration window titled "Wireless Mode". It has a header bar with the title in orange. Below the header, there are several configuration options:

- Wireless mode:** Two radio buttons are present: "AP" (which is selected) and "Station".
- SSID:** A text input field.
- MAC:** A text input field.
- Channel:** A dropdown menu currently showing "1".
- Security Mode:** A dropdown menu currently showing "WEP-PSK".

Below these fields is a button labeled "Open Scan". At the bottom of the window, there are two buttons: "Apply" and "Cancel".

- **AP Mode:** ZSR4134WE serves as an access point to be connected. The work stations around will be connected with ZSR4134WE by SSID to share the Internet resources. To configure the AP mode, open the Basic Setting and Security Setting windows in the Wireless Setting folder.
- **SSID:** SSID is the unique ID name of access point. The wireless work station must keep the same SSID name with the AP's for connections. By enabling **Open Scan** button, the device can search available APs.
- **MAC:** To connect certain AP, you need to know the AP's MAC address. By enabling **Open Scan** button to find out the available AP's MAC address.
- **Channel:** By enabling **Open Scan** button to find out the available AP's channel.
- **Security Mode:** ZSR4134WE provides security authentication methods including: WEP, WPA-Pre-Shared Key and WPA2-Pre-Shared Key.

## b. Station Mode

The screenshot shows a configuration window titled "Wireless Mode". At the top, there are two radio buttons: "AP" (unselected) and "Station" (selected). Below this are several fields and dropdown menus:

- SSID: A text input field.
- MAC: A text input field.
- Channel: A dropdown menu showing "1".
- Security Mode: A dropdown menu showing "WEP-PSK".
- WEP Mode: A dropdown menu showing "OPEN".
- Default Key: A dropdown menu showing "Key 1".
- Key Format: A dropdown menu showing "ASCII".
- WEP Key 1: A text input field.
- WEP Key 2: A text input field.
- WEP Key 3: A text input field.
- WEP Key 4: A text input field.

At the bottom of the configuration area is a button labeled "Open Scan". At the very bottom of the window are two buttons: "Apply" and "Cancel".

- **Station Mode:** ZSR4134WE is used as a work station to be connected with an AP by scanning the AP's SSID and provides the security authentication.
- **SSID:** SSID is the unique ID name of access point. The wireless work station must keep the same SSID name with the AP's for connections. By enabling **Open Scan** button, the device can search available APs.
- **MAC:** To connect certain AP, you need to know the AP's MAC address. By enabling **Open Scan** button to find out the available AP's MAC address.
- **Channel:** By enabling **Open Scan** button to find out the available AP's channel.
- **Security Mode:** ZSR4134WE provides security authentication methods including: WEP, WPA-Pre-Shared Key and WPA2-Pre-Shared Key.
- **WEP Mode:** The shared key requires the same WEP keys between the access point and work station.
- **Default KEY:** After entering the WEP keys, select one key as the default one, for example, Key 1
- **KEY Format:**
  - ◆ ASCII: Enter 13 characters with case sensitive ("a-z", "A-Z" and "0-9").
  - ◆ Hex: enter 26 Hex characters ("A-F", "a-f" and "0~9").
- **KEY 1:** If the KEY 1 is selected as default key, the key will be enabled.
- **KEY 2:** If the KEY 2 is selected as default key, the key will be enabled.
- **KEY 3:** If the KEY 3 is selected as default key, the key will be enabled.
- **KEY 4:** If the KEY 4 is selected as default key, the key will be enabled.
- **WPA/WPA2 Algorithm:** When WPA-PSK /WPA2-PSK is selected, you can

select **TKIP** or **AES**.

- **Password:** When WPA-PSK /WPA2-PSK is selected, enter the access password provided by AP users.

## Basic Settings

The screenshot shows a 'Basic Settings' window with the following configuration:

Network Mode	11b/g/n mixed mode
Main SSID	Wireless_N
Minor SSID	
Broadcast(SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	00:B0:0C:17:6C:0E
Channel	2437MHz (Channel 6)
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2417MHz (Channel 2)
Aggregation MSDU (A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Buttons: Apply, Cancel

- **Network Mode:** Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.
- **Main SSID:** Main Service Set Identifier. It's the name of your wireless network.
- **Minor SSID:** Minor Service Set Identifier. It is optional.
- **Broadcast (SSID):** Decide if ZSR4134WE will broadcast its own ESSID or not.
- **BSSID:** It is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC address of the AP
- **Channel:** Select the channel used for wireless communication from drop-down list. Available channel numbers are 1 to 13 for European countries, 1 to 11 for USA.
- **Channel Bandwidth:** Select wireless work frequency 20M or 20/40M.

# Wireless Security Settings

## a. Mixed WEP

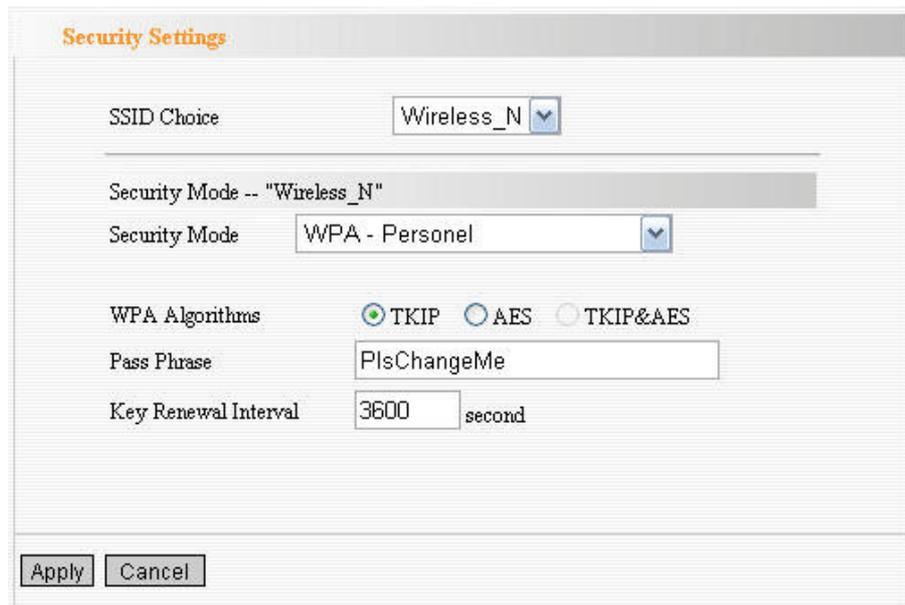
WEP (Wired Equivalent Privacy) is an encryption method used to protect your wireless data communications. WEP uses a combination of 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission.

The screenshot shows a 'Security Settings' dialog box. At the top, 'SSID Choice' is set to 'Wireless\_N'. Below that, 'Security Mode -- "Wireless\_N"' is displayed, and 'Security Mode' is set to 'Mixed WEP'. Under 'Default Key', 'Key 1' is selected. There are four rows for WEP keys, each with a text input field containing '12345' and a dropdown menu set to 'ASCII'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- **SSID Choice:** ZSR4134WE supports to configure different security classes between the main SSID and the subordinate SSID.
- **Default Key:** You can set up to four sets of WEP key, and you can decide which key is being used by default here.
- **WEP Key1, 2, 3, 4:** Input WEP key characters here, the number of characters must be the same as the number displayed at "Key Format" field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select "ASCII" key format, and if you select "Hex" as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same with each other.

## b. WPA-Personal

Wi-Fi Protected Access (WPA) is an advanced security standard. It uses TKIP and AES to change the encryption key frequently.

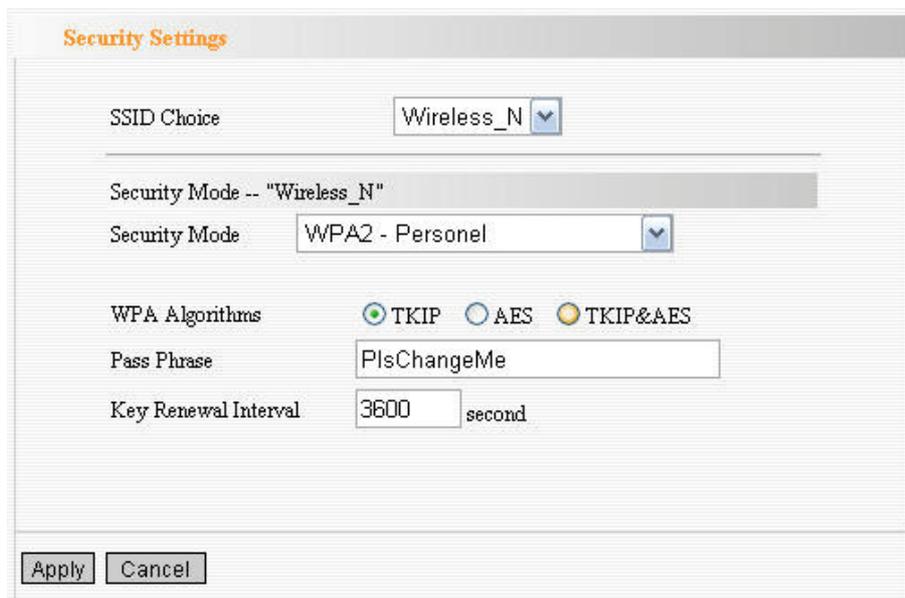


The screenshot shows a 'Security Settings' dialog box. At the top, 'SSID Choice' is set to 'Wireless\_N'. Below that, 'Security Mode -- "Wireless\_N"' is displayed, and 'Security Mode' is set to 'WPA - Personal'. Under 'WPA Algorithms', the 'TKIP' radio button is selected, while 'AES' and 'TKIP&AES' are unselected. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Apply' and 'Cancel' buttons.

- **WPA Algorithms:** Select one encryption type, AES, TKIP or TKIP&AES.
- **Pass Phrase:** Enter the key which must have 8-63 ASCII characters.
- **Key Renewal Interval:** Specifies the timer the WPA key must changes. The change is done automatically between the server and the client.

## c. WPA2-Personal

The WPA2 is a stronger version of WPA.



The screenshot shows a 'Security Settings' dialog box. At the top, 'SSID Choice' is set to 'Wireless\_N'. Below that, 'Security Mode -- "Wireless\_N"' is displayed, and 'Security Mode' is set to 'WPA2 - Personal'. Under 'WPA Algorithms', the 'TKIP&AES' radio button is selected, while 'TKIP' and 'AES' are unselected. The 'Pass Phrase' field contains 'PlsChangeMe'. The 'Key Renewal Interval' is set to '3600' seconds. At the bottom, there are 'Apply' and 'Cancel' buttons.

- **WPA Algorithms:** Select one encryption type, AES, TKIP or TKIP&AES.
- **Pass Phrase:** Enter the key which must have 8-63 ASCII characters.
- **Key Renewal Interval:** Specifies the timer the WPA key must changes. The change is done automatically between the server and the client.

#### d. WPA-Enterprise

This security mode is used when a RADIUS server is connected to ZSR4134WE.

The screenshot shows the 'Security Settings' dialog box. The 'SSID Choice' is set to 'Wireless\_N'. The 'Security Mode' is set to 'WPA - Enterprise'. Under 'WPA Algorithms', 'TKIP' is selected. The 'Key Renewal Interval' is set to 3600 seconds. The 'Radius IP Address' is 192.168.0.100, 'Radius Port' is 1812, 'Shared Key' is 'PlsChangeMe', and 'Session Timeout' is 3600. There are 'Apply' and 'Cancel' buttons at the bottom.

- **Radius IP Address:** Please input the IP address of Radius server here.
- **Radius Port:** Please input the port number of the Radius server here. Default setting is **1812**.
- **Shared key:** The encryption key that ZSR4134WE is authenticated through RADIUS server
- **Session Timeout:** The recertification time interval between ZSR4134WE and the Radius server. The default value is **3600**.

#### e. WPA2-Enterprise

This security mode is used when a RADIUS server is connected to ZSR4134WE.

**Security Settings**

SSID Choice: Wireless\_N

Security Mode -- "Wireless\_N"

Security Mode: WPA2 - Enterprise

WPA Algorithms:  TKIP  AES  TKIP&AES

Key Renewal Interval: 3600 second

PMK Cache Period: 10 minute

Pre-Authentication:  Disable  Enable

Radius IP Address: 192.168.0.100

Radius Port: 1812

Shared Key: PlsChangeMe

Session Timeout: 3600

Apply Cancel

- **WPA Algorithms:** Select one encryption type, AES, TKIP or TKIP&AES.
- **Radius IP Address:** Please input the IP address of Radius server here.
- **Radius Port:** Please input the port number of the Radius server here. Default setting is **1812**.
- **Shared key:** The encryption key that ZSR4134WE is authenticated through RADIUS server
- **Session Timeout:** The recertification time interval between ZSR4134WE and the Radius server. The default value is **3600**.

#### **f. 802.1X**

This security mode is used when a RADIUS server is connected to ZSR4134WE. IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to ZSR4134WE before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication.

The screenshot shows a 'Security Settings' dialog box with the following configuration:

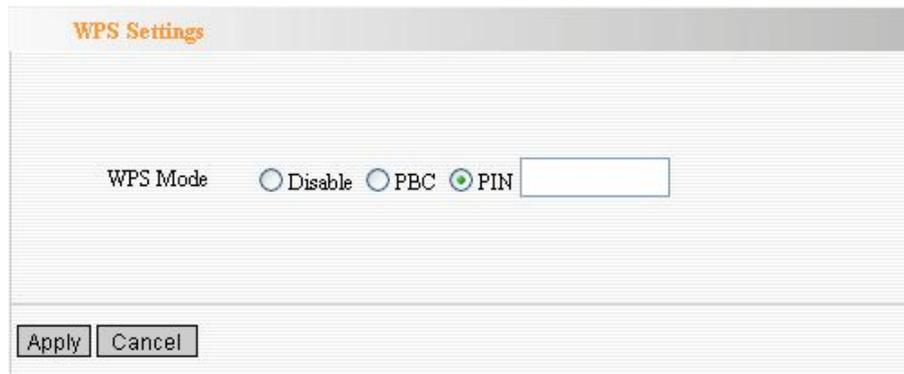
- SSID Choice: Wireless\_N
- Security Mode -- "Wireless\_N": 802.1X
- WEP:  Disable,  Enable
- Radius IP Address: 192.168.0.100
- Radius Port: 1812
- Shared Key: PlsChangeMe
- Session Timeout: 3600

- **WEP:** Select **Enable** or **Disable** WEP encryption which indicates the authentication process between wireless adapter and ZSR4134WE.
- **Radius IP Address:** Please input the IP address of Radius server here.
- **Radius Port:** Please input the port number of the Radius server here. Default setting is **1812**.
- **Shared key:** The encryption key that ZSR4134WE is authenticated through RADIUS server
- **Session Timeout:** The recertification time interval between ZSR4134WE and the Radius server. The default value is **3600**.

**NOTE:** To improve security level, do not use those words which can be found in a dictionary or too easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it's worth to use complicated WEP key to improve security level.

## WPS Settings

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and ZSR4134WE. You don't have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client, you only have to press a button on wireless client and this wireless router, and the WPS will do the rest for you.



WPS Settings

WPS Mode  Disable  PBC  PIN

Apply Cancel

- **WPS Mode:** Supports two ways to configure WPS settings: PBC) and PIN code.
  - ◆ **PBC(Push-Button Configuration):** If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch ZSR4134WE to WPS mode too. You can push WPS button of ZSR4134WE, or click **PBC** button in the web configuration interface to enable WPS

**Note:** Press WPS button of ZSR4134WE for one second and WPS indicator will blinking for 2 minutes. During the blinking time, you can enable another Router to implement the WPS/PBC negotiation between them. At present, the WPS only support one client access. Two minutes later, the WPS indicator will be off.

- ◆ **PIN:** if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to ZSR4134WE.

## WDS Settings

In this mode, you can expand the scope of network by combining up to four other access points together, and every access point can still accept wireless clients.

The screenshot shows the 'WDS Settings' dialog box. The 'WDS Mode' dropdown is set to 'Bridge Mode'. The 'Encrypt Type' dropdown is open, showing 'Disable', 'Lazy Mode', 'Bridge Mode', and 'Repeater Mode'. There are four empty input fields for 'AP MAC' addresses. At the bottom, there are 'Save' and 'Cancel' buttons, and an 'Open Scan' button.

- **WDS Mode:**
  - ◆ **Lazy Mode:** You need to configure ZSR4134WE's BSSID into another device, but don't need to input another device's BSSID in ZSR4134WE, and they will connect together automatically.
  - ◆ **Bridge Mode:** You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into ZSR4134WE's AP MAC address table or select one from the scanning table. At the same time, the connecting device should be in Lazy, Repeater or Bridge mode.
  - ◆ **Repeater Mode:** You can select the mode to extend the distance between the two WLAN devices. Functioning as a WDS repeater, ZSR4134WE connects to both a client card as an AP and to another AP. In typical repeater applications, APs connecting to other APs equipped with WDS functionality must also support WDS. In this mode, you need to add the MAC address of the connecting device into ZSR4134WE's AP MAC address table and the connecting client should be in Lazy, Repeater or client mode.
- **Encrypt Type:** You can select from WEP mode, TKIP mode, AES mode for security here.
- **Pass phrase:** Enter the key, the key format according to encryption you selected.
- **AP MAC:** Input the MAC address of another wireless router.

**NOTE:** Two wireless routers must use the same band, channel number, and security setting.

## Advanced Wireless Settings

ZSR4134WE provides some advanced control of wireless parameters, if you want to configure these settings, please click "Wireless" menu on the left of web management interface, then click "Advanced Settings", and the following message will be displayed on your web browser:

The screenshot shows the "Advanced Settings" web interface. It contains the following fields and options:

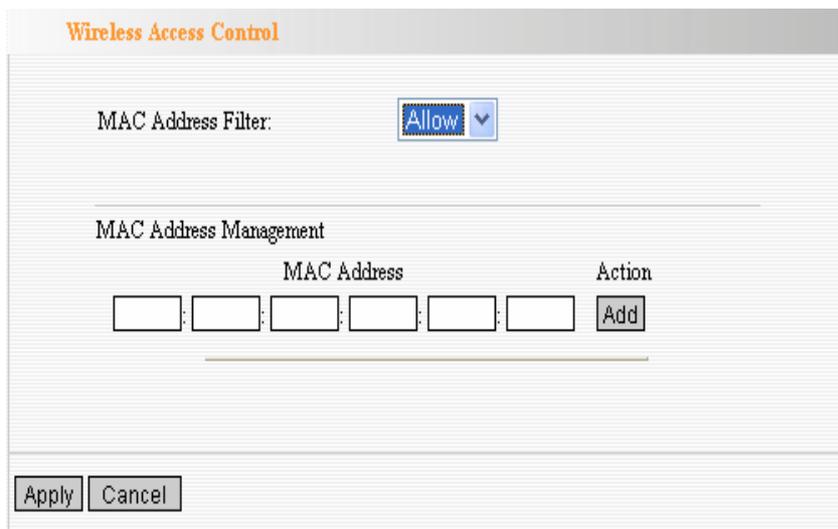
- BG Protection Mode: Auto (dropdown)
- Basic Data Rates: Default(1-2-5.5-11 Mbps) (dropdown)
- Beacon Interval: 100 ms (range 20 - 999, default 100)
- Fragment Threshold: 2346 (range 256 - 2346, default 2346)
- RTS Threshold: 2347 (range 1 - 2347, default 2347)
- TX Power: 100 (range 1 - 100, default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

At the bottom, there are "Save" and "Cancel" buttons.

- **BG protection Mode:** Auto by default. You can also select On or Off.
- **Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Default value is (1-2-5.5-11Mbps...).
- **Beacon Interval:** Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.
- **Fragment Threshold:** Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
- **RTS Threshold:** Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.
- **TX Power:** You can set the output power of wireless radio. Unless you're using ZSR4134WE in a really big space, you may not have to set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your ZSR4134WE).
- **WMM Capable:** 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 / not sure if you need it, it's safe to set this option to 'Enable', default value is Enable.
- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

## Wireless Access Control

This function will help you to prevent unauthorized users from connecting to ZSR4134WE; only those wireless devices who have the MAC address you assigned here can gain access to your ZSR4134WE. You can use this function with other security measures described in previous section, to create a safer wireless environment.



Wireless Access Control

MAC Address Filter: Allow

---

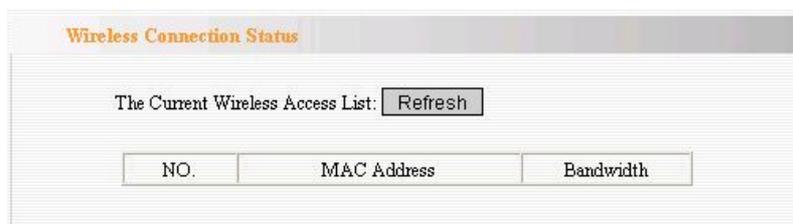
MAC Address Management

MAC Address	Action
<input type="text"/> : <input type="text"/>	<input type="button" value="Add"/>

- **MAC Address Filter:** If you want to access ZSR4134WE from any external IP Address, please select **Disable**.
- **MAC Address:** To specify an external IP address, please add the MAC address manually and click **Add**.
- **MAC Address List:** The added MAC addresses are listed here. Click **Delete** to delete the filter management for this MAC address.

## Wireless Connection Status

Click **Refresh** to update the wireless connection information.



Wireless Connection Status

The Current Wireless Access List:

NO.	MAC Address	Bandwidth
-----	-------------	-----------

- **MAC Address:** Shows the connecting PC's MAC address.
- **Bandwidth:** displays the channel bandwidth of the host to be connected.

# Chapter 7 DHCP Server

These settings are only available when **DHCP Server** in **LAN IP** section is **Enable**.

DHCP Server	
DHCP Server	<input checked="" type="checkbox"/> Enable
IP Address Start	192.168.0. <input type="text" value="110"/>
IP Address End	192.168.0. <input type="text" value="200"/>
Lease Time	<input type="text" value="Two days"/> ▼

- **DHCP Server:** Activate the checkbox to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP address for DHCP server distribution.
- **Lease Time:** choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by ZSR4134WE from dropdown menu.

## DHCP Server List

**DHCP Client List**

**Static IP**

IP Address 192.168.0.

MAC Address  :  :  :  :  :

NO.	IP Address	MAC Address	Delete
-----	------------	-------------	--------

Host Name	IP Address	MAC Address	Lease
fanyi	192.168.0.110	00:E0:4C:01:9C:92	1days 22:09:25

- **IP Address:** Input the IP address for the computer on the LAN network.
- **MAC Address:** Enter the MAC address of the computer you want to assign. And then click **Add** to add to the list.
- **Hostname:** The name of the computer.
- **Lease Time:** The time length of the corresponding IP address lease.

# Chapter 8 Virtual Server

## Single Port Forwarding

ZSR4134WE can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

**NOTE:** the virtual server uses known host-name or public IP address.

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

Note: the virtual server uses known host-name or public IP address.

NO.	External-Port	Internal-Port	To IP Address	Protocol	Enable	Delete
1.	66	21	192.168.0.10	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.			192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: DNS(53)  ID 1

- **External Port:** This is the external port number for server or Internet application, for example, port 21 for ftp service.
- **Internal Port:** This is the port number of LAN computer set by ZSR4134WE. The Internet traffic from the external port will forward to the internal port. For example, you can set the internal port 66 to act as the external port 21 for ftp service.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.

- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Delete/Enable:** Click to check it for corresponding operation.

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

## Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.

**Port Range Forwarding**

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

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

Well-Known Service Port:   ID

- **Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Delete/Enable:** Click to check it for corresponding operation.

## Port Trigger Settings

Port Trigger Settings

Port Trigger

IP Range	Trigger Port	External Port
192.168.0. [ ] ~ [ ]	[ ] ~ [ ]	[ ] ~ [ ]

Protocol: TCP&UDP ▾

Apply:

Add

Num	IP	Trigger Port	External Port	Protocol	Apply	Edit	Del
-----	----	--------------	---------------	----------	-------	------	-----

Apply Cancel

When internal clients have access to external server in the Internet for some applications, the clients request to connect with servers, and the server will also ask to connect with client. But in the default setting, ZSR4134WE will refuse to accept any request from WAN, which will bring communication halt. The port triggering is used to define triggering rules. So when clients have access to the server, the device will open the port through which the server sends the request to client.

- **IP Range:** The internal IP address range for requesting external server application.
- **Trigger Port:** The port range through which the internal clients send request traffics to external server with the range of 1~65535. Note that the low number first and two blanks can keep the same number if needed.
- **External Port:** The port range through which the external server send request traffics to internal clients with the range of 1~65535. Note that the low number first and two blanks can keep the same number if needed.
- **Apply:** Select the checkbox to enable the rule.
- **Add:** After edit the rule, click the "add" button to add the current entry to port triggering list.

**NOTE:** The special application can be only used in one PC. If there is more than one PC to open the same triggering port, the external port will be connected to the last PC for the application.

## ALG Service Settings

Application Layer Gateway (ALG) is a special function of ZSR4134WE. In the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications etc.

In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

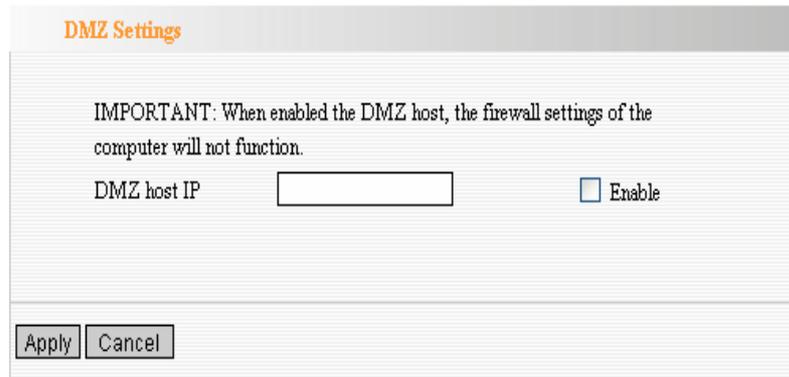
Usually allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.



In default ALG settings, FTP/TFTP/PPTP/IPSEC/L2TP protocols are enabled. It is recommended to keep the settings unchanged.

## DMZ Settings

The DMZ(Demilitarized Zone) function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.

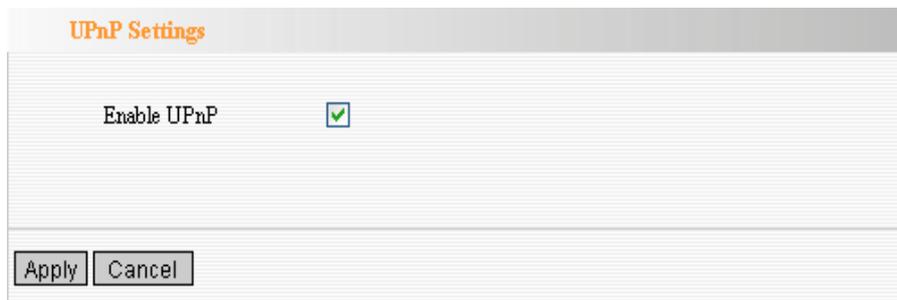


- **DMZ Host IP Address:** The IP address of the computer you want to expose.
- **Enable:** Select the checkbox to enable the DMZ host.

**IMPORTANT:** When enabled the DMZ host, the firewall settings of the DMZ host will not function.

## UPnP Settings

Universal Plug and Play function enables network auto-configuration for peer-to-peer communications. With this function, network devices will be able to communicate with other devices directly, and learn about information about other devices. Many network device and applications rely on UPnP function nowadays.



- **Enable UPnP:** Select the checkbox to enable the UPnP.

# Chapter 9 Traffic Control

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

**Traffic Control Settings**

Traffic Control

Interface: Upload BW: 512 Download BW: 2048 (KByte/s)

Services: Protocol: TCP&UDP Port: 0 Service: All

IP: 192.168.0. ~

Up/Down: Up

BW Range: ~ (KByte/s)

Apply:

Add

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

Apply Cancel

- **Traffic Control:** Select the checkbox to enable the internal IP bandwidth control.
- **Interface:** To limit the uploading and downloading bandwidth in WAN port.
- **Service:** To select the controlled service type, such as HTTP service.
- **IP Starting Address:** The first IP address for traffic control.
- **IP Ending Address:** The last IP address for traffic control.
- **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- **Bandwidth:** To specify the uploading/downloading Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.
- **Apply:** Select the checkbox to enable the current editing rule.
- **Add:** After edit the rule, click the **Add** button to add the current rule to rule list.

**Note:** It is allowed to delete or modify the previous rules in the list table.

# Chapter 10 Security Settings

## Client Filter

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.

**Client Filter**

Client Filtering Settings

Access Policy: 10

Enable:  Delete the Policy:

Filtering Mode:  Disable access the Internet  
 Enable

Policy Name:

Start IP: 192.168.0.

End IP: 192.168.0.

Port:  -

Type: TCP

Times: 0:0 ~ 0:0

Date:  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

- **Client Filtering Settings:** Select the checkbox to enable client filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Select the checkbox to enable the access policy.
- **Delete the Policy:** Click **Clear** button to clear all settings for the policy.
- **Filtering Mode:** Select one button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **Start/End IP:** Enter the starting/ending IP address.
- **Port:** Enter the port range over the protocol for access policy.
- **Type:** Select one protocol (TCP/UDP/Both) from drop-down menu.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.

## URL Filter

If you want to prevent computers in local network from accessing certain website (like pornography, violence, or anything you want to block), you can use this function to stop computers in local network from accessing the site you defined here.

The screenshot shows the 'URL Filter' configuration window. It includes the following elements:

- URL Filtering Setting:** A checkbox labeled 'Enable' which is checked.
- Access Policy:** A dropdown menu currently set to '10'.
- Enable:** A checkbox which is unchecked.
- Delete the Policy:** A button labeled 'Clear'.
- Filtering Mode:** Two radio buttons. 'Disable' is selected, and 'Enable' is unselected. The text 'access the Internet' is positioned to the right of the 'Enable' radio button.
- Policy Name:** An empty text input field.
- Start IP:** A text input field containing '192.168.0.'.
- End IP:** A text input field containing '192.168.0.'.
- DNS:** An empty text input field.
- Times:** Four dropdown menus, each showing '0'.
- Date:** A series of checkboxes for 'Everyday' (checked), 'Sun', 'Mon', 'Tue', 'Wen', 'Thr', 'Fri', and 'Sat'.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom left.

- **URL Filtering Setting:** Select the checkbox to enable URL filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Select the checkbox to enable the access policy.
- **Delete the Policy:** Click **Clear** button to clear all settings for the policy.
- **Filtering Mode:** Select one button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **Start/End IP:** Enter the starting/ending IP address.
- **DNS:** Input the string or keyword which is contained in URL. If any part of the URL contains these strings or words, the web page will not be accessible and display.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.

## MAC Filter

MAC Filtering Settings:  Enable

Access Policy: 10

Enable:  Delete the Policy: Clear

Filtering Mode:  Disable  Enable access the Internet

Policy Name:

MAC Address:  :  :  :  :  :

Times: 0 : 0 ~ 0 : 0

Date:  Everyday  Sun  Mon  Tue  Wen  Thr  Fri  Sat

Apply Cancel

- **MAC Filtering Settings:** Select the checkbox to enable MAC address filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Select the checkbox to enable the access policy.
- **Delete the Policy:** Click **Clear** button to clear all settings for the policy.
- **Filtering Mode:** Select one button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **MAC Address:** Enter the MAC address you want to run the access policy.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.

## Prevent Network Attack

This function is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, ZSR4134WE will restrict its bandwidth automatically.

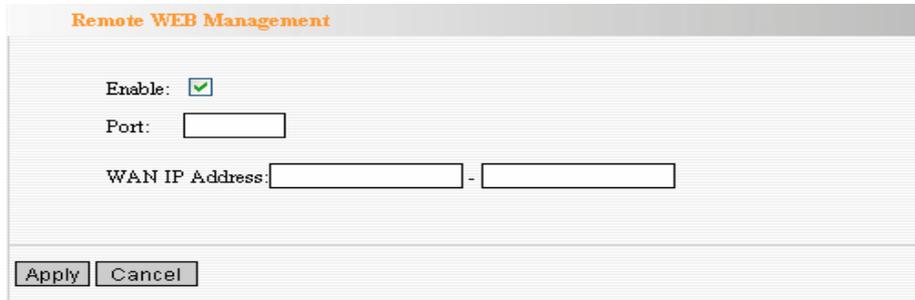
Prevent Network Attack

Apply Cancel

- **Prevent Network Attack:** Select the checkbox to enable it.

## Remote Web Management

This function is to allow the network administrator to manage ZSR4134WE remotely. If you want to access ZSR4134WE from outside the local network, please select the **Enable**.



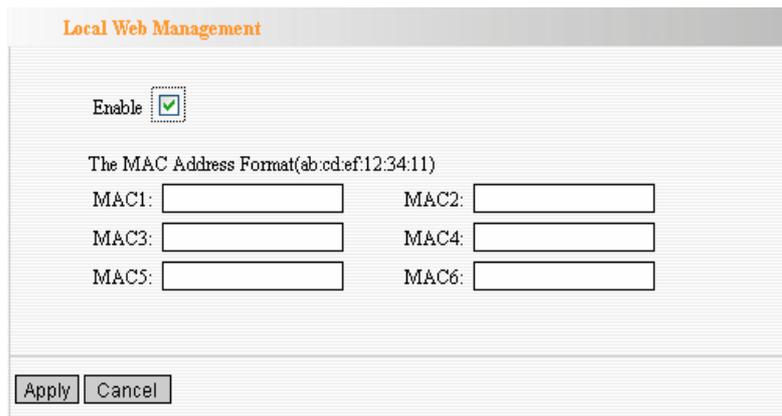
The screenshot shows a configuration window titled "Remote WEB Management". It contains the following fields and controls:

- Enable:** A checkbox that is checked.
- Port:** An empty text input field.
- WAN IP Address:** Two empty text input fields separated by a hyphen.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

- **Enable:** Select the checkbox to enable remote web management.
- **Port:** The management port open to outside access. Default value is 80.
- **WAN IP Address:** Specify the range of the WAN IP address for remote management.

## Local Web Management

This function allows the network administrator to manage ZSR4134WE in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.



The screenshot shows a configuration window titled "Local Web Management". It contains the following fields and controls:

- Enable:** A checkbox that is checked.
- The MAC Address Format(ab:cd:ef:12:34:11):** A label above six input fields.
- MAC1:** An empty text input field.
- MAC2:** An empty text input field.
- MAC3:** An empty text input field.
- MAC4:** An empty text input field.
- MAC5:** An empty text input field.
- MAC6:** An empty text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

- **Enable:** Select the checkbox to enable the local web management.
- **MAC #:** Enter the MAC addresses of LAN computers.

## WAN Ping

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



The screenshot shows a dialog box titled "WAN Ping". Inside the dialog, there is a checkbox labeled "Disable the Ping for WAN" which is checked. At the bottom of the dialog, there are two buttons: "Apply" and "Cancel".

- **Disable the Ping for WAN:** Select the checkbox to enable it.

# Chapter 11 Routing Settings

## Routing Table

The main duty for ZSR4134WE is to look for a best path for every data frame, and transfer this data frame to destination. So, it's essential for ZSR4134WE to choose the best path. In order to finish this function, many transferring paths are saved in ZSR4134WE for choosing when needed.

Destination IP	Subnet Mask	Gateway	Metric	Interface
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.100	0	eth2.2

Refresh

## Static Routing

Static Routing is set by administrator in advance. Usually, it is set according to network configuration when installing the operation system. It would not be changed according to network structure's change.

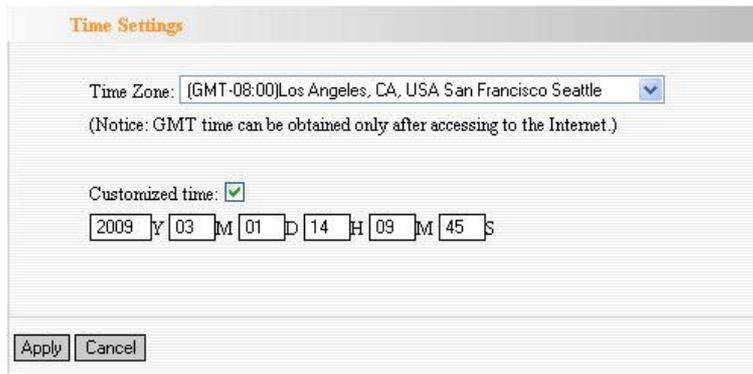
Destination LAN IP	Subnet Mask	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add

- **Destination LAN IP:** The address of the remote host with which you want to construct a static routing.
- **Subnet Mask:** The network portion of the Destination LAN IP.
- **Gateway:** The gateway of the next hop.

# Chapter 12 System Tools

## Time Settings

This function is to select the time zone for your location. If you turn off ZSR4134WE, the time settings will disappear. However, ZSR4134WE will automatically obtain the GMT time again once it access to the Internet.



The screenshot shows a window titled "Time Settings". It contains a "Time Zone:" dropdown menu with the selected value "(GMT-08:00)Los Angeles, CA, USA San Francisco Seattle". Below this is a notice: "(Notice: GMT time can be obtained only after accessing to the Internet.)". There is a "Customized time:" checkbox which is checked. Below the checkbox is a date and time input field showing "2009" for year, "03" for month, "01" for day, "14" for hour, "09" for minute, and "45" for seconds. At the bottom of the window are "Apply" and "Cancel" buttons.

- **Time Zone:** Select your time zone from the drop-down menu.
- **Customized time:** Select the checkbox and input the time you customize.

## DDNS

DDNS (Dynamic Domain Name System) is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind ZSR4134WE. If you want to activate this function, please select Enable and a DDNS service provider to sign up.



The screenshot shows a window titled "DDNS". It contains a "DDNS" section with two radio buttons: "Enable" (selected) and "Disable". Below this is a "Service Provider" dropdown menu with "DynDNS.org" selected and a "Sign up" button. There are three text input fields: "User Name", "Password", and "Domain Name" (with "(optional)" next to it). At the bottom of the window are "Apply" and "Cancel" buttons.

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

## Backup/Restore

**Backup/Restore**

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

Please choose restore file:

- **Backup:** Click to back up ZSR4134WE's configurations.
- **Browse:** Click to browse the path where you want to save files.
- **Restore:** Click to restore ZSR4134WE's configurations.

## Firmware Upgrade

**Upgrade**

Select the firmware version:

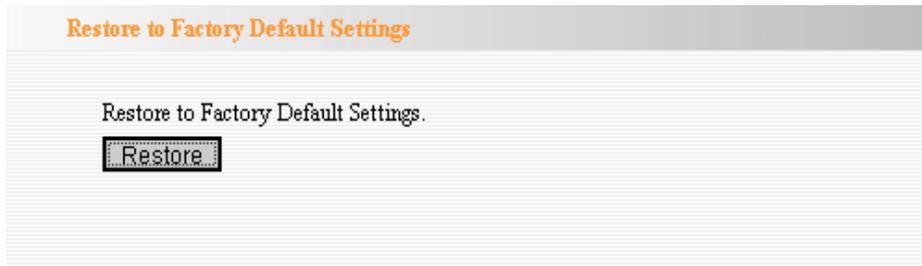
The current firmware version: H1\_V3.2.4h-Feb 9 2009

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

- **Browse:** Click to browse the path to the upgraded firmware files.
- **Upgrade:** Click to start upgrade.

**IMPORTANT:** Do not power off the system during the firmware upgrade to avoid damaging. ZSR4134WE will reboot automatically after the upgrade.

## Restore to Factory Default Settings



- **Restore to Factory Default Settings:** Click to restore to default settings.

Factory Default Settings:

User Name: **admin**

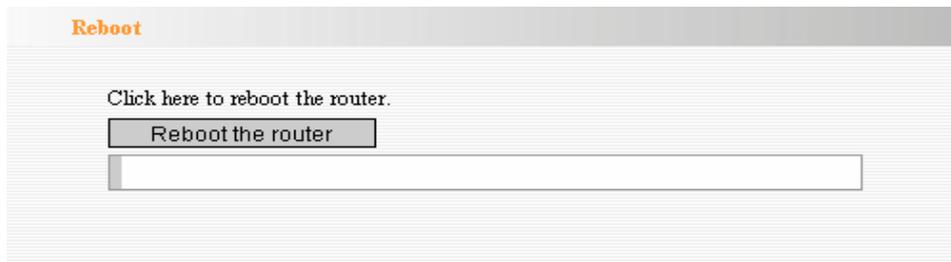
Password: **admin**

IP Address: **192.168.0.1**

Subnet Mask: **255.255.255.0**

**NOTE:** After restoring to default settings, please reboot ZSR4134WE so the settings will take effect.

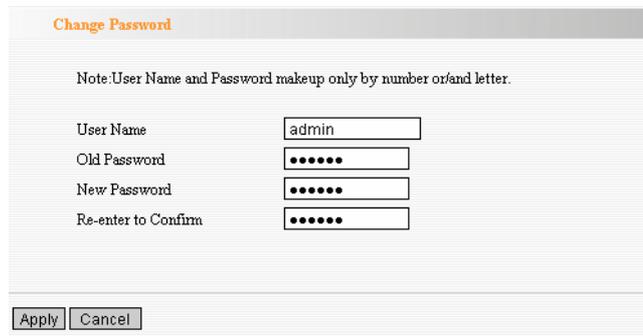
## Reboot



- **Reboot the router:** Click to reboot ZSR4134WE.

## Change Password

The new password should be less than 14 characters.



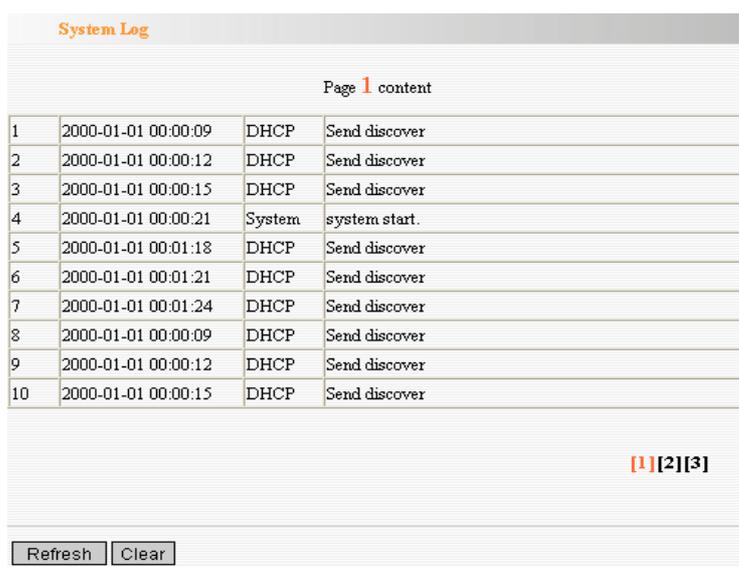
The image shows a 'Change Password' form with a title bar. Below the title bar is a note: 'Note: User Name and Password makeup only by number or/and letter.' There are four input fields: 'User Name' containing 'admin', 'Old Password' with six dots, 'New Password' with six dots, and 'Re-enter to Confirm' with six dots. At the bottom are 'Apply' and 'Cancel' buttons.

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

**NOTE:** It is highly recommended to change the password to secure your network and ZSR4134WE.

## System Log

If the log is over 150 records, it will clear them automatically.



The image shows a 'System Log' table with a title bar. Below the title bar is the text 'Page 1 content'. The table has 10 rows and 4 columns. The columns are: Index, Time, Protocol, and Action. Below the table are 'Refresh' and 'Clear' buttons. In the bottom right corner, there are page navigation links: [1] [2] [3].

Index	Time	Protocol	Action
1	2000-01-01 00:00:09	DHCP	Send discover
2	2000-01-01 00:00:12	DHCP	Send discover
3	2000-01-01 00:00:15	DHCP	Send discover
4	2000-01-01 00:00:21	System	system start.
5	2000-01-01 00:01:18	DHCP	Send discover
6	2000-01-01 00:01:21	DHCP	Send discover
7	2000-01-01 00:01:24	DHCP	Send discover
8	2000-01-01 00:00:09	DHCP	Send discover
9	2000-01-01 00:00:12	DHCP	Send discover
10	2000-01-01 00:00:15	DHCP	Send discover

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

# Appendix 1: Product Features & Specifications

## Features:

- Integrates router, wireless access point, four-port switch and firewall in one
- Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
- MIMO technology utilizes reflection signal to increase 8 times transmission distance of original
- 802.11g standard and reduces the "dead spots" in the wireless coverage area
- Provides 300Mbps receiving rate and 300Mbps sending rate
- Supports WMM for Multimedia Applications with Quality of Service in Wi-Fi® Networks
- Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
- WPS (Wi-Fi Protected Setup) simplify the security setup and management of Wi-Fi networks.
- Supports remote/local Web management
- Supports wireless Roaming technology and ensures high-efficient wireless connections
- Supports wireless SSID stealth mode and MAC address access control
- Supports Auto MDI/MDIX
- Provides system log to record the status of the router
- Supports MAC address filtering, NAT, NAPT
- Supports UPnP and DDNS
- Supports the access control over 30 MAC addresses
- Supports DHCP server/client
- Supports SNTP
- Supports virtual server and DMZ host
- Supports auto wireless channel selection
- Supports WDS function (wireless distribution system)

## Specifications:

<b>General Features</b>	
Standards	IEEE 802.11n (Draft 2.0), IEEE 802.11g, IEEE 802.11b
OS	Windows 2000, XP, Vista; Firefox
User interface	Easy to use user configuration software
Transmit distance	Indoor up to 100M, Outdoor up to 300M
roaming	Support multipoint auto roaming and configuration; Support wireless network environments auto detect.
LED	LAN 1-4/WAN/WLAN/SYS/POWER
Antenna type	Two detachable antennas
<b>RF and baseband Technical Features</b>	
Frequency range	2.4GHz ~ 2.4835GHZ
Radio data rate	11n: 300/150/130/117/104/78/52/39/26/13Mbps 65/58.5/52/39/26/19.5/13/6.5Mbps 11g: 54/48/36/24/18/12/9/6Mbps 11b: 11/5.5/2/1Mbps
Modulation	OFDM, CCK, BPSK, QPSK
Spectrum Spread Technology	DSSS
Transmit output power	11n 20MHz/40MHz: -65dBm 54Mbps: -72dBm 11Mbps: -88dBm
Antenna Gain	(3dBi*2) Detachable
Flash	4M Bytes
System Memory	16M Bytes
RF Power	17-20 dbm peak power 14-17 dbm RMS power
Channels	11 Channels (USA, Canada) 13 Channels (Europe)
Media Access Protocol	WMM
Data security	WPA/WPA2; 64/128-bit WEP; TKIP/AES
<b>Environmental and Physical</b>	
Operation Temp.	0°C ~40°C
Storage Temp.	-20°C~70°C
Operation Humidity	10%~90% RH no condensing

## Appendix 2: Troubleshooting

### **Q1. I Can not login to the Web interface of ZSR4134WE after entering the IP address in the address field?**

- Step 1: check ZSR4134WE if it works well. Once the device is powered on for a few seconds, the SYS indicator on the panel will be turned on. If it is not, please contact us.
- Step 2: check the network cable if it is work and the corresponding indicator is "Always ON". Sometimes, the indicator is "Always ON", but it does not mean it gets through.
- Step 3: Run "Ping" command and check if it can ping ZSR4134WE's LAN IP address 192.168.0.1. If it is OK, please make sure your browser does not access the Internet by proxy server. If the ping fails, you can press the "RESET" button for 7 seconds to restore to default settings. And then repeat the ping operation. If it still does not work, please contact us.

### **Q2. I forget the login password and can not enter the setting page. What can I do?**

Press the "RESET" button for 7 seconds to restore ZSR4134WE to default settings.

### **Q3. The computer connected with ZSR4134WE shows IP address conflict. What can I do?**

Check if there are other DHCP servers in the LAN. If there have, disable them. The default IP address of ZSR4134WE is 192.168.0.1 and please maker sure the address is not occupied by other devices. If there are two computers with the same IP addresses, please modify one.

### **Q4. I can not use E-mail and access the Internet. What can I do?**

It happens in ADSL connection and Dynamic IP users. And you need modify the default MTU value (1492). Please in the "WAN Setting" modify the MTU value with the recommended value as 1450 or 1400.

## **Q5. How to configure and access the Internet via Dynamic IP?**

In Setup Wizard of the Web utility interface, select "Dynamic IP" connection type and click "Save" to activate it. As some ISPs bind the user computer's MAC address, you need to clone ZSR4134WE's WAN MAC address to the binding PC's MAC address. Select "MAC Address Clone" in "Advanced Setting" to input your computer's MAC address and click "Apply" to activate it.

## **Q6. How to share my computer's source with other users in Internet?**

If you want Internet users to access the internal server via ZSR4134WE such as e-mail server, Web, FTP, you can configure the "Virtual Server" to come true.

Step 1: create your internal server, make sure the LAN users can access these servers and know related service port. For example, Web server's port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: in the Router's web click "Virtual Server" and select "Single Port Forwarding".

Step 3: input the external service port given by the Router, for example, 80.

Step 4: input the internal Web service port, for example, 80.

Step 5: Input the internal server's IP address. If your Web server's IP address is 192.168.0.10, please input it.

Step 6: select the communication protocol used by your internal host: TCP, UDP, ICMP.

Step 7: click "Apply" to activate the settings.

## **Q7. How to connect Xbox360 and PlayStation to ZSR4134WE?**

You must obtain a Static IP address from your ISP. Follow the instruction in the CD ROM filename ***Xbox360.pdf*** and setup your game console properly. After you have successfully configured your game console, you have to open ports from the ZSR4134WE to allow two way communications. For more information on port forwarding instruction, please refer this user manual to Chapter 8.