

Wireless LAN Device Series

IEEE 802.11 b/g/n Wireless Router

ZW-N5800 S/C User's Manual

Version. 1 (Draft. 2009.1.9)

Notice

FCC Warning

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the 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.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC 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 or more 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 RF 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. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Shielded interface cables must be used in order to comply with emission limits.

CE Statement

ZINWELL, hereby declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

This device will be sold in the following EEA countries: Austria, Italy, Belgium, Liechtenstein, Denmark, Luxembourg, Finland, Netherlands, France, Norway, Germany, Portugal, Greece, Spain, Iceland, Sweden, Ireland, United Kingdom, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Slovakia, Poland, Slovenia, Bulgaria, Romania.

Preface

This guide is for the experienced user who installs and manages the Zinwell ZW-N5800S product hereafter referred to as the “device”. To use this guide, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of wireless local area networks.

TABLE OF CONTENTS

NOTICE	2
PREFACE.....	4
CH 1. ZW-N5800S INSTALLATION	7
PACKING LIST	7
CONNECTORS, BUTTONS AND LEDS.....	7
HARDWARE INSTALLATION	8
CH 2. FIRST TIME CONFIGURATION.....	9
BEFORE START TO CONFIGURE	9
KNOWING THE NETWORK APPLICATION	10
CH 3. DETAIL CONFIGURATION	10
TCP/IP SETTINGS	10
Configuring WAN Interface.....	10
Static IP	10
DHCP Client (Dynamic IP)	11
PPPoE	11
Configuring LAN Interface.....	13
Advanced LAN Routing	15
WIRELESS SETTINGS.....	17
Basic.....	17
Advanced	19
Security	20
WPS	23
Station List.....	25
FIREWALL	26
MAC/IP/Port Filtering Settings	26
Port Forwarding / Virtual Server Settings.....	27
DMZ Settings.....	28
System Security Settings.....	29
Content Filter	29
MANAGEMENT.....	29
Status.....	29
Statistic.....	30
System Management	31
Upgrade Firmware	31
Save/Reload Settings	32
System Command	32

System Log	32
CHANNEL NUMBER.....	33
SPECIFICATION.....	34

Ch 1. ZW-N5800S Installation

Packing List

Before starting the installation of the device, please make sure the package contains the following items:

- ZW-N5800S AP/Router unit x 1
- Power Adapter x 1
- RJ-45 Cable x 1



Connectors, Buttons and LEDs

Front Panel



From Left to right:

Power LED: The LED lights when power on.

LAN 4/3/2/1: The LED lights when the respective Ethernet port is plugged and flashes when it is transmitting.

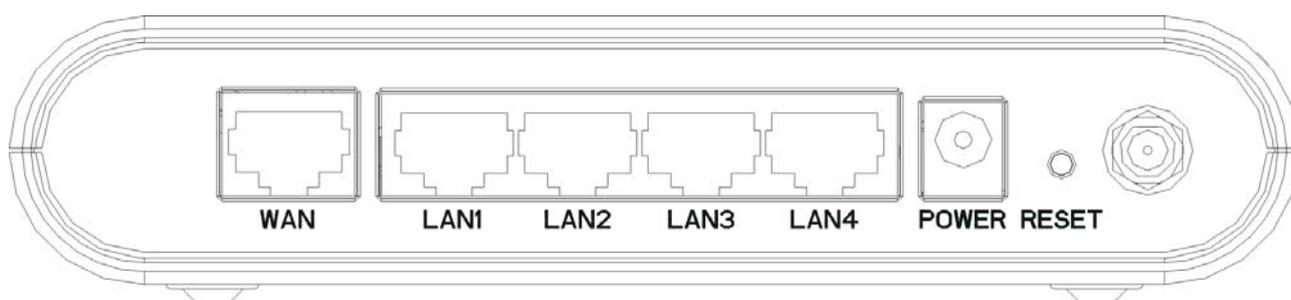
WAN: The LED lights when the Ethernet port is plugged and flashes when it is transmitting.

WLAN: The LED flashes when WLAN is working.

WPS LED: The LED lights when the WPS button is pushed.

WPS Button: Press it to enable PBC (Press Button Communication) for WPS authentication.

Back Panel



From left to right:

WAN: You can connect the Ethernet port from ISP such as ADSL ITU-R, Cable MODEM.

LAN 1/2/3/4: 4 Ethernet ports for the LAN connection.

POWER: Please supply the power in 12V and 1A.

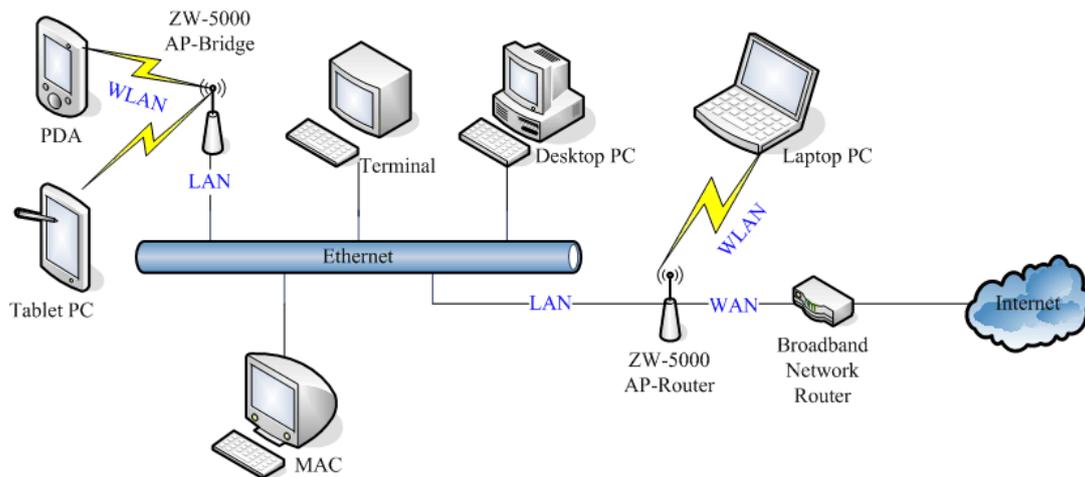
Reset Button: Press Reset button to revert it to factory default.

Antenna port: For ZW-N5800S, there is an antenna port (RP-SMA type) in the left side. Connect the antenna into the port.

For ZW-N5800C, the antenna is fixed to the device. Please adjust the angle of antenna for the better radio receives.

Hardware Installation

Once you check everything from the package, you can start to install the device. You can use the wall mount hole on the bottom of the device to mount the device on the wall, or just put the device on the desktop. The administrator can refer to the figure below while in the process of constructing your WLAN environment.



Ch 2. First Time Configuration

Before Start to Configure

The configuration of this device is through web-browser. To access the configuration interfaces, make sure you are using a computer connected to the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0. For the first time configuration, please login with username: **root** and password: **root**.



Please note that the DHCP server inside the device is default to up and running. Do not have multiple DHCP servers in your network environment, otherwise it will cause abnormal situation.

Knowing the Network Application

The device is a WLAN Access Point and also a Network Address Translator (residential gateway/router). The WLAN stations (Client) can connect to this device and then go through the Internet.

Router mode:

The wired Ethernet (WAN) port is used to connect with ADSL/Cable modem and the wireless NIC is used for your private WLAN. The other wired Ethernet (LAN) port bridges to the private WLAN. The NAT is existed between WAN and WLAN/LAN and all the wireless and wired clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

Ch 3. Detail Configuration

TCP/IP Settings

Configuring WAN Interface

The device supports four kinds of IP configuration for WAN interface, including Static IP, DHCP Client, PPPoE and PPTP/L2TP. You can select one of the WAN Access Types depend on your ISP required. The default WAN Access Type is “Static IP”.

Static IP

You can get the IP configuration data of Static-IP from your ISP. You will need to fill the fields of IP address, subnet mask, gateway address, and one of the DNS addresses.

Item	Description
IP Address:	The Internet Protocol (IP) address of WAN interface provided by your ISP or MIS. The address will be your network identifier besides your local network.
Subnet Mask:	The number used to identify the IP subnet network, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.

Default Gateway:	The IP address of Default Gateway provided by your ISP or MIS. Default Gateway is the intermediate network device that has knowledge of the network IDs of the other networks in the Wide Area Network, so it can forward the packets to other gateways until they are delivered to the one connected to the specified destination.
Primary & Secondary DNS:	The IP addresses of DNS provided by your ISP. DNS (Domain Name Server) is used to map domain names to IP addresses. DNS maintain central lists of domain name/IP addresses and map the domain names in your Internet requests to other servers on the Internet until the specified web site is found.
MAC Clone:	Clone device MAC address to the specify MAC address required by your ISP. Fill my MAC button: You can manually input the MAC Address for MAC clone, or click the button to input the MAC Address of the PC which you are using it to configure the device.

DHCP Client (Dynamic IP)

All IP configuration data besides DNS will obtain from the DHCP server when DHCP-Client WAN Access Type is selected.

Item	Description
Host Name:	Input the host name for the device. This value is optional and not required for the general case.
MAC Clone:	Clone device MAC address to the specify MAC address required by your ISP

PPPoE

When the PPPoE (Point to Point Protocol over Ethernet) WAN Access Type is selected, you must fill the fields of User Name, Password provided by your ISP. The IP configuration will be done when the device successfully authenticates with your ISP.

Item	Description
User Name:	The account provided by your ISP.
Password/ Verify Password:	The password for your account. It is required to input again to verify.

Operation Mode:	The available options are: “Keep Alive”, “On Demand”, and “Manual”. If your ISP charges you with a standard monthly fee, you can select “Keep Alive” to keep a continue connection. If your ISP charges you by a minute usage plan, you can select the “On Demand” or “Manual” for the connection if necessary. When the WAN network is idle in “On Demand” mode, the WAN will disconnect. You can also setup the idle time for On Demand mode. For the “Manual” mode, you can click “Connect” in the status page to connect the WAN and then click “Disconnect” to disconnect.
Redial Period	When selecting the “Keep Alive” mode, the redial time can be set in this field. It will redial the connection to keep it online. The default value is 60 seconds.
On demand idle time	When selecting the “On Demand” mode, the idle time can be set in this field. If the network is idle more than this time, the WAN will disconnect.
MAC Clone	Clone device MAC address to the specify MAC address required by your ISP.

Configuring LAN Interface

ZW-N5800 Series

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.2.254
Subnet Mask	255.255.255.0
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:05:9E:8D:55:7A
DHCP Type	Server ▼
Start IP Address	192.168.2.1
End IP Address	192.168.2.100
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
Lease Time	86400
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

Item	Description
IP Address	This is the IP Address for this device. You can login this IP Address via LAN/WLAN, and you can change it if you want to.
Subnet Mask	This is the subnet mask for the LAN. The default value is "255.255.255.0".
LAN2	The secondary LAN can be enabled for the special application such as dynamic routing with another domain of network.
LAN2 IP Address	This is the IP Address for the secondary LAN interface.
LAN2 Subnet Mask	This is the subnet mask for the secondary LAN.
MAC Address	The MAC Address of LAN is showed in this field.
DHCP Type	You can select to enable DHCP server. When enabling the DHCP server, you must setup the information below.
Start IP Address	This is the first IP Address of the IP pool which the server assigns the IP Address from.
End IP Address	This is the last IP Address of the IP pool.

Subnet mask	This is the subnet mask of this domain. The default value is "255.255.255.0".
Primary DNS Server	This is the primary DNS server for the LAN PCs.
Secondary DNS Server	This is the second DNS server for the LAN PCs.
Default Gateway	This is the default gateway for the LAN PCs.
Lease Time	This is the DHCP lease time. When it is short, the IP release/renew of the LAN will be faster but the network congestion will be more.
Statically Assigned	You can manually assign the IP Address to the certain PCs. Enter the MAC Address and IP Address in the table.
802.1d Spanning Tree:	Enable this function to prevent the broadcast storm in the LAN.
LLTD	Enable this function to support LLTD (Link Layer Topology Discovery) for Windows Vista. It shows the status of connection in the Windows Vista.
IGMP Proxy	Enable this option to provide the relay of Multicast.
UPNP	Enable this option to active the function. The UPNP application such as MSN messenger detects and setup through UPNP.
DNS Proxy	Enable this option to perform DNS relay. The hosts in the LAN can set the DNS server to this device, and this device forwards the DNS request to the remote DNS server in the WAN. The built-in DNS catch in the device can also help to check the domain name. To match this function, the primary DNS server should be set to the LAN to utilize this function.

ZW-N5800 Series

- Site contents
- TCP/IP Settings
 - WAN
 - LAN
 - DHCP clients
 - Advanced Routing
 - Wireless Settings
 - Firewall
 - Management

DHCP Client List

You could monitor DHCP clients here.

MAC Address	IP Address	Expires in
00:13:A9:F2:AF:53	192.168.2.1	23:37:31
00:1B:77:96:4F:51	192.168.2.2	23:36:15

Advanced LAN Routing

User can set the routing information let the Router knows what routing is correct also it can not learn automatically through other means.

ZW-N5800 Series

Static Routing Settings

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

Add a routing rule

Destination:

Range: Host ▾

Gateway:

Interface: LAN ▾

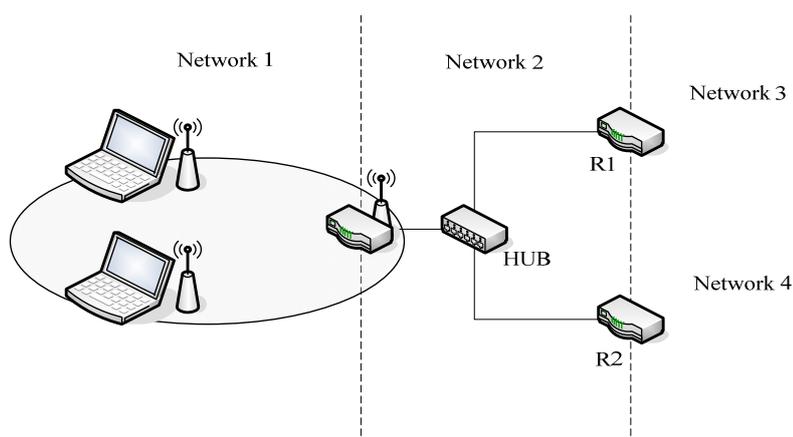
Comment:

(The maximum rule count is 10.)

Apply

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
3	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN	



For example, if user wants to link the Network 3 and Network 4 separately from Network 1 that Routing Table configuration as below:

1. Enter IP Address of Network 3, Subnet Mask and IP Address of Router (R1) in Default

Gateway field final click Apply Change button.

2. Enter IP Address of Network 4, Subnet Mask and IP Address of Router (R2) in Default Gateway field final click Apply Change button.
3. In current Routing table there have two routings for Network 3 and Network 4.

Static Routing Settings:

Add a routing rule table:

Item	Description
Destination	Input the destination IP domain.
Range	Choose the range from Host and Net. When selecting "Net", the Netmask option is opened for configuration.
Netmask	Enter the network mask for this route.
Gateway	Enter your gateway for this route.
Interface	WAN, LAN, Custom
Comment	Enter your note about this route.

Current Routing table in the system:

Current Routing table in the system:									
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1 <input type="checkbox"/>	192.168.3.0	255.255.255.255	192.168.2.254	7	0	0	0	LAN (br0)	
2	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
3 <input type="checkbox"/>	192.168.4.0	255.255.255.255	172.1.1.1	7	0	0	0	WAN (eth2.2)	
4 <input type="checkbox"/>	192.168.10.0	255.255.255.255	192.168.2.254	7	0	0	0	LAN (br0)	
5 <input type="checkbox"/>	192.168.4.0	255.255.255.0	192.168.2.254	3	0	0	0	LAN (br0)	
6	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	
7	172.1.1.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN (eth2.2)	
8	0.0.0.0	0.0.0.0	172.1.1.254	3	0	0	0	WAN (eth2.2)	

This table lists the current routes of the device. You can select the number the static route and click "Delete" to delete the route. Click the "Reset" button to clear the selected check box.

Wireless Settings

Basic

Basic Settings	
Item	Description
Radio On/Off	Click the "RADIO OFF" button to turn off the radio. Click it again to turn on the radio.
Network Mode	The available options are "11b/g mixed mode", "11b only", "11g only" and "11b/g/n mixed mode". We recommend selecting the default value "11b/g/n mixed mode".
Network Name (SSID)	The SSID, which is also called ESSID is a unique identifier that wireless networking devices use in order to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters.
Broadcast Network Name (SSID)	Disable this function to hide SSID. With hidden SSID, the AP can't be scanned and the wireless client must input SSID manually to associate this AP.
AP Isolation	The device supports isolation function. If you are building a public Wireless Network, enable this function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can't see each other.
BSSID	The BSSID is displayed in this field.
Frequency (Channel)	Click the drop down box to select the radio channel. Select the unused channel to prevent the radio overlapping. If you are not sure which channel is used, select "AutoSelect" to let the device to detect and select the available channel.

HT Physical Mode	
Item	Description
Operating Mode	<p>Default: Mixed (Mixed, Green Field).</p> <p>Mixed mode: In this mode the device transmits the packets with preamble compatible legacy (802.11g), so they can be decoded by legacy devices. The device receives and decodes both Mixed Mode packets and legacy packets.</p> <p>Green Field mode: the device transmits HT packets</p>

	without legacy compatible part. But the device receives and decodes both Green Field and legacy packets.
Channel Bandwidth	This option only works when selecting Band mode in 802.11b/g/n Mixed mode. Click the radio button to choose between 20 MHz or 20/40MHz. This option affects the Phy data rate of radio. Please refer to the table below
Guard Interval	The 11n device inserts the Guard Interval into the signal. You can choose the interval between “Long” and “Auto”. This option affects the Phy data rate of radio. Please refer to the table below.
MCS	It is Modulation Coding Scheme. The available options are “Auto, 0, 1, ..., 32”. It changes the modulation of this device and effect the maximum Phy data rate. We recommend “Auto” setting. For the details, please refer to the table below.
Reverse Direction Grant (RDG)	This is the 11n performance parameter. Enable it if needed.
Extension Channel	The “20/40” bandwidth mode uses 5 channels. For example, selecting channel 7 and you can select 3 or 11 for extension channel. Choose the unused channel for the extension channel.
Aggregation MSDU (A-MSDU)	The multiple HT packets can be transmitted with single ACK reply packet. Enable it to apply this function and reduce the network congestion.
Auto Block ACK	It is another aggregation technique which prevents sending ACK in the communication to increase the throughput. If this option is enabled, the device will activate this function when transmitting massive data.
Decline BA Request	Enable this option to decline the Block ACK request addressed by the other devices.

The table below shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Data Rate Mbps MCS	Bandwidth = 20MHz		Bandwidth = 40MHz	
	Short Guard Interval	Long Guard Interval	Short Guard Interval	Long Guard Interval
0 (1S)	7.2	6.5	15	13.5
1	14.4	13	30	27
2	21.7	19.5	45	40.5
3	28.9	26	60	54
4	43.3	39	90	81
5	57.8	52	120	108
6	65	58.5	135	121.5

7	72.2	65	150	135
8 (2S)	14.4	13	30	27
9	28.9	26	60	54
10	43.3	39	90	81
11	57.8	52	120	108
12	86.7	78	180	162
13	115.6	104	240	216
14	130	117	270	243
15	144.4	130	300	270
32	Not Supported	Not Supported	6.7	6

MCS: Modulation Coding Scheme

MCS=0~7 (1S, One Tx Stream)

MCS=8~15 (2S, Two Tx Stream)

MCS 32: BPSK

Advanced

Advanced Wireless	
Item	Description
BG Protection Mode	Default: Auto. You can select the other options including On and Off. The B/G protection technology is CTS-To-Self. It will try to reserve the throughput for 11g clients from 11b clients connecting to the device as AP mode.
Basic Data Rates	Choose the ACK rate for this device in B/G mode.
Beacon Interval	Beacons are the packets sending by Access point to synchronize the wireless network. The beacon interval is the time interval between beacons sending by this unit in AP or AP+WDS mode. The default and recommended beacon interval is 100 milliseconds.
Data Beacon Rate (DTIM)	This is the Delivery Traffic Indication Map. It is used to alert the clients that multicast and broadcast packets buffered at the AP will be transmitted immediately after the transmission of this beacon frame. You can change the value from 1 to 255. The AP will check the buffered data according to this value. For example, selecting "1" means to check the buffered data at every beacon.
Fragment Threshold	The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of

	radio interference. This function will help you to improve the network performance.
RTS Threshold	The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.
TX Power	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> TX Power <input style="width: 50px;" type="text" value="100"/> (range 1 - 100, default 100) </div> The default TX power is 100%. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power. For example, input 80 to apply 80% Tx power.
Short Preamble	Default: Disable. It is a performance parameter for 802.11 b/g mode and not supported by some of very early stage of 802.11b station cards. If there is no such kind of stations associated to this AP, you can enable this function.
Short Slot	For a WLAN network with 802.11g/n devices, the time slot can be set short to increase the throughput. Disable this option for the backward compatibility with 802.11b device.
Tx Burst	The device will try to send a serial of packages with single ACK reply from the clients. Enable this function to apply it.

Wi-Fi Multimedia	
Item	Description
WMM Capable	Choose "Enable" to enable WMM function.
WMM Parameter	Click the button to edit the WMM parameter.

Multicast-to-Unicast Converter	
Item	Description
Multicast-to-Unicast	Enable/Disable to enable this function.

Security

Wireless Security/Encryption Settings

Select SSID	
Item	Description
SSID choice	Choose the ESSID to configure the security setting.

Wireless Security/Encryption Settings	
Item	Description
Security Mode	Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 PSK, WPA/WPA2, 802.1X.

The available options are showed according to the numbers of the BSSID in the Basic Setting. Each SSID can setup different encryption type. For example, set up 4 BSSID and 4 sets of security shows on this page:

- Security Mode: Choose one as the wireless authentication among the following types: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2-PSK, WPA/WPA2, and 802.1 X.
- Encryption Type: Select one for the encryption type. The options vary depending on the Authentication mode. The corresponding options shows below.

Authentication	Encryption type	Key option
Open/Shared/WEP Auto	WEP	Default Key ID, Key content of Key 1/2/3/4
WPA/WPA2-PSK (Pre-Shared Key)	TKIP, AES, TKIP/AES	Pass Phrase (8-32 bytes), Key Renewal Interval
WPA/WPA2 Enterprise	TKIP, AES, TKIP/AES	Radius Server Network/Address/Port/Key/Session timeout

WEP Encryption Setting

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be as same as each client in your wireless network.

- Authentication Type: Open, Shared and Auto. When choose “Open” or “Shared”, all of the clients must select the same authentication to associate this AP. If select “WEP Auto”, the clients don’t have to use the same “Open” or “Shared” authentication. They can choose any one to authenticate.
- Default Key ID: Select whether the Key ID as the default Key.
- Key 1/2/3/4: Select “ASCII” or “Hex” and then type the key in the text field.
 - 64-bit WEP Encryption : 64-bit WEP keys are as same as the encryption method of 40-bit WEP. When input 10 hexadecimal digits (0-9, a-f or A-F) or 5 ACSII chars as the key, it is using 64-bit WEP encryption.

- 128-bit WEP Encryption : 128-bit WEP keys are as same as the encryption method of 104-bit WEP. When input 26 hexadecimal digits (0-9, a-f or A-F) or 10 ACSII chars, it is using 128-bit WEP encryption.

WPA Authentication Mode

This device supports six WPA modes including WPA-PSK (Pre-Shared Key), WPA, WPA2-PSK, WPA2 and additional WPA/WPA2 PSK and WPA/WPA2 mixed mode. For individual and residential user, it is recommended to select WPA-PSK or WPA2-PSK to encrypt the link without additional RADIUS server. This mode requires only an access point and client station that supports WPA-PSK. For WPA/WPA2, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.

- **WPA/WPA2-PSK:**

- **Pass Phrase:**

Option: Pass Phrase (8-32bytes). This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ACSII chars.

- **Key Renewal Interval:**

The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds and you can adjust the time interval.

- **WPA/WPA2:**

When selecting WPA/WPA2, you have to add user accounts and the target device to the RADIUS Server. In the device, you need to specify the Server Network, Server address, Server Port and Server Key of the target RADIUS server.

- **WPA Algorithms:** TKIP, AES, TKIP/AES. Select the encryption type. When selecting TKIP/AES, the client can use whether TKIP or AES for the authentication.

- **Pre-Authentication Support option:** This option only appears when selecting WPA2 or WPA/WPA2 as the authentication mode. Enable it to use this function.

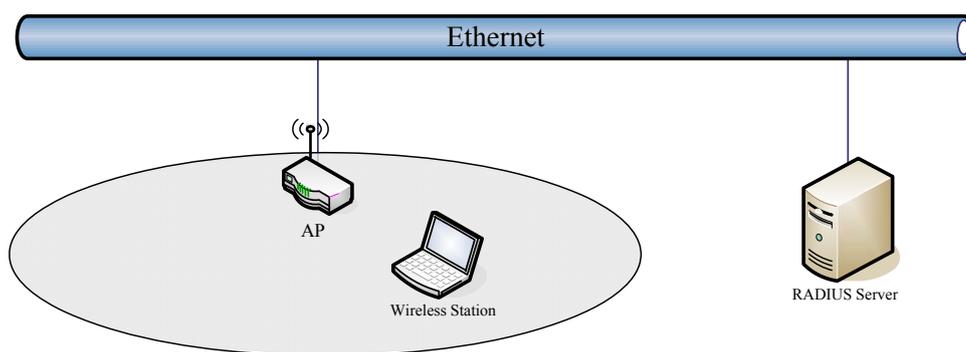
- **Radius Server setting:**

- **IP Address:** Input the IP Address of the Radius server.

- **Port:** Input the port of the Radius server. The default port is 1812.

- **Shared Secret:** Input the Authentication Key.

- **Session Timeout:** Input the maximum idle time for this connection.



Access Policy

For each SSID, the Access Policy can be selected and setup. The policy includes “**Reject**” and “**Allow**”. The Reject policy rejects the station according to the MAC table in the policy configuration, and let the other stations to connect. The allow policy performs reversely.

Add a station MAC: Key in station MAC Address in the text field. The valid format of the MAC Address is “00:11:22:33:44:55”. The station MAC Address can be found on the label or configure utility of the WLAN card. For deleting one record in the table, click the “Del” button of the record.

Access Policy	
Policy	Reject ▾
Del 00:11:33:44:55:66	Del 88:99:00:22:aa:bb
Add a station Mac:	<input type="text"/>

WPS

This function helps to establish the Wi-Fi security. For AP mode, it can be setup one WPS method including PIN (Personal Identification Number) and PBC (Push Button Communication).

To begin the WPS progress, the WLAN security must be setup first. Please setup one among WPAPSK, WPA2PSK, WPA/WPA2PSK and then apply WPS setting.

PIN: query the PIN code in the utility of WLAN client, and then enter it in the PIN field. The Wi-Fi link between the WLAN client and the device should be encrypted.

PBC: Select PBC, and then you can begin the PBC process. Press the PBC button in the front panel can also trigger this process. Press or click the PBC button on the WLAN client to finish the communication. You can press the PBC button on the WLAN client first and then click the PBC button on this device to establish the encryption.

The options and the information fields are showed below.

WPS Config	
Item	Description
WMM Capable	Select to enable this function.

WPS Summary	
Item	Description
WPS Current Status	It shows the current status of the WPS process.
WPS Configured	It indicated whether the WPS is configured.
WPS SSID	It is the first SSID of the device.
WPS Auth Mode	It indicates the authenticate mode of this device. It can be configured in the wireless security page.
WPS Encryp Type	It indicates the encryption method of this device. Like WPS authentication mode, it can be configured in the wireless security page.
AP PIN	It shows the current PIN number of this device.
Reset OOB button	Press this button to reset the WPS of this device. The AP PIN number will be changed.

WPS Progress	
Item	Description
WPS mode	Choose to use PIN (Personal Identification Number) or PBC (Push Button Communication).
PIN	Input the 8-digit PIN of client.

WPS Config

WPS:	Enable ▾
<input type="button" value="Apply"/>	

WPS Summary

WPS Current Status:	Configured
WPS Configured:	Yes
WPS SSID:	ZW-N5900-FAE
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	TKIP
AP PIN:	67127719
<input type="button" value="Reset OOB"/>	

WPS Progress

WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN	<input style="width: 100%;" type="text"/>
<input type="button" value="Apply"/>	

WPS Status

WSC Success

Station List

ZW-N5800 Series

- Site contents
- TCP/IP Settings
- Wireless Settings
 - Basic
 - Advanced
 - Security
 - WPS
 - Station List
- Firewall
- Management

Station List

You could monitor stations which associated to this AP here.

MAC Address	Aid	PSM	MimoPS	MCS	BW	SIGI	STBC
00:1B:77:96:4F:51	1	0	0	7	20M	0	0

In the Station list, the information of associated clients is displayed.

Firewall

MAC/IP/Port Filtering Settings

You can setup the filter to block the malicious traffic from Internet or local area network.

Basic Settings	
Item	Description
MAC/IP/Port Filtering	Enable or Disable the filtering. When enable the setting, all the traffic flow from WAN to LAN will apply to the rules below.
Default Policy	The packet that don't match with any rules would be: "Accepted/Dropped". Select "Accepted" and only the rule matching traffic can pass through this device. Select "Dropped" and the rule matching traffic will be dropped.

MAC/IP/Port Filter Settings	
Item	Description
MAC Address	This is the MAC Address applying to this rule.
Dest. IP Address	This is the range of the destination IP Address.
Source IP Address	This is the range of the source IP Address.
Protocol	Select one protocol to apply to this rule. The available options are "None, TCP, UDP and ICMP".
Dest. Port Range	This is the range of the destination port.
Source Port Range	This is the range of the source port.
Action	This is the policy of this rule. The available options are "Drop and Accept".
Comment	You can add your note for this rule.

Current MAC/IP/Port filtering rules in system:

The current configured rules are listed in this table. To delete a rule, check the box in front of the rule and click "Delete Selected" button.

Current MAC/IP/Port filtering rules in system:								
No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment
1	<input type="checkbox"/>	00:22:44:55:66:77	-	-	-	-	Accept	
Others would be dropped								
<input type="button" value="Delete Selected"/>								

Port Forwarding / Virtual Server Settings

This function allows you to redirect common network services to a specific machine behind the NAT firewall. For the certain application, like on line game or web/mail server, it is necessary to redirect the port to the PC/server on the private local network behind the device's NAT firewall.

Virtual Server Settings	
Item	Description
IP Address	Input the LAN IP Address of the server.
Port Range	This is the range of the port for this server.
Protocol	Choose the protocol for this rule. It can be UDP, TCP or both.
Comment	You can add your note about this rule.

For looking for the well-known ports for all kinds of application, please refer to the URL: <http://www.iana.org/assignments/port-numbers>.

The configured rules are listed in the table. If you want to delete any rule, check the box in front of the rule and click “Delete Selected”.

Virtual Server Settings

Virtual Server Settings: Enable ▾

IP Address:

Port Range: -

Protocol: TCP&UDP ▾

Comment:

(The maximum rule count is 21.)

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	192.168.2.3	80 - 80	TCP + UDP	http

DMZ Settings

A DeMilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. So that all inbound packets will be redirected to the computer you set. Generally it is not recommended to setup DMZ due to fully exposed the PC/server to the Internet; but for some application using uncertain incoming ports such as Internet games, it is could be useful to setup DMZ for the application.

Item	Description
DMZ Settings	Enable this setting, and then click "Apply" button to save the changes.
DMZ IP Address	Input the IP Address of the computer that you want to expose to Internet.

System Security Settings

Remote management via WAN: you can select “Deny” or “Allow” to decide whether the WAN of the device can be accessed. If it isn’t accessible, then you can’t open the web page from WAN.

Ping from WAN Filter: If you allow the WAN interface to reply ping, then you can enable it.

SPI Firewall: Enable this option to activate the Stateful Packet Inspection firewall.

Content Filter

Webs Content Filter

Filters: Proxy, Java, ActiveX. Check the box to use the respective function.

Webs URL Filter Settings

Add a URL filter: Input the URL to filter and click “Add” button to apply.

Current Webs URL Filter Settings: It shows the current URL records in the filter. To delete one record, check it and then click the delete button.

For example, input the URL <http://www.zintech.com.tw/modules/product/index.php> to the filter to block it, so this URL can’t be browsed by the PC in the LAN. Check the URL and click “delete” button to delete this URL.

Webs Host Filter Settings

Add a Host (keyword) Filter: Input the URL of the host to the filter. For example, input www.zintech.com.tw to the filter, so the host can’t be browsed by the PC in the LAN.

Current Website Host Filters: It shows the current records in the filter. To delete one record, check it and then click the delete button.

Management

Status

System Info

Item	Description
Model	It shows the model name of the device.
Firmware Version	It shows the version of firmware on this device.
System Time	It indicates the time on this device. If the NTP client is

	enabled, the time will sync with the NTP server.
Operation Mode	It shows the operation mode of this device.

Internet Configurations

Item	Description
Connected Type	It shows the WAN type such as DHCP, Static IP, PPPoE, etc.
WAN IP Address	It shows the IP Address of the WAN interface.
Subnet Mask	This is subnet mask of the WAN interface.
Default Gateway	It is the default gateway of WAN interface.
Primary Domain Name Server	It shows the primary DNS server.
Secondary Domain Name Server	It shows the current secondary DNS server.
MAC Address	This is the MAC Address of the WAN interface.

Local Network

Item	Description
Local IP Address	This is the IP Address of the LAN interface.
Local Netmask	This is the Netmask for the LAN.
MAC Address	This is the MAC Address of the LAN interface.

Wireless Information

Item	Description
Mode	This is the wireless mode for the device such as AP, client mode.
Band	It shows the current radio mode such as "B+G+N", "B+G", "B only" and "G only".
SSID	It shows the SSID of this device.
Channel	It shows the current channel of the radio.
Encryption	It indicates the encryption type for the radio.
Bssid	It is the current BSSID of the radio. In this device, it is also the MAC Address of the WLAN interface.
Associated Clients	The number of associated WLAN clients show in this field.
Driver Vision	This is the driver version.

Statistic

Memory

Item	Description
Memory total	This is the total memory size for this device.
Memory left	The available memory size shows in this field.

WAN/LAN

The information below shows the transmit status.

WAN Rx packets, WAN Rx bytes, WAN Tx packets, WAN Tx bytes, LAN Rx packets, LAN Rx bytes, LAN Tx packets, LAN Tx bytes.

All interfaces

The information likes “Rx Packet”, “Rx Byte”, “Tx Packet” and “Tx Byte” shows the status of all interface including “eth2, lo, ra0, ra1, ra2, ra3, wds0, wds1, wds2, wds3, eth2.1, eth2.2, br0”

System Management

Administrator Settings

Enter the account for login the web interface.

Account: enter the name for login. The default name is “root”.

Password: enter the password for login. The default password is “root”.

NTP Settings

Current Time: The current time on the device shows in this field. Click “Sync” button to sync the time with NTP server.

Time Zone: Select local time zone.

NTP Server: Input the NTP server address. If you are not sure about the local NTP server address, you can input pool.ntp.org.

NTP synchronization (hours): This is the time interval of NTP synchronization. The range is 1-300 hours. It is the necessary field for NTP setting and please input it to apply.

DDNS

You can setup the dynamic domain name for this device to help connect to this device from Internet. You have to register a DDNS account before setup this option.

Dynamic DNS Provider: please select one DDNS provider among the available options: “Dyndns.org, freedns.afraid.org, www.zoneedit.com, www.no-ip.com”.

Account: enter your account for DDNS.

Password: enter your password for DDNS.

DDNS: enter your dynamic domain name in this field.

Reboot System

Click the button to reboot the device.

Upgrade Firmware

This page provides the firmware upgrade function. Click the browse button to browse the

file and click “open” button to select the file. The upgrade process takes about 1 minute and do not power off the device during this period.

Save/Reload Settings

In this page, you can export the setting, import the setting or load the factory default.

Export Settings:

To export the settings, click “Export” button to open or save the configuration. In the pop up window, click “Open” to open the configuration. You can read the configuration in the next page. Click “Save” to save the configuration file. The file extension is “.dat”.

Import Settings:

To import the settings, click “Browse” to browse the file, and then click “Import” to import the setting file.

Load Factory Defaults:

Click “Load Default” button to reset the device to factory default. All users’ settings will be cleared.

System Command

The linux command can be input in this field. It is recommended to not to use this function unless the experts.

System Log

The system log shows in this window. For technical support, you may need to copy and save the log to text file and send it to the technical service. Click “Refresh” button to refresh the page or “Clear” button to clear the log.

Channel Number

The following table is the available frequencies (in MHz) for the 2.4 GHz radio:

Channel No.	Frequency	Country Domain
1	2412	Americas, EMEA, Japan, and China
2	2417	Americas, EMEA, Japan, and China
3	2422	Americas, EMEA, Japan, Israel, and China
4	2427	Americas, EMEA, Japan, Israel, and China
5	2432	Americas, EMEA, Japan, Israel, and China
6	2437	Americas, EMEA, Japan, Israel, and China
7	2442	Americas, EMEA, Japan, Israel, and China
8	2447	Americas, EMEA, Japan, Israel, and China
9	2452	Americas, EMEA, Japan, Israel, and China
10	2457	Americas, EMEA, Japan, and China
11	2462	Americas, EMEA, Japan, and China
12	2467	EMEA and Japan
13	2472	EMEA and Japan
14	2484	Japan only

*: EMEA (Europe, the Middle East and Africa).

The available channel is set by the factory according to the region of distribution and can't be changed by user. For example, the available channel of the American model is from ch1 to ch11.

Specification

Frequency Range	2.4~2.4835GHz
802.11b TX power	17dBm ± 1dB@11Mbps
802.11g TX power	14dBm ± 1dB@54Mbps
802.11n TX power	14dBm ± 1dB@150Mbps
802.11b RX sensitivity	-89dBm ± 2dB@11Mbps
802.11g RX sensitivity	-74dBm ± 2dB@54Mbps
802.11n RX sensitivity	-66dBm ± 2dB@150Mbps
Data Rate	802.11b: 11, 5.5, 2, 1Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9, 6Mbps 802.11n (20MHz): MCS0~7, Up to 72Mbps 802.11n (40MHz): MCS0~7, Up to 150Mbps
Standards	WLAN: IEEE 802.11 b/g, IEEE 802.11n Draft 4.0 LAN: IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.1d
Operation Mode	Wireless Access Point mode
Security	Password Protection, MAC filtering, Hidden SSID Broadcasting, 64/128-bit WEP Encryption, SPI (Stateful Packet Inspection) firewall, WPS Push button and PIN code, WPA for 802.1x and WPA-PSK, WPA2 / IEEE 802.11i
Antenna type	1T1R 2dBi ZW-N5800S: RP-SMA external antenna x1 ZW-N5800C: fixed antenna x1
Operating Environment	Temperature 0~60℃ Humidity 10~90%(non-condensing)
Power Consumption	12Vdc +/- 5%, 1A
Dimension	146 x 101.5 x 33.5 mm
Software Feature	WLAN: b/g protection, Block WLAN Relay, Tx Burst, Tx Short Preamble, Packet Aggregation, HT Operation mode, HT Guard Interval, MAC ACL. WAN: MAC Clone, Static IP/DHCP/PPPoE LAN: 802.1d Spanning Tree, DHCP server. Routing: Static Route Firewall: NAT, Port Filtering, IP Filtering, MAC Filtering, Port Forwarding, DMZ, URL Filter, Host Filter. Management: DDNS, NTP Client, System log, Upload

	config file, Firmware upgrade, password management.
Certification	CE, FCC, NCC, TELEC, BSMI, VCCI, Anatel, Wi-Fi compliant