

# User's Guide

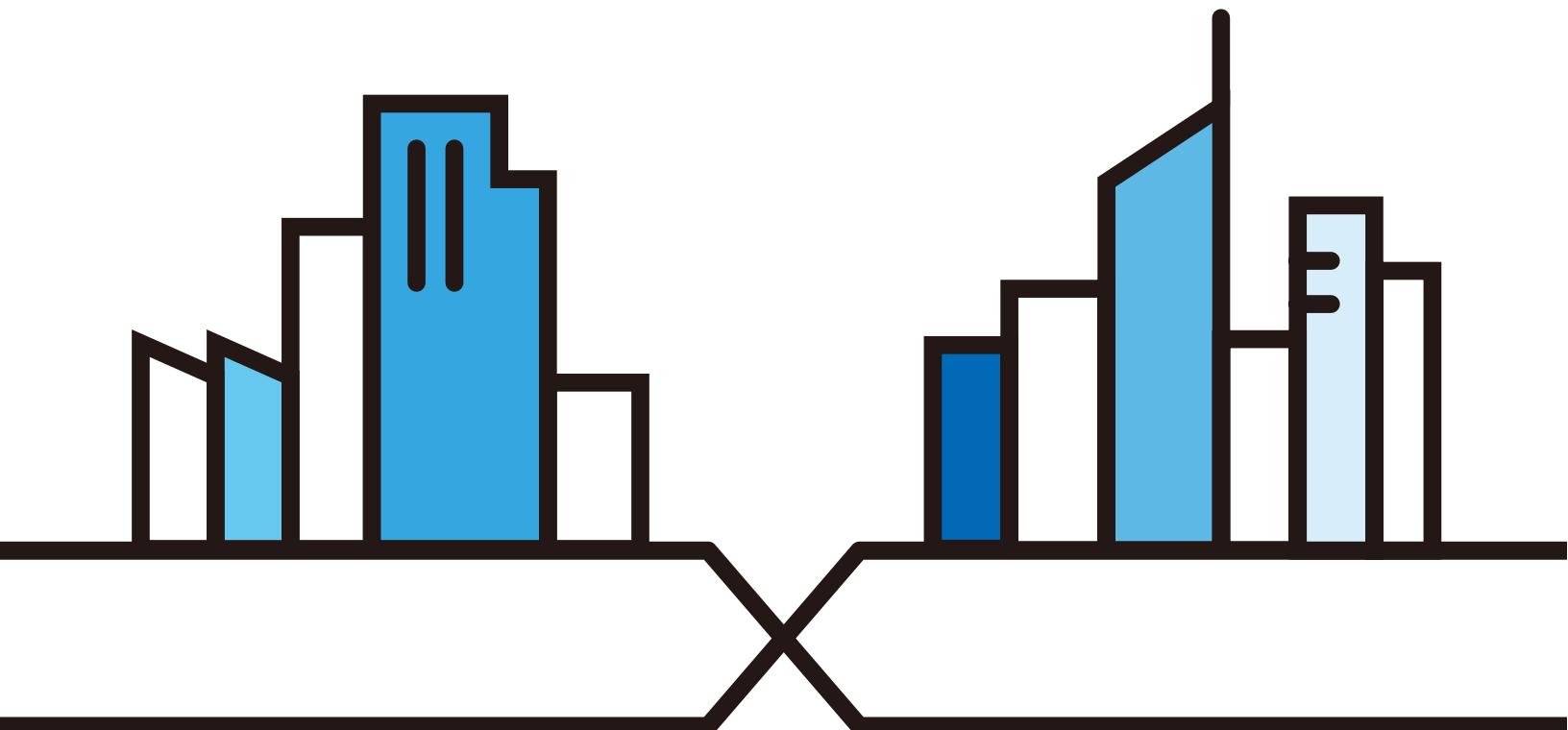
## WAH7706

LTE Portable Router

### Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

Version 1.10 Edition 2, 02/2017



---

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

This is a User's Guide for a system managing a series of products. Not all products support all features. Menushots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

## **Related Documentation**

- Quick Start Guide

The Quick Start Guide shows how to connect the managed device.

- More Information

Go to [support.zyxel.com](http://support.zyxel.com) to find other information on the WAH7706.



# Contents Overview

<b>User's Guide .....</b>	<b>7</b>
Introduction .....	8
The Web Configurator .....	12
<b>Technical Reference .....</b>	<b>19</b>
Home .....	20
Internet .....	24
Wi-Fi .....	31
Router .....	50
Applications .....	59
System .....	66
Troubleshooting .....	76

# Table of Contents

Contents Overview .....	3
Table of Contents.....	4
Part I: User's Guide.....	7
<b>Chapter 1</b>	
Introduction .....	8
1.1 Overview .....	8
1.2 Ways to Manage the WAH7706 .....	8
1.3 Good Habits for Managing the WAH7706 .....	9
1.4 Hardware Connections .....	9
1.5 Turn on/off the WAH7706 .....	9
1.6 OLED Display and Icons .....	9
1.7 Resetting the WAH7706 .....	11
1.7.1 How to Use the Physical Reset Button .....	11
<b>Chapter 2</b>	
The Web Configurator.....	12
2.1 Overview .....	12
2.2 Login Accounts .....	12
2.3 Access .....	12
2.4 Navigating the Web Configurator .....	14
2.4.1 Title Bar .....	15
2.4.2 Navigation Panel .....	15
Part II: Technical Reference.....	19
<b>Chapter 3</b>	
Home.....	20
3.1 Overview .....	20
3.2 Home .....	20
3.3 Setup Wizard .....	21
3.3.1 Internet .....	21
3.3.2 Wi-Fi .....	22

<b>Chapter 4</b>	
Internet.....	24
4.1 Overview .....	24
4.1.1 What You Can Do in this Chapter .....	24
4.2 Internet Status Screen .....	25
4.3 PIN Settings Screen .....	26
4.4 APN Configuration Screen .....	27
4.5 Network Selection Screen .....	28
4.6 Data Usage/Statistic Screen .....	28
<b>Chapter 5</b>	
Wi-Fi.....	31
5.1 Overview .....	31
5.1.1 What You Can Do in this Chapter .....	31
5.1.2 What You Need to Know .....	32
5.2 Wi-Fi Status Screen .....	32
5.3 Wi-Fi Settings Screen .....	33
5.4 MAC Filter Screen .....	35
5.5 WPS Screen .....	37
5.6 Technical Reference .....	38
5.6.1 Wireless Network Overview .....	38
5.6.2 Additional Wireless Terms .....	40
5.6.3 Wireless Security Overview .....	40
5.6.4 Signal Problems .....	42
5.6.5 WiFi Protected Setup (WPS) .....	43
<b>Chapter 6</b>	
Router.....	50
6.1 Overview .....	50
6.1.1 What You Can Do in this Chapter .....	50
6.2 LAN IP Screen .....	50
6.3 DHCP Server Screen .....	51
6.4 DNS Settings Screen .....	53
6.5 Connected Devices Screen .....	53
6.6 IPv4/Port Filter Screen .....	54
6.7 IPv6/Port Filter Screen .....	55
6.8 URL Filter Screen .....	56
6.9 IP/Port Forwarding Screen .....	57
<b>Chapter 7</b>	
Applications.....	59
7.1 Overview .....	59
7.1.1 What You Can Do in this Chapter .....	59

---

---

## Table of Contents

---

7.2 Contact List Screen .....	59
7.3 SIM Contacts Screen .....	60
7.4 Contacts Settings Screen .....	61
7.5 New SMS Screen .....	61
7.6 Inbox Screen .....	62
7.7 Outbox Screen .....	63
7.8 Draft Screen .....	63
7.9 SIM SMS Screen .....	64
7.10 File Sharing Screen .....	65
<b>Chapter 8</b> <b>System.....</b>	<b>66</b>
8.1 Overview .....	66
8.1.1 What You Can Do in this Chapter .....	66
8.2 System Information Screen .....	66
8.3 User Account Screen .....	67
8.4 Settings Profile Screen .....	68
8.4.1 Reset Settings .....	69
8.4.2 Save Current Settings .....	69
8.4.3 Import & Export Settings Profile .....	70
8.5 Firmware Upgrade Screen .....	70
8.6 Time Settings Screen .....	71
8.7 Power Saving Screen .....	73
8.8 System Log Screen .....	73
<b>Chapter 9</b> <b>Troubleshooting.....</b>	<b>76</b>
9.1 Overview .....	76
9.2 Power, and Hardware Installation .....	76
9.3 WAH7706 Access and Login .....	76
9.4 Internet Access .....	78
9.5 Wireless Connections .....	79
9.6 Getting More Troubleshooting Help .....	79
Appendix A Customer Support.....	80
Appendix B Common Services.....	86
Appendix C Legal Information .....	89
<b>Index .....</b>	<b>97</b>

---

# PART I

# User's Guide

---

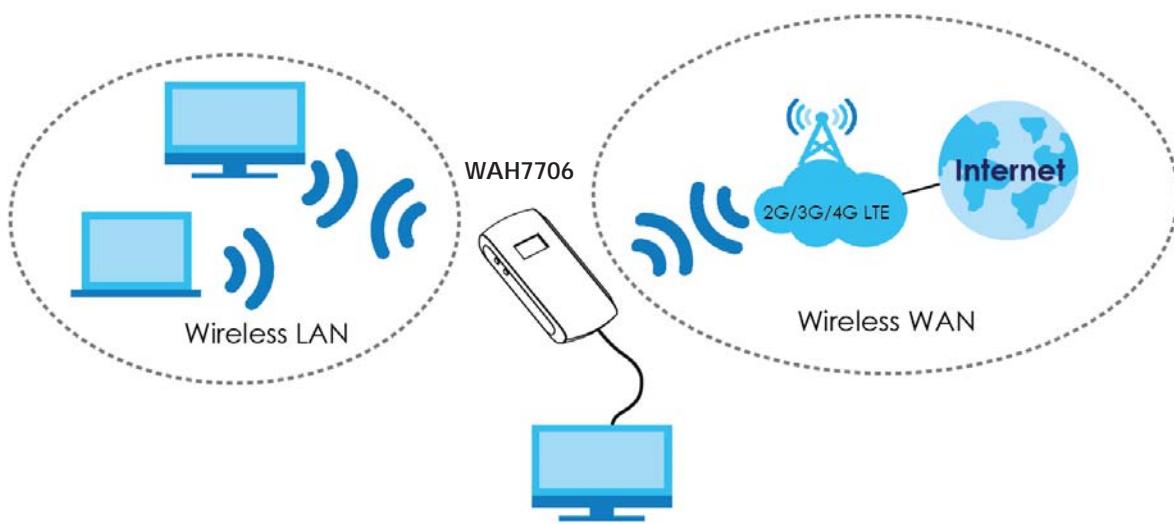
# CHAPTER 1

# Introduction

## 1.1 Overview

This chapter introduces the main features and applications of the WAH7706.

The WAH7706 is a wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to mobile users without additional wiring. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.



A range of services such as a firewall are also available for secure Internet computing.

Optionally, you can insert a micro SD card up to 32GB in size to use the WAH7706 as a portal storage device at the same time.

Your WAH7706 is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance. See the Quick Start Guide for how to make hardware connections.

## 1.2 Ways to Manage the WAH7706

You can use the following way to manage the WAH7706.

## Web Configurator

The Web Configurator allows easy WAH7706 setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

## 1.3 Good Habits for Managing the WAH7706

Do the following things regularly to make the WAH7706 more secure and to manage it more effectively.

- Change the password often. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WAH7706 to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the WAH7706; you can simply restore your last configuration.

## 1.4 Hardware Connections

See your Quick Start Guide for information on making hardware connections. You need to insert a SIM card before you can use the WAH7706.

## 1.5 Turn on/off the WAH7706

To turn on the device, press the power button and hold until the Zyxel logo displays in the OLED screen.

To turn off the device, press the power button and hold until the word "Shut Down" displays in the OLED screen.

## 1.6 OLED Display and Icons

The OLED display is enabled by default when you turn on the WAH7706. You can check the icons display in the OLED screen to see the connection status, battery life and signal strength.

Note: To enable or disable the OLED display, press the power or the WPS button and release after the WAH7706 is turned on.

**Figure 1** WAH7706 OLED Display



The following table describes the OLED icons.

Table 1 WAH7706 OLED Icons

ICONS	DESCRIPTION
	The more bars that display, the stronger the signal strength.
	The type of the mobile network to which the WAH7706 is connecting.
	The Wi-Fi signal strength and the number of wireless clients which are currently connecting to the WAH7706.
	The current battery level and charging state.
	There is no SIM card inserted.
	There is an error on your SIM card.
	There is PIN code authentication on the inserted SIM card.

Table 1 WAH7706 OLED Icons (continued)

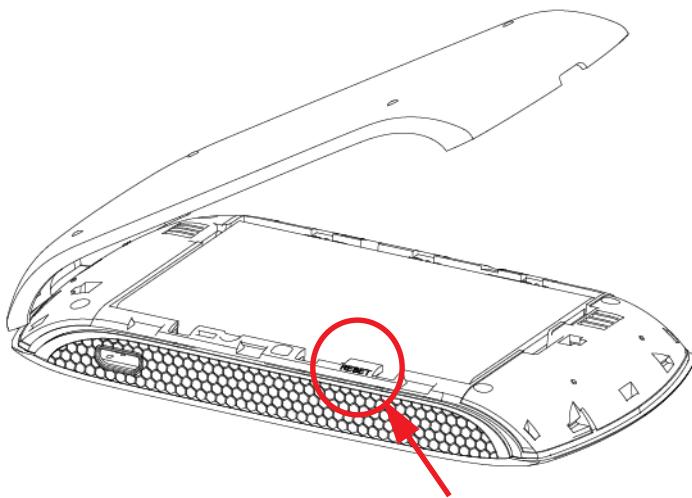
ICONS	DESCRIPTION
	This shows the number of unread text messages in the SMS inbox. The icon is grayed out if there is no messages.
	The WAH7706 is sending and receiving data to/from the WAN.

## 1.7 Resetting the WAH7706

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the physical **Reset** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to **1234** and the IP address will be reset to **192.168.1.1**.

### 1.7.1 How to Use the Physical Reset Button

- 1 Make sure the WAH7706 is turned on.
- 2 Remove the bottom cover and press the **Reset** button until the WAH7706 reboot and set the WAH7706 back to its factory-default configurations.



# CHAPTER 2

# The Web Configurator

## 2.1 Overview

The WAH7706 Web Configurator allows easy management using an Internet browser.

In order to use the Web Configurator, you must:

- Use Internet Explorer 8.0 and later versions, Mozilla Firefox 43.0 and 44.0 versions, Safari 7.0 and 8.0 versions, or Google Chrome 40.0 and 41.0 versions.
- Allow pop-up windows.
- Enable JavaScript (enabled by default).
- Enable Java permissions (enabled by default).
- Enable cookies.

The recommended screen resolution is 1024 x 768 pixels and higher.

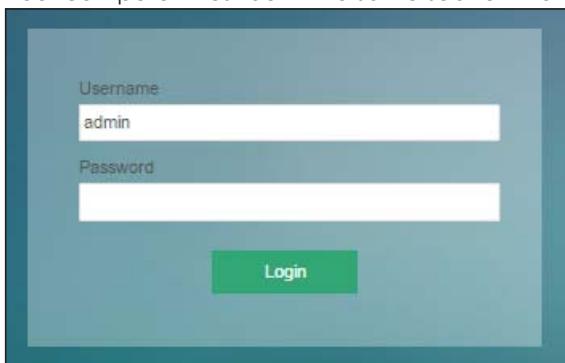
## 2.2 Login Accounts

There is one system account that you can use to log in to the WAH7706: “**admin**”. The **admin** account allows you full access to all system configurations. The default admin user name is “admin” and password is “1234”.

## 2.3 Access

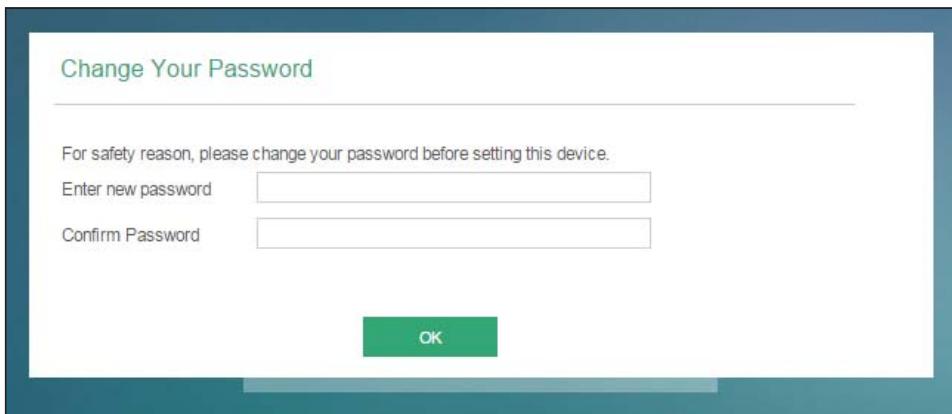
- 1 Make sure your WAH7706 hardware is properly connected. See the Quick Start Guide.
- 2 Launch your web browser.

- 3 Type "http://192.168.1.1" as the website address. The **Login** screen appears.  
Your computer must be in the same subnet in order to access this website address.



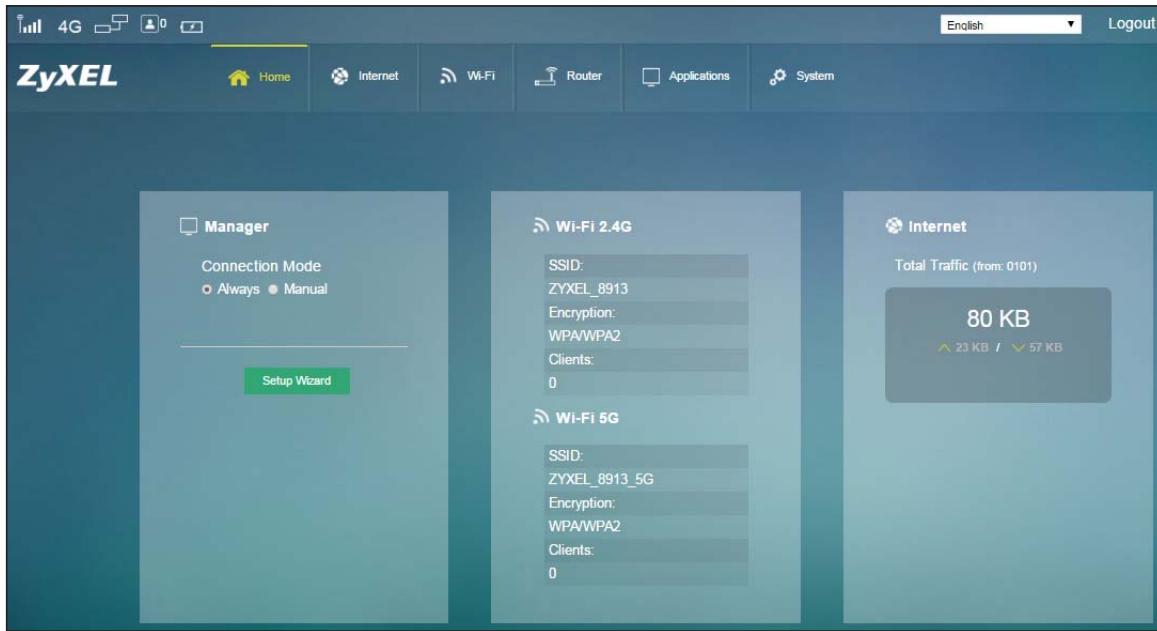
The image shows a login interface with a teal header and footer. It has two input fields: 'Username' containing 'admin' and 'Password'. A green 'Login' button is at the bottom.

- 4 Enter the user name (default: "admin" ) and password (default: "1234" ). See [Section 2.2 on page 12](#) for more information about login accounts. Click **Login**.
- 5 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **OK**.



The image shows a 'Change Your Password' dialog. It says 'For safety reason, please change your password before setting this device.' There are two input fields: 'Enter new password' and 'Confirm Password'. A green 'OK' button is at the bottom.

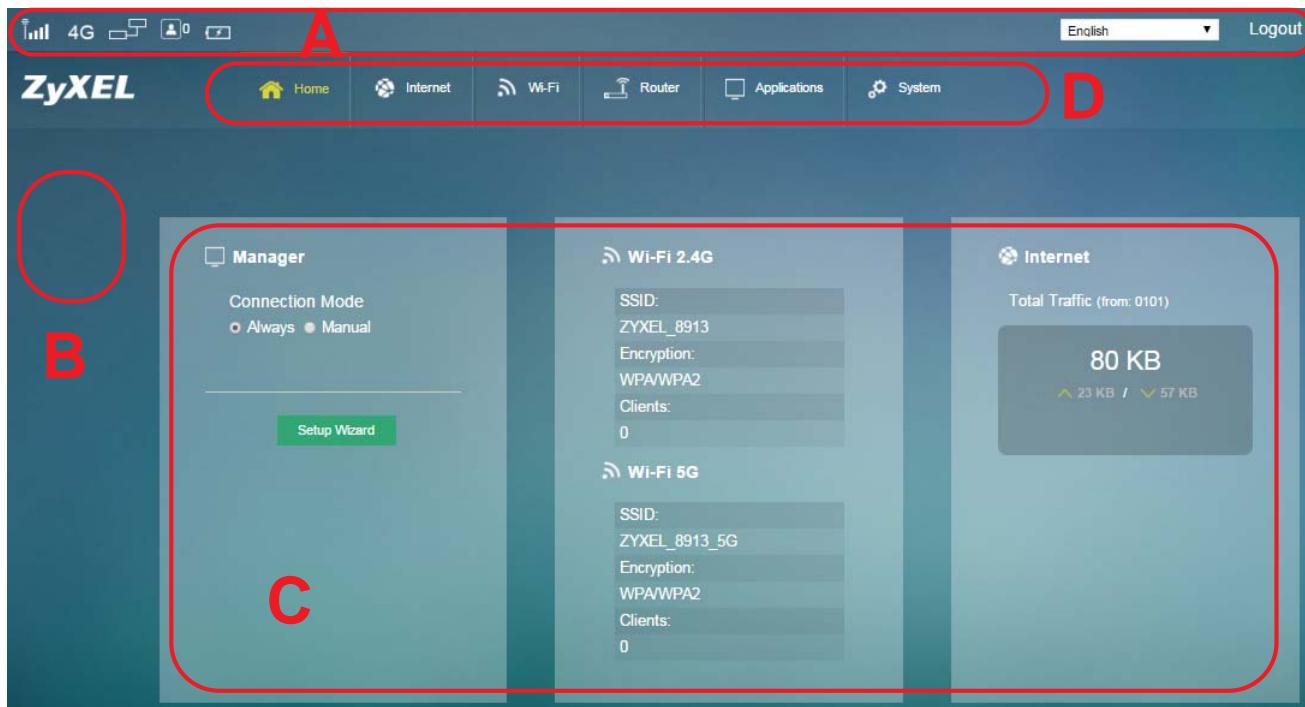
- 6 The **Home** screen appears.



## 2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Home** screen.

Figure 2 The Web Configurator's Main Screen



The Web Configurator's main screen is divided into these parts:

- A - Title Bar
- B - Navigation Panel\_Sub-Menus
- C - Main Window
- D - Navigation Panel\_Main Menus

## 2.4.1 Title Bar

The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

**Figure 3** Title Bar



The icons provide the following functions.

**Table 2** Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
SIM	This shows whether a SIM card is inserted in the WAH7706. The icon shows  if there is no SIM card inserted.
Signal Strength	This shows the current signal strength to the mobile network. The icon is grayed out if the mobile data connection is not up.
Service Provider	This shows the name of the service provider for the mobile network to which the WAH7706 is connected. This shows <b>Searching...</b> if the WAH7706 is not connected to a mobile network yet.
Roaming	This shows whether the WAH7706 is connected to another service provider's mobile network using roaming. The icon is grayed out if roaming is disabled on the WAH7706.
Internet	This shows whether the WAH7706 has an Internet connection. The icon shows  if the WAH7706 is not connected to the Internet.
Wi-Fi	This shows whether the WAH7706's Wi-Fi network is active and the number of the connected wireless clients.
Battery	The icon shows the battery status.
Language	Choose your language from the drop-down list on the upper right corner of the title bar.
Logout	Click this to log out of the Web Configurator.

## 2.4.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure WAH7706 features. The following sections introduce the WAH7706's navigation panel menus and their screens.

**Figure 4** Navigation Panel



## Home Menu

The dashboard displays general device information, system status, system resource usage, and interface status.

The Home menu screens display status and statistics information.

Table 3 Home Menu Screens Summary

LABEL	DESCRIPTION
Home	Display connection mode, wireless LAN information and the WAH7706's traffic statistics. Use this screen to access the wizard.

## Internet Menu

Table 4 Internet Menu Screens Summary

LABEL	DESCRIPTION
Internet	
Internet Status	Configure the WAN settings on the WAH7706 for Internet access.
PIN Settings	Configure the PIN code when PIN code authentication is enabled. Change the PIN code for the inserted SIM card.
APN Configuration	Configure user-defined connection profiles.
Network Selection	Display available Public Land Mobile Networks and select a preferred network for roaming.
Data Usage/ Statistic	Specify limiting the amount of the package data and view the WAH7706's traffic statistics.

## WiFi Menu

Table 5 WiFi Menu Screens Summary

LABEL	DESCRIPTION
WiFi	
Wi-Fi Status	Display information about the 2.4GHz/5GHz wireless LAN.
Wi-Fi Settings	Enable the wireless LAN and configure the basic wireless settings.
MAC Filter	Deny wireless clients based on their MAC addresses from connecting to the WAH7706.
WPS	Activate WPS.

## Router Menu

Table 6 Router Menu Screens Summary

LABEL	DESCRIPTION
LAN IP	Configure the management IP address for the WAH7706 LAN interface.
DHCP Server	Enable the DHCP server on the WAH7706.  Configure static DHCP entries.
DNS Settings	Configure the first and second DNS server IP addresses.
Connected Devices	View current clients information of network clients connected to the WAH7706.
Firewall	
IPv4/Port Filter	Configure IPv4/Port filtering rules.
IPv6/Port Filter	Configure IPv6/Port filtering rules.
URL Filter	Configure URL filtering rules.
IP/Port Forwarding	Configure port forwarding rules.

## Applications Menu

Table 7 Applications Menu Screens Summary

LABEL	DESCRIPTION
Contacts	Configure the contact list saved on the WAH7706.
SIM Contacts	Display the contact list saved on the SIM card.

Table 7 Applications Menu Screens Summary (continued)

LABEL	DESCRIPTION
Contacts Settings	Import or export your contacts.
Short Message	
New SMS	Send new SMS messages.
Inbox	Display messages received on the WAH7706.
Outbox	Display messages sent from the WAH7706.
Draft	Display messages not yet sent from the WAH7706.
SIM SMS	Display messages received on the SIM card.
File Sharing	Enable file sharing through the WAH7706.

## System Menu

Table 8 System Menu Screens Summary

LABEL	DESCRIPTION
System	
System Information	Display the WAH7706's basic information and restart the WAH7706.
User Account	Change administrative settings and the password of your WAH7706.
Settings Profile	Backup and restore device configurations, or reset your device settings back to the factory default.
Firmware Upgrade	Upload new firmware to the WAH7706.
Time Settings	Change the WAH7706's time and date. Select your time zone and configure daylight saving time.
Power Saving	Enable and configure the power saving settings in the WAH7706.
System Log	Configure to where the WAH7706 is to send logs. View the logged messages.

---

# PART II

# Technical Reference

---

# CHAPTER 3

# Home

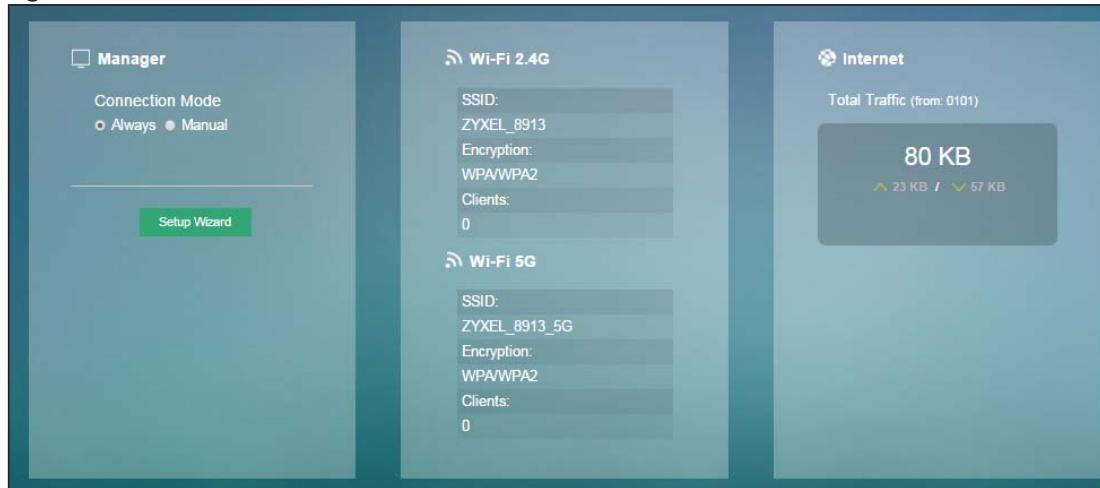
## 3.1 Overview

Use the **Home** screen to check status information about the WAH7706. Use the **Wizard** screens to configure the WAH7706's basic Internet access, wireless settings, and the password of your WAH7706.

## 3.2 Home

This screen is the first thing you see when you log into the WAH7706. It also appears every time you click the **Home** icon in the navigation panel. The **Home** screen displays the WAH7706's connection mode, wireless LAN information and traffic statistics.

Figure 5 Home



The following table describes the labels in this screen.

Table 9 Home

LABEL	DESCRIPTION
Manager	
Connection Mode	This field displays the connected mode of the WAH7706. Select <b>Always</b> to connect to the mobile network automatically if there is an available mobile network. Otherwise, select <b>Manual</b> .
Setup Wizard	Click this button to set up the Internet and Wi-Fi.
Wi-Fi 2.4G	
SSID	This displays a descriptive name used to identify the WAH7706 in the 2.4GHz wireless LAN.
Encryption	This displays the level of wireless security the WAH7706 is using.
Clients	This field displays the total number of the associated stations.

Table 9 Home (continued)

LABEL	DESCRIPTION
Wi-Fi 5G	
SSID	This displays a descriptive name used to identify the WAH7706 in the 5GHz wireless LAN.
Encryption	This displays the level of wireless security the WAH7706 is using.
Clients	This field displays the total number of the associated stations.
Internet	This field displays the total amount of data in kilobytes that has been transmitted and received on the WAN interface since the WAH7706 last restarted.

## 3.3 Setup Wizard

Click Home > Setup Wizard to open the wizard screen.

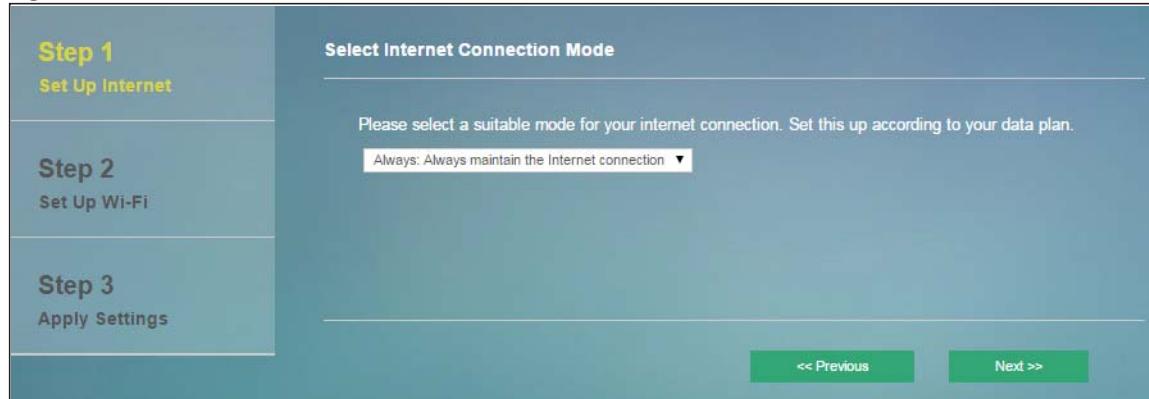
### 3.3.1 Internet

Select the **Auto** option if you did not configure the connection profile. Click **Next** to continue.

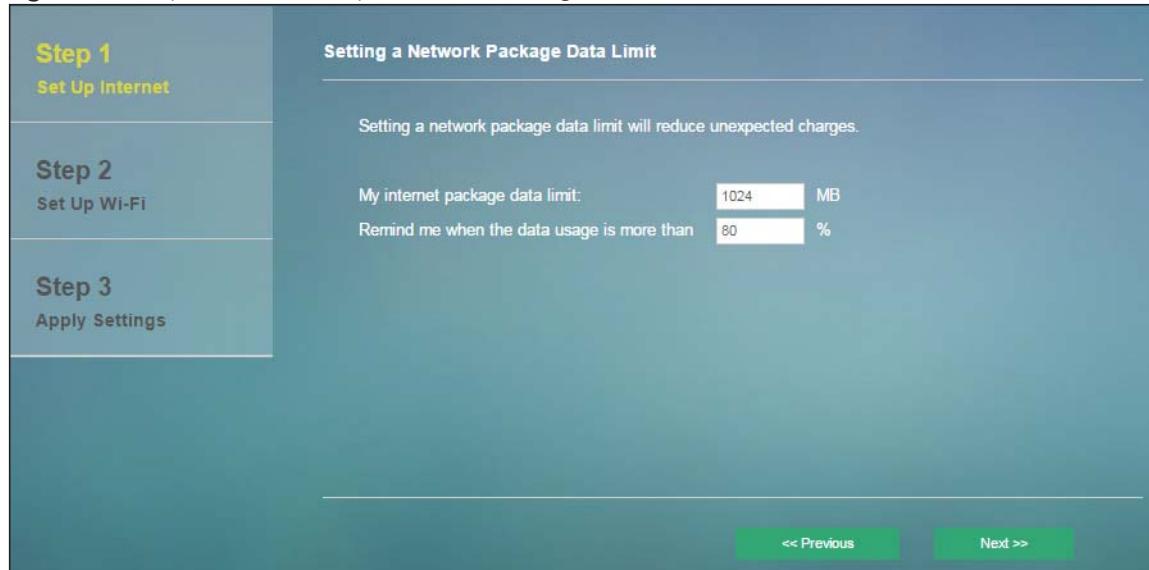
Figure 6 Setup Wizard &gt; Set Up Internet: APN Profile

The screenshot shows the 'Set Up Internet Connection' page of the Setup Wizard. On the left, a vertical sidebar lists three steps: Step 1 Set Up Internet (which is highlighted in yellow), Step 2 Set Up Wi-Fi, and Step 3 Apply Settings. The main content area is titled 'Set Up Internet Connection' and contains the instruction 'Please set your APN.' Below this, there are four input fields: 'Select APN Profile' (a dropdown menu currently set to 'Auto'), 'APN' (a text input field containing 'internet'), 'Username' (an empty text input field), and 'Password' (an empty text input field). At the bottom right of the main area is a green rectangular button labeled 'Next >>'. The overall background of the page is a gradient from light blue to dark blue.

Select the Internet connection mode of the WAH7706. Click **Next** to continue.

**Figure 7** Setup Wizard > Set Up Internet: Connection Mode

Specify limiting the amount of the package data and reminding the percentage of the package data usage. Click **Next** to configure the Wi-Fi settings.

**Figure 8** Setup Wizard > Set Up Internet: Package Data Limit

### 3.3.2 Wi-Fi

This screen shows the default Wi-Fi key and SSID for the WAH7706's wireless network. If you set up a new key and SSID, the wireless clients will lose their wireless connection and need to use new wireless settings. Click **Next** to change the login password.

**Figure 9** Wizard > Set Up Wi-Fi

**Step 1**  
Set Up Internet

**Step 2**  
Set Up Wi-Fi

**Step 3**  
Apply Settings

**Set Up Wi-Fi**

For security reasons, please change the Encryption Key before your first use.

Network Name (SSID 1)  Encryption Mode

Encryption Type  Auto  AES-CCMP  
Encryption Key  ASCII

Network Name (SSID 2)  Encryption Mode

Encryption Type  Auto  AES-CCMP  
Encryption Key  ASCII

[<< Previous](#) [Next >>](#)

Click **Apply** to save your changes. The WAH7706 will restart.

Table 10 Apply Settings

**Step 1**  
Set Up Internet

**Step 2**  
Set Up Wi-Fi

**Step 3**  
Apply Settings

**Apply your settings**

Note: Applying settings may cause the Wi-Fi to disconnect and lose connection to this website.

Please check all the changes before you click "Apply".

[<< Previous](#) [Apply](#)

# CHAPTER 4

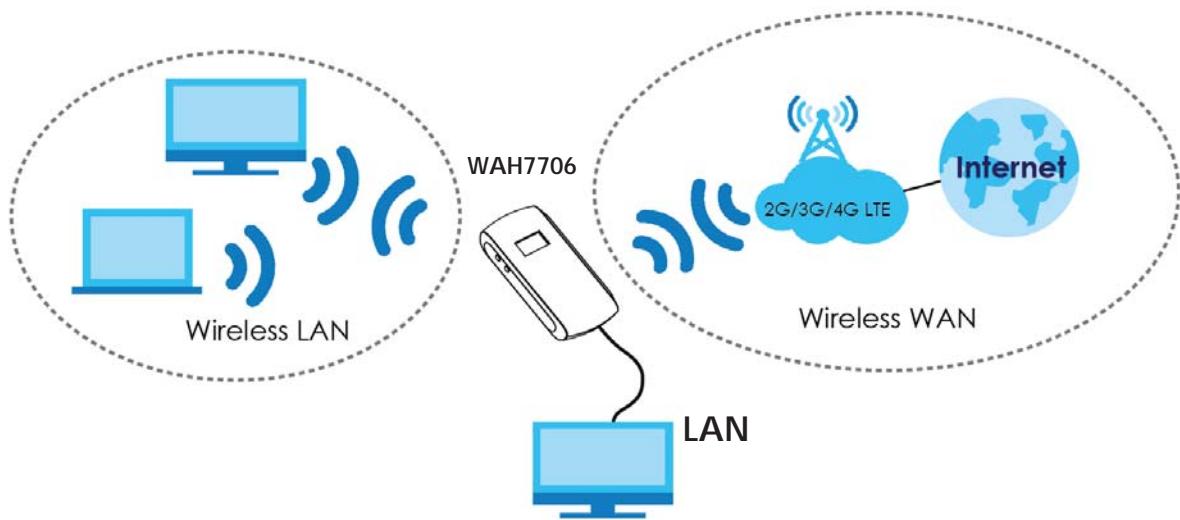
# Internet

## 4.1 Overview

This chapter discusses the WAH7706's **Internet** screens. Use these screens to configure your WAH7706 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

**Figure 10** LAN/Wireless LAN and Wireless WAN



### 4.1.1 What You Can Do in this Chapter

- Use the **Internet Status** screen to configure the WAN settings on the WAH7706 for Internet access ([Section 4.2 on page 25](#)).
- Use the **PIN Settings** screen to enable or disable PIN code authentication ([Section 4.3 on page 26](#)).
- Use the **APN Configuration** screen to configure user-defined connection profiles ([Section 4.4 on page 27](#)).
- Use the **Network Selection** screen to display available Public Land Mobile Networks and select a preferred network for roaming ([Section 4.5 on page 28](#)).
- Use the **Data Usage/Statistic** screen to specify limiting the amount of the package data and view the WAH7706's traffic statistics ([Section 4.6 on page 28](#)).

## 4.2 Internet Status Screen

Use this screen to change your WAH7706's Internet access settings. Click **Internet > Internet Status**. The screen appears as shown next.

**Figure 11** Internet > Internet Status

The following table describes the labels in this screen.

**Table 11** Internet > Internet Status

LABEL	DESCRIPTION
<b>Internet Status</b>	
Network Provider	This shows the name of the service provider for the mobile network to which the WAH7706 is connected.
Internet Status	This shows the mobile data connection status.
IP Address (IPv4)	This field displays the current IPv4 address assigned to the WAN interface.
IP Address (IPv6)	This field displays the current IPv6 address assigned to the WAN interface.
Signal Level	This shows the current signal strength to the mobile network in dBm.
Network Type	This shows the type of the mobile network (such as LTE, UMTS, GSM, HSPA+, etc.) to which the WAH7706 is connecting.
Connection Time	This field displays how long you connect to the Internet through IPv4.
<b>Internet Settings</b>	
Allow Data Roaming	Select this check box to enable data roaming on the WAH7706.  4G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your WAH7706 is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.

Table 11 Internet &gt; Internet Status (continued)

LABEL	DESCRIPTION
Cellular Network Mode	Select the type of the network ( <b>4G Mode</b> , <b>3G Mode</b> , or <b>2G Mode</b> ) to which you want the WAH7706 to connect and click <b>Apply</b> to save your settings.  Otherwise, select <b>Auto</b> to have the WAH7706 connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the WAH7706 switches to another available mobile network.
Internet Connection Method	Select <b>Always</b> to connect to the mobile network automatically if there is an available mobile network. Otherwise, select <b>Manual</b> .
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 4.3 PIN Settings Screen

Use this screen to turn on or turn off PIN code authentication on the inserted SIM card. Click **Internet > PIN Settings**. The screen appears as shown next.

Figure 12 Internet &gt; PIN Settings

The screenshot shows the 'PIN Protection' screen with the following interface elements:

- PIN Protection**: A section with a radio button labeled 'Off' and another labeled 'On' (which is selected).
- Change PIN Code**: A section with three input fields:
  - Current PIN**: An input field with a note '[ 3 ] Attempts Remaining'.
  - New PIN**: An input field.
  - Confirm New PIN**: An input field.
- Buttons**: Two green buttons at the bottom labeled 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 12 Internet &gt; PIN Settings

LABEL	DESCRIPTION
<b>PIN Protection</b>	
Enable PIN Protection	Click <b>On</b> to turn on PIN code authentication. Otherwise, click <b>Off</b> to turn off PIN code authentication.  A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.
<b>Change PIN Code</b>	
Current PIN	Enter the default or existing PIN code for the inserted SIM card.

Table 12 Internet &gt; PIN Settings

LABEL	DESCRIPTION
New PIN	Configure a new PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code.
Confirm New PIN	Enter the new PIN code again for confirmation.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 4.4 APN Configuration Screen

Use this screen to view or configure a connection profile. A connection profile defines the parameters that you need to connect to a mobile network, such as the APN, user name and password. Click **Internet > APN Configuration**. The screen appears as shown next.

Figure 13 Internet &gt; APN Configuration

The screenshot shows the 'APN Configuration' screen. At the top, it says 'APN Configuration'. Below that, there is a dropdown menu labeled 'Select APN Profile:' with 'Manual' selected. Underneath, there are three input fields: 'APN' containing 'internet', 'Username' (empty), and 'Password' (empty). At the bottom of the screen are two green buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 13 Internet &gt; APN Configuration

LABEL	DESCRIPTION
Select APN Profile	Select <b>Auto</b> to reload the default profile. Otherwise, select <b>Manual</b> to configure a connection profile.
APN	This field displays the Access Point Name (APN) in the profile.  Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method.  You can enter up to 30 printable ASCII characters. Spaces are allowed.
Username	This field displays the user name in the profile.  Type the user name (of up to 31 printable ASCII characters) given to you by your service provider.
Password	This field displays the password in the profile.  Type the password (of up to 31 printable ASCII characters) associated with the user name above.

Table 13 Internet &gt; APN Configuration

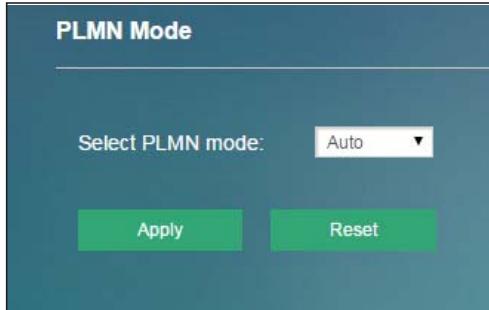
LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 4.5 Network Selection Screen

This screen allows you to view available Public Land Mobile Networks (PLMNs) and select your preferred network when the WAH7706 is outside the geographical coverage area of the network to which you are registered and roaming is enabled.

Click **Internet > Network Selection**. The screen appears as shown next.

Figure 14 Internet &gt; Network Selection



The following table describes the labels in this screen.

Table 14 Internet &gt; Network Selection

LABEL	DESCRIPTION
Select PLMN Mode	Select <b>Auto</b> to have the WAH7706 automatically connect to the first available mobile network using roaming when it is outside the coverage area of the original service provider's network. Select <b>Manual</b> to display the network list and manually select a preferred network.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 4.6 Data Usage/Statistic Screen

This screen allows you to configure limiting the amount of the package data and view the WAH7706's traffic statistics.

Click **Internet > Data Usage/Statistic**. The screen appears as shown next.

Figure 15 Internet &gt; Data Usage/Statistic

**Package Data Limit Setting**

- Enable Data Limit
- My internet package data limit is  MB
- Remind me when data usage is more than  %
- Usage cycle reset date  (Date of each month)

**Reset Network Statistics**

Reset all statistics and histories

**Current Connection Statistics**

Data Flow	▲ Sent	▼ Received
193KB	70 KB 0 KB/s (Max 2.56 KB/s)	123 KB 0 KB/s (Max 9.44 KB/s)

**Total Connections Statistics (from 01/01)**

Data Flow	▲ Sent	▼ Received
193KB	70 KB (Max 2.56 KB/s)	123 KB (Max 9.44 KB/s)

The following table describes the labels in this screen.

Table 15 Internet &gt; Data Usage/Statistic

LABEL	DESCRIPTION
Package Data Limit Setting	
Enable Data Limit	Select the check box to enable data limits.
My Internet package data limit is	Specify the limiting the amount of the package data in this field.

Table 15 Internet &gt; Data Usage/Statistic

LABEL	DESCRIPTION
Remind me when data usage is more than	Specify the reminding percentage of the package data usage in this field.
Usage cycle reset date	Specify the date that you want the WAH7706 to restart calculating the amount of the package data per month.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.
Reset Network Statistics	
Reset all statistics and histories	Click <b>Reset</b> to remove all traffic statistics.
Current Connection Statistics	
Data Flow	This indicates the current traffic flow transmitting from/to the WAH7706.
Sent	This indicates the number of transmitted packets on the WAH7706.
Received	This indicates the number of received packets on the WAH7706.
Total Connection Statistics	
Data Flow	This indicates total traffic flows transmitting from/to the WAH7706.
Sent	This indicates the number of transmitted packets on the WAH7706.
Received	This indicates the number of received packets on the WAH7706.

# CHAPTER 5

# Wi-Fi

## 5.1 Overview

This chapter describes the WAH7706's **Wi-Fi** screens. Use these screens to set up your WAH7706's wireless LAN connection.

### 5.1.1 What You Can Do in this Chapter

- Use the **Wi-Fi Status** screen to view information about the 2.4GHz/5GHz wireless LAN ([Section 5.2 on page 32](#)).
- Use the **Wi-Fi Settings** screen to enable the wireless LAN, enter the SSID and select the wireless security mode ([Section 5.3 on page 33](#)).
- Use the **MAC Filter** screen to deny wireless clients based on their MAC addresses from connecting to the WAH7706 ([Section 5.4 on page 35](#)).
- Use the **WPS** screen to activate WPS via PBC or PIN configuration ([Section 5.5 on page 37](#)).

## 5.1.2 What You Need to Know

### Wireless Basics

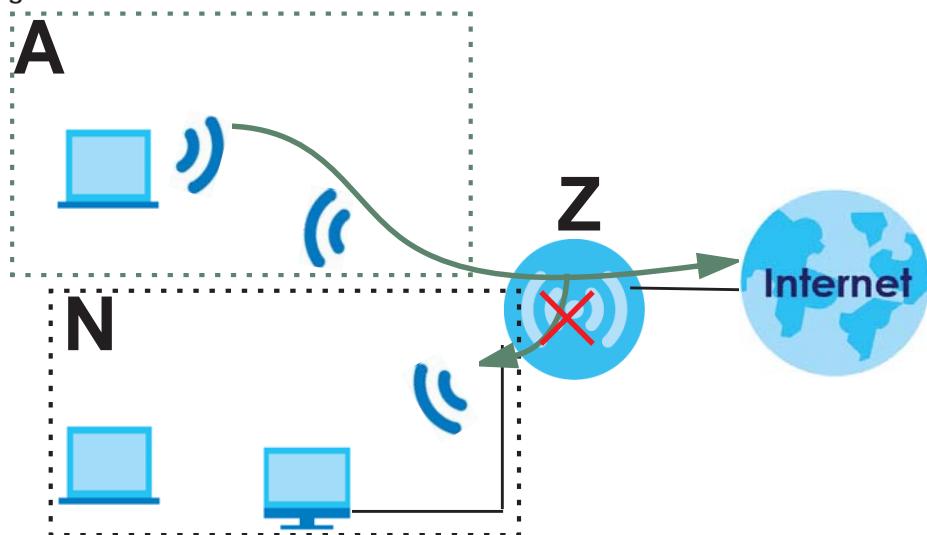
"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

### Guest WLAN

Guest WLAN allows you to set up a wireless network where users can access to Internet via the WAH7706 (Z), but not other networks connected to the Z. In the following figure, a guest user can access the Internet from the guest wireless network A via Z but not the home or company network N.

Note: The home or company network N and Guest WLAN network are independent networks.

**Figure 16** Guest Wireless LAN Network



### Finding Out More

See Section 5.6 on page 38 for advanced technical information on wireless networks.

## 5.2 Wi-Fi Status Screen

Use this screen to view information about the 2.4GHz/5GHz wireless LAN. Click **Wi-Fi > Wi-Fi Status** to access this screen.

**Figure 17** Wi-Fi > Wi-Fi Status

Wi-Fi Status	
SSID 1:	ZYXEL_8913
Encryption:	WPA/WPA2
MAC Address:	A0:E4:CB:FF:89:13
Channel:	Auto
SSID 2:	ZYXEL_8913_5G
Encryption:	WPA/WPA2
MAC Address:	A2:E4:CB:FF:89:13
Channel:	Auto

The following table describes the labels in this screen.

Table 16 Wi-Fi &gt; Wi-Fi Status

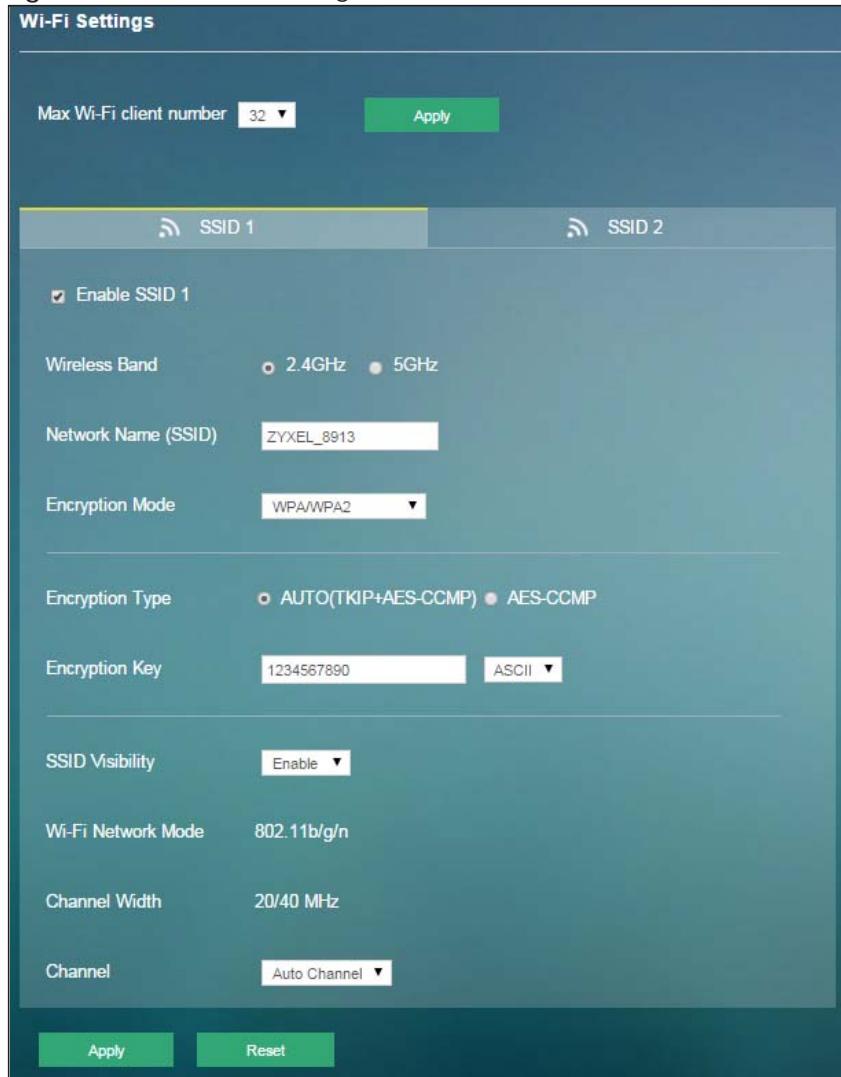
LABEL	DESCRIPTION
Wi-Fi Status	
SSID 1 / SSID2	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. This displays the basic wireless settings of <b>SSID 1</b> and <b>SSID 2</b> .
SSID 1 / SSID2	This displays a descriptive name used to identify the WAH7706 in the 2.4GHz/5GHz wireless LAN.
Encryption	This field displays the level of wireless security the WAH7706 is using.
MAC Address	This field displays the 2.4GHz/5GHz wireless adapter MAC Address of your device.
Channel	This field displays the channel number which you select manually.

## 5.3 Wi-Fi Settings Screen

Use this screen to enable the wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the WAH7706 from a computer connected to the wireless LAN and you change the WAH7706's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAH7706's new settings.

To access this screen, click **Wi-Fi > Wi-Fi Settings**.

**Figure 18** Wi-Fi > Wi-Fi Settings

The following table describes the labels in this screen.

**Table 17** Wi-Fi > Wi-Fi Settings

LABEL	DESCRIPTION
Max Wi-Fi client number	Select a number to specify maximum client the Guest Wi-Fi network can use. Click <b>Apply</b> to save your changes.
SSID 1 / SSID 2	Select <b>SSID 1</b> (or <b>SSID 2</b> ) to configure the basic wireless settings.
Enable SSID 1 (or SSID 2)	Select the check box to enable the wireless LAN of the WAH7706.
Wireless Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default <b>2.4GHz</b> or <b>5GHz</b> wireless LAN.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.

Table 17 Wi-Fi &gt; Wi-Fi Settings

LABEL	DESCRIPTION
Encryption Mode	Select <b>WPA</b> , <b>WPA2</b> , or <b>WPA/WPA2</b> to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the WAH7706. When you select to use a security, additional options appears in this screen.  Select <b>WPA/WPA2</b> to allow wireless devices that support either WPA or WPA2 to connect to your WAH7706's wireless network.  Select <b>WPA</b> to allow only wireless devices that support WPA to connect to your WAH7706's wireless network.  Select <b>WPA2</b> to allow only wireless devices that support WPA2 to connect to your WAH7706's wireless network.  Or you can select <b>NO ENCRYPTION</b> to allow any client to associate this network without any data encryption or authentication.
SSID Visibility	Select <b>Disable</b> to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Otherwise, select <b>Enable</b> .
Wi-Fi Network Mode	If you set <b>Wireless Band</b> to <b>2.4GHz</b> , you can use the 802.11 mode from the following: <ul style="list-style-type: none"><li>• <b>802.11 bgn</b>: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the WAH7706. The transmission rate of your WAH7706 might be reduced.</li></ul> If you set <b>Wireless Band</b> to <b>5GHz</b> , you can use the 802.11 mode from the following: <ul style="list-style-type: none"><li>• <b>802.11a/n/ac</b>: allows IEEE802.11n, IEEE802.11a and IEEE 802.11c compliant WLAN devices to associate with the WAH7706.</li></ul>
Channel Width	This field displays the wireless channel width used by WAH7706.  A standard 20MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHz) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHz).
Channel	Set the channel depending on your particular region.  Select a channel or use <b>Auto Channel</b> to have the WAH7706 automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the WAH7706 is currently using then displays next to this field.
	The following fields are available if you set <b>Encryption Mode</b> to <b>WPA</b> , <b>WPA2</b> , or <b>WPA/WPA2</b> .
Encryption Type	Select the encryption type ( <b>AES-CCMP</b> or <b>AUTO</b> ) for data encryption.  Select <b>AES-CCMP</b> if your wireless clients can all use <b>AES-CCMP</b> .  Select <b>AUTO (TKIP+AES-CCMP)</b> to allow the wireless clients to use either TKIP or <b>AES-CCMP</b> .
Encryption Key	The WEP keys are used to encrypt data. Both the WAH7706 and the wireless clients must use the same WEP key for data transmission.  Select <b>ASCII</b> in order to enter ASCII characters as WEP key. Select <b>HEX</b> in order to enter hexadecimal characters as a WEP key.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

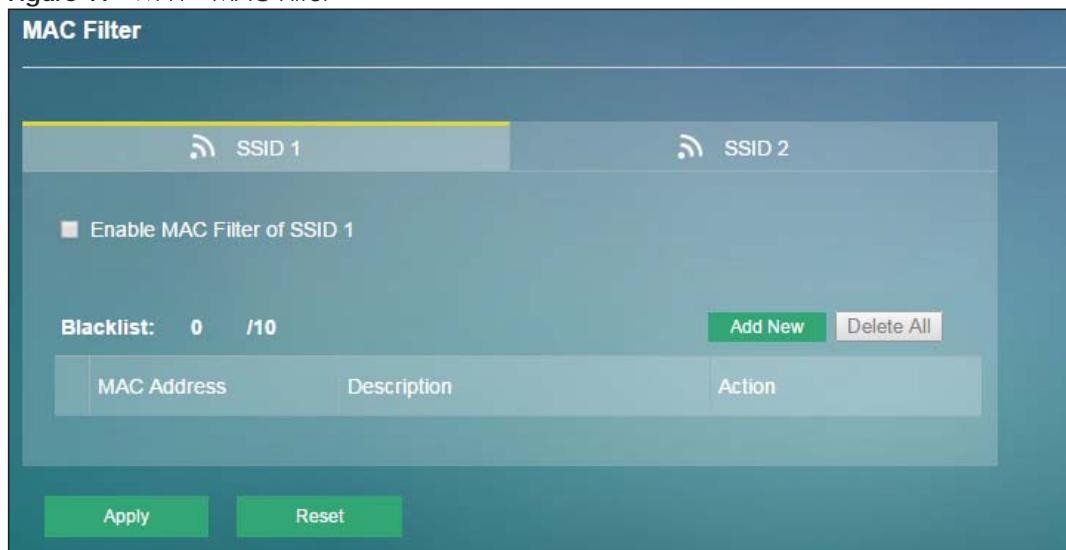
## 5.4 MAC Filter Screen

This screen allows you to configure the WAH7706 to exclude specific devices from accessing the WAH7706 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC

address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your WAH7706's MAC filter settings and add new MAC filter rules. Click **Wi-Fi > MAC Filter**. The screen appears as shown.

**Figure 19** Wi-Fi > MAC Filter



The following table describes the labels in this screen.

**Table 18** Wi-Fi > MAC Filter

LABEL	DESCRIPTION
SSID 1 / SSID 2	Select SSID 1 (or SSID 2) to configure the MAC filtering rules.
Enable MAC Filter of SSID 1 (or SSID 2)	Select Enable MAC Filter of SSID 1 (or SSID 2) to prohibit devices with the MAC addresses you configured.
Blacklist	This field displays how many entries you display on this page.
Add New	Click Add New to create a new entry.
Delete All	Click Delete All to remove all entries.
	This field displays the index number of the MAC address entry.
MAC Address	This field displays the MAC addresses of the wireless devices that are allowed or denied access to the WAH7706.  Click Add New or Edit to enter or change the MAC address of the wireless devices that are allowed or denied access to the WAH7706 in this field. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Description	This field displays the name of the MAC address entry.  Click Add New or Edit to enter a descriptive name to identify the MAC address entry. You can enter up to 20 printable ASCII characters. Spaces are allowed.
Action	Click Edit to go to the screen where you can edit the rule.  Click Delete to remove the MAC address entry.
Apply	Click Apply to save your changes back to the WAH7706.
Reset	Click Reset to reload the previous configuration for this screen.

## 5.5 WPS Screen

Use this screen to configure Wi-Fi Protected Setup (WPS) on your WAH7706.

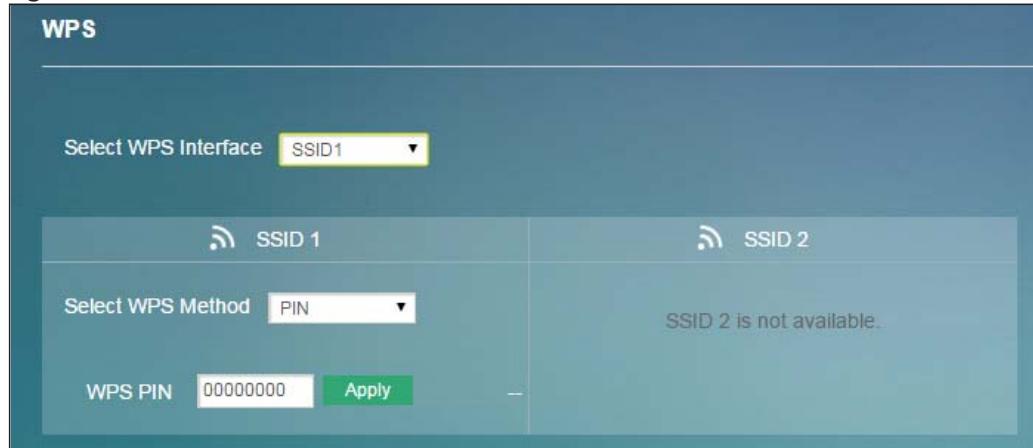
WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 5.6.5.3 on page 45](#) for more information about WPS.

Note: To use the WPS feature, make sure you have wireless enabled in the **Wi-Fi > Wi-Fi Settings** screen.

Note: If you want to use the WPS feature set the security type to **WPA** or **None**.

Click **Wi-Fi > WPS**. The following screen displays.

Figure 20 Wi-Fi > WPS



The following table describes the labels in this screen.

Table 19 Wi-Fi > WPS

LABEL	DESCRIPTION
Select WPS Interface	Select SSID 1 (or SSID 2) to configure WPS.
Enable	Select <b>On</b> to activate WPS on the WAH7706. Otherwise, select <b>Off</b> .

Table 19 Wi-Fi &gt; WPS (continued)

LABEL	DESCRIPTION
Select WPS Method	<ul style="list-style-type: none"> <li>Select <b>PBC</b> to set up a WPS wireless network using Push Button Configuration (PBC). If you select <b>PBC</b>, click <b>Activate</b> to add another WPS-enabled wireless device (within wireless range of the WAH7706) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the <b>Connect</b> button on this screen.</li> </ul> <p>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.</p> <ul style="list-style-type: none"> <li>Select <b>PIN</b> to set up a WPS wireless network by entering the PIN of the client into the WAH7706.</li> </ul>
WPS PIN	<p>This field is available only when you set <b>Select WPS Method</b> to <b>PIN</b>.</p> <p>Select this option and enter the PIN of the device that you are setting up a WPS connection with and click <b>Apply</b> to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the WAH7706.</p>

## 5.6 Technical Reference

This section discusses wireless LANs in depth.

### 5.6.1 Wireless Network Overview

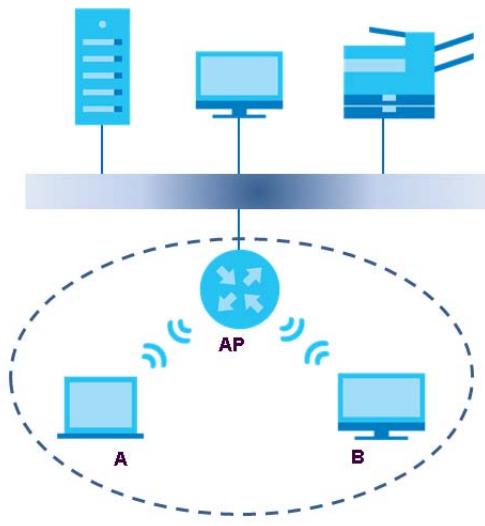
Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

**Figure 21** Example of a Wireless Network

The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your WAH7706 is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.  
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.  
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

## 5.6.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the WAH7706's Web Configurator.

Table 20 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.  By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the WAH7706. The lower the value, the more often the devices must get permission.  If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the WAH7706.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the WAH7706 does, it cannot communicate with the WAH7706.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

## 5.6.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

### 5.6.3.1 SSID

Normally, the WAH7706 acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the WAH7706 does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 5.6.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the WAH7706 which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

### 5.6.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

- 
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
  2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

### 5.6.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 5.6.3.3](#) on [page 41](#) for information about this.)

Table 21 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the WAH7706 and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption.

The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your WAH7706, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the WAH7706.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

### 5.6.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

## 5.6.5 WiFi Protected Setup (WPS)

Your WAH7706 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### 5.6.5.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the WAH7706, see [Section 5.5 on page 37](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the WAH7706 you must press the WPS button for more than three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### 5.6.5.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first

device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

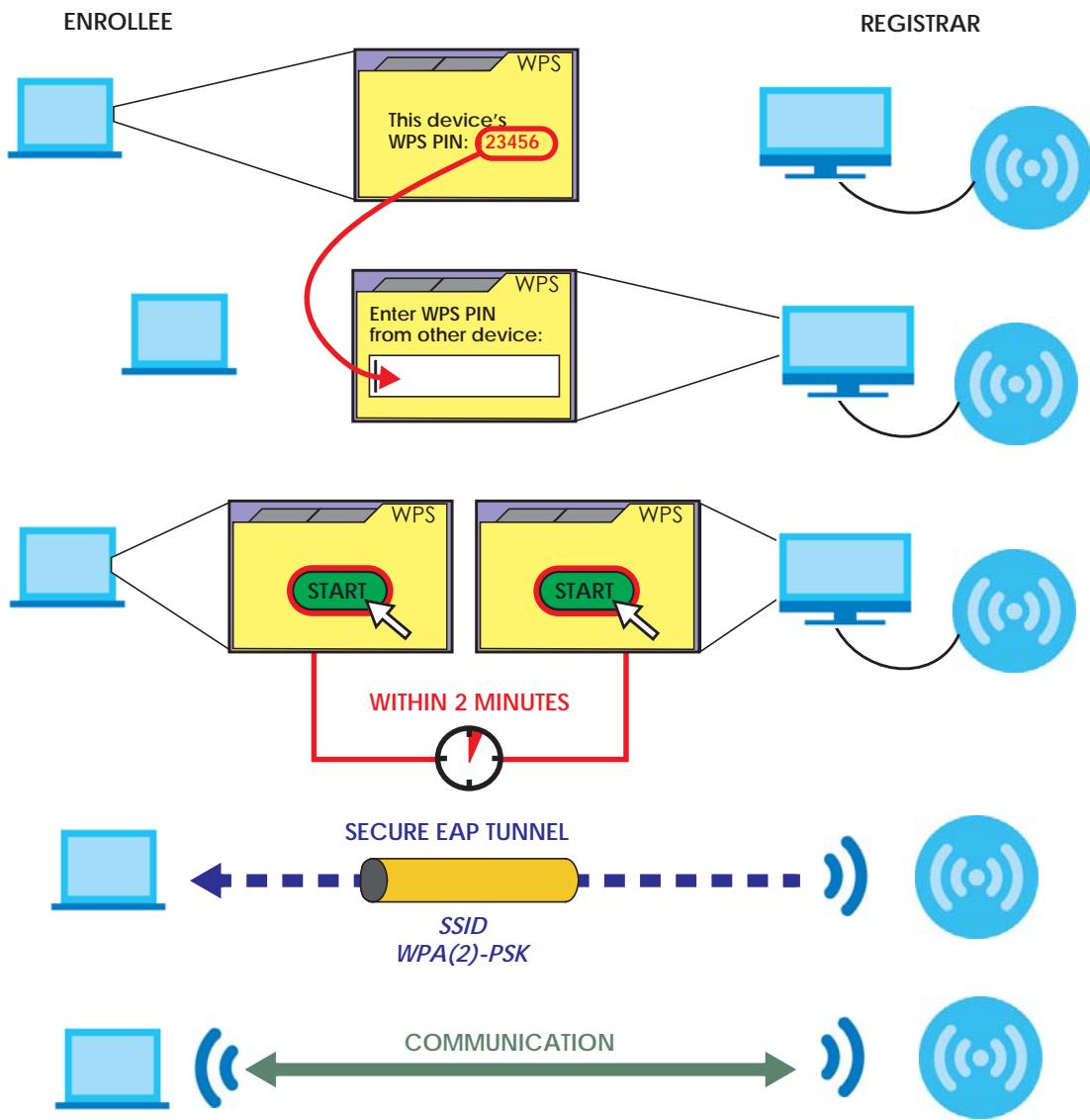
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1** Ensure WPS is enabled on both devices.
- 2** Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3** Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the WAH7706, see [Section 5.5 on page 37](#)).
- 4** Enter the client's PIN in the AP's configuration interface.
- 5** If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6** Start WPS on both devices within two minutes.
- 7** Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8** On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 22 Example WPS Process: PIN Method

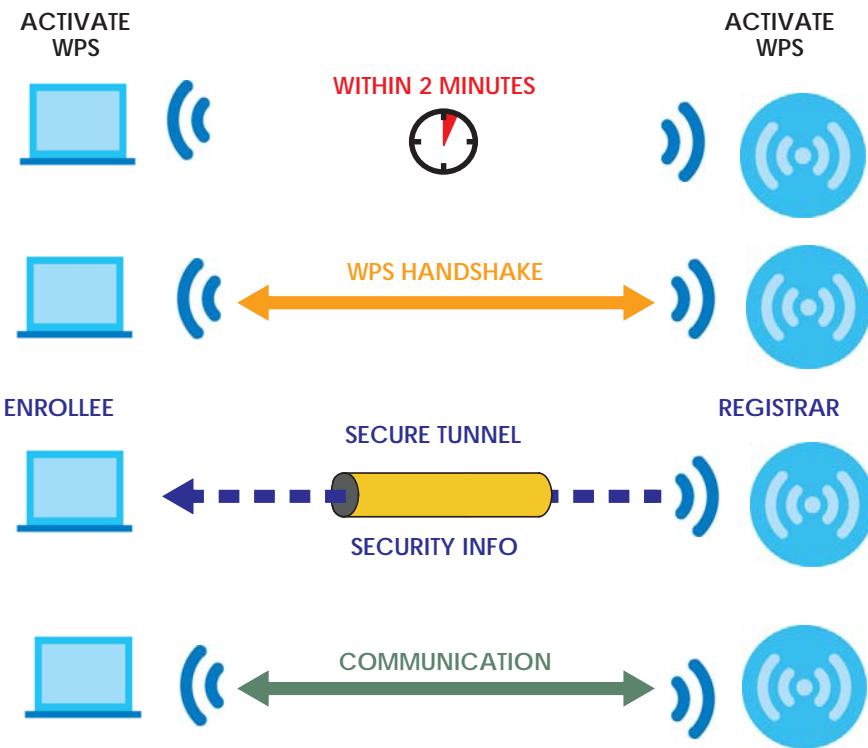


### 5.6.5.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 23 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

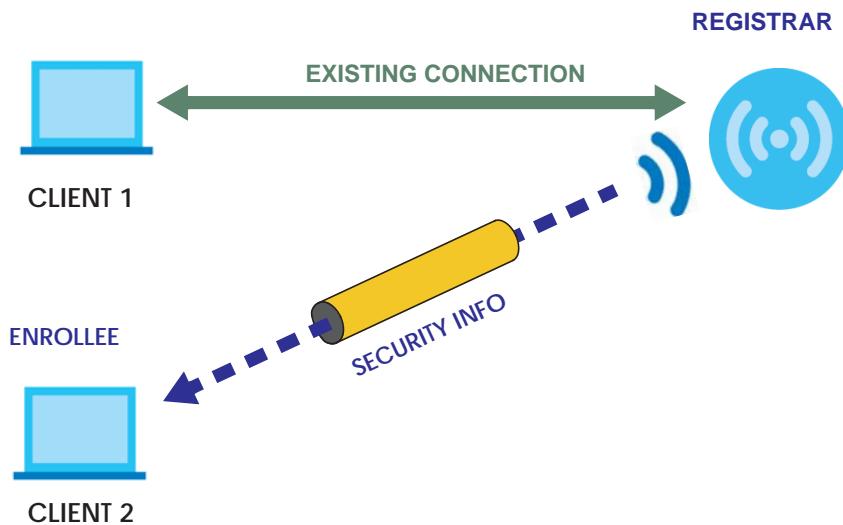
#### 5.6.5.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

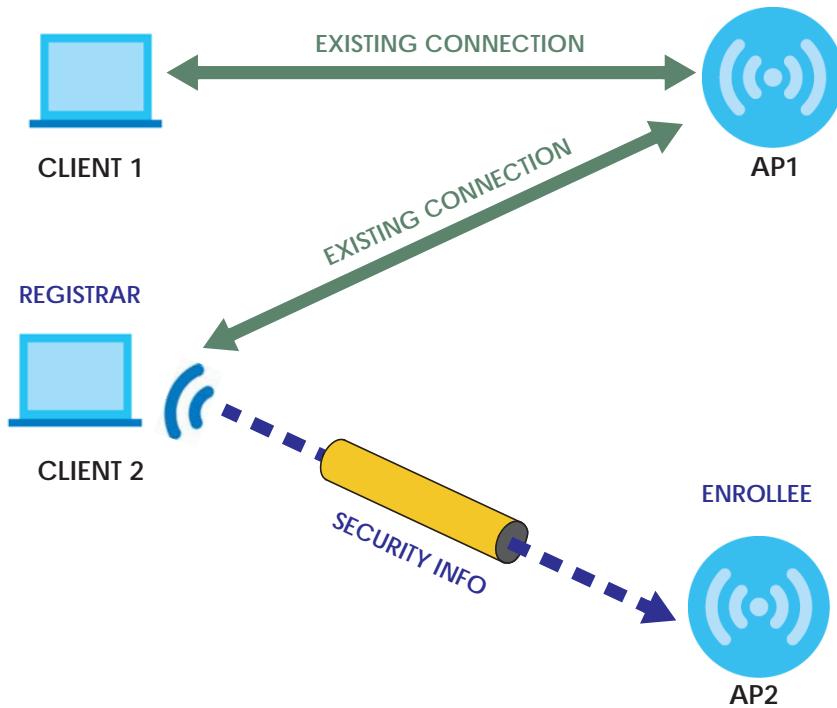
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 24** WPS: Example Network Step 1

In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

**Figure 25** WPS: Example Network Step 2

In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 26** WPS: Example Network Step 3

### 5.6.5.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

# CHAPTER 6

# Router

## 6.1 Overview

This chapter describes how you can configure the management IP address, DHCP settings of your WAH7706, the IP filtering and content filtering settings.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

### 6.1.1 What You Can Do in this Chapter

- Use the **LAN IP** screen to configure the WAH7706's LAN IP address ([Section 6.2 on page 50](#)).
- Use the **DHCP Server** screen to enable the DHCP server on the WAH7706 ([Section 6.3 on page 51](#)).
- Use the **DNS Settings** screen to configure the WAH7706's DNS settings ([Section 6.4 on page 53](#)).
- Use the **Connected Devices** screen to view current clients information ([Section 6.5 on page 53](#)).
- Use the **IPv4/Port Filter** screen to view and configure IPv4/Port filtering rules ([Section 6.6 on page 54](#)).
- Use the **IPv6/Port Filter** screen to view and configure IPv6/Port filtering rules ([Section 6.7 on page 55](#)).
- Use the **URL Filter** screen to view and configure content filtering rules ([Section 6.8 on page 56](#)).
- Use the **IP/Port Forwarding** screen to view and configure port forwarding rules ([Section 6.9 on page 57](#)).

## 6.2 LAN IP Screen

Use this screen to view or configure the management IP address for your WAH7706. To access this screen, click **Router > LAN IP**.

Note: If you change the WAH7706's IP address, you need to use the new IP address to access the WAH7706's web configurator.

**Figure 26** Router > LAN IP

The screenshot shows a configuration interface for a router's LAN IP settings. The title bar at the top says "Router > LAN IP". The main area contains three input fields: "Host Name" with the value "WAH7706", "IP Address" with the value "192.168.1.1", and "Subnet Mask" with the value "255.255.255.0". At the bottom of the screen are two green rectangular buttons labeled "Apply" and "Reset".

The following table describes the labels in this screen.

Table 22 Router &gt; LAN IP

LABEL	DESCRIPTION
Host Name	This shows the default host name. Enter the new host name for the WAH7706 if you want to change it.
IP Address	This shows the default LAN IP address. Enter the new IP address for the WAH7706's LAN interface if you want to change it.
Subnet Mask	This shows the default subnet mask. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.3 DHCP Server Screen

The WAH7706 has built-in DHCP server capability that assigns IP addresses to systems that support DHCP client capability. Use this screen to enable the DHCP server. To access this screen, click **Router > DHCP Server**.

Figure 27 Router &gt; DHCP Server

**DHCP Settings**

■ Enable DHCP Server

Start IP 192.168.1.10

End IP 192.168.1.250

Lease Time 1440 minutes

**Static DHCP List: 0 /30**

	IP Address	Mac Address	Action
1	192.168.1.100	00:AC:00:AC:00:AC	Edit Delete

Apply Reset

The following table describes the labels in this screen.

Table 23 Router &gt; DHCP Server

LABEL	DESCRIPTION
<b>DHCP Settings</b>	
Enable DHCP Server	Select the check box to enable the DHCP server on the WAH7706.
Start IP	The WAH7706 is pre-configured with a pool of 100 IP addresses starting from 192.168.0.100 to 192.168.0.199. This field specifies the first of the contiguous addresses in the IP address pool.
End IP	This field specifies the last of the contiguous addresses in the IP address pool.
Lease Time (minutes)	Specify how long (in minutes) each computer can use the information (especially the IP address) before it has to request the information again.
<b>Static DHCP List</b>	
Add New	Click <b>Add New</b> to create a new entry.
	This field displays the index number of the static IP address entry.
IP Address	This field displays the IP address that the WAH7706 assigns to a device with the entry's MAC address.
MAC Address	This field displays the MAC address of the device to which the WAH7706 assigns the entry's IP address.
Action	Click <b>Edit</b> to go to the screen where you can edit the static IP address. Click <b>Delete</b> to remove the static IP address entry.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.4 DNS Settings Screen

Click **Router > DNS Settings** to configure the WAH7706's DNS settings. The following screen displays.

**Figure 28** Router > DNS Settings

The screenshot shows the 'DNS Settings' configuration page. At the top, there is a radio button for 'DNS Mode' with options 'Auto' (selected) and 'Manual'. Below this are two input fields: 'Primary DNS' containing '8.8.8.8' and 'Secondary DNS' also containing '8.8.8.8'. At the bottom are two green buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 24** Router > DNS Settings

LABEL	DESCRIPTION
DNS Mode	Select <b>Auto</b> if your ISP dynamically assigns DNS server information (and the WAH7706's WAN IP address). Otherwise, select <b>Manual</b> if you have the IP address of a DNS server.
Primary DNS	Select <b>Manual</b> if you have the IP address of a DNS server.
Secondary DNS	Enter the DNS server's IP address in the field.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.5 Connected Devices Screen

Click **Router > Connected Devices** to view current clients information (including IP Address, Host Name and MAC Address) of network clients connected to the WAH7706. The following screen displays.

**Figure 29** Router > Connected Devices

The screenshot shows the 'Connected Devices' table with the title 'Connected Devices ( 2 clients connected )'. The table has four columns: 'MAC Address', 'Host Name (if any)', and 'IP Address'. There are two rows of data:

	MAC Address	Host Name (if any)	IP Address
Wi-Fi 1	90:e7:c4:14:bf:34	android-bbdfea32480	192.168.1.12
Wi-Fi 1	0c:8b:fd:88:17:1a	T1-1-1-Q-19314	192.168.1.11

The following table describes the labels in this screen.

Table 25 Router &gt; Connected Devices

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the device.
Host Name (If any)	This field displays the device host name.
IP Address	This field displays the IP address that the WAH7706 assigns to the device.

## 6.6 IPv4/Port Filter Screen

The WAH7706 firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application. Use this screen to configure IP filtering rules. To access this screen, click **Router > Firewall > IPv4/Port Filter**.

Figure 30 Router &gt; Firewall &gt; IPv4/Port Filter

Index	Source IP	Port	Protocol	Dest. IP	Port	Comment	Action
1	192.168.1.100	80	TCP+UDP	192.168.1.120	80		Edit   Delete

The following table describes the labels in this screen.

Table 26 Router &gt; Firewall &gt; IPv4/Port Filter

LABEL	DESCRIPTION
IPv4/Port Filter	
Enable IPv4/Port Filter	Select the check box to enable the rule.
IPv4/Port Filter List	
Add New	Click <b>Add New</b> to create a new rule.
	This field displays the rule index number.
Source IP	This field displays the source IP addresses to which this rule applies.
Port	This field displays a single port number of the source or the starting port number of a range. Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP or <b>any</b> ) used to transport the packets for which you want to apply the rule.
Dest. IP	This field displays the destination IP addresses to which this rule applies.

Table 26 Router &gt; Firewall &gt; IPv4/Port Filter

LABEL	DESCRIPTION
Port	This field displays a single port number of the destination or the starting port number of a range. Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Comment	Enter descriptions of the rule in this field.
Action	Click <b>Edit</b> to go to the screen where you can edit the filtering rule. Click <b>Delete</b> to remove the filtering rule.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.7 IPv6/Port Filter Screen

The WAH7706 firewall is a packet filtering firewall and restricts access based on the source/destination computer network address of a packet and the type of application. Use this screen to configure IP filtering rules. To access this screen, click **Router > Firewall > IPv6/Port Filter**.

Figure 31 Router &gt; Firewall &gt; IPv6/Port Filter



The following table describes the labels in this screen.

Table 27 Router &gt; Firewall &gt; IPv6/Port Filter

LABEL	DESCRIPTION
IPv6/Port Filter	
Enable IPv6/Port Filter	Select the check box to enable the rule.
IPv6/Port Filter List	
Add New	Click <b>Add New</b> to create a new rule.
	This field displays the rule index number.
Source IP	This field displays the source IP addresses to which this rule applies.
Port	This field displays a single port number of the source or the starting port number of a range. Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.

Table 27 Router &gt; Firewall &gt; IPv6/Port Filter

LABEL	DESCRIPTION
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP or any) used to transport the packets for which you want to apply the rule.
Dest. IP	This field displays the destination IP addresses to which this rule applies.
Port	This field displays a single port number of the destination or the starting port number of a range. Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Comment	Enter descriptions of the rule in this field.
Action	Click <b>Edit</b> to go to the screen where you can edit the filtering rule. Click <b>Delete</b> to remove the filtering rule.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.8 URL Filter Screen

Use this screen to block the users on your network from accessing certain web sites. To access this screen, click Router > Firewall > URL Filter.

Figure 32 Router &gt; Firewall &gt; URL Filter

URL filter List: 1 / 15		
<a href="#">Add New</a>		
Keywords of URL or Domain		Action
1	yahoo.com	<a href="#">Edit</a> <a href="#">Delete</a>

[Apply](#) [Reset](#)

The following table describes the labels in this screen.

Table 28 Router &gt; Firewall &gt; URL Filter

LABEL	DESCRIPTION
URL filter	
Enable URL Filter	Select the check box to enable the rule.
URL filter List	
Add New	Click <b>Add New</b> to create a new rule.

Table 28 Router &gt; Firewall &gt; URL Filter

LABEL	DESCRIPTION
	This field displays the rule index number.
Keywords of URL or Domain	This field displays the website URL to which the WAH7706 blocks.
Action	Click <b>Edit</b> to go to the screen where you can edit the filtering rule. Click <b>Delete</b> to remove the filtering rule.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 6.9 IP/Port Forwarding Screen

Use this screen to configure port forwarding rules. To access this screen, click **Router > Firewall > IP/Port Forwarding**.

Figure 33 Router &gt; Firewall &gt; IP/Port Forwarding

	Private IP	Private Port	Global Port	Protocol	Action
1	192.168.1.15	80	80	TCP	<b>Edit</b> <b>Delete</b>

The following table describes the labels in this screen.

Table 29 Router &gt; Firewall &gt; IP/Port Forwarding

LABEL	DESCRIPTION
<b>IP/Port Forwarding</b>	
Enable IP/Port Forwarding	Select the check box to enable port forwarding rules.
<b>Filter List</b>	
Add New	Click <b>Add New</b> to create a new rule.
	This field displays the rule index number.
Private IP	This field displays the inside IP address of the server. Enter the inside IP address of the virtual server here.

Table 29 Router &gt; Firewall &gt; IP/Port Forwarding

LABEL	DESCRIPTION
Private Port	A private port is a port that causes (or triggers) the WAH7706 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.  Enter the port number/range of the private in this field.
Global Port	A global port is a port that a server on the WAN uses when it sends out a particular service. The WAH7706 forwards the traffic with this port to the client computer on the LAN that requested the service.  Enter the port number/range of the global in this field.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
Action	Click <b>Edit</b> to go to the screen where you can edit the port forwarding rule.  Click <b>Delete</b> to remove the port forwarding rule.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

# CHAPTER 7

# Applications

## 7.1 Overview

This chapter shows you how to set up a contact list, send and view the text messages, and configure file sharing.

SMS (Short Message Service) allows you to send and view the text messages that the WAH7706 received from mobile devices or the service provider.

When the SMS box is full the WAH7706 will begin to delete older entries as it adds new ones.

### 7.1.1 What You Can Do in this Chapter

- Use the **Application > Contacts > Contact List** screen to configure the contact list saved on the WAH7706 ([Section 7.2 on page 59](#)).
- Use the **Application > Contacts > SIM Contacts** screen to view the contact list saved on the SIM card ([Section 7.3 on page 60](#)).
- Use the **Application > Contacts > Contacts Settings** screen to import or export the contacts files ([Section 7.4 on page 61](#)).
- Use the **Application > Short Message > New SMS** screen to send new messages ([Section 7.5 on page 61](#)).
- Use the **Application > Short Message > Inbox** screen to view messages received on the WAH7706 ([Section 7.6 on page 62](#)).
- Use the **Application > Short Message > Outbox** screen to view messages sent from the WAH7706 ([Section 7.7 on page 63](#)).
- Use the **Application > Short Message > Draft** screen to view messages not yet sent from the WAH7706 ([Section 7.8 on page 63](#)).
- Use the **Application > Short Message > SIM SMS** screen to view messages received on the SIM card ([Section 7.9 on page 64](#)).
- Use the **Application > File Sharing** screen to allow file sharing via the WAH7706 using Windows Explorer or the workgroup name ([Section 7.10 on page 65](#)).

## 7.2 Contact List Screen

Use this screen to configure the contact list saved on the WAH7706. To access this screen, click **Application > Contacts > Contact List**.

**Figure 34** Application > Contacts > Contact List

Contact List			
	Contact Name	Number	Actions
<input checked="" type="checkbox"/>	USER1	0912345678	<b>Edit</b>

The following table describes the labels in this screen.

**Table 30** Application > Contacts > Contact List

LABEL	DESCRIPTION
Delete	Select the check box which next to the contact name and click <b>Delete</b> to remove the entry.
New	Click <b>New</b> to create a new entry.
Contact Name	This field displays a descriptive name used to identify contacts.
Number	This field displays the mobile phone number of contacts.
Actions	Click <b>Edit</b> to go to the screen where you can edit the contact details.

## 7.3 SIM Contacts Screen

Use this screen to view the contact list saved on the SIM card. To access this screen, click **Application > Contacts > SIM Contacts**.

**Figure 35** Application > Contacts > SIM Contacts

SIM Contacts		
	Contact Name	Number

The following table describes the labels in this screen.

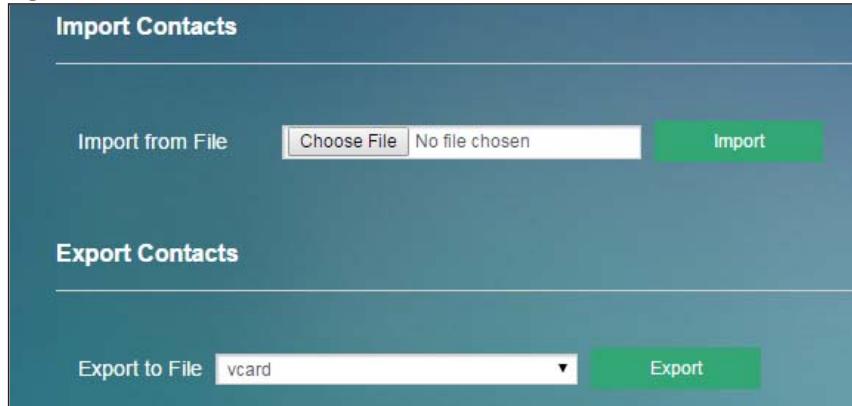
**Table 31** Application > Contacts > SIM Contacts

LABEL	DESCRIPTION
	This field displays the index number of the contacts.
Contact Name	This field displays a descriptive name used to identify contacts.
Number	This field displays the mobile phone number of contacts.

## 7.4 Contacts Settings Screen

Use this screen to import or export the contacts files. To access this screen, click **Application > Contacts > Contacts Settings**.

Figure 36 Application > Contacts > Contacts Settings



The following table describes the labels in this screen.

Table 32 Application > Contacts > Contacts Settings

LABEL	DESCRIPTION
<b>Import Contacts</b>	
Import from File	Click <b>Choose File</b> to find the .csv file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. Click <b>Import</b> to begin the upload process.
<b>Export Contacts</b>	
Export to File	A <b>CSV</b> (comma-separated values) file is a way to store textual and numeric data. A <b>vCard</b> is an electronic business card, and it can store images and sound as well as text. Select a contact format from the drop-down list box to export your contacts. Click <b>Export</b> to begin the download process.

## 7.5 New SMS Screen

Use this screen to send messages using the WAH7706. To access this screen, click **Application > Short Message > New SMS**.

Type a phone number and message content. You can type up to 70 characters in one message. If the message exceeds 70 characters, more than one SMS will be sent. The maximum number of SMS that can be sent is 20 (1000 characters total). Click **Send** to send the message. Click **Save** to store the message as a draft. Click **Reset** to reload the previous configuration for this screen.

**Figure 37** Application > Short Message > New SMS

New Message

Receiver

Add Receiver

Content

Send Save Reset

## 7.6 Inbox Screen

Use this screen to view messages received on the WAH7706. To access this screen, click **Application > Short Message > Inbox**.

**Figure 38** Application > Short Message > Inbox

Inbox

Delete All

	From	Time	Content	Action

The following table describes the labels in this screen.

Table 33 Application &gt; Short Message &gt; Inbox

LABEL	DESCRIPTION
Delete All	Click <b>Delete All</b> to remove all messages.
	This field displays the index number of the message.
From	This field displays the name from which the message is sent.
Time	This field displays the date and time the message was received.
Content	This field displays the content of the message.
Action	Click <b>Delete</b> to remove the message record.

## 7.7 Outbox Screen

Use this screen to view messages sent from the WAH7706. To access this screen, click **Application > Short Message > Outbox**.

Figure 39 Application > Short Message > Outbox

Outbox				
<input type="button" value="Delete All"/>				
	To	Time	Content	Action
1	USER1	2015/09/04,03:26:11	Test	<input type="button" value="Delete"/>
2	USER1	2015/09/04,03:25:58	Test	<input type="button" value="Delete"/>

The following table describes the labels in this screen.

Table 34 Application > Short Message > Outbox

LABEL	DESCRIPTION
Delete All	Click <b>Delete All</b> to remove all messages.
	This field displays the index number of the message.
To	This field displays the name the message is sent to.
Time	This field displays the date and time the message was sent.
Content	This field displays the content of the message.
Action	Click <b>Delete</b> to remove the message record.

## 7.8 Draft Screen

Use this screen to view messages not yet sent from the WAH7706. To access this screen, click **Application > Short Message > Draft**.

Figure 40 Application > Short Message > Draft

Draft				
<input type="button" value="Delete All"/>				
	To	Time	Content	Action
1	USER1	2015/09/04,03:27:29	123	<input type="button" value="Delete"/> <input type="button" value="Send"/>

The following table describes the labels in this screen.

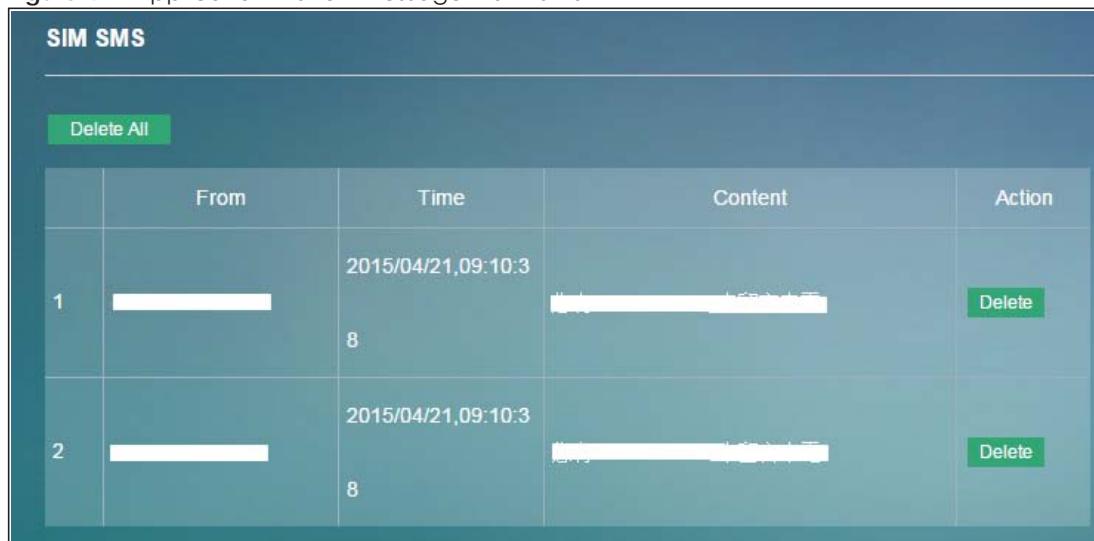
Table 35 Application &gt; Short Message &gt; Draft

LABEL	DESCRIPTION
Delete All	Click <b>Delete All</b> to remove all messages.
	This field displays the index number of the message.
To	This field displays the name the message is sent to.
Time	This field displays the date and time the message was sent.
Content	This field displays the content of the message.
Action	Click <b>Delete</b> to remove the message record. Click <b>Send</b> to deliver the message.

## 7.9 SIM SMS Screen

Use this screen to view messages received on the SIM card. To access this screen, click **Application > Short Message > SIM SMS**.

Figure 41 Application &gt; Short Message &gt; SIM SMS



The following table describes the labels in this screen.

Table 36 Application &gt; Short Message &gt; SIM SMS

LABEL	DESCRIPTION
Delete All	Click <b>Delete All</b> to remove all messages.
	This field displays the index number of the message.
From	This field displays the mobile phone number from which the message is sent.
Time	This field displays the date and time the message was received.
Content	This field displays the content of the message.
Action	Click <b>Delete</b> to remove the message record.

## 7.10 File Sharing Screen

Use this screen to share files on a micro SD card connected to your WAH7706 with users on your network. To access this screen, click **Application > File Sharing**.

Figure 42 Application > File Sharing

The screenshot shows the 'File Sharing' configuration page. At the top, there is a radio button group for 'Enable File Sharing' with 'On' selected. Below it are two input fields: 'Server Name' containing 'WAH7706' and 'Sharing Name' containing 'ZyXEL'. At the bottom are two green buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 37 Application > File Sharing

LABEL	DESCRIPTION
Enable File Sharing	Select this to enable file sharing through the WAH7706 using Windows Explorer or by browsing to your work group.
Server Name	Specify the name to identify the WAH7706 in a work group.
Sharing Name	You can add the WAH7706 to an existing or a new workgroup on your network. Enter the name of the workgroup which your WAH7706 automatically joins. You can set the WAH7706's workgroup name to be exactly the same as the workgroup name to which your computer belongs to.  Note: The WAH7706 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Apply	Click this button to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

# CHAPTER 8

# System

## 8.1 Overview

Use the system screens to configure general WAH7706 settings.

### 8.1.1 What You Can Do in this Chapter

- Use the **System Information** screen to view basic information about the WAH7706 and restart the WAH7706 ([Section 8.2 on page 66](#)).
- Use the **User Account** screen to set the domain name and change the WAH7706's system password ([Section 8.3 on page 67](#)).
- Use the **Settings Profile** screen to reset your device settings back to the factory default, backup configuration, and restoring configuration ([Section 8.4 on page 68](#)).
- Use the **Firmware Upgrade** screen to upload new firmware to your WAH7706 ([Section 8.5 on page 70](#)).
- Use the **Time Settings** screen to change the WAH7706's time and date and configure daylight saving time ([Section 8.6 on page 71](#)).
- Use the **Power Saving** screen to enable and configure the power saving settings in the WAH7706 ([Section 8.7 on page 73](#)).
- Use the **System Log** screens to view logged messages and specify to where the WAH7706 is to send logs ([Section 8.8 on page 73](#)).

## 8.2 System Information Screen

Use this screen to view basic information about the WAH7706 and restart the WAH7706. To access this screen, click **System > System Information**.

**Figure 43** System > System Information

The following table describes the labels in this screen.

Table 38 System &gt; System Information

LABEL	DESCRIPTION
About the 4G Hotspot	
Firmware Version	This displays the current firmware version of the WAH7706.
IMEI	This displays the International Mobile Equipment Number (IMEI) which is the serial number of the built-in 3G module. IMEI is a unique 15-digit number used to identify a mobile device.
Hardware Version	This displays the hardware version of the WAH7706.
Wi-Fi1 MAC Address	This is the MAC address of the wireless network.
Wi-Fi2 MAC Address	
Reboot Device	
Reboot Device	Click <b>Reboot</b> to restart the device. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

## 8.3 User Account Screen

This screen allows you to set the domain name and change the WAH7706's system password. It is strongly recommended that you change your WAH7706's system password. To access this screen, click **System > User Account**.

See [Section 2.2 on page 12](#) for more information about login accounts.

**Figure 44** System > User Account

**Login Web URL Setting**

Web Domain Name   
(ex1: http://demourl.hotspot), (ex2: http://ghostspot.myap)

**User Settings**

Username	<input type="text" value="admin"/>
Password	<input type="password" value="****"/>
Confirm Password	<input type="password" value="****"/>
Auto Logout After	<input type="text" value="999"/> minutes

**Buttons:**

The following table describes the labels in this screen.

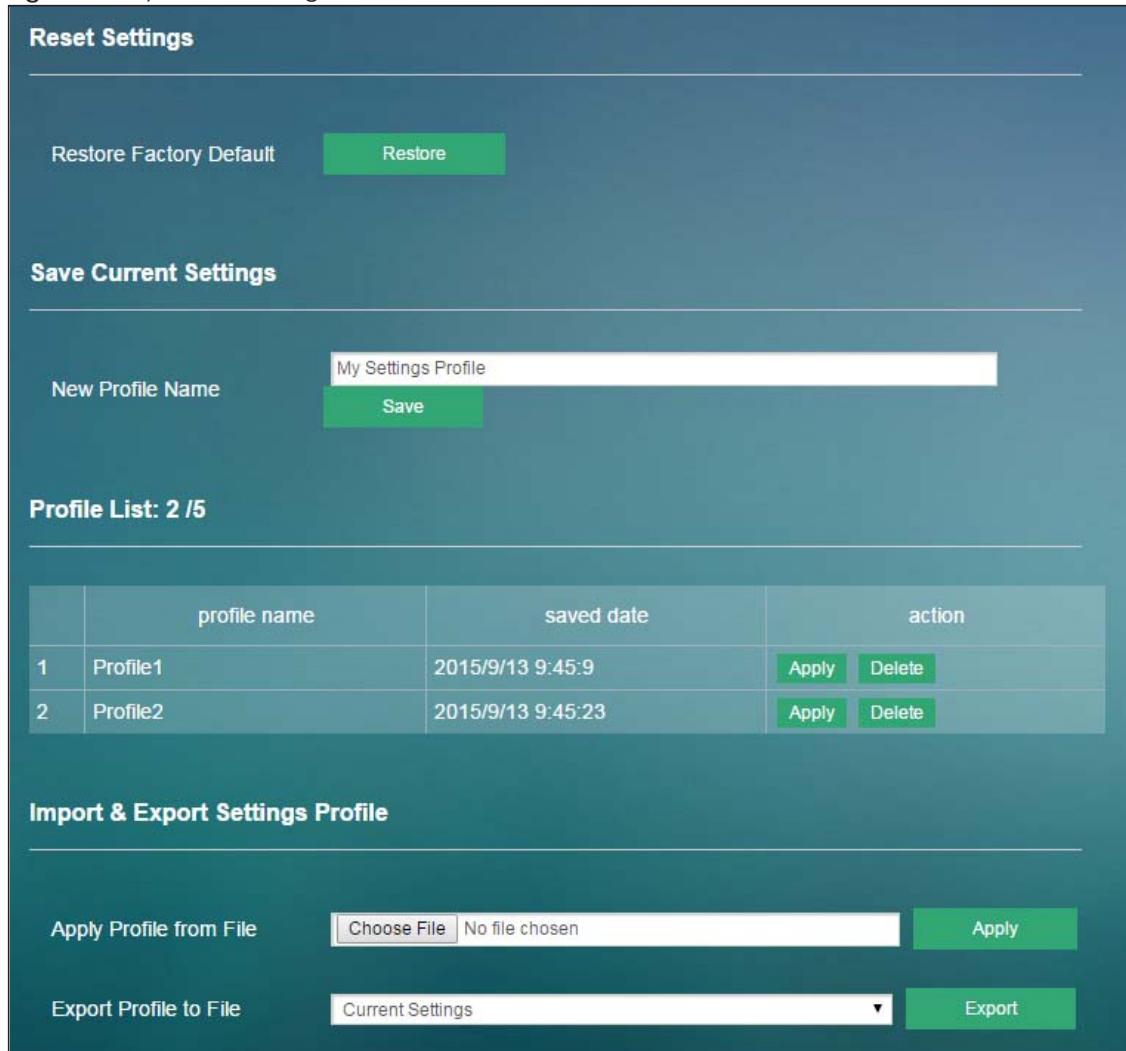
Table 39 System &gt; User Account

LABEL	DESCRIPTION
Login Web URL Setting	
Web Domain Name	Enter the domain name you want to give to the WAH7706.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
User Settings	
Username	Username is a unique name to identify the WAH7706 in an Ethernet network.
Password	Type your new system password of between 4 and 24 characters. Note that as you type a password, the screen displays as dot (.) for each character you type.
Confirm Password	Type the new password again in this field.
Auto Logout After	Type how many minutes a management session can be left idle before the session times out. The default is 3 minutes. After it times out you have to log in with your password again.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 8.4 Settings Profile Screen

The **Settings Profile** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default. To access this screen, click **System > Settings Profile**.

Figure 45 System &gt; Settings Profile



### 8.4.1 Reset Settings

Click the **Restore** button to clear all user-entered configuration information and return the WAH7706 to its factory defaults. The WAH7706 automatically restarts.

You can also press the **Reset** button on the rear panel to reset the factory defaults of your WAH7706. Refer to [Section 1.7 on page 11](#) for more information on the **Reset** button.

### 8.4.2 Save Current Settings

Enter the profile name you specified in the **New Profile Name** field, and click **Save**. The profile you saved will be displayed in the **Profile List** field.

The following table describes the labels in this screen.

Table 40 System > Settings Profile

LABEL	DESCRIPTION
	This field displays the index number of the profile.
profile name	This field displays the profile name you specified in the <b>New Profile Name</b> field.
saved date	This field displays the saved time and date of the profile.
Action	Click <b>Apply</b> to use the configuration to the WAH7706. Click <b>Delete</b> to go to the screen where you can remove the profile.

### 8.4.3 Import & Export Settings Profile

This screen allows you to upload a new or previously saved configuration file from your computer to your WAH7706.

Type in the location of the file you want to upload in the **Apply Profile from File** field or click **Choose File** to find it. Click **Apply** to begin the upload process. The WAH7706 automatically restarts.

**Do not turn off the WAH7706 while configuration file upload is in progress.**

Backup Configuration allows you to back up (save) the WAH7706's current configuration to a file on your computer. The configuration file should be saved and edited in UTF-8 (without BOM) format, if you're using Windows Notepad, make sure you choose **File > Save as** UTF-8 in the text editor. Once your WAH7706 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Select one profile from the drop-down list box in the **Export Profile to File** field, and click **Export** to save the WAH7706's current configuration to your computer.

After the WAH7706 configuration has been restored successfully, the login screen appears. If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

## 8.5 Firmware Upgrade Screen

This screen allows you to upload new firmware to your WAH7706. You can download new firmware releases from your nearest Zyxel FTP site (or [www.zyxel.com](http://www.zyxel.com)) to use to upgrade your device's performance.

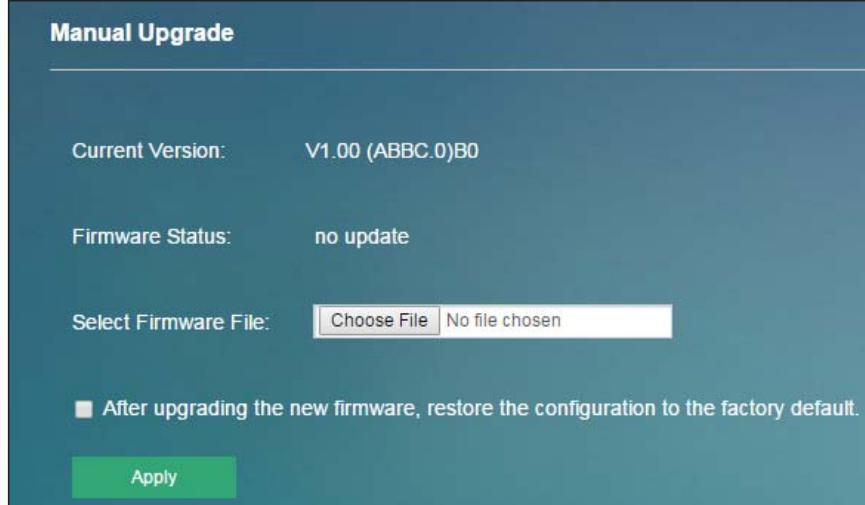
**Only use firmware for your device's specific model.**

To access this screen, click **System > Firmware Upgrade**. This screen displays the current firmware version and status of the WAH7706. Type in the location of the file you want to upload in the **Select Firmware File** field or click **Choose File** to find it. Remember that you must decompress compressed (.ZIP) files before you can upload them. You can select the check box to return the WAH7706 to its factory defaults after upgrading the new firmware. Click **Apply** to begin the upload process.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

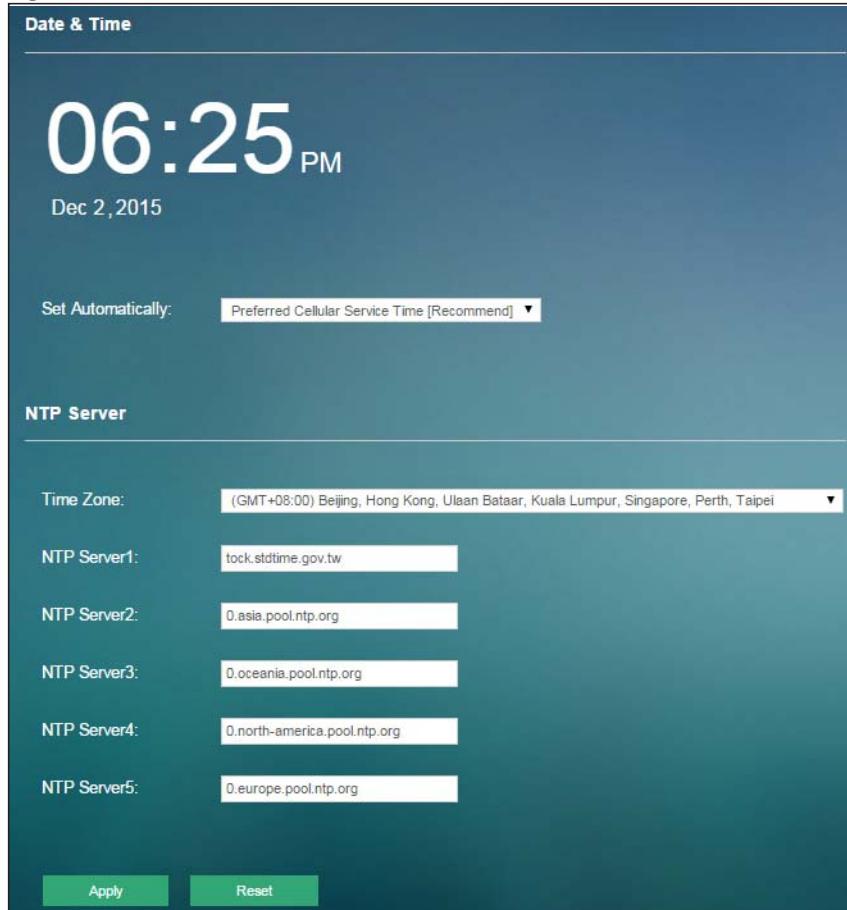
**Do NOT turn off the WAH7706 while firmware upload is in progress!**

**Figure 46** System > Firmware Upgrade



## 8.6 Time Settings Screen

For effective scheduling and logging, the WAH7706 system time must be accurate. The WAH7706 has a software mechanism to get the current time and date from an external server. To change your WAH7706's time zone, click **System > Time Settings**. The screen displays as shown. You can have the WAH7706 get the date and time from a time server or change the IP address or URL of your time server.

**Figure 47** System > Time Settings

The following table describes the labels in this screen.

**Table 41** System > Time Settings

LABEL	DESCRIPTION
Date & Time	
Device time	This field displays the present time and date of your WAH7706.
Set Automatically	Select <b>Prefer Cellular Service Time</b> to have the WAH7706 get the time and date from the cellular service server. Select <b>Prefer NTP server</b> to have the WAH7706 get the time and date from the time server you specify.
NTP Server	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
NTP Server 1~5	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 8.7 Power Saving Screen

This screen allows you to enable and configure the power saving settings in the WAH7706. To access this screen, click **System > Power Saving**.

**Figure 48** System > Power Saving



The following table describes the labels in this screen.

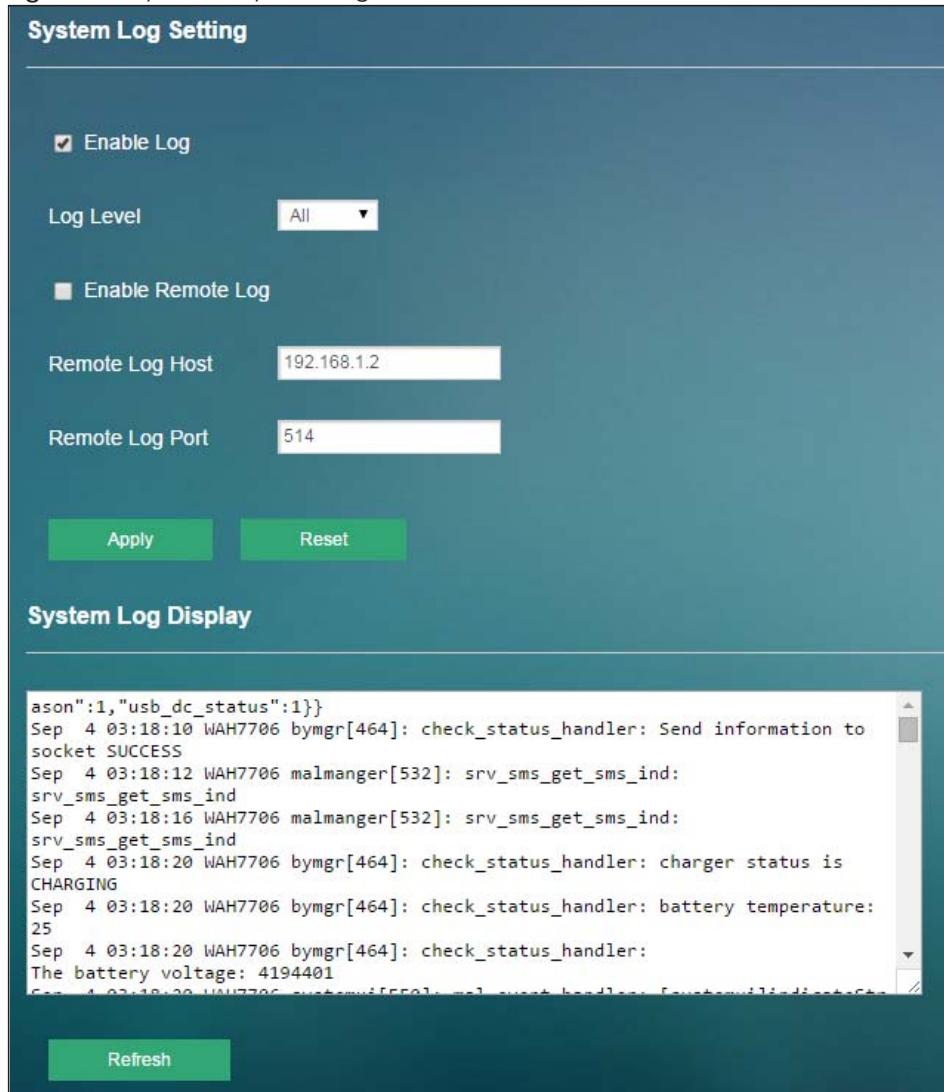
**Table 42** System > Power Saving

LABEL	DESCRIPTION
WiFi Power Saving	Select the number of minutes the WAH7706 waits before it turns off wireless connections to save battery power when the USB port is not connected and there is no wireless clients associating with the WAH7706.
WWAN Power Saving	Select the number of minutes the WAH7706 waits before it turns off the mobile network to save battery power when the USB port is not connected and there is no wireless clients associating with the WAH7706.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 8.8 System Log Screen

Use this screen to specify which logs to display and to where the WAH7706 is to send logs. Click **System > System Log**. The screen displays as shown.

Figure 49 System &gt; System Log



The following table describes the labels in this screen.

Table 43 System &gt; System Log

LABEL	DESCRIPTION
<b>System Log Setting</b>	
Enable Log	Select the check box to enable system logging.
Log Level	Select the level of the logs that the WAH7706 is to record and send to the syslog server. The WAH7706 displays and records the logs with the level equal to or higher than what you selected.
Enable Remote Log	Select the check box to enable syslog logging. Syslog logging sends a log to an external log server.
Remote Log Host	Enter the server name or IP address of the syslog server that will log the selected log level of logs.
Remote Log Port	Enter the port number of the syslog server.
Apply	Click <b>Apply</b> to save your changes back to the WAH7706.

Table 43 System &gt; System Log

LABEL	DESCRIPTION
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.
System Log Display	
The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the <b>Log Level</b> drop list. When you select a log level, the WAH7706 searches through all logs of that level or higher. The screen displays the time the log message was recorded. It also displays the reason the log message was generated.	
Refresh	Click <b>Refresh</b> to renew the log screen.

# CHAPTER 9

# Troubleshooting

## 9.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, and Hardware Installation](#)
- [WAH7706 Access and Login](#)
- [Internet Access](#)
- [Wireless Connections](#)

## 9.2 Power, and Hardware Installation

---

The WAH7706 does not turn on. The OLED display is not on.

---

- 1 Make sure the WAH7706 is correctly installed (refer to your Quick Start Guide).
- 2 Make sure the battery is installed and charged. Press the power button to turn the WAH7706 on. See [Section 1.5 on page 9](#) and [Section 1.6 on page 9](#).
- 3 If the problem continues, contact the vendor.

## 9.3 WAH7706 Access and Login

---

I forgot the IP address for the WAH7706.

---

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

---

I cannot see or access the **Login** screen in the web configurator.

---

- 1** Make sure you are using the correct IP address.
  - The default IP address is 192.168.1.1.
  - If you changed the IP address, use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the WAH7706](#).
- 2** Make sure the WAH7706 is correctly installed and turned on. See the Quick Start Guide and [Section 1.5 on page 9](#).
- 3** Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4** Make sure your computer is connected to the WAH7706 and is in the same subnet as the WAH7706.
- 5** Reset the device to its factory defaults, and try to access the WAH7706 with the default IP address. See [Section 1.7 on page 11](#).
- 6** Disconnect your computer from the Internet (Wireless and/or Ethernet) and then insert the WAH7706 again.
- 7** If the problem continues, contact the vendor.

---

[I forgot the password](#).

---

- 1** The default password is **admin** or **guest**.
- 2** If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

---

I can see the **Login** screen, but I cannot log in to the WAH7706.

---

- 1** Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2** This can happen when you fail to log out properly from your last session. Try logging in again after five minutes.
- 3** Disconnect and connect to the WAH7706 again.
- 4** If this does not work, you have to reset the device to its factory defaults. See [Section 1.7 on page 11](#).

## 9.4 Internet Access

---

I cannot access the Internet through a 3G/4G wireless WAN connection.

---

- 1 Make sure you insert a 4G SIM card into the card slot before turning on the WAH7706.
- 2 Make sure your mobile access information (such as APN) is entered correctly in the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on. Check with your service provider for the correct APN if you don't have it.
- 3 Make sure your SIM card's account is valid and has an active data plan. Check your service contract or contact your service provider directly.
- 4 If you are using a pre-paid SIM card, insert the SIM card on another mobile device to check if the SIM card still works. If the SIM card works without any problems on another mobile device, contact the vendor. Otherwise, contact your service provider.
- 5 If the problem continues, contact your ISP.

---

I cannot access the Internet anymore. I had access to the Internet (with the WAH7706), but my Internet connection is not available anymore.

---

- 1 Reboot the WAH7706.
- 2 If the problem continues, contact your ISP.

---

The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. If the WAH7706 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the WAH7706 closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the WAH7706.
- 4 If the problem continues, contact the network administrator or vendor.

## 9.5 Wireless Connections

---

I cannot access the WAH7706 or ping any computer from the WLAN.

---

- 1 Make sure the wireless LAN is enabled on the WAH7706.
  - 2 Make sure the wireless adapter (installed on your computer) is working properly.
  - 3 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the WAH7706's active radio.
  - 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAH7706.
  - 5 Check that both the WAH7706 and your computer are using the same wireless and wireless security settings.
- 

Hackers have accessed my WEP-encrypted wireless LAN.

---

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

---

I can only see newer logs. Older logs are missing.

---

When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

## 9.6 Getting More Troubleshooting Help

Search for support information for your model at [www.zyxel.com](http://www.zyxel.com) for more troubleshooting suggestions.

# APPENDIX A

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also  
[http://www.zyxel.com/about\\_zyxel/zyxel\\_worldwide.shtml](http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml) for the latest information.

Please have the following information ready when you contact an office.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

### Corporate Headquarters (Worldwide)

#### Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

#### Asia

##### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

##### India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

##### Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

## **Korea**

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

## **Malaysia**

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

## **Pakistan**

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

## **Philippines**

- Zyxel Philippines
- <http://www.zyxel.com.ph>

## **Singapore**

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

## **Taiwan**

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

## **Thailand**

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

## **Vietnam**

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

## **Europe**

### **Austria**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

### **Belarus**

- Zyxel BY
- <http://www.zyxel.by>

## **Belgium**

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

## **Bulgaria**

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

## **Czech Republic**

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

## **Denmark**

- Zyxel Communications A/S
- <http://www.zyxel.dk>

## **Estonia**

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

## **Finland**

- Zyxel Communications
- <http://www.zyxel.fi>

## **France**

- Zyxel France
- <http://www.zyxel.fr>

## **Germany**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

## **Hungary**

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

## **Italy**

- Zyxel Communications Italy
- <http://www.zyxel.it/>

## **Latvia**

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

## **Lithuania**

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

## **Netherlands**

- Zyxel Benelux
- <http://www.zyxel.nl>

## **Norway**

- Zyxel Communications
- <http://www.zyxel.no>

## **Poland**

- Zyxel Communications Poland
- <http://www.zyxel.pl>

## **Romania**

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

## **Russia**

- Zyxel Russia
- <http://www.zyxel.ru>

## **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

## **Spain**

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

## **Sweden**

- Zyxel Communications
- <http://www.zyxel.se>

## **Switzerland**

- Studerus AG

- <http://www.zyxel.ch/>

## **Turkey**

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

## **UK**

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

## **Ukraine**

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

## **Latin America**

### **Argentina**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

### **Brazil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

### **Ecuador**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

## **Middle East**

### **Israel**

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

### **Middle East**

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

## Oceania

### Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

## Africa

### South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

# APPENDIX B

## Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 44 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 44 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
RExec	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

Table 44 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

# APPENDIX C

## Legal Information

### Copyright

Copyright © 2017 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

### Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Regulatory Notice and Statement

#### UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

#### FCC EMC Statement

- The device complies with Part 15 of 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.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 device generates, uses, and can radiate radio frequency energy and, if not installed and used according to 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 device does cause harmful interference to radio or television reception, which is found by turning the device 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 devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

#### FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

#### CANADA

The following information applies if you use the product within Canada area.

#### Industry Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

#### Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

- This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz , the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégorie) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2.3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

### Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

### Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

### EUROPEAN UNION



The following information applies if you use the product within the European Union.

### Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE).
- This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EC.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulirott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htiġijiet essenzjalji u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezență, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenčina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklaerer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.

### National Restrictions

- This product may be used in all EU countries (and other countries following the EU Directive 1999/5/EC) without any limitation except for the countries mentioned below:
- Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposé la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:
- Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:
- Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs. The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":.

#### Belgium

- The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.
- Draadloze verbindingen voor buiten gebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.
- Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

#### Denmark

- In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.
- I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

#### Italy

- This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.
- Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

- The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.
- 2.4 GHz frekvenējušas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

### List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

### Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Environment Statement

### ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten nå slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



Environmental Product Declaration

Български (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
<p>Екологична продуктова декларация</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/22/CE REACH REGLAMENT (CE) n. 1907/2006 ErP Direktiv 2009/125/EG</p> <p>Име/ имя : Richard Heu / Quality Management Division Senior Manager Роден/а : Datum (dd/mm/yy): 01/10/2014 <i>Richard Heu</i></p>  	<p>Environmentální prohlášení o produkту</p> <p>RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/22/ES REACH Nařízení (ES) č. 1907/2006 ErP Směrnice 2009/125/ES</p> <p>Jméno/ titul : Richard Heu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yy): 01/10/2014 <i>Richard Heu</i></p>  	<p>Miljøvaredeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/22/EF REACH Forskrift (EG) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ titl : Richard Heu / Quality Management Division Senior Manager Underskrift : Datum (dd/mm/yy): 01/10/2014 <i>Richard Heu</i></p>  	<p>Produkt-Umweltdeklaration</p> <p>RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/22/CE REACH VERORDNUNG (EG) Nr. 1907/2006 ErP Richtlinie 2009/125/EG</p> <p>Name/ titl : Richard Heu / Quality Management Division Senior Manager Unterschrift : Datum (dd/mm/yy): 01/10/2014 <i>Richard Heu</i></p>  
<p>Toote keskkonnadeklaratsiooni</p> <p>RoHS Direktiv 2011/65/EL WEEE Direktiv 2012/19/EL PPW Direktiv 94/22/EL REACH MÄÄRUS (EU) nr. 1907/2006 ErP Direktiv 2009/125/EL</p> <p>Nimi/ pealkiri : Richard Heu / Quality Management Division Senior Manager Allikas : Kusipäev (pp/ka/aaa): 01/10/2014 <i>Richard Heu</i></p>  	<p>Environmental product declaration</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/22/CE REACH REGOLAMENT (CE) n. 1907/2006 ErP Directive 2009/125/CE</p> <p>Name/ titl : Richard Heu / Quality Management Division Senior Manager Signature : Date (dd/mm/yyyy): 01/10/2014 <i>Richard Heu</i></p>  	<p>Declaraciones Ambientales de Producto</p> <p>RoHS Directiva 2011/65/EU WEEE Directiva 2012/19/EU PPW Directiva 94/22/CE REACH REGULAMIENTO (CE) n. 1907/2006 ErP Directiva 2009/125/CE</p> <p>Nombr/ tulo : Richard Heu / Quality Management Division Senior Manager Firma : Fecha (aaaa/mm/aa): 2014/10/01 <i>Richard Heu</i></p>  	<p>Profil environnemental de produit</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/22/CE REACH REGLEMENT (CE) N° 1907/2006 ErP Directive 2009/125/CE</p> <p>Nom/ titl : Richard Heu / Quality Management Division Senior Manager Signature : Date (aaaa/mm/aa): 2014/10/01 <i>Richard Heu</i></p>  
<p>Deklaracija o zbrinjanju proizvoda</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/EZ REACH Uredba (EZ) br. 1907/2006 ErP Direktiva 2009/125/EZ</p> <p>Ime/ naziv : Richard Heu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014 <i>Richard Heu</i></p>  	<p>Dichiarazione ambientale di prodotto</p> <p>RoHS Direttiva 2011/65/EU WEEE Direttiva 2012/19/EU PPW Direttiva 94/22/CE REACH REGOLAMENTO (CE) N° 1907/2006 ErP Direttiva 2009/125/CE</p> <p>Nome/ titlo : Richard Heu / Quality Management Division Senior Manager Firma : Data (aaaa/mm/gg): 2014/10/01 <i>Richard Heu</i></p>  	<p>Produktas vides ietekmējuma deklarācija</p> <p>RoHS Direktīva 2011/65/EU WEEE Direktīva 2012/19/EU PPW Direktīva 94/22/CE REACH REĢIS (EK) Nr. 1907/2006 ErP Direktīva 2009/125/EU</p> <p>Nosaukums/ tulu : Richard Heu / Quality Management Division Senior Manager Paraksts : Datums (aaaa/mm/ggg): 01/10/2014 <i>Richard Heu</i></p>  	<p>Aplinkosauging gaminio deklaracija</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/EB REACH REGLAMENTAS (EE) Nr. 1907/2006 ErP Direktiva 2009/125/EU</p> <p>Vardas/ titulus : Richard Heu / Quality Management Division Senior Manager Paradas : Data (aaaa/mm/aaaa): 01/10/2014 <i>Richard Heu</i></p>  
<p>Környezetvédelmi terméknövelekkel</p> <p>RoHS 2011/65/EU Irányelv 2012/19/EU Irányelv PPW 94/22/KE REACH 1907/2006/EK Rendelezet ErP 2009/125/EK Irányelv</p> <p>Név/ cím : Richard Heu / Quality Management Division Senior Manager Aláírás : Dátum (kkkk/rrrr): 2014/10/01 <i>Richard Heu</i></p>  	<p>Dikjarazjoni Ambjentali dwar il-Prodott</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/CE REACH REGOLAMENT (CE) N° 1907/2006 ErP Direktiva 2009/125/KE</p> <p>Item/ titlu : Richard Heu / Quality Management Division Senior Manager Firma : Data (aaaa/xx/xx): 2014/10/01 <i>Richard Heu</i></p>  	<p>Milieuproductverklaring</p> <p>RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/22/ES REACH Verordnung (EG) nr. 1907/2006 ErP Richtlinie 2009/125/E</p> <p>Naam/ titel : Richard Heu / Quality Management Division Senior Manager Handtekening : Datum (dd/mm/jaar): 01/10/2014 <i>Richard Heu</i></p>  	<p>Deklaracj̄ środowiskowej produktu</p> <p>RoHS Dyrektywa 2011/65/EU WEEE Dyrektywa 2012/19/EU PPW Dyrektywa 94/22/ES REACH Rozporządzenie (WE) nr 1907/2006 ErP Dyrektywa 2009/125/EU</p> <p>Nazwisko/ imię : Richard Heu / Quality Management Division Senior Manager Podpis : Data (aaaa/mm/rrr): 2014/10/01 <i>Richard Heu</i></p>  
<p>Magyar (Hungarian)</p>	<p>Malti (Maltese)</p>	<p>Nederlands (Dutch)</p>	<p>Polski (Polish)</p>
<p>Standardi perustuva ympäristösuhteistoisto</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/CE REACH Regulamento (CE) n.º 1907/2006 ErP Direktiva 2009/125/EY</p> <p>Nume/ titlu : Richard Heu / Quality Management Division Senior Manager Assinatura : Data (aaaa/xx/xx): 01/10/2014 <i>Richard Heu</i></p>  	<p>Declaração ambiental do produto</p> <p>RoHS Diretiva 2011/65/EU WEEE Diretiva 2012/19/EU PPW Diretiva 94/22/CE REACH Regulamento (CE) n.º 1907/2006 ErP Diretiva 2009/125/E</p> <p>Nome/ titlu : Richard Heu / Quality Management Division Senior Manager Assinatura : Data (aaaa/xx/xx): 01/10/2014 <i>Richard Heu</i></p>  	<p>Declaratie de mediu privind produsele</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/CE REACH REGULAMENTUL (CE) N.º 1907/2006 ErP Direktiva 2009/125/E</p> <p>Nume/ titlu : Richard Heu / Quality Management Division Senior Manager Semnătură : Data (zz/ll/aaaa): 01/10/2014 <i>Richard Heu</i></p>  	<p>Vyhľásenie o environmentálnom výrobku</p> <p>RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EU PPW Smernica 94/22/ES REACH Nariadenie (ES) č. 1907/2006 ErP Smernica 2009/125/E</p> <p>Menú/ titlu : Richard Heu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/rrr): 01/10/2014 <i>Richard Heu</i></p>  
<p>Suomi (Finnish)</p>	<p>Svenska (Swedish)</p>	<p>Ελληνικά (Greek)</p>	<p>Norsk (Norwegian)</p>
<p>Standardi perustuva ympäristösuhteistoisto</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/22/CE REACH ASETUS (EY) N:o 1907/2006 ErP Direktiva 2009/125/EY</p> <p>Nume/ titlu : Richard Heu / Quality Management Division Senior Manager Allekirjoitus : Päivämäärä (pp/ka/aaa): 01/10/2014 <i>Richard Heu</i></p>  	<p>Miljöproduktdeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/22/EG REACH Förordning (EG) nr 1907/2006 ErP Direktiv 2009/125/EU</p> <p>Namn/ titl : Richard Heu / Quality Management Division Senior Manager Namnteckning : Datum (dd/mm/åååå): 01/10/2014 <i>Richard Heu</i></p>  	<p>Περιβαλλοντική δήλωση προϊόντος</p> <p>RoHS Οδηγία 2011/65/EU WEEE Οδηγία 2012/19/EU PPW Οδηγία 94/22/ΕΚ REACH Ε. ονομώση (ΕΥ) αρ. 1907/2006 ErP Οδηγία 2009/125/EU</p> <p>Δημόσιος/ Λογαριασμός : Richard Heu / Quality Management Division Senior Manager Υπογεγραφή : Ημερομηνία (ημ/μη/άμη): 01/10/2014 <i>Richard Heu</i></p>  	<p>Miljødeklarasjon</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/22/EF REACH Forordning (EF) nr. 1907/2006 ErP Direktiv 2009/125/EF</p> <p>Navn/ titl : Richard Heu / Quality Management Division Senior Manager Signatur : Datum (dd/mm/åååå): 01/10/2014 <i>Richard Heu</i></p>  

台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 秒赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 秒赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

**安全警告 - 為了您的安全，請先閱讀以下警告及指示：**

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用者或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

## Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

## Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

## Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

## Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

## Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

# Index

## A

access **12**  
authentication **40, 41**  
RADIUS server **41**

## B

Broadband **24**

certifications **92**  
viewing **96**  
channel, wireless LAN **39**  
configuration **8**  
contact information **80**  
cookies **12**  
copyright **89**  
CTS threshold **40**  
current date/time **71**  
customer support **80**

## D

data fragment threshold **40**  
date **71**  
disclaimer **89**

## E

encryption **42**  
ESSID **79**  
Extended Service Set IDentification **34**

## F

filters  
MAC address **36, 41**  
Firefox **12**  
fragmentation threshold **40**

## G

General wireless LAN screen **33**

## H

hardware connections **9**  
  
**I**  
  
installation **8**  
Internet Explorer **12**  
IP Address **50**

## J

Java  
permissions **12**  
JavaScripts **12**

## L

LEDs **9, 11**  
limitations  
wireless LAN **42**  
WPS **48**

logout  
Web Configurator **15**

## M

MAC address  
filter **36, 41**  
MAC authentication **36**  
maintenance **8**  
management **8**  
managing the device  
good habits **9**

## N

Netscape Navigator **12**

## O

overview **8**

## P

PBC **43**  
PIN, WPS **43**  
example **45**  
pop-up windows **12**  
preamble **40**  
Push Button Configuration, see PBC  
push button, WPS **43**

## R

RADIUS server **41**  
RTS threshold **40**

## S

screen resolution **12**  
security  
wireless LAN **40**  
Service Set **34**  
SIM card **9**  
SSID **41**  
status **20**  
supported browsers **12**

## T

thresholds  
data fragment **40**  
RTS/CTS **40**  
time **71**

## U

use **8**

## W

WAN  
Wide Area Network, see WAN **24**  
warranty **96**  
note **96**  
Web Configurator **9, 12**  
access **12**  
requirements **12**  
supported browsers **12**  
web configurator **8**  
WEP **42**  
Wi-Fi **31**  
wireless channel **79**  
wireless LAN **31, 38, 79**  
authentication **40, 41**  
channel **39**  
encryption **42**  
example **38**  
fragmentation threshold **40**

limitations **42**  
MAC address filter **36, 41**  
preamble **40**  
RADIUS server **41**  
RTS/CTS threshold **40**  
security **40**  
SSID **41**  
WEP **42**  
WPA **42**  
WPA-PSK **42**  
WPS **43, 45**  
example **46**  
limitations **48**  
PIN **43**  
push button **43**  
wireless security **79**  
WPA **42**  
WPA-PSK **42**  
WPS **43, 45**  
example **46**  
limitations **48**  
PIN **43**  
example **45**  
push button **43**