



User's Manual

802.11n Wall Plug Universal WiFi Repeater MNAP-1260



www.PLANET.com.tw

Copyright

Copyright © 2012 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

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

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

FCC Caution:

To assure continued compliance, (example-use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions:

- (1) This device may not cause harmful interference
- (2) This Device must accept any interference received, including interference that may cause undesired operation.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Stand by mode operation.

For energy saving, please remove the device from the power circuit.

Without remove the device, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the the device if this device is not intended to be active.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)

Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications
Russian Federation	None	Only for indoor applications

WEEE Regulation



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 802.11n Wall Plug Universal WiFi Repeater Model: WNAP-1260 Rev: 1.0 (May, 2012) Part No. EM-WNAP-1260_v1.0 (2081-E10450-000)

CONTENTS

Chapter 1. Product Introduction	1
1.1. Package Contents	1
1.2. Product Description	1
1.3. Product Features	4
1.4. Product Specification	5
Chapter 2. Hardware Interface	8
2.1. Overview	8
2.2. Front Panel and LED Indications	9
2.3. Rear / Side Panel and Interface Description	10
Chapter 3. Operation Mode Introduction	11
3.1. Wireless Universal Repeater / WDS Mode	11
3.2. AP Mode	11
3.3. Router Mode	12
3.4. Client Mode	13
Chapter 4. Installation Guide	14
4.1. System Requirements	14
4.2. Before You Begin	14
4.3. Operation Range	14
4.4. Manual Network Setup – TCP / IP Configuration	14
4.4.1. Obtain an IP Address Automatically	15
4.4.2. Configure the IP address manually	17
4.5. Hardware Installation	19
4.6. Starting Setup in Web UI	21
Chapter 5. Quick Mode Configuration	24
5.1. Repeater Mode Configuration	24
5.2. WDS Mode Configuration	26
5.2.1. Repeater Configuration in the WDS Mode	26
5.2.2. Central Base Station Configuration in the WDS Mode	27
5.2.3. WDS Application	
5.3. Bridge Mode Configuration	29
5.4. Router Mode Configuration	
5.5. Client Mode Configuration	32
Chapter 6. Web Configuration for the Wireless Universal Repeater Mode	34
6.1. Running Status	34
6.1.1. System Status	
6.1.2. Clients List	
6.2. Setup Wizard.	
6.3. Repeater Mode Setting	
6.4. Network Settings	
6.4.1. LAN Interface Settings	36

	6.4.2. DHCP Server	.36
	6.5. Wireless Settings	. 38
	6.5.1. Wireless Universal Repeater	.38
	6.5.2. WPS Setup	.39
	6.5.3. Wireless Client Function	.41
	6.6. Management Function	.42
	6.6.1. Backup Settings	.42
	6.6.2. Reboot Device	.43
	6.6.3. Set Password	.43
	6.6.4. Upgrade	.44
Chap	oter 7. Web Configuration for the Bridge Mode	.45
	7.1. Bridge / AP Mode Topology	.45
	7.2. Hardware Setting	.45
	7.3. Running Status	.45
	7.3.1. System Status	.45
	7.3.2. Clients List	.46
	7.4. Setup Wizard	.46
	7.5. Mode Setting	.46
	7.6. Network Settings	.47
	7.6.1. LAN Interface Settings	.47
	7.6.2. DHCP Server	.48
	7.7. Wireless Settings	.49
	7.7.1. Wireless Basic Settings	.49
	7.7.2. Multiple SSID	.53
	7.7.3. Wireless Advanced Settings	.54
	7.7.4. WPS Setup	.57
	7.8. Management Function	.59
	7.8.1. Backup Settings	.60
	7.8.2. Reboot Device	.60
	7.8.3. Set Password	.61
	7.8.4. Upgrade	.01
Chap	oter 8. Web Configuration for the Router Mode	.62
	8.1. Router Mode Topology	.62
	8.2. Hardware Setting	.62
	8.3. Running Status	.62
	8.3.1. System Status	.63
	8.3.2. Clients List	.65
	8.4. Setup Wizard	.65
	8.5. Mode Setting	.65
	8.6. Network Settings	.66
	8.6.1. LAN Interface Settings	.66
	8.6.2. WAN Interface Settings	.66
	8.6.3. DHCP Server	.73
	8.6.4. VPN Passtnrougn	. 75
	8.7. Wireless Settings	.76

8.7.1. Wireless Basic Settings	
8.7.2. Multiple SSID	79
8.7.3. Wireless Advanced Settings	81
8.7.4. WDS Function	84
8.7.5. WPS Setup	85
8.8. Network Application	87
8.8.1. Port Forwarding	
8.8.2. Port Triggering	88
8.8.3. UPnP	90
8.8.4. IGMP Proxying	91
8.8.5. DMZ Server	91
8.8.6. Dynamic DNS	
8.8.7. Static Routes	
8.9. Security Options	94
8.9.1. Block Sites	
8.9.2. Block Services	95
8.9.3. Protection	
8.10. Management Function	
8.10.1. Backup Settings	
8.10.2. Remote Management	
8.10.3. Schedules	
8.10.4. SNTP	
8.10.5. Reboot Device	
8.10.6. Set Password	
8.10.7. Upgrade	
Chapter 9 Web Configuration for the WDS Mode	104
Chapter 9. Web Configuration for the WDS Mode	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2 Hardware Setting	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3 Running Status	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 0.4. Setur Wizerd	104 104 104 104 104 104 105
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard	104 104 104 104 104 104 105 105
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server	104 104 104 104 104 104 104 105 105 105 105 106 106 106
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings	104
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings 9.7.1. WDS Function	104 104 104 104 104 104 104 105 105 105 105 106 106 106 108 108 108
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings 9.7.1. WDS Function 9.7.2. Wireless Basic Settings	104
 Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings 9.7.1. WDS Function 9.7.2. Wireless Basic Settings 9.8. Management Function 	104 104 104 104 104 104 104 105 105 105 105 105 106 106 106 106 108 108 108 109 113
Chapter 9. Web Configuration for the WDS Mode	104 104 104 104 104 104 104 105 105 105 105 105 106 106 108 109 113
Chapter 9. Web Configuration for the WDS Mode	104 104 104 104 104 104 104 105 105 105 105 105 106 106 108 109 113 114
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings 9.7.1. WDS Function 9.7.2. Wireless Basic Settings 9.8.1. Backup Settings 9.8.2. Reboot Device 9.8.3. Set Password	104 104 104 104 104 104 104 105 105 105 105 105 106 106 108 109 113 114
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Settings 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7.1. WDS Function 9.7.2. Wireless Basic Settings 9.8.1. Backup Settings 9.8.2. Reboot Device 9.8.3. Set Password 9.8.4. Upgrade	104 104 104 104 104 104 104 104 105 105 105 105 106 106 108 109 113 114 115
Chapter 9. Web Configuration for the WDS Mode 9.1. WDS Mode Topology 9.2. Hardware Setting 9.3. Running Status 9.3.1. System Status 9.3.2. Clients List 9.4. Setup Wizard 9.5. Mode Setting 9.6. Network Settings 9.6.1. LAN Interface Settings 9.6.2. DHCP Server 9.7. Wireless Settings 9.7.1. WDS Function 9.7.2. Wireless Basic Settings 9.8.1. Backup Settings 9.8.2. Reboot Device 9.8.3. Set Password 9.8.4. Upgrade Chapter 10. Web Configuration for the Client Mode	104 104 104 104 104 104 105 105 105 105 105 105 106 106 108 109 113 114 114 115 116

10.2. Hardware Setting	116
10.3. Running Status	116
10.3.1. System Status	
10.3.2. Clients List	117
10.4. Setup Wizard	117
10.5. Network Settings	117
10.5.1. LAN Interface Settings	
10.5.2. DHCP Server	118
10.6. Wireless Settings	120
10.6.1. WPS Setup	120
10.6.2. Wireless Client Function	121
10.7. Management Function	122
10.7.1. Backup Settings	122
10.7.2. Reboot Device	123
10.7.3. Set Password	124
10.7.4. Upgrade	
Chapter 11. Quick Connection to a Wireless Network	125
11.1. Windows XP (Wireless Zero Configuration)	125
11.2. Windows 7 (WLAN AutoConfig)	127
11.3. Mac OS X	129
11.4. iPhone / iPod Touch / iPad	134
Appendix A. Planet Smart Discovery Utility	137
Appendix B. FAQ	138

Chapter 1. Product Introduction

1.1. Package Contents

The following items should be contained in the package:

- WNAP-1260 Wall Plug Universal WiFi Repeater
- Ethernet Cable
- Quick Installation Guide
- CD-ROM (User's Manual included)

If there is any item missed or damaged, please contact the seller immediately.

1.2. Product Description

WNAP-1260, a WiFi Repeater, is case-shaped, easy to carry, and easy to install. Its wireless transmission rate is up to 300 Mbps. It is a high-performance and IEEE802.11b/g/n-compatible network access device that can provide reliable and convenient network access service for individual users and SOHO (Small Office, Home Office). It features Web-based GUI, allowing users to easily modify settings to connect the device to ISP (Internet Service Provider) and conveniently perform upgrade using the WEB page.



In addition, WNAP-1260 has a three-way switch on the side panel that enables users to change the device's working mode among **AP**, **Repeater**, and **Client**. In the AP mode, the device functions as a wireless router to achieve wireless connection for the wired LAN. In the Repeater mode, the device provides the URM (Universal Repeater Mode) function for users to expand wireless coverage of the existing AP in a quick and easy way. In the Client mode, the device functions as a wireless network adapter but it can provide a better transmission and connection performance.



Multiple Wireless Network Technologies for Greater Access

PLANET Wall Plug Universal WiFi Repeater, the WNAP-1260 features 802.11n radio with 2T2R antenna technology compliant with 802.11b/g/n standards. Compared with general wireless routers, the WNAP-1260 offers more powerful and flexible capability for business demands to access Internet with true mobility and range extension of wireless network.

More Flexibility and Mobility

With the tiny-sized and wall plug design, the WNAP-1260 is easy to plug to wall outlet for wireless access in any place. It can operate in various environments with the hardware switch modes including AP, Repeater, and Client, which helps to immediately set up a wireless network without software configuration. The wall plug design and operation flexibility make the WNAP-1260 suitable for range extending.



Figure 1-1

One-touch Secure WiFi Extension

In order to simplify security settings for home and SOHO network, the WNAP-1260 supports **W**i-Fi **P**rotected **S**etup (**WPS**) with configuration in PBC and PIN type. Just push the WPS button or key in the PIN code, the secure connection between the WNAP-1260 and the Access Point can be built immediately, which offers users a convenient and fast method to extend a secure wireless network.





Wide Range of Wireless Security Support

To secure the wireless communication, the WNAP-1260 supports most up-to-date encryptions including WPA/WPA2-PSK with TKIP/AES. Made to fulfill enterprise and various applications demand, the WNAP-1260 enhances security and management features such as multiple SSID support. It can create up to 5 virtual standalone AP with 5 different SSID according to individual security levels and encryption scheme of various wireless devices.

Internet Broadband Sharing

PLANET Wall Plug Universal WiFi Repeater, WNAP-1260, provides home and SOHO users a reliable and cost effective wireless solution by featuring WAN Internet access and high speed IEEE 802.11n wireless transmission. The WNAP-1260 is equipped with one LAN/WAN port for connection to local network or for wired cable / xDSL service connection. The WNAP-1260 provides more flexible and easier way for users to share an instant wireless network service via range extension wherever at Home, Hotspot, or in public places like transportation, outdoor events, and etc.

Advanced Firewall Security

In the Router mode, the WNAP-1260 supports NAT functions and allows multiple users to access Internet via only one single legal IP. It provides Port Forwarding and DMZ for LAN PC to act as an application server. Furthermore, the advanced firewall by the WNAP-1260 can protect your Intranet clients from unauthorized accesses and various DoS attacks from the Internet. In aspect of the firewall, the WNAP-1260 provides IP/ MAC/ Port/ URL filtering, and prevents possible hackers attack.

Easy Setup Anytime Anywhere

The WNAP-1260 provides a total solution for home and business users. With the High Speed 802.11n wireless technology, the WNAP-1260 is easy to integrate the wireless devices with existing wired network.



1.3. Product Features

Industrial Compliant Wireless LAN & LAN

- Compliant with IEEE 802.11n wireless technology capable of up to 300Mbps data rate
- Backward compatible with 802.11b/g standard
- Equipped with 10/100Mbps RJ-45 Ports for LAN/ WAN, Auto MDI/ MDI-X supported

Fixed-network Broadband Router

- Supported connection types: Dynamic IP/ Static IP / PPPoE / PPTP / L2TP
- Support Static Routing, IGMP Proxy
- Support multiple sessions SIP ALG, IPSec, L2TP and PPTP VPN pass-through
- Support DMZ, Port Forwarding and Port Triggering for various networking applications
- Support DHCP Server, UPnP, Planet Dynamic DNS

Wireless Network Range Extender

- Multiple Wireless Modes: AP, WDS, Repeater, Universal Repeater, Client
- Support Multiple SSID to allow users to access different networks through a single AP
- Support WMM (Wi-Fi Multimedia), Wireless QoS
- Support IAPP (Inter Access Point Protocol), Wireless Roaming

Secure Network Connection

- Advanced security: 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK(TKIP/AES)
- Built-in NAT firewall features, with SPI function to protect against DoS attacks.
- Support IP/ MAC/ URL/ DNS Filtering

Easy Installation & Management

- Web-based UI and Quick Setup Wizard for easy configuration
- Remote Management allows configuration from a remote site
- System status monitoring includes DHCP Client and Associated Client list

Flexible Usage & Compact Design

- Built-in Power Supply & Wall-Plug design
- Hardware switchable operation modes: AP / Repeater / Client
- Easy Sync by One-touch Wi-Fi Protected Setup (WPS)

Product	WNAP-1260		
Troduct	300Mbps 802.11n Wall Plug Universal WiFi Repeater		
Hardware Specificati	on		
Interface	LAN/WAN	1 x 10/100Mbps Auto MDI/MDI-X RJ45 port	
Antenna	Gain:	2 x Internal 2dBi Antenna	
Antenna	Orientation:	Horizontal and Vertical	
Button/Switch	Mode Selec WPS Button Reset buttor *Push about	tion Switch (AP / Repeater / Client) n : 3~6 seconds to reset to factory default settings	
LED Indicators	PWR, WPS,	Ethernet, WLAN	
Power Consumption	On-state: 2. Low power s	1W state: 1.5W	
Material	Plastic		
Dimension	75 x 55 x 40	mm (L x W x H)	
Weight	80g (gross v	veight)	
Wireless interface Sp	pecification		
Standard	Compliance	with IEEE 802.11b/g/n	
Frequency Band	2.4~2.48350	GHz	
Extend Frequency	DSSS		
Modulation Type	DBPSK, DQPSK, QPSK, CCK and OFDM (BPSK/QPSK/16-QAM/ 64-QAM)		
Data Transmission Rates	11n (40MHz 11n (20MHz 11g: 54/48/3 11b: 11/5.5/2): 270/243/216/162/108/81/54/27Mbps 135/121.5/108/81/54/40.5/27/13.5Mbps (Dynamic)): 130/117/104/78/52/39/26/13Mbps 65/58.5/52/39/26/19.5/13/6.5Mbps (Dynamic) 26/24/18/12/9/6Mbps (Dynamic) 2/1Mbps (Dynamic)	
Transmission Distance	Indoor up to outdoor up t	100m o 300m (it is limited to the environment)	
Channel	America/ FC Europe/ ETS Japan/ TELE	CC: 2.412~2.462GHz (11 Channels) SI: 2.412~2.472GHz (13 Channels) EC: 2.412~2.484GHz (14 Channels)	
Channel Width	20/ 40MHz		
Max. RF Power	11b: 17±1.50 11g: 14±1.50 11n (20MHz 11n (40MHz	dBm dBm): 14±1.5dBm): 14±1.5dBm	
Receive Sensitivity	11b: -92dBn 11g: -88dBn 11n: -90dBn	n @ 1Mbps; -85dBm @ 11Mbps, PER < 8% n @ 6Mbps; -73dBm @ 54Mbps, PER <10% n @ MCS8; -70dBm @ MCS15, PER <10%	

1.4. Product Specification

Software Features				
	AP/Router			
Operation Mode				
	(Switchable by H/W)			
	AP Client WDS PTP WDS PTMP Repeater (WDS+AP) Universal			
Wireless Mode	Repeater (AP+Client)			
	WEP (64/128-bit) encryption security			
Encryption Security	WPA / WPA2 (TKIP/AES)			
	WPA-PSK / WPA2-PSK (TKIP/AES)			
	Provide wireless LAN ACL (Access Control List) filtering			
Wireless Security	Wireless MAC address filtering up to 16 entries			
wireless Security	Support WPS (Wi-Fi Protected Setup)			
	Enable / Disable SSID Broadcast			
	WMM(Wi-Fi Multimedia): 802.11e Wireless QoS			
	Multiple SSID: up to 4			
	Wireless Isolation: Enable it to isolate each connected wireless clients, to			
wireless Auvanceu	ble / Disable SSID Broadcast vl(Wi-Fi Multimedia): 802.11e Wireless QoS iple SSID: up to 4 less Isolation: Enable it to isolate each connected wireless clients, to iem cannot access mutually. 2 (Inter Access Point Protocol): 802.11f Wireless Roaming ride Wireless Statistics :: 253 less: 32 res data and Internet access for users, supporting following internetess: Dynamic IP Static IP			
	IAPP(Inter Access Point Protocol): 802.11f Wireless Roaming			
	Provide Wireless Statistics			
Max Clients	Wire: 253			
	Wireless: 32			
	Shares data and Internet access for users, supporting following internet			
	access:			
Internet Connection	■ Static IP			
Туре	■ PPPoE			
	NAT firewall with SPI (Stateful Packet Inspection)			
Firowall	Built-In NAT server supporting Port Forwarding, Port Higgering, and Diviz			
Thewan	Support ICMP ELOOD, UDP ELOOD, TCP SYN ELOOD, filter, Dos			
	support ICMP-FLOOD, ODP-FLOOD, TCP-STN-FLOOD IIIter, Dos			
Routing Protocol	Static Routing			
VPN Pass-through				
Vi i i i u u u u u u u u u u u u u u u u	Built-in DHCP server supporting static IP address distributing			
LAN	Support UPnP Dynamic DNS			
	Support IGMP Proxy			
	Web-based (HTTP) management interface			
System	ystem SNTP time synchronize			
Management	Easy firmware upgrade			

Standards Conformance			
	IEEE 802.11n (2T2R, up to 300Mbps)		
	IEEE 802.11g		
	IEEE 802.11b		
IEEE Standards	IEEE 802.11i		
	IEEE 802.3 10Base-T		
	IEEE 802.3u 100Base-TX		
	IEEE 802.3x Flow Control		
Others Protocols and Standards	CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP		

Chapter 2. Hardware Interface

2.1. Overview





Figure 2-2

2.2. Front Panel and LED Indications

The LEDs on the top panel indicate the instant status of **System power**, **WPS**, **Wireless data activity**, **Ethernet port links and data activity**, and help monitor and troubleshoot when needed. Figure 2-3 and Table 2-1 show the LED indications of the WNAP-1260.





LED Definition

LED	COLOR	STATE	FUNCTION
	Green	On	The device is working normally.
U Power	Red	On	The system is in the process of self-inspection or fails the self-inspection. Or it is in the process of software upgrade.
		Off	The WPS session is down.
		On	The WPS indicator keeps on for 5 minutes after WPS (Wi-Fi Protected Setup) connection succeeds.
1 WPS	Green	Quick blink	A terminal is attempting to connect to the WNAP-1260 through WPS but fails.
		Quick blink with a certain interval	Multiple terminals are connecting to the WNAP-1260 through WPS at the same time. WPS sessions conflict.
		Slow blink	The WPS session is up.
		Off	The Ethernet port is in the non-communication state.
Ethernet	Green	On	The Ethernet port is in the communication state.
		Blink	The Ethernet port is transmitting and receiving data.
		Off	The WLAN connection is in the non-communication state.
😨 wlan	Green	On	The WLAN connection is in the communication state.
		Blink	Data is being transmitted and received in the WLAN.

Table 2-1

2.3. Rear / Side Panel and Interface Description





Side Panel





Object	Description
WAN / LAN	If WNAP-1260 is set to the Router mode , the interface is a WAN interface which connects WNAP-1260 to WAN or uplink network devices.
	If WNAP-1260 is set to the Repeater / Client mode , the interface is an LAN interface.
Reset	Press the Reset button gently for 3-6 seconds and then release it. The system restores to the factory default settings.
	It is used for setting WNAP-1260 to the AP, Repeater, or
	Client mode.
AP / Repeater / Client	AP mode—including the Bridge and router modes
	Repeater mode—to expand wireless network coverage
	Client mode—equivalent to a wireless network adapter
WPS	For enabling WPS PBC mode. For more information, refer to
WF3	WPS descriptions for each mode.



Chapter 3. Operation Mode Introduction

3.1. Wireless Universal Repeater / WDS Mode

In the Wireless Universal Repeater / WDS mode, WNAP-1260 expands wireless coverage of the existing AP. Computers can connect to WNAP-1260 in either a wired or wireless way.

Operation Mode Switch - Repeater Mode



Typical Application

In the Wireless Universal Repeater / WDS mode, WNAP-1260 extends the coverage of AP, even if your AP/Router doesn't have WDS function.



Figure 3-1

3.2. AP Mode

In the AP (Access Point) mode, WNAP-1260 works as a wireless router to achieve wireless connection for the wired LAN.

Operation Mode Switch – AP Mode



Typical Application

In AP Mode, the **NAT** (Network Address Translation) function and DHCP server are both disabled, and all wireless clients obtain the IP address from the network device connected with LAN port of the WNAP-1260. They can certainly assign the IP address for themselves as well in the Control Panel of Windows. The WNAP-1260 is supposed to bridge to the Ethernet directly by UTP cable.



Figure 3-2

3.3. Router Mode

In the Router mode, WNAP-1260 works as a domestic gateway.

Operation Mode Switch – Router Mode



Typical Application

In Router Mode, the NAT (Network Address Translation) function and DHCP server are both enabled, and all wireless clients share the same public IP assigned by ISP through WAN port of the WNAP-1260. The WNAP-1260 is supposed to connect with the Cable / xDSL Modem by UTP cable.



Figure 3-3

3.4. Client Mode

In the Client mode, WNAP-1260 provides Internet access for a set-top box or a computer with a network adapter.

■ Operation Mode Switch – Client Mode



Typical Application

In Client Mode, the WNAP-1260 is supposed to act as a wireless station for the PC. Users can site survey the available local AP and choose someone to connect with.



Figure 3-4

Chapter 4. Installation Guide

4.1. System Requirements

Before installing the device, please ensure that the following items are available:

- PCs with a working Ethernet Adapter and an Ethernet cable with RJ-45 connectors
- PC of subscribers running Windows 98/ME, NT4.0, 2000 / XP, Windows Vista / Win 7, MAC OS 9 or later, Linux, UNIX or other platform compatible with TCP / IP protocols
- Above PC installed with WEB Browser
- Broadband Internet Access Service (Cable / xDSL / Ethernet connection; for Router mode only)
- One Cable / xDSL Modem that has an RJ-45 connector (not necessary if the WNAP-1260 is connected directly to the Ethernet.)



It is recommended to use Internet Explorer 7.0 or above to access the WNAP-1260.

4.2. Before You Begin

Before you install the device, please pay attention to the following items:

- The Ethernet cables that are used to connect the device to a computer, hub, router, or switch should be less than 100 meters.
- Do not place this device on an uneven or unstable surface. Do not put this device on the ground.
- Keep the device clean. Prevent the device from direct sunlight. Avoid any metal in the device.
- Place the device in the center of the area to optimize the wireless coverage.

4.3. Operation Range

The operation range of WNAP-1260 WiFi repeater depends on the actual environment. The path and effect of signal transmission vary with the deployment in a house or an office. For example, the outdoor straight transmission distance for a certain device can reach 300 meters and the indoor transmission distance can reach 100 meters.

4.4. Manual Network Setup – TCP / IP Configuration

The default IP address of the WNAP-1260 is **192.168.1.253**, and the default Subnet Mask is **255.255.255.0**. These values can be changed as you desire in the web UI of the WNAP-1260. In this section, we use all the default values for description.

No matter you want to configure the WNAP-1260 via wired or wireless connection, the PC need to be assigned an IP address first. Before you connect the local PC to the WNAP-1260 via wired or wireless connection, please configure the IP address for your PC in the following two ways first.

- Obtain an IP address automatically
- Configure the IP address manually

The following sections will introduce how to install and configure the TCP / IP correctly in **Windows 7**. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter's manual if needed.

4.4.1. Obtain an IP Address Automatically

If you are sure the DHCP server of WNAP-1260 is enabled (the default setting of Router Mode), you can set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. And then the WNAP-1260 built-in DHCP server will assign an IP address to the PC automatically.

- 1) On the Windows taskbar, click the Start button, point to Control Panel, and then click it.
- 2) Under the **Network and Internet** icon, click on the **View network status and tasks.** And then click **Change adapter settings**.

Control Panel	All Control Panel Items Network and Sharing Center	_
Control Panel Home	View your basic network information and set up connections	
Manage wireless networks Change adapter settings Change advanced sharing	See full m R600 (This computer)	əp
sectings	View your active networks Connect to a networks	nie
	Set up a new connection of network Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access poin Connect to a network Connect or reconnect to a wireless, wired, dial-up, or VPN network connection. Choose homegroup and sharing options Access files and printers located on other network computers, or change sharing settings.	vt.
See also HomeGroup iCloud Internet Options MobileMe	Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.	

Figure 4-1

3) Right-click on the **Wireless Network Connection**, and select **Properties** in the appearing window.



Figure 4-2

 In the prompt window shown below, double click on the Internet Protocol Version 4 (TCP/IPv4).

UVITE Wireless Network Connection Properties
Networking
Connect using:
Intel(R) Wireless WiFi Link 4965AGN
Configure
This connection uses the following items:
 Client for Microsoft Networks QoS Packet Scheduler Ele and Printer Sharing for Microsoft Networks
 Reliable Multicast Protocol
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
 ✓ → Link-Layer Topology Discovery Mapper I/O Driver ✓ → Link-Layer Topology Discovery Responder
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

Figure 4-3

5) Choose **Obtain an IP address automatically**, and **Obtain DNS server address automatically** as shown in the figure below. Then click **OK** to save your settings.

Internet Pr	otocol Version 4 (TCP/II	Pv4) Prope	erties			?	x
General	Alternate Configuration						
You can this cap for the	n get IP settings assigned a bability. Otherwise, you ne appropriate IP settings.	automatica ed to ask y	lly if y our n	our networ	etwork : k admin	suppor istrato	ts r
() ()	otain an IP address autom	atically					
	e the following IP address	:					
IP ad	ddress:						
Subn	net mask:		\mathbf{C}	•			
Defa	ult gateway:		1				
() Ob	otain DNS server address a	automatical	ly				
- Us	e the following DNS serve	r addresse	s:				
Prefe	erred DNS server:						
Alter	nate DNS server:		•				
Va	alidate settings upon exit				Adva	anced.	
				ОК		Car	ncel

Figure 4-4

4.4.2. Configure the IP address manually

If you are sure the DHCP server of WNAP-1260 is disabled (the default setting of AP Mode and Client Mode), you can configure the IP address manually. The IP address of your PC should be 192.168.1.xxx (the same subnet of the IP address of WNAP-1260, and "xxx" is any number from 1 to 254), Subnet Mask is 255.255.255.0, and the Gateway is 192.168.1.253 (The default IP address of WNAP-1260)

- 1) Continue the settings from the last figure, select **Use the following IP address** radio button.
- If the LAN IP address of the WNAP-1260 is 192.168.1.253, enter IP address 192.168.1.x (x is from 1 to 254), and Subnet mask 255.255.255.0.
- Enter the LAN IP address of the WNAP-1260 (the default IP is 192.168.1.253) into the Default gateway field.
- Select Use the following DNS server addresses radio button. In the Preferred DNS Server field, you can enter the DNS server IP address provided by your local ISP. Then click OK to save your settings.

Internet Protocol Version 4 (TCP/IPv	4) Properties
General	
You can get IP settings assigned aut this capability. Otherwise, you need for the appropriate IP settings.	tomatically if your network supports to ask your network administrator
Obtain an IP address automatic	ally
• Use the following IP address:	
IP address:	192.168.1.200
S <u>u</u> bnet mask:	255.255.255.0
<u>D</u> efault gateway:	192.168.1.1
Obtain DNS server address auto	omatically
─	ddresses:
Preferred DNS server:	8.8.8.8
Alternate DNS server:	8.8.4.4
Validate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Figure 4-5

4.5. Hardware Installation





STEP 3: Using WPS Button to establish connection with AP:

- (1) In the existing Wireless Router or AP, push the **WPS Button** within 2 minutes.
- (2) In the WNAP-1260, push the **WPS Button** from the side panel within 2 minutes.
- (3) Wait for the connection being established. If connection is successfully established, the "**WPS**" LED will light for 5 minutes.







For the first time setup, you can move WNAP-1260 close to the access point you wish to connect, after connection established, you can move WNAP-1260 to the place you wish to use.

4.6. Starting Setup in Web UI

Default SSID: WiFiRepeater-001

*Default Wireless Security: None

lease use your PC to site survey the wireless signal of WNAP-1260, and connect
our PC with it wirelessly.
Not connected Image: Connections are available Wireless Network Connection WiFiRepeater-001 Image: Connect automatically Connect Name: WiFiRepeater-001 Signal Strength: Excellent Security Type: WPA2-PSK Radio Type: 802.11n SSID: WiFiRepeater-001 Open Network and Sharing Center



PLANET Networking & Companying	
UserName: Password:	admin ••••• Login Reset
Default IP Address: 192.168.1.253 Default Username: admin Default Password: admin Default SSID: WiFiRepeater-001	

STEP 3: When you have successfully logged in, select "**Setup wizard**". You will then be able to select one of two options, choose "**Wireless Universal repeater mode**" and click next to continue.

Se	tup Wizard							
Step2: Please configure the wireless client first. Click "Site Survey" button to survey wireless sites when cl ient mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next". Site Survey								
Number of Sites Scaned : 8								
Nur	nber of Sites Scane	ed :			8			
Nur Sit #	nber of Sites Scane e Survey List SSID	ed : BSSID	Channel	Signal	8 Encrypt	Select		
Nur Sit #	nber of Sites Scane e Survey List SSID WiFi_Original	ed : BSSID 00:30:4F:11:22:33	Channel 11	Signal	8 Encrypt WPA2-PSK(AES)	Select		
Nur Sit # 1	nber of Sites Scane e Survey List SSID WiFi_Original C3220	ed : BSSID 00:30:4F:11:22:33 (00:30:4F:81:86:34	Channel 11 11	Signal 100% 86%	8 Encrypt WPA2-PSK(AES) WPA-PSK(AES)/WPA2- PSK(AES)	Select		

STEP 5: You'll be prompted to input Uplink Wireless Router /AP's wireless security key, input it in 'KEY' field and click 'Next' to continue.

Step3: You should configure your wire the network which you selected. Then	eless client manually so it has the same wireless security settings a t click "Next".
Wireless Client Security Options	
Wireless Client Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	PlanetWiFi (8-63 characters or 64 hex digits)

TEP 6:	WNAP-1260 provid Wireless Universal	es the wireless roaming funct Repeater's And Uplink AP's	ion if you select "Synchronize SSID And Security Options".
	Click Finish. Then, t	he client can communicate with	the selected network.
Setup	Wizard		
Step4: T n, your w d configu	his page provides an easy vireless universal repeater v ure SSID of Extended Interf	way to configure wireless universal r would use same SSID and security of face and Security Options manually. I	epeater. If you enable the functio ptions with uplink AP, or you shoul Finally click "Finish".
Wireless	Universal Repeater Sett	ings	
🗹 Sync	hronize Wireless Univers	al Repeater's And Uplink AP's SSI	D And Security Options
SSID of E	Extended Interface :	WiFiRepeater-001	
Security	Options :	none	v
Note: If y wireless options a	you changed settings of wir universal repeater need co again.	eless universal repeater, the wireless nnect to wireless universal repeater v	s clients connecting to your with new SSID and security
	_	Back Finish Cancel	

You have already finished the wireless range extension configuration of the WNAP-1260. Now you can use your iPhone, iPad, laptop, and any other Wi-Fi devices to connect with it wirelessly and start to surf the Internet.



If you change the setting of wireless universal repeater through wireless connection, the wireless clients connecting to your WNAP-1260 need connect to WNAP-1260 with new SSID and security options again.

The next chapter will introduce the functions of the web UI.

Chapter 5. Quick Mode Configuration

Mode	Mode Available In the Web	LAN1 (Management IP Address)	LAN2 (DHCP)	DHCP Server	Way of connecting to PC
Repeater	Wireless Universal Repeater (default) WDS	192.168.1.253	Yes	Disable	Ethernet cable /Wireless
AP	Bridge (default)	102 168 1 253	No	Disable	Ethernet cable /Wireless
~	Router	192.100.1.200	No	Enable	Wireless only
Client	Client (default)	192.168.1.253	No	Disable	Ethernet cable only

Table 4.1 IP information of AP/Repeater/Client modes of WNAP1260

Step 1 Set the three-way switch on the case of WNAP-1260 to the mode you want.

Step 2 Run the Internet Explorer (IE). Enter the management IP address of **192.168.1.253** and press **Enter**. In the login window that is displayed, enter the user name and password (both **admin**), and click **Login**.

PLANET Networking & Communication	
UserName:	admin
Password:	Login Reset

Figure 5-1



Terminal devices can access the network through WNAP-1260 after you finish configuration by following procedures in the sections below.

5.1. Repeater Mode Configuration

Step 1 Set the three-way switch on the side panel to **Repeater** after WNAP-1260 is powered on. Log in to the configuration page after the system is started.



Step 2 Click Setup Wizard in the navigation bar on the left pane of the page. Select Wireless Universal Repeater Mode and click Next.

Setup Wizard
Step1: There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or Wireless Unive rsal Repeater Mode.
Please choose your repeater mode as follows:
O WDS Mode
Wireless Universal Repeater Mode
Next



Step 3 Click Site Survey to search for the wireless network you want to connect. Select a desired network. Click Next.

Se	Setup Wizard							
Step2: Please configure the wireless client first. Click "Site Survey" button to survey wireless sites when cl ient mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".								
Site	Site Survey							
Site	e Survey List	a :			0			
#	SSID	BSSID	Channel	Signal	Encrypt	Select		
1	WiFi_Original	00:30:4F:11:22:33	11	100%	WPA2-PSK(AES)	۲		
2	2 C3220 00:30:4F:81:86:34 11 86% WPA-PSK(AES)/WPA2- PSK(AES) ©							
	Back Next							

Figure 5-3

Step 4 Configure the repeater with the same security option as its uplink network. (The following figure takes the security option of WPA2-PSK[AES] as an example.) Set the encryption password and note it down. Click Next.

Setup Wizard	
Step3: You should configure your wirel the network which you selected. Then a	ess client manually so it has the same wireless security settings as click "Next".
Wireless Client Security Options	
Wireless Client Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	PlanetWiFi (8-63 characters or 64 hex digits)
	Back Next

Figure 5-4

Step 5 WNAP-1260 provides the wireless roaming function if you select Synchronize Wireless
 Universal Repeater's And Uplink AP's SSID And Security Options. Otherwise, manually configure the SSID and security options for the repeater. Click Finish to complete setup wizard.

Setup Wizard	
Step4: This page provides an easy way t n, your wireless universal repeater would d configure SSID of Extended Interface a	o configure wireless universal repeater. If you enable the functio use same SSID and security options with uplink AP, or you shoul nd Security Options manually. Finally click "Finish".
Wireless Universal Repeater Settings	
🗵 Synchronize Wireless Universal Re	peater's And Uplink AP's SSID And Security Options
SSID of Extended Interface :	WiFiRepeater-001
Security Options :	none
Note: If you changed settings of wireless wireless universal repeater need connect options again.	universal repeater, the wireless clients connecting to your to wireless universal repeater with new SSID and security
Ba	ack Finish Cancel

Figure 5-5

5.2. WDS Mode Configuration

5.2.1. Repeater Configuration in the WDS Mode

Step 1 Set the three-way switch on the side panel to **Repeater** after WNAP-1260 is powered on. Log in to the configuration page after the system is started.



Step 2 Click Setup Wizard in the navigation bar on the left pane of the page. Select WDS Mode and click Next. (Note: The WDS function cannot be used if the channel is set to Auto) Manually set all WDS devices to the same channel.

Setup Wizard
Step1: There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or Wireless Unive rsal Repeater Mode.
Please choose your repeater mode as follows:
WDS Mode
O Wireless Universal Repeater Mode
Next

Figure 5-6

Step 3 Set the IP address of the LAN port of the repeater and enter the MAC address of the basic station. Click Next.

Setup Wizard	
Step2: In WDS Mode, the device would work as a Repea u must enter the wireless MAC address of the other Bas enter the wireless MAC address of router in the other Ba d result the change of LAN IP Address.	ter and could communicate only with another Base Station-mode wireless station. Yo e Station-mode wireless station in the field named "Basic Station MAC Address" and se Station-mode wireless station webpage. The change of Repeater IP Address woul
WDS Settings	
Wireless MAC of this router: 00:30:4F:21:D4:37	
Repeater IP Address:	
Basic Station MAC Address:	
	Back Next



Step 4 Set the SSID, channel, and security encryption for the repeater. The channel cannot be set toAuto. It is recommended to configure the repeater with the same security option as its base station. Set the encryption password and note it down. Click Finish to complete the settings.

Setup Wizard		
Step3: WEP can (and should) be used	to protect WDS communication. "Auto" channel can not be used.	
Other Wireless Settings		
Name(SSID):	PlanetAP	
Channel :	1 🗸	
Security Options :	None	
	Back Finish Cancel	

Figure 5-8

5.2.2. Central Base Station Configuration in the WDS Mode

Step 1 Set WNAP-1260 to the Router mode. (Set the three-way switch on the side panel to AP)



AP/Repeater/Client

Step 2 Click Mode Settings and select Router Mode. (The default mode is Bridge Mode.)

Step 3 Choose Wireless Settings > WDS Function, select Enable WDS Function

Step 4 Enter the MAC address of the Repeater

Disable Wireless Clients Associati	on
Wireless MAC of this router: 00:20:4	
Wheless MAC of this fouter. 00.30.4	F:91:1C:4B
Wireless Basic Station	
Repeater MAC Address 1:	0.30.4F 99.29.14
Repeater MAC Address 2:	
Repeater MAC Address 3:	
Repeater MAC Address 4	
Repeater MAC Address 2: Repeater MAC Address 3:	

Figure 5-9



One basic station can connect to a maximum of 4 repeaters

5.2.3. WDS Application

The following figure shows a wireless network for Humans Resource Department (marked as A in the figure), Finance Department (marked as B), and Marketing Department (marked as C) in an enterprise.

If the three departments share one wireless router, signals searched by computers may be rather weak or even no signals are available. However, if each of the three departments uses a wireless router, we can use WDS to connect the three routers to provide perfect wireless coverage for the whole areas.



Configure the three routers in this way:

Wireless router B functions as the wireless basic station; wireless routers A and C connect to wireless router B by using WDS.

- (1) Configuring wireless router B as the wireless basic station
 - Step 1 Log in to the Web management page of wireless router B. Choose Wireless Settings > Wireless Basic Settings and set the SSID, channel, and wireless encryption information. Write down the SSID, channel, and wireless encryption information that are required when you are configuring wireless router A and C.
Step 2 Choose Wireless Settings > WDS Function and enable the WDS function. Enter MAC addresses of repeaters (that is, wireless routers A and C in this example). Click Apply to save the settings.

(2) Configuring wireless router A

Do as follows to establish WDS connection between wireless routers A and B:

- **Step 1** Set wireless router A with the same channel and encryption information as wireless router B.
- Step 2 Choose Wireless Settings > WDS Function and enable the WDS function. Set the IP address of wireless router B different from that of wireless router B to avoid IP address conflict (for example, change the IP address to 192.168.100.20 in the LAN Interface Settings page and log in to the Web management page again).

Step 3 Enter the MAC address of the wireless basic station.

Step 4 Click **Apply** to save the settings.

Then, WDS connection is established between wireless routers A and B.

(3) Configuring wireless router C

Configure wireless router C in the same way as wireless router A. Note that the IP address of the LAN interface must be changed to an IP address that does not conflict with IP addresses of existing computers or devices in the network.

5.3. Bridge Mode Configuration

Step 1 Set the three-way switch on the side panel to **AP** after WNAP-1260 is powered on. Log in to the configuration page after the system is started.



Step 2 Click **Setup Wizard** in the navigation bar on the left pane of the page. Set the SSID and encryption password and note them down. Click **Finish** to complete the settings.

Setup Wizard		
This setup wizard helps you to config	ire wireless settings in birdge mode.	
Enable Wireless Router Radio		
Name(SSID)		
Name(SSID) :	WiFiRepeater-001	
Security Options		
Security Options :	None	
	Finish Cancle	

Figure 5-11

5.4. Router Mode Configuration

Step 1 Set the three-way switch on the side panel to **AP** after WNAP-1260 is powered on. Log in to the configuration page after the system is started.



Step 2 Click Mode Settings and select Router Mode. (The default mode is Bridge Mode.)

Step 3 Connect your PC to WNAP-1260 using a wireless network adapter after WNAP-1260 is restarted successfully. Log in to the configuration page. Click Setup Wizard in the navigation bar on the left pane of the page. Select Yes and click Next. WNAP-1260 will automatically detect the broadband type.

Step 4 WNAP-1260 can detect three types of broadband: DHCP, Static IP, and PPPoE. Perform configurations according to the broadband type you are using.

Parameter configuration for DHCP

Setup Wizard	
Dynamic IP (DHCP) detected Successfully detected the type of Internet connection you have.	
Back Next	
Dynamic IP Address	Enter the account name
Account Name (If Required)	provided by your ISP. Leave it blank if your ISP does not provide the account name.

Figure 5-12

Parameter configuration for static IP

Setup Wizard	
	Static IP (Fixed) detected
If you believe you have received th this screen, and reopen a new We	Successfully detected the type of internet connection you have. is message in error, please power cycle your modern (unplug the modern and plug it back in). Then close ob browser (e.g., Internet Explorer)
	Back
Static IP (Fixed) Addre	ISSOS
Your Internet service provides the	static IP (Fixed) settings.
Be sure to enter the correct IP add Address fields and the IP Address	ress for each static IP sattings. For example, be sure to enter the Gateway IP Address in the Cateway in the IP Address fields without mbing them up.
Internet IP Address	
IP Address	
D Cube at March	

nternet IP Address		
IP Address		
P Subnet Mask		Required
Gateway IP Address		7
Domain Name Server (DNS) Address	1 1	
Primary DNS		Ontinuel
Secondary DNS		Optional

Figure 5-13

Parameter configuration for PPPoE

Setup Wizard	
Su	PPPoE detected cessfully detected the type of Internet connection you have.
	Back
PPPoE	,
Password Setting	
Login :	Enter the account name and
Password :	password for Internet connection
Service Name (If required) :	
Domain Name Server(DNS) Address	Enter the DNS address provided
Get Automatically From ISP	If your ISP does not provide it,
O Use These DNS Servers	select Get Automatically From ISF
Primary DNS :	
Secondary DNS :	

Apply Cancel

Figure 5-14

Step 5 Click Next. Set the SSID and password and note them down. Click Finish to complete the settings.

Wireless Settin	gs		
Enable Wireless De	vice Radio		
Name(SSID)			Value and use the default SSID
Name(SSID) :	H560L_178957		However, we suggest modifying
Security Options			the SSID.
Security Options :	None	×	Set the wireless encryption
E	Back Finish Cancle		mode and password.



5.5. Client Mode Configuration

Step 1 Set the three-way switch on the side panel to **Client** after WNAP-1260 is powered on. Log in to the configuration page after the system is started.



Step 2 Click Setup Wizard in the navigation bar on the left pane of the page. Click Site Survey to

search for the wireless network you want to connect.

Wire	less Client Function	n				
This p Step1: displa	age help you to configure the Click "Site Survey" button to su yed in the Site Survey List three	wireless client. urvey wireless sites when client r e seconds later, you could select	mode is enabled. anyone to connec	lf any Access P t it manually. Tl	oint or IBSS is found, the re hen click "Next".	sults will be
Site	Survey					
Numbe Site Si	er of Sites Scaned :8 urvey List					
#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	PlanetAP	00:30:4F:21:D4:37	1	100%	WPA2-PSK(AES)	۲
2	default_2.4G	00:30:4F:7C:84:50	11	100%	None	0
3	C3220	00:30:4F:81:86:34	11	86%	None	0
4	RTL8186-default	00:30:4F:55:AA:CC	1	60%	None	0
		Figu	Next			

Step 3 Enter encryption information of the selected wireless network. Click Next.

Wireless Client Function	
Step2: You should configure your wireless client manual hen click "Next".	ly so it has the same wireless security settings as the network which you selected. T
Security Options	
Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)
	Back

Figure 5-17

Step 4 Check Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options if you want to sync the SSID & Security key. Click Finish to complete the settings.

Wireless Client Function	
Step3: This page provides an easy way to configure wireless universal repeater. If you enable the function, your wireless universal repeater ould use same SSID and security options with uplink AP. Finally click "Finish".	N
Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options Note: If you changed settings of wireless universal repeater, the wireless clients connecting to your wireless universal repeater need connect wireless universal repeater with new SSID and security options again.	to
Back Finish	

Figure 5-18

Chapter 6. Web Configuration for the Wireless Universal Repeater Mode

6.1. Running Status

Click **Running Status** and the extended navigation menu is shown as follows:

Running Status
- System Status
- Clients List

Click the submenu to enter a specific configuration page.

6.1.1. System Status

Choose Running Status > System Status and the System Status page is displayed.

System Status	
System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	WiFi Repeater
Work Mode	Repeater Mode
Time and Date	1971-01-01 10:16:00
LAN1 Port	
MAC Address	0
IP Address	192.168.1.253
IP Subnet Mask	255.255.255.0
LAN2 Port	
DHCP	Enabled
IP Address	192.168.1.126
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Wireless Client	
Wireless Network Selected Name (SSID)	WiFi_Original
Wireless Channel	2.412GHz- CH1
Wi-Fi Protected Setup(WPS)	ON

Figure 6-1

In this page, you can view information about the current running status of WNAP-1260, including system information, LAN port status, wireless client information, and wireless universal repeater status.

6.1.2. Clients List

Choose Running Status > Clients List and the Clients List page is displayed.

Wireless Devices/Wireless intruders also show up here)				
#	IP Address	MAC Address	Device Name	
1	192.168.1.200	00:30:4F:19:9D:11	unknown	
1	192.168.1.200	00:30:4F:19:9D:11	unknown	

Figure 6-2

This page displays information of devices connected to WNAP-1260, including the IP address, device name, and MAC address of each device.

6.2. Setup Wizard

For settings, refer to section 5.3. "Repeater Mode Configuration".

6.3. Repeater Mode Setting

Click **Repeater Mode Settings** and the **Repeater Mode Settings** page is displayed. Select **Wireless Universal Repeater Mode**.

Repeater Mode Settings
There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or UR Mode.
Please choose your repeater mode as follows:
O WDS Mode
⊙ Wireless Universal Repeater Mode
Apply Cancel

Figure 6-3

6.4. Network Settings

Click Network Settings and the extended navigation menu is shown as follows:

Network Settings
- LAN Interface Settings
- DHCP Server

Click a submenu to perform specific parameter configurations.

6.4.1. LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings	
LAN1 TCP/IP Setup	
IP Address	192 . 168 . 1 . 253
IP Subnet Mask	255 . 255 . 255 . 0
LAN2 TCP/IP Setup	
DHCP	Enable Obisable
LAN2 Status	
IP Address	192.168.40.5
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.40.254
	Apply Cancel

Figure 6-4

You can modify the IP address and IP subnet mask of the LAN port as required.



If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

6.4.2. DHCP Server

Choose Network Settings > DHCP Server and the DHCP Server page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, WNAP-1260 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHC	P Server			
D U	lse Router as D	HCP Server		
Startin	Starting IP Address 192 . 168 . 1 . 2			192. 168. 1. 2
Endin	Ending IP Address		192 . 168 . 1 . 200	
DHCF	PLease Time(1	- 160 hours)		24
Addre	ess Reservation	ı		
	#	IP Address	Device Name	MAC Address
			Add Edit Delete	
			ApplyCancel	



Using the Router as a DHCP Server

- Use Router as DHCP Server: If you select the Use Router as DHCP Server check box, WNAP-1260 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- Starting IP Address/Ending IP Address: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set Starting IP Address/Ending IP Address, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- DHCP Lease Time: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

Addre	ss Reserva	ation		
	#	IP Address	Device Name	MAC Address
			Add Edit Delete	

Figure 6-6

To reserve an IP address:

Step 1	Click Add to enter the	Address Reservation page.
--------	------------------------	---------------------------

Address R	eservation T	able		
	#	IP Address	Device Name	MAC Address
\circ	1	192.168.1.11	dW5rbm93bg==	00:01:6C:FC:F9:74
P Address				
MAC Addre	SS			
Device Nar	ne			

Figure 6-7

Step 2 Select one item from Address Reservation Table, or enter the IP address in the IP Address field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.100.x). Enter the MAC address and device name of the computer or server.

Step 3 Click Add to add a new item into Address Reservation.

Step 4 Click **Apply** to save the settings.

6.5. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

6.5.1. Wireless Universal Repeater

In universal repeater mode, WNAP-1260 acts as the AP and client simultaneously.

Choose Wireless Settings > Wireless Universal Repeater and the Wireless Universal Repeater page is displayed.

Wireless Universal Repeater	
SSID of Extended Interface :	WiFiRepeater-001
Security Options	
Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)
	Apply Cancel

Figure 6-8

- SSID of Extended Interface: Set the SSID of the repeater.
- **Security Options**: Set the security encryption mode for the repeater. It is recommended to configure the repeater with the same encryption mode as that of its uplink AP.

After finishing settings, click **Apply** to save the settings.

6.5.2. WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

In the **Repeater mode** with WDS disabled, WNAP-1260 can perform WPS encrypted connection to both the uplink AP and the downlink client device.



The following describes how to configure WPS for the Repeater mode.

Using the WPS Button

• WPS connection to the uplink AP

In the Repeater mode with WDS disabled, press the **WPS** button on the side panel of WNAP-1260 in 3 seconds and release it. And press the **WPS** button on the uplink AP. Then they can start WPS session.

• WPS connection to the downlink client device

In the Repeater mode with WDS disabled, press the **WPS** button on the side panel of WNAP-1260 for 3-10 seconds and release it. And press the **WPS** button on the client device. Then they can start WPS session.



The SSID, authentication and pre-shared key for WNAP-1260 will automatically change to the same as those of its uplink AP after WNAP-1260 succeeds in connecting to the uplink AP through the WPS button mode.

Using the Web Page

You can perform WPS settings using the Web page for configuration.

Choose Wireless Settings > WPS Setup to display the WPS Setup page.

WPS Setup	
WPS Setup	
WPS status: Enable	Disable WPS Function
As Client, Select a setup method:	
 Push Button (recommended) 	
You can either press the Push Button physically on th below (soft Push Button).	e router or press the Button Start PBC
OPIN (Personal Identification Number)	
As AP, Select a setup method:	
 Push Button (recommended) 	
You can either press the Push Button physically on th below (soft Push Button).	e router or press the Button Start PBC
OPIN (Personal Identification Number)	

Figure 6-9

- As an AP

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings** > **WPS Setup** to display the WPS page.

PBC mode

Step 1 Select Push Button and click Start PBC. WPS encrypted connection starts.

Step 2 Press the WPS button on the network adapter or click the PBC button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

PIN mode

- Step 1 Select PIN, enter the PIN code of the network adapter (refer to the client of the network adapter), and click Start PIN to start WPS connection.
- Step 2 Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

As a client

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings** > **WPS** to display the WPS page.

PBC mode

Step 1 Select Push Button and click Start PBC. WPS encrypted connection starts.

Step 2 Start the WPS PBC process. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

• PIN mode

Step 1 Select PIN, click Generate New PIN, and click Start PIN to start WPS connection.

Step 2 Start the WPS PBC process within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

6.5.3. Wireless Client Function

Choose Wireless Settings > Wireless Client Function and the Wireless Client Function page is displayed.

Wire This p	Wireless Client Function						
Step1: display	Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".						
Site Numbe	Site Survey						
Site Si	urvey List						
#	SSID	BSSID	Channel	Signal	Encrypt	Select	
1	PlanetAP	00:30:4F:21:D4:37	1	100%	WPA2-PSK(AES)	$\overline{oldsymbol{\circ}}$	
2	default_2.4G	00:30:4F:7C:84:50	11	100%	None	0	
3	airlive	00:30:4F:81:96:D1	11	86%	None	0	
4	RTL8186-default	00:30:4F:55:AA:CC	1	60%	None	\circ	
		r					
		l	Next				



Step 1 Click Site Survey to search for the wireless network you want to connect.

Step 2 Enter encryption information of the selected wireless network.

Step 3 Configure the client with the same security settings as the selected network. Click Next.

Wireless Client Function	
Step2: You should configure your wireless client manual hen click "Next".	lly so it has the same wireless security settings as the network which you selected. T
Security Options	
Security Options :	WPA2-PSK[AES] 🗸
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)
	Back Next



Step 4 WNAP-1260 provides the wireless roaming function if you select Synchronize Wireless
 Universal Repeater's And Uplink AP's SSID And Security Options. Click Finish.
 Then, the client can communicate with the selected network.

Wireless Client Function
Step3: This page provides an easy way to configure wireless universal repeater. If you enable the function, your wireless universal repeater w ould use same SSID and security options with uplink AP. Finally click "Finish".
Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options Note: If you changed settings of wireless universal repeater, the wireless clients connecting to your wireless universal repeater need connect to wireless universal repeater with new SSID and security options again.
Back Finish

Figure 6-12

6.6. Management Function

Click Management Function and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

6.6.1. Backup Settings

Choose Management Function > Backup Settings and the Backup Settings page is displayed.

Backup Settings	
Save a Copy of Current Settings	
	Backup
Restore Saved Setting from a File	
Browse	Restore
Revert to Factory Default Settings	
	Erase

Figure 6-13

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

Backup

Click Backup and save configuration information of the router as a local file.



Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Restore

The Backup and Restore options in the Backup Settings page let you save and retrieve a file containing your router's configuration settings.

Click Browse... to select the configuration file restored in your computer and click Restore to load the file to the router.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click Erase to restore the factory default settings of the router. This operation has the same effect as pressing the Reset button on the side panel for 3-6 seconds.

6.6.2. Reboot Device

Choose Management Function > Reboot Device and the Reboot Device page is displayed.

Reboot Device	
Reboot Device	
	Reboot



Click Reboot to reboot the router. After the router is rebooted, the system jumps to the login page.

6.6.3. Set Password

Choose Management Function > Set Password and the Set Password page is displayed.

Set Password			
Set Password			
Old Password			
Set Password			
Repeat New Password			
	Appry Cancer		
Web Idle Time Out Settings			
Web Idle Time Out	5 (5 ~ 30 minutes)		
	Apply Cancel		



In this page, you can change the password of the administrator and set the page timeout time.



For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

6.6.4. Upgrade

Choose Management Function > Upgrade and the Upgrade page is displayed.

Upgrade	
Locate and select the upgrade file from your hard disk:	
Browse	Clear Config
Upload Cancel	



Upgrade the software of the router in the following steps:

Step 1 Click **Browse...** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click Upload to start upgrade.

After the upgrade is completed, the router automatically reboots.



After the software upgrade, WNAP-1260 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software. Do not power off the device during upgrade.

Chapter 7. Web Configuration for the Bridge Mode



7.1. Bridge / AP Mode Topology

7.2. Hardware Setting

Set the three-way switch on the side panel to **AP** after WNAP-1260 is powered on.



7.3. Running Status

Log in to the configuration page after the system is started.

Click Running Status and the extended navigation menu is shown as follows:

Running Status
- System Status
- Clients List

Click the submenu to enter a specific configuration page.

7.3.1. System Status

Choose Running Status > System Status and the System Status page is displayed.

System Status	
System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	WiFi Repeater
Work Mode	Bridge Mode
Time and Date	1971-01-01 08:01:20
LAN Port	
MAC Address	00:30:4F:21:D4:37
IP Address	192.168.1.253
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	WiFiRepeater-001
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

Figure 7-1

In this page, you can view information about the current running status of WNAP-1260, including system information, LAN port status, and wireless network status.

7.3.2. Clients List

Choose Running Status > Clients List and the Clients List page is displayed.

	Filents List			
Wireless D		MAC Address	Deules News	
#	IP Address	MAC Address	Device Name	
1	192.168.1.200	00:30:4F:19:9D:11	unknown	
		Refresh		

Figure 7-2

This page displays information of computers connected to the router, including the IP adress, and MAC address of each computer.

7.4. Setup Wizard

For settings, refer to section 5.3. "Bridge Mode Configuration".

7.5. Mode Setting

Click Mode Settings and the Mode Settings page is displayed.

Mode Settings		
Please choose your mode as follows:		
OBridge Mode		
In this mode, the port is used as a lan port. You can login web by either connecting you wired network card and the lan port with ethernet cable or using your wireless network card to connect this wireless network.	View Wireless Basic Config	
O Router Mode		
Apply Cancel		

Figure 7-3

- **Bridge Mode**: The interface on its case is an LAN interface. Users can connect WNAP-1260 and the PC using an RJ45 cable or a wireless network card.
- Router Mode: Computers can connect to WNAP-1260 in a wireless way only.

7.6. Network Settings

Click LAN Interface Settings and the extended navigation menu is shown as follows:

Network Settings
- LAN Interface Settings
- DHCP Server

Click a submenu to perform specific parameter configurations.

7.6.1. LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings		
LAN TCP/IP Setup		
IP Address		192 . 168 . 1 . 253
IP Subnet Mask		255 . 255 . 255 . 0
	Apply Cancel	



You can modify the IP address and IP subnet mask of the LAN port as required.



- If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access.
- The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

7.6.2. DHCP Server

Choose Network Settings > DHCP Server and the DHCP Server page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, WNAP-1260 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHC	P Serv	/er		
Π.	lse Router	as DHCP Server		
Startin	ng IP Addre	ss		192. 168. 1. 2
Endin	g IP Addre	SS		192 . 168 . 1 . 200
DHCF	^o Lease Tir	ne(1 - 160 hours)		24
Addre	ess Reserv	ation		
	#	IP Address	Device Name	MAC Address
			Add Edit Delete	
			Apply Cancel	

Figure 7-5

Using the Router as a DHCP Server

- Use Router as DHCP Server: If you select the Use Router as DHCP Server check box, WNAP-1260 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- Starting IP Address/Ending IP Address: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set Starting IP Address/Ending IP Address, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

Step 1 Click Add to enter the Address Reservation page.

MAC Address 00:01:6C:FC:F9:74	# IP Address Device Nam	#	#	
00:01:6C:FC:F9:74	1 192 168 1 11 dW5rbm93b			
	1 102.100.1.11 dwolbinoob	1) 1	0
			dress	P Address
		s	Address	MAC Addre
		e	e Name	Device Nar
		ie	e Name	Device Nar
	Add Cancel R	is le	\ddress e Name	MAC Addre Device Nar



Step 2 Select one item from Address Reservation Table, or enter the IP address in the IP Address field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.1.x). Enter the MAC address and device name of the computer or server.

Step 3 Click Add to add a new item into Address Reservation.

Step 4 Click Apply to save the settings.

7.7. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:

🖻 Wireless Settings	
Wireless Basic Settings	
- Multiple SSID	
- Wireless Advanced Settings	
- WPS Setup	

Click a submenu to perform specific parameter configurations.

7.7.1. Wireless Basic Settings

Choose Wireless Settings > Wireless Basic Settings and the Wireless Basic Settings page is displayed.

Wireless Basic Settings	
Region Selection	
Region :	Europe
Wireless Network	
Enable SSID Broadcast	
Enable Wireless Isolation	
Name(SSID) :	WiFiRepeater-001
Mode :	Mixed 802.11b/g/n 🐱
Channel:	Auto 🗸
Band Width :	Auto 🗸
Max Transmission Rate :	Auto 💟 Mbps
Security Options	
Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)
	Apply Cancel

Figure 7-7

Object	Description
Region:	Select the region where you are located.
Enable SSID Broadcast:	If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.
Enable Wireless Isolation:	If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.
Name (SSID):	Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive
• Mode:	Select the wireless mode. Mixed 802.11b/g/n is recommended.
Channel:	The channel for transmitting wireless signals. When you select Auto, WNAP-1260 automatically selects the best channel from the available channels according to actual situations. The default channel is Auto .
Band Width:	The bandwidth occupied for wireless signal transmission.
Max Transmission Rate:	The maximum transmission rate of WNAP-1260.
Security Options:	Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

- None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	none

Figure 7-8

- WEP

Wired Equivalent Privacy. You can use WEP 64- or 128-bit encryption.

Security Options	
Security Options :	WEP
Security Encryption(WEP)	
Authentication Type :	Automatic 🗸
Encryption Type :	ASCII 💌
Encryption Strength :	64 bits 🐱
Security Encryption(WEP) Key	
Key 1 : 💿	(5 ASCII characters)
Key 2 : 🔘	(5 ASCII characters)
Key 3 : 🔘	(5 ASCII characters)
Key 4 : 🔘	(5 ASCII characters)



Object	Description
	Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and Shared keys.
	 Automatic: If selected, the router uses an authentication type of Open or Shared keys according to the request of the host.
Authentication Type: Type: Type:	Open: If selected, hosts in the wireless network can pass the authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.
	■ Shared keys:
	If selected, hosts in the wireless network can pass
	authentication only when the correct password is entered.
	Otherwise, the hosts cannot connect to the wireless network.
	available.
Encryption Type:	■ Hex : Valid characters for keys contain 0–9 and A–F.
	 ASCII: Valid characters for keys contain all characters of the key board.

	The encryption strength determines the length of the key.	
Encryption	■ If Encryption Strength is set to 64 bits, set the key to 10	
Strength:	 hexadecimal digits or 5 ASCII characters. If Encryption Strength is set to 128 bits, set the key to 26 hexadecimal digits or 13 ASCII characters. 	
• Key 1/2/3/4:	Set the key based on the selected encryption type and encryption strength.	

WPA-PSK[TKIP] or WPA2-PSK[TKIP]

- WPA-PSK: Preshared key Wi-Fi protection access
- WPA2-PSK: Preshared key Wi-Fi protection access version 2
- **TKIP**: Temporal Key Integrity Protocol

Security Options	
Security Options :	WPA-PSK[TKIP]
Security Options(WPA-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Figure 7-10

Security Options	
Security Options :	WPA2-PSK[TKIP]
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Figure 7-11

■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.



WPA-PSK[AES] or WPA2-PSK[AES]

- WPA-PSK: Preshared key Wi-Fi protection access.
- WPA2-PSK: Preshared key Wi-Fi protection access version 2.
- AES: Advanced Encryption Standard

Security Options	
Security Options :	WPA-PSK[AES]
Security Options(WPA-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Security Options : WPA2-PSK[AES] Security Options(WPA2-PSK)	Security Options	
Security Options(WPA2-PSK)	Security Options :	WPA2-PSK[AES]
	Security Options(WPA2-PSK)	
PassPhrase : 0987654321 (8-63 characters or 64 hex digits)	PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Figure 7-12

PassPhrase: Enter 8-63 ASCII characters or 64 hexadecimal digits.

- WPA-PSK/WPA2-PSK+[TKIP]/[AES]

It allows the client to use either WPA-PSK[TKIP]/[AES] or WPA2-PSK[TKIP]/[AES].

Security Options	
Security Options :	WPA-PSK/WPA2-PSK+[TKIP]/[AES]
Security Options(WPA-PSK+WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Figure 7-13

■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.



After you complete configuring wireless settings for WNAP-1260, only hosts that have the same wireless settings (for example, the SSID) as WNAP-1260 can connect to it.

If you configure security settings for WNAP-1260, hosts must have the same security settings (for example, the password) as WNAP-1260 in order to connect to WNAP-1260.

7.7.2. Multiple SSID

If you do not want visitors to know your wireless security key, you can use the Multiple SSID to allow them to use your Internet without knowing your wireless connection password.

Choose Wireless Settings > Multiple SSID and the Multiple SSID page is displayed.

Multiple	SSID					
Network P	rofiles					
	Scheme	SSID		Security	Apply	SSID Broadcast
۲	1	WiFiRepeater-	002	None	NO	YES
0	2	WiFiRepeater-	003	None	NO	YES
0	3	WiFiRepeater-	004	None	NO	YES
0	4	WiFiRepeater-	005	None	NO	YES
Wireless S	ettingsProfile 1					
Enable	Multiple SSID					
Enable	SSID Broadcast					
Allow G	uest to access My l	Local Network				
Enable	Wireless Isolation					
Guest Wire	less Network Nam	e(SSID):	WiFiRepeater-	-002		
Security O	ptionsProfile 1					
Security Op	tions :		None		~	
			Apply	Cancel		

Figure 7-14

Object	Description	
Network Profiles:	Brief description of the created Multiple SSID. You can create up to four Multiple SSIDs. A network profile contains the SSID and encryption mode, whether to use the Multiple SSID, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.	
Enable Multiple SSID:	If enabled, both you and visitors can connect to the network by using the SSID of the Multiple SSID.	
Enable SSID Broadcast:	If enabled, WNAP-1260 broadcasts its SSID to all wireless stations.	
Allow Guest to access My Local Network:	abled, visitors using the SSID of a guest network can access not the Internet but also the LAN of WNAP-1260, like users using primary SSID of the network. If disabled, visitors using the SSID guest network cannot access the LAN of WNAP-1260.	
Enable Wireless Isolation:	If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.	
 Guest Wireless Network Name (SSID): 	Set the name of the Multiple SSID.	
Security Options:	Refer to security option descriptions in section "Wireless Basic Settings".	

After finishing settings, click **Apply** to save the settings.

7.7.3. Wireless Advanced Settings

Choose Wireless Settings > Wireless Advanced Settings and the Wireless Advanced Settings page is displayed.

Wireless Advanced Settings	
Wireless Advanced Setting	
Enable Wireless Router Radio	
Enable WMM (Wi-Fi multi-media) Settings	
Fragmentation Length (256-2346)	2346
DTIM (1-255)	1
Beacon Interval (20-1000)	100
MAX Clients (0-12)	0
CTS/RTS Threshold (1-2347)	2346
Preamble Mode	Long preamble 🐱
Guard Interval	Short GI 🐱
Transmit Power Control	100% 🗸
Wireless Card Access List	
Setup Access List	
	Apply Cancel

Figure 7-15

Object	Description	
Enable Wireless Router Radio:	If you disable the wireless router radio, wireless devices cannot connect to the WNAP-1260 router. If you do not use your wireless network for a period of time, you can clear this check box and disable all wireless connectivity	
 Enable WMM (Wi-Fi multi-media) Settings: 	 WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled 	
 Fragmentation Length (256-2346): 	Set the threshold of fragmentation length. If the length of a packet exceeds the set value, the packet is automatically fragmented into several packets. The value of Fragmentation Length cannot be too small because excessive packets reduce wireless network performance. The default value is 2346.	
• DTIM (1-255):	Set the interval for sending DTIM frames	
 Beacon Interval (20-1000): 	The beacon interval is the frequency of sending Beacon frames. Set the interval for sending Beacon frames. The unit is millisecond (ms). The default value is 100 ms	
• MAX Clients (0-12):	Set the maximum number of clients. 0 indicates the number of connected clients is not limited	
CTS/RTS Threshold (1-2347):	Set the CTS/RTS threshold. If the length of a packet is greater than	

	the specified RTS value, WNAP-1260 sends an RTS frame to the
	destination station to negotiate. After receiving an RTS frame, the
	wireless station responds with a Clear to Send (CTS) frame to
	WNAP-1260, notifying that they can communicate with each other
	A preamble (especially the 802.11b High Rate/DSSS PHY field; 56
	digits synchronized field for short preamble) defines the length of the
	CRC correction block for communication between wireless devices.
Preamble Mode:	Short preamble should be applied in a network with intense traffics.
	It helps improve the efficiency of a wireless network responding to
	applications that have high requirement of real-time, such as
	streaming video and voice-over-IP telephony.
	Short GI:
	The interval is 400 ns. When short GI is enabled, WNAP-1260
Guard Interval:	improve the transmission rate of WNAP-1260.
	Long GI:
	The interval is 800 ns.
Transmit Power	Set the transmit power of the wireless network. It is recommended to
Control:	use the default setting of 100% .

Restricting wireless access by MAC address

When a wireless card access list is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computer list.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only. The MAC address is in the format of XX:XX:XX:XX:XX:XX.

To restrict wireless access by MAC address:

Step 1	Click Setup Access List button in the Wireless Advanced Settings page to display the
	Wireless Card Access List page.

Wireless Card Access List	
Setup Access List	
\downarrow	
Wireless Card Access List	
Turn Access Control On	
Device Name	Mac Address
Add Edit	Delete
Apply	ancel

Figure 7-16

Step 2 Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup page is displayed.

Available Wireles	ard Access Setup	
	Device Name	Mac Address
0	unknown	00:30:4F:81:86:34
Wireless Card Er	ntry(Max of terms:16)	
Device Name		
Mac Address		
	Add Can	cel Refresh

Figure 7-17

- Step 3 If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to obtain its MAC address. Otherwise, you can manually enter a name and MAC address of the computer to be authorized. Generally, the MAC address is labeled on the bottom of the wireless device.
- **Step 4** Click **Add** to add this wireless device to the wireless card access list. The page jumps to the list page.
- Step 5 Select Turn Access Control On. If selected, you can restrict PCs' access to the wireless network, only allowing specified PCs to access your network according to their MAC addresses.

Step 6 Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the WNAP-1260 router.

7.7.4. WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

The following describes how to configure WPS for the AP mode.

Using the WPS Button

In the AP mode with WDS disabled, press the **WPS** button on the side panel of WNAP-1260 and the **WPS** button on the client device. WNAP-1260 can perform WPS encrypted connection to the downlink client device.



WPS (Wi-Fi Protected Setup)-AP Mode

Quick & Easy Wireless Connection



Using the Web Page

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

PBC mode



WPS	
As AP, Select a setup method:	
PBC mode(recommended)	
You can either press the PBC Button physically on the device or press the Button right (soft PBC Button).	Start PBC
OPIN (Personal Identification Number)	



Step 2 Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection.

Connect to a Netwo	ork	— ×
Type the networ	k security key	
Security key:		
	Hide characters	
0	You can also connect by pushing the button on the router.	
	ОК	Cancel

Step 3 After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



Figure 7-20

PIN mode

Step 4 Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.

WPS	
As AP, Select a setup method:	
O PBC mode(recommended)	
PIN (Personal Identification Number)	
If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.	Enter Client's PIN: Start PIN

Figure 7-21

Step 5 Click the PIN button on the network adapter within 2 minutes to start WPS connection.

Step 6 After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Succ	ess
	The wireless client has been added to the network successfully. Click OK to go back to the Wi-Fi Protected Setup page
	ΟΚ

Figure 7-22

7.8. Management Function

Click Management Function and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

7.8.1. Backup Settings

Choose Management Function > Backup Settings and the Backup Settings page is displayed.

Backup Settings		
Save a Copy of Current Settings		
	Backup	
Restore Saved Setting from a File		
	Browse	
	Restore	
Revert to Factory Default Settings		
	Erase	

Figure 7-23

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

Backup

Click Backup and save configuration information of the router as a local file.



Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Restore

The Backup and Restore options in the Backup Settings page let you save and retrieve a file containing your router's configuration settings.

Click Browse... to select the configuration file restored in your computer and click Restore to load the file to the router.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click Erase to restore the factory default settings of the router. This operation has the same effect as pressing the Reset button on the side panel for 3-6 seconds.

7.8.2. Reboot Device

Choose Management Function > Reboot Device and the Reboot Device page is displayed.

Reboot Device	
Reboot Device	
Reboot	

```
Figure 7-24
```

Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

7.8.3. Set Password

Choose Management Function > Set Password and the Set Password page is displayed.

Set Password	
Set Password	
Old Password	
Set Password	
Repeat New Password	
	[Apply] Cancel
Web Idle Time Out Settings	
Web Idle Time Out	5 (5 ~ 30 minutes)
	Apply Cancel

Figure 7-25

In this page, you can change the password of the administrator and set the page timeout time.



For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

7.8.4. Upgrade

Choose Management Function > Upgrade and the Upgrade page is displayed.

Upgrade				
Locate and select the upgrade file from your hard disk:				
Browse	Clear Config			
Upload Cancel				

Figure 7-

Upgrade the software of the router in the following steps:

Step 1 Click Browse... to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select Clear Config, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click Upload to start upgrade.

After the upgrade is completed, the router automatically reboots.

Chapter 8. Web Configuration for the Router Mode

In the Router mode, WNAP-1260 works as a domestic gateway.

8.1. Router Mode Topology

In Router Mode, the NAT (Network Address Translation) function and DHCP server are both enabled, and all wireless clients share the same public IP assigned by ISP through WAN port of the WNAP-1260. The WNAP-1260 is supposed to connect with the Cable / xDSL Modem by UTP cable.



8.2. Hardware Setting

Set the three-way switch on the side panel to AP after WNAP-1260 is powered on.



8.3. Running Status

Log in to the configuration page after the system is started.

Click Running Status and the extended navigation menu is shown as follows:

Running Status
- System Status
- Clients List

Click the submenu to enter a specific configuration page.

8.3.1. System Status

Choose Running Status > System Status and the System Status page is displayed.

System Info			
Hardware Version	V1.0.0		
Firmware Version	V1.0.0		
Product Name	WiFi Repeater		
Work Mode	Router Mode		
Time and Date	1971-01-01 08:21:16		
Internet Port			
MAC Address	00:30:4F:91:1C:49		
Internet Access Mode	Disconnected(DHCP)		
IP address	0.0.0		
IP Subnet mask	0.0.0		
Default Gateway	0.0.0.0		
Domain Name Server	0.0.0.0		
LAN Port			
MAC Address	00:30:4F:91:1C:4B		
IP Address	192.168.1.253		
IP Subnet Mask	255.255.255.0		
Wireless Port			
Wireless Network Name (SSID)	WiFiRepeater-001		
Region	Europe		
Wireless Channel	2.437GHz- CH6		
802.11 Mode	Mixed 802.11b/g/n		
Wireless Radio	Enabled		
Broadcast Name	ON		
Wireless Isolation	OFF		
Wi-Fi Protected Setup(WPS)	ON		
Wireless Security Mode	WPA2-PSK[AES]		

Figure 8-1

In this page, you can view information about the current running status of WNAP-1260, including system information, connection status of the Internet port, LAN port status, and wireless network status.

Click **Show Statistics** and the **Statistic Information** page as shown in the following figure is displayed:

10/0.01				Complotio	IX D/S	KX B/S	up lime
WAN	100M/Full	38	1113	0	7860	145814	00:02:43
WLAN	Auto	835	2278	0	611468	497560	00:01:14
ystem Up Time		00:02:53					
oll Interval							



In this page, you can view performance statistics information of WNAP-1260, including the numbers of sent and received packets at each port.

- Set Interval: Set the interval for traffic statistics.
- Stop: If you click this button, this page always displays statistics information that was refreshed for • the last time and it is not refreshed any more.

Click Connection Status in the System Status page, and the Connection Status page is displayed. This page displays current connection information of WNAP-1260.

The following takes WAN connection of **DHCP** as an example.

Connection S	tatus		
IP Address	10.1.1.155		
Subnet Mask	255.255.255.0		
Default Gateway	10.1.1.254		
DHCP Server	10.1.1.2		
DNS Server	10.1.1.2,10.1.1.3		
Lease Obtained	2Day,0Hour,0Minute		
Lease Expires	1Day,23Hour,55Minute		
	Release		
Close Window			

Figure 8-3

- **Release**: Click the button and WNAP-1260 sends a request to the ISP for releasing the IP address, the subnet mask, the default gateway, and DNS server settings.
- Renew: Click the button and WNAP-1260 dynamically obtains an IP address, a subnet mask, the • default gateway, and DNS server settings from the ISP. The information will be displayed in this page.

For details of WAN connection modes, refer to section "Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings		
LAN TCP/IP Setup		
IP Address		192 . 168 . 1 . 253
IP Subnet Mask		255 . 255 . 255 . 0
	Apply Cancel	
	Figure 8-6	

rigure 8-6

You can modify the IP address and IP subnet mask of the LAN port as required.



If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.
8.3.2. Clients List

Choose Running Status > Clients List and the Clients List page is displayed.

Clients	List		
Wireless D	evices(Wireless intruders also sho	w up here)	
#	IP Address	MAC Address	Device Name
1	192.168.1.200	00:30:4F:19:9D:11	unknown
	······································	Refresh	

Figure 8-4

This page displays information of computers connected to WNAP-1260, including the IP address and MAC address of each computer.

8.4. Setup Wizard

For settings, refer to section 錯誤!找不到參照來源。"錯誤!找不到參照來源。".

8.5. Mode Setting

Click Mode Settings and the Mode Settings page is displayed.

Mode Settings	
Please choose your mode as follows:	
O Bridge Mode	
Router Mode ■ Content Content	
In this mode, the port is used as a wan port. You can only login web by using your wireless network card to connect this network. Please remenber SSID and Security Options of your wireless network before you change to this mode.	View Wireless Basic Config
Apply Cancel	

Figure 8-5

- **Bridge Mode**: The interface on its case is an LAN interface. Users can connect WNAP-1260 and the PC using an RJ45 cable or a wireless network card.
- Router Mode: Computers can connect to WNAP-1260 in a wireless way only.

8.6. Network Settings

Click Wired Network Settings and the extended navigation menu is shown as follows:

Network Settings
- LAN Interface Settings
- WAN Interface Settings
- DHCP Server
- VPN Passthrough

Click a submenu to perform specific parameter configurations.

8.6.1. LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings		
LAN TCP/IP Setup		
IP Address		192 . 168 . 1 . 253
IP Subnet Mask		255 . 255 . 255 . 0
Apply Cancel		
	Figure 9 6	

Figure 8-6

You can modify the IP address and IP subnet mask of the LAN port as required.



If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

8.6.2. WAN Interface Settings

Choose Network Settings > WAN Interface Settings and the WAN Interface Settings page is displayed.

The router supports 5 modes of WAN connection, including **Dynamic IP (DHCP)**, **Static IP**, **PPPoE**, **PPTP**, **and L2TP**. Select the WAN connection you use. Contact your ISP if you do not know your WAN connection mode.

(1) Dynamic IP (DHCP)

If you select dynamic IP (DHCP), WNAP-1260 automatically obtains the IP address from the ISP automatically. Select DHCP when the ISP does not provide any IP network parameters. See the following figure:

WAN Interface Settings			
Does your Internet Connection Require A Login? O Yes O No			
Account Name (If Required)]
Internet IP Address			
Get Dynamically From ISP			
O Use Static IP Address			
IP Address			
IP Subnet Mask			
Gateway IP Address			
Domain Name Server (DNS) Addres	S		
Get Automatically From ISP			
O Use These DNS Servers			
Primary DNS			
Secondary DNS			
MTU Setting			
MTU Size(616~1500 bytes)	1500		
Device MAC Address			
Ose Default Address			
O Use Computer MAC Address			
O Use This MAC Address	00:17:89:17	7:89:56	
(Apply C:	ancel	

Figure 8-7

Object	Description
Account Name:	The account name is provided by your ISP. If the ISP does not
	provide it, you can leave the item blank.
	Select Use These DNS Servers if you know that your ISP does not
 Domain Name Service (DNS) 	automatically transmit DNS addresses to the router during login.
Address:	And enter the IP address of your ISP's primary DNS server. Enter a
	secondary DNS server address if available
	Set the maximum transmission unit. The default value is
• WITO 5126.	recommended
•	
	Physical address of the router.
Device MAC	Generally, select Use Default Address.
Address:	If the ISP requires MAC address authentication, Select Use
	Computer MAC Address or Use This MAC Address.

• If you select Use Computer MAC Address, the MAC address of
the current computer serves as the MAC address of the router. If
you select Use This MAC Address, you need to enter the MAC
address of another computer. The format of an MAC address is
XX:XX:XX:XX:XX:XX.

(2) Static IP

If the ISP provides the IP address, subnet mask, and information about the gateway and DNS server, select Static IP. Contact your ISP if you do not know the information.

WAN Interface Settings				
Does your Internet Connection Require A Login? O Yes O No				
Account Name (If Required)]	
Internet IP Address				
O Get Dynamically From ISP				
Ose Static IP Address				
IP Address				
IP Subnet Mask		[
Gateway IP Address		[
Domain Name Server (DNS) Addres	ss			
○ Get Automatically From ISP				
Our Servers ● ONS ● ON				
Primary DNS		[
Secondary DNS				
MTU Setting	MTU Setting			
MTU Size(616~1500 bytes)	1500			
Device MAC Address				
Ose Default Address				
O Use Computer MAC Address				
O Use This MAC Address	00:17:89:17	7:89:56		
	Apply Ca	ancel		

Figure 8-8

Object	Description
Account Name:	The account name is provided by your ISP. If the ISP does not provide it, you can leave the item blank

	Enter the WAN IP address provided by the ISP. The parameter must
• IP Address.	be entered
D Subnet Meek	Enter the WAN subnet mask provided by the ISP. It varies with the
• IP Subhet Wask.	network type. It is usually 255.255.255.0 (Class C)
 Gateway IP 	Enter the IP address of the gateway provided by the ISP. It is the IP
Address	address used for connecting to the ISP.
• Primary DNS:	Enter the IP address of the primary DNS server if necessary
	Enter the IP address of that DNS server if the ISP provides another
• Secondary DNS:	DNS server
	Set the maximum transmission unit. The default value is
• WITU SIZE.	recommended
Router MAC	See descriptions on setting Router MAC Address for DHCP.
Address:	

(3) PPPoE

If the ISP provides the user name and password for PPPoE (Point-to-Point Protocol over Ethernet) dialup, select PPPoE.

WAN Interface Setting	S	
Does your Internet Connection Require A Login? Yes ONo		
Internet Service Provider	PPPoE 🗸	
Login		
Password		
Service Name (If Required)		
Connection Mode Always On		
Idle Timeout (In minutes)	5	
Domain Name Server (DNS) Addre	\$\$\$	
Get Automatically From ISP		
O Use These DNS Servers		
Primary DNS		
Secondary DNS		
MTU Setting		
MTU Size(616~1492 bytes)	1492	
Device MAC Address		
Ose Default Address		
O Use Computer MAC Address		
○ Use This MAC Address	00:17:89:17:89:56	
	Apply Cancel	

Figure 8-9

Object	Description		
• Login:	Enter the user name for PPPoE dialup provided by the ISP		
• Password:	Enter the password for PPPoE dialup provided by the ISP		
Service Name:	If several PPPoE servers are available, specify one in this field		
	Always On: If you select it, the system automatically establishes a connection. If WNAP-1260 is disconnected from the network because of external factors when you are using the Internet access service, the system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we recommend you to use this connection mode.		
Connection Mode:	Dial On Demand: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of Idle Timeout, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.		
	Manually Connect: If you select it, you need to manually set dialup connection after startup.		
Idle Timeout:	If the system does not detect any Internet access behavior within the specified time of Idle Timeout , the system interrupts the Internet connection.		
 Domain Name Server (DNS) Address: Select Use These DNS Servers if you know that your ISP doe automatically transmit DNS addresses to the router during And enter the IP address of your ISP's primary DNS server. E secondary DNS server address if available 			
MTU Size:	Set the maximum transmission unit. The default value is recommended		
Router MAC Address:	See descriptions on setting Router MAC Address for DHCP.		

(4) PPTP

If the ISP provides the user name and password for PPTP dialup, select PPTP.

Does your Internet Connection Requi	re A Login? 💿 Yes 🔘 No
Internet Service Provider	PPTP 🗸
Login	
Password	
Connection Mode	Always On 🗸
Idle Timeout (In minutes)	5
My IP Address	
Subnet Mask	
Server Address	
Gateway IP Address	· · · · · · · · · · · · · · · · · · ·
Domain Name Server (DNS) Address	\$
Set Automatically From ISP	
OUse These DNS Servers	
Primary DNS	,, ,, ,,
Secondary DNS	
MTU Setting	
MTU Size(616~1450 bytes)	1450
Device MAC Address	
Ose Default Address	
OUse Computer MAC Address	
O Use This MAC Address	00:1E:E3:90:B3:62

Figure 8-10

Object	Description
• Login:	Enter the user name for PPTP dialup provided by the ISP
Password:	Enter the password for PPTP dialup provided by the ISP
Connection Mode:	• Always On: If you select it, the system automatically establishes a connection. If WNAP-1260 is disconnected from the network because of external factors when you are using the Internet access service, the system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we

	recommend you to use this connection mode.
	 Dial On Demand: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of Idle Timeout, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access. Manually Connect: If you select it, you need to manually set dialup connection after startup.
Idle Timeout:	If the system does not detect any Internet access behavior within the specified time of Idle Timeout , the system interrupts the Internet connection
My IP Address:	Enter your IP address. You can also leave this field blank
Subnet Mask:	Enter the subnet mask. You can also leave this field blank
Sever Address:	Enter the IP address of the server. You can also leave this field blank
Gateway IP Address:	Enter the IP address of the gateway. You can also leave this field blank
 Domain Name Server (DNS) Address: 	Select Use These DNS Servers if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available
MTU Size:	Set the maximum transmission unit. The default value is recommended
Router MAC Address:	See descriptions on setting Router MAC Address for DHCP

(5) L2TP

If the ISP provides the user name and password for L2TP dialup, select L2TP.

WAN Interface Settings		
Does your Internet Connection Require A Login?		
Internet Service Provider	L2TP 💌	
Login		
Password		
Connection Mode	Always On 🗸	
Idle Timeout (In minutes)	5	
My IP Address	· · · · · · · · · · · · · · · · · · ·	
Subnet Mask		
Server Address		
Gateway IP Address	· · · · · · · · · · · · · · · · · · ·	
Domain Name Server (DNS) Address		
Oet Automatically From ISP		
O Use These DNS Servers		
Primary DNS		
Secondary DNS		
MTU Setting		
MTU Size(616~1450 bytes)	1450	
Device MAC Address		
Ose Default Address		
O Use Computer MAC Address		
O Use This MAC Address	00:1E:E3:90:B3:62	
	Apply Cancel	

Figure 8-11

For details of parameter settings for this page, refer to previous parameter descriptions for PPTP.

8.6.3. DHCP Server

Choose Network Settings > DHCP Server and the DHCP Server page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, WNAP-1260 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol parameters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHCP Server			
Use Router as DHCP Server			
Starting IP Address 192 . 168 . 1 . [192. 168. 1. 2	
Ending IP Address		192 . 168 . 1 . 200	
DHCP Lease Time(1 - 160 hours	24 24		24
Address Reservation			
# IP #	ddress	Device Name	MAC Address
Add Edit Delete			
Apply Cancel			

Figure 8-12

Using the Router as a DHCP Server

- Use Router as DHCP Server: If you select the Use Router as DHCP Server check box, WNAP-1260 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- Starting IP Address/Ending IP Address: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set Starting IP Address/Ending IP Address, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- DHCP Lease Time: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

Address R	eservation 1	lable		
	#	IP Address	Device Name	MAC Address
0	1	192.168.1.11	dW5rbm93bg==	00:01:6C:FC:F9:74
IP Address	;			
MAC Addre	ss			
Device Na	me			

To reserve an IP address:



- Step 2 Select one item from Address Reservation Table, or enter the IP address in the IP Address field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.1.x). Enter the MAC address and device name of the computer or server.
- Step 3 Click Add to add a new item into Address Reservation.
- **Step 4** Click Apply to save the settings.

8.6.4. VPN Passthrough

Choose Network Settings > VPN Passthrough and the VPN Passthrough page is displayed.

VPN Passthrough	
☑ Disable SIP ALG	
Disable IPSEC Pass-Through	
Disable L2TP Pass-Through	
Disable PPTP Pass-Through	
	Apply Cancel

Figure 8-14

Object	Description	
	Certain SIP applications have special mechanisms for passing	
Disable SIP ALG:	through the NAT firewall and SIP ALG may have conflicts with these	
	mechanisms. In most cases, please disable SIP ALG	
Distal	IPSEC/PPTP/L2TP Pass-Through provides a secure	
	communication method for remote computers in the wide area	
	network (WAN) (for example, the Internet).	
IPSEC/L2TP/PPTP Pass-Through:	Enable the corresponding VPN pass-through function if an intra-network host needs to use a VPN protocol (such as the PPTP, L2TP, IPSEC) to connect to a remote VPN network through the	
	router	

After finishing settings, click **Apply** to save the settings.

8.7. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:

Wireless Settings	
- Wireless Basic Settings	
- Multiple SSID	
- Wireless Advanced Settings	
- WDS Function	
- WPS Setup	

Click a submenu to perform specific parameter configurations.

8.7.1. Wireless Basic Settings

Choose Wireless Settings > Wireless Basic Settings and the Wireless Basic Settings page is displayed.

Wireless Basic Settings		
Region Selection		
Region :	Europe 💌	
Wireless Network		
Enable SSID Broadcast		
Enable Wireless Isolation		
Name(SSID) :	WiFiRepeater-001	
Mode :	Mixed 802.11b/g/n 🐱	
Channel:	1 💌	
Band Width :	Auto 🐱	
Max Transmission Rate : Auto 💌 Mbps		
Security Options		
Security Options :	None	
	Apply Cancel	



Object	Description
Region:	Select the region where you are located.
Enable SSID Broadcast:	If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.
Enable Wireless Isolation:	If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.

Name (SSID):	Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive	
• Mode:	Select the wireless mode. Mixed 802.11b/g/n is recommended.	
Channel:	The channel for transmitting wireless signals. When you select Auto, WNAP-1260 automatically selects the best channel from the available channels according to actual situations. The default channel is Auto .	
Band Width:	The bandwidth occupied for wireless signal transmission.	
Max Transmission Rate:	The maximum transmission rate of WNAP-1260.	
Security Options:	Set the security encryption of the wireless network, to prevent unauthorized access and listening.	

Security Options

- None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	none

Figure 8-16

- WEP

Wired equivalent privacy. You can use WEP 64- or 128-bit encryption.

Security Options			
Security Options :	WEP		
Security Encryption(WEP)			
Authentication Type :	Automatic 🗸		
Encryption Type :	ASCII 🗸		
Encryption Strength :	64 bits 💌		
Security Encryption(WEP) Key			
Key 1: 💿	(5 ASCII characters)		
Key 2 : 🔘	(5 ASCII characters)		
Кеу 3 : 🔘	(5 ASCII characters)		
Key 4 : 🔘	(5 ASCII characters)		

Figure 8-17

Object	Description		
Authentication Type:	Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and		
	Shared keys.		

	Automatic:				
	If selected, the router uses an authentication type of Open or				
	Shared keys according to the request of the host.				
	■ Open:				
	If selected, hosts in the wireless network can pass the				
	authentication and connect to the wireless network without				
	using a password. However, the password is required if you				
	want to transmit data.				
	■ Shared keys:				
	If selected, hosts in the wireless network can pass				
	authentication only when the correct password is entered. Otherwise, the hosts cannot connect to the wireless network.				
	The type of the key to be set. Hexadecimal and ASCII code are available.				
Encryption Type:	■ Hex : Valid characters for keys contain 0–9 and A–F.				
	 ASCII: Valid characters for keys contain all characters of the key board. 				
	The encryption strength determines the length of the key.				
Encryption	■ If Encryption Strength is set to 64 bits, set the key to 10				
Strength:	hexadecimal digits or 5 ASCII characters.				
	■ If Encryption Strength is set to 128 bits, set the key to 26 bevadecimal digits or 13 ASCII characters				
	Set the key based on the selected encryption type and encryption				
• Key 1/2/3/4:	strength.				

WPA-PSK[TKIP] or WPA2-PSK[TKIP]

- WPA-PSK: Preshared key Wi-Fi protection access
- WPA2-PSK: Preshared key Wi-Fi protection access version 2
- **TKIP**: Temporal Key Integrity Protocol

Security Options	
Security Options :	WPA-PSK[TKIP]
Security Options(WPA-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)



Security Options	
Security Options :	WPA2-PSK[TKIP]
Security Options(WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)

Figure 8-19

■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.



The 802.11n mode does not support the TKIP algorithm.

WPA-PSK[AES] or WPA2-PSK[AES]

- WPA-PSK: Preshared key Wi-Fi protection access.
- WPA2-PSK: Preshared key Wi-Fi protection access version 2.
- **AES:** Advanced Encryption Standard

Security Options	
Security Options :	WPA-PSK[AES]
Security Options(WPA-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)
Figure 8-20	

Security Options		
Security Options :	WPA2-PSK[AES]	
Security Options(WPA2-PSK)		
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)	



■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.

WPA-PSK/WPA2-PSK+[TKIP]/[AES]

It allows the client to use either WPA-PSK[TKIP]/[AES] or WPA2-PSK[TKIP]/[AES].

Security Options	
Security Options :	WPA-PSK/WPA2-PSK+[TKIP]/[AES]
Security Options(WPA-PSK+WPA2-PSK)	
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)



PassPhrase: Enter 8-63 ASCII characters or 64 hexadecimal digits.



After you complete configuring wireless settings for WNAP-1260, only hosts that have the same wireless settings (for example, the SSID) as WNAP-1260 can connect to it. If you configure security settings for WNAP-1260, hosts must have the same security settings (for example, the password) as WNAP-1260 in order to connect to WNAP-1260.

8.7.2. Multiple SSID

If you do not want visitors to know your wireless security key, you can use the Multiple SSID to allow

them to use your Internet without knowing your wireless connection password.

Choose Wireless Settings > Multiple SSID	and the $\ensuremath{\textbf{Multiple SSID}}$ page is displayed.
--	--

Multiple SSID						
Network P	rofiles					
	Scheme	SSID		Security	Apply	SSID Broadcast
۲	1	WiFiRepeater-002		None	NO	YES
\circ	2	WiFiRepeater-0	003	None	NO	YES
0	3	WiFiRepeater-0	004	None	NO	YES
0	4	WiFiRepeater-0	005	None	NO	YES
Wireless S	SettingsProfile 1					
Enable	Multiple SSID					
Enable SSID Broadcast						
Allow Guest to access My Local Network						
Enable Wireless Isolation						
Guest Wire	Guest Wireless Network Name(SSID) : WiFiRepeater-002					
Security OptionsProfile 1						
Security Options : None 💌						
			Apply	Cancel		

Figure 8-23

Object	Description
Network Profiles:	Brief description of the created Multiple SSID. You can create up to four Multiple SSIDs. A network profile contains the SSID and encryption mode, whether to use the Multiple SSID, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.
Enable Multiple SSID:	If enabled, both you and visitors can connect to the network by using the SSID of the Multiple SSID.
Enable SSID Broadcast:	If enabled, WNAP-1260 broadcasts its SSID to all wireless stations.
 Allow Guest to access My Local Network: 	If enabled, visitors using the SSID of a guest network can access not only the Internet but also the LAN of WNAP-1260, like users using the primary SSID of the network. If disabled, visitors using the SSID of a guest network cannot access the LAN of WNAP-1260.
Enable Wireless Isolation:	If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.
Guest Wireless Network Name (SSID):	Set the name of the Multiple SSID.
Security Options:	Refer to security option descriptions in section "Wireless Basic Settings".

After finishing settings, click **Apply** to save the settings.

8.7.3. Wireless Advanced Settings

Choose Wireless Settings > Wireless Advanced Settings and the Wireless Advanced Settings page is displayed.

Wireless Advanced Settings			
Wireless Advanced Setting			
Enable Wireless Router Radio			
Enable WMM (Wi-Fi multi-media) Settings			
Fragmentation Length (256-2346)	2346		
DTIM (1-255)	1		
Beacon Interval (20-1000)	100		
MAX Clients (0-12)	0		
CTS/RTS Threshold (1-2347)	2346		
Preamble Mode	Long preamble 🗸		
Guard Interval	Short GI 🗸		
Transmit Power Control	100% 🗸		
Wireless Card Access List			
Setup Access List			
	Apply Cancel		

Figure 8-24

Object	Description
Enable Wireless Router Radio:	If you disable the wireless router radio, wireless devices cannot connect to the WNAP-1260 router. If you do not use your wireless network for a period of time, you can clear this check box and disable all wireless connectivity
 Enable WMM (Wi-Fi multi-media) Settings: 	WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled
 Fragmentation Length (256-2346): 	Set the threshold of fragmentation length. If the length of a packet exceeds the set value, the packet is automatically fragmented into several packets. The value of Fragmentation Length cannot be too small because excessive packets reduce wireless network performance. The default value is 2346.
• DTIM (1-255): Set the interval for sending DTIM frames	
 Beacon Interval (20-1000): 	The beacon interval is the frequency of sending Beacon frames. Set the interval for sending Beacon frames. The unit is millisecond (ms). The default value is 100 ms

• MAX Clients (0-12)	Set the maximum number of clients. 0 indicates the number of
	connected clients is not limited
	Set the CTS/RTS threshold. If the length of a packet is greater than
	the specified RTS value, WNAP-1260 sends an RTS frame to the
CIS/RIS Threshold (1-2347):	destination station to negotiate. After receiving an RTS frame, the
	wireless station responds with a Clear to Send (CTS) frame to
	WNAP-1260, notifying that they can communicate with each other
	A preamble (especially the 802.11b High Rate/DSSS PHY field; 56
	digits synchronized field for short preamble) defines the length of the
	CRC correction block for communication between wireless devices.
Preamble Mode:	Short preamble should be applied in a network with intense traffics.
	It helps improve the efficiency of a wireless network responding to
	applications that have high requirement of real-time, such as
	streaming video and voice-over-IP telephony.
	Short GI:
	The interval is 400 ns. When short GI is enabled, WNAP-1260
Guard Interval:	improve the transmission rate of WNAP-1260
	Long GI
	The interval is 800 ns
Transmit Power	Set the transmit nower of the wireless network. It is recommended to
• Transmit Power Control:	use the default setting of 100%

Restricting wireless access by MAC address

When a wireless card access list is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computer list.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only. The MAC address is in the format of XX:XX:XX:XX:XX:XX.

To restrict wireless access by MAC address:

Step 1 Click Setup Access List button in the Wireless Advanced Settings page to display the Wireless Card Access List page.

Wireless Card Access List Setup Access List		
	Ļ	
Wireless Card Access Lis	st	
Turn Access Control On		
Device Name	Add Edit Delete	Mac Address
	Apply Cancel	



Step 2 Click Add to add a wireless device to the wireless access control list. The Wireless Card Access Setup page is displayed.

Wireless Card Access Setup			
Available Wireless	Cards		
	Device Name	Mac Address	
0	unknown	00:30:4F:81:86:34	
Wireless Card Entry(Max of terms:16)			
Device Name			
Mac Address			
Add Cancel Refresh			



- Step 3 If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to obtain its MAC address. Otherwise, you can manually enter a name and MAC address of the computer to be authorized. Generally, the MAC address is labeled on the bottom of the wireless device.
- **Step 4** Click Add to add this wireless device to the wireless card access list. The page jumps to the list page.
- Step 5 Select Turn Access Control On. If selected, you can restrict PCs' access to the wireless network, only allowing specified PCs to access your network according to their MAC addresses.

Step 6 Click Apply to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the WNAP-1260 router.

8.7.4. WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. If you want to use WDS to achieve wireless repeating or bridging, enable WDS.

Choose Wireless Settings > WDS Function and the WDS Function page is displayed.

WDS Function	
Enable WDS Function	
Disable Wireless Clients Association	
Wireless MAC of this router: 00:30:4F:91:1C:44	
Wireless Basic Station	
Repeater MAC Address 1:	00:30:4F:99:29:14
Repeater MAC Address 2:	
Repeater MAC Address 3:	
Repeater MAC Address 4:	
	Apply Cancel



Object	Description
Enable WDS	Enable the WDS function if you want to use this function. Note that
Function:	the WDS function cannot be enabled if the channel is set to Auto
Enable Wireless Clients Association	If not selected, the wireless basic station does not transmit any signals to clients that are directly connected to it
	In this mode, the router serves as a basic station to communicate
Control Rose	with repeaters. The basic station forwards the data of
• Central Base Station:	communication between repeaters to the destination repeaters.
	Repeaters should be configured accordingly. Note that a wireless
	basic station can be configured with up to four repeaters.
Repeater MAC Address 1/2/3/4:	Enter the MAC address of the repeater

After finishing settings, click **Apply** to save the settings.

For WDS application description, refer to section 5.2.3. "WDS Application".

8.7.5. WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

The following describes how to configure WPS for the AP mode.

Using the WPS Button

In the AP mode with WDS disabled, press the **WPS** button on the side panel of WNAP-1260 and the **WPS** button on the client device. WNAP-1260 can perform WPS encrypted connection to the downlink client device.





Figure 8-28

Using the Web Page

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

• PBC mode

Step 1 Select Push Button and click Start PBC. WPS encrypted connection starts.

WPS	
As AP, Select a setup method:	
PBC mode(recommended)	
You can either press the PBC Button physically on the device or press the Button right (soft PBC Button).	Start PBC
O PIN (Personal Identification Number)	



Step 2 Press the **WPS button** on the network adapter or click the **PBC button** in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



Figure 8-30

• PIN mode

Step 1 Select PIN, enter the PIN code of the network adapter (refer to the client of the network adapter), and click Start PIN to start WPS connection.

WPS		
As AP, Select a setup method:		
O PBC mode(recommended)		
PIN (Personal Identification Number)		
If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.	Enter Client's PIN: Start PIN	

Figure 8-31

Step 2 Click the **PIN** button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Succ	ess
	The wireless client has been added to the network successfully. Click OK to go back to the Wi-Fi Protected Setup page
	OK

Figure 8-32

8.8. Network Application

Click **Network Application** and the extended navigation menu is shown as follows:

Network Application
- Port Forwarding
- Port Triggering
- UPnP
- IGMP Proxying
- DMZ Server
- Dynamic DNS
- Static Routes

Click a submenu to perform specific parameter configurations.

8.8.1. Port Forwarding

By default, the firewall function of the router hides your LAN. As a result, other users on the Internet can detect only the router, but cannot access a certain PC in the LAN directly. If you want to access a PC in an LAN, you need to configure port forwarding for the router and map the desired port to the corresponding PC in the LAN. The router forwards packets to the PC according to the port mapping rule after receiving an access request from the Internet. In this way, communication is successfully established between the Internet and the PC in the LAN.

Choose Network Application > Port Forwarding and the Port Forwarding page is displayed.

Service Name FTP Image: Service IP Address 192. 168. 192. 168. 192. 168. Service List Max of rules: 32 # Server Name Start Port End Port Server IP Address	Port Forwarding		
FTP Service IP Address 192. 168. 192. 168. Service List Max of rules: 32 # Server Name Start Port End Port Server IP Address	Service Name		
Service IP Address 192. 168. 100. Add Service List Max of rules: 32 # Server Name Start Port End Port Server IP Address	FTP 💌		
192. 168. 100. Add Service List Max of rules: 32 # Server Name Start Port End Port Server IP Address Edit Service Delete Service	Service IP Address		
Service List Max of rules: 32 # Server Name Start Port End Port Server IP Address	192 . 168 . 100 . Add		
Max of rules: 32 # Server Name Start Port End Port Server IP Address Edit Service Delete Service	Service List		
# Server Name Start Port End Port Server IP Address	Max of rules: 32		
Edit Service Delete Service	# Server Name Start Port	End Port	Server IP Address
Add Custom Service			

Figure 8-33

- Service Name: Select a service type.
- Service IP Address: Enter the IP address of the computer that provides services.

Click the Add Custom Service button and the Ports - Custom Service page is displayed:

Ports - Custom Service	
Service Name:	
Protocol :	TCP 💙
Starting Port	(1~65535)
Ending Port	(1~65535)
Server IP Address	192 . 168 . 1 .
	Apply Cancel



Object	Description
Service Name:	Select a service type
Protocol:	The protocol used at the mapping port. You can select TCP/UDP , TCP , or UDP . It is recommended to use TCP/UDP if you do not know which protocol should be used.
Starting Port:	After the connection to the mapping port is established, the corresponding port is open and the application can initiate subsequent connection requests to the open port
Ending Port:	Set the end port of the mapping port range
Service IP Address:	Enter the IP address of the computer that provides services

8.8.2. Port Triggering

Certain applications, such as WAN network games, video conferences, and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on an NAT router.

When an application sends a connection request to a trigger port, the corresponding ports are open for later connection and service provision.

Choose Network Application > Port Triggering and the Port Triggering page is displayed.

Port Triggering			
Enable Port Triggering			
Port Triggering Timeout(in r	ninutes) 20	(1-9999)	
Max of rules: 32			
# Server Name	Service Type	Required Inbound Connection	Service User
	Add Service	Edit Service Delete Service	
	[Apply Cancel	

Figure 8-35

Object	Description
Enable Port Triggering:	If Enable Port Triggering box is not checked, all port triggering function will be disabled
Port Triggering Timeout:	The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled

Click the **Add Service** button and the **Port Triggering – Services** page is displayed:

Port Triggering - Services	
Service Name	
Service User	Any
Service Type	ТСР
Triggering Starting Port	(1~65535)
Triggering Ending Port	(1~65535)
Required Inbound Connecti	on
Connection Type	TCP 💌
Starting Port	(1~65535)
Ending Port	(1~65535)
	Apply Cancel

Figure 8-36

Object	Description	
Service Name:	Enter a service name	
Service User:	 Any: Allow everybody in the user network to use the service. Single address: Enter the IP address of the network adapter on the PC. Then, the service is applied only on the specific network adapter of the PC. 	
Service Type:	The protocol used at the triggering port. You can select TCP/UDP , TCP , or UDP	
Triggering Starting Port:	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.	
 Triggering Ending Port: 	Set the end port of the triggering port range.	
Starting Port:	The starting port of the port range	
Ending Port:	The ending port of the port range.	

After finishing settings, click **Apply** to add a port triggering rule.

8.8.3. UPnP

By using the Universal **Plug and Play (UPnP)** protocol, a host in the LAN can ask the router to perform specific port conversion, to enable an external host to access resources on the internal host when necessary. For example, if MSN Messenger is installed on Windows ME and Windows XP operating systems, UPnP can be used for audio and video conversations. In this way, functions restricted by NAT can work properly.

Choose **Network Application > UPnP** and the **UPnP** page is displayed.

Description



Object	Description
• Turn UPnP On:	If selected, UPnP is enabled
 Advertisement Period (in minutes): 	Set the broadcast interval. It indicates the interval for the router broadcasting its UPnP information. The value should be in the range of 1 to 1440 minutes and the default is 30 minutes
 Advertisement Time To Live (in hops): 	The time for the broadcast to live. It is the number of hops after each UPnP packet is sent. The number of hops is the times that each packet can be broadcast before it vanishes. The value is in the range of 1 to 255 hops and the default is 4 hops
UPnP Portable Table:	This table shows the IP addresses of UPnP devices that are connected to the router and open (internal and external) ports on the devices. It also lists the types and status of the open ports.



8.8.4. IGMP Proxying

Click Network Application > IGMP Proxying and the IGMP Proxying page is displayed.

IGMP Proxying	
Disable IGMP Proxying	
	Apply Cancel
	(Apply Contect



- Enable IGMP proxying: IGMP proxying enables a PC in the LAN to receive desired multicast traffic from the Internet.
- Disable IGMP proxying if you do not need this function.

After finishing the setting, click **Apply** to apply the setting.

8.8.5. DMZ Server

DMZ (Demilitarized Zone), a special network zone that is different from the external network or the internal network. Servers that are allowed to access the external network, such as Web and e-mail, connect to the DMZ. The internal network is protected behind the Trust Zone interface, and is not allowed any user to access. Therefore, the internal and external networks are separated, which can meet user's secrecy demand.

Usually, there are some public servers in DMZ, such as Web, Mail, and FTP. Users from the external network can access services in DMZ, but they cannot obtain the company's secret information or personal information that is stored on the internal network. Even though servers in the DMZ are damaged, it does not cause secret information loss on the internal network.

Choose Network Application > DMZ Server and the DMZ Server page is displayed.

DMZ Server	
Default DMZ Server	192. 168. 1
	Apply Cancel



• Default DMZ Server: Enter the IP address of a PC that serves as the DMZ server.



When PC on the internal network is set to be the DMZ host, all interfaces of the PC will be exposed to the Internet and the PC will risk great security.

Unless necessary, please do not set the DMZ casually. After the DMZ host is set, mappings of all the interfaces will point to the DMZ host and the port mappings that point to other hosts will be invalid.

8.8.6. Dynamic DNS

Dynamic domain name resolution (DDNS) is mainly used to achieve resolution between fixed domain names and dynamic IP addresses. For a user that uses a dynamic IP address, after the user obtains a new IP address in the Internet access, the dynamic domain name software installed in the host sends the IP address to the DDNS server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Choose Network Application > Dynamic DNS and the Dynamic DNS page is displayed.

Dynamic DNS	
Use a Dynamic DNS Service	3
Service Provider	dyndns.org
Host Name	myhostname
User Name	User
Password	•••••
	Apply Cancel

Figure 8-40

Object	Description
Use a Dynamic DNS Service:	If you have registered with a DDNS service provider, select Use a Dynamic DNS Service .
Service Provider:	Select your DDNS service provider.
Host Name:	Enter the host name or domain name provided by your DDNS service provider
User Name:	Enter the name of your DDNS account
Password:	Enter the password of the DDNS account

After finishing the settings, click **Apply** to apply the settings.

8.8.7. Static Routes

Static routing is a special type of routing that can be applied in a network to reduce the problem of routing selection and data flow overload caused by routing selection so as to improve the packets forwarding speed. You can set the destination IP address, subnet mask, and gateway to specify a routing rule. The destination IP address and subnet mask determine a destination network or host to which the router sends packets through the gateway.

Choose Network Application > Static Routes and the Static Routes page is displayed.

Static Routes					
Max	of rules: 32				
	#	Active	Name	Destination	Gateway
			Add	Edit Delete	

Figure 8-41

Click **Add** to add a static routing rule.

Static Routes	
Active	
Route Name	
Destination IP Address	
IP Subnet Mask	
Gateway IP Address	
Metric	
	Apply Cancel

Figure 8-42

Object	Description
Active:	The static routing rule can take effect only if the Active check box is selected.
Route Name:	Enter the name of the static route.
 Destination IP Address: 	The destination address or network that you want to access. This IP address cannot be in the same network segment as the IP address of the WAN or LAN interface of WNAP-1260.
IP Subnet Mask:	This IP subnet mask together with the destination IP address identify the target network
 Gateway IP Address: 	The IP address of the next node to which packets are sent. The gateway IP address must be in the same network segment as the IP address of the WAN or LAN interface of WNAP-1260.
• Metric:	The number of other routers in the user network. The value ranges from 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direct connection, set Metric to 2

After finishing settings, click **Apply** to save the settings.

8.9. Security Options

Click Security Options and the extended navigation menu is shown as follows:

Security Options
- Block Sites
- Block Services
- Protection

Click a submenu to perform specific parameter configurations.

8.9.1. Block Sites

WNAP-1260 allows you to restrict access based on WEB addresses and WEB address keywords. When a user tries accessing a restricted website, a message is displayed, indicating that the firewall restricts access to the website.

Choose Security Options > Block Sites and the Block Sites page is displayed.

Block Sites			
Keyword Blocking			
© Never			
Per Schedule			
Always			
Type Keyword or Domain Name Here.			
Add Keyword			
Block Sites Containing these Keywords or Domain Names(Max of terms: 32) :			
Delete Keyword Clear List			
Allow Trusted IP Address To Visit Blocked Sites			
Trusted IP Address			
192 . 168 . 1 .			
Apply Cancel			

Figure 8-43

To block access to Internet sites:

Step 1 Select Per Schedule or Always to enable keyword blocking.

To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section 8.10.3. "Schedules".

Step 2 Enter keywords or domain names that you want to block in the keyword field and click Add Keyword. The keyword or domain name then appears in the Block Sites Containing these Keywords or Domain Names list.

Keyword application examples:		
国		If the keyword XXX is specified, the URL www.aabbcc.com/xxx.html is blocked.
Noto		If the keyword .com is specified, only websites with other domain suffixes (such
Note		as .eduorg. or .gov) can be accessed.

Step 3You can specify one trusted user, which is a computer that has no restriction in network
access. To specify a trusted user, enter the computer's IP address in the Trusted IP
Address field and select the Allow Trusted IP Address To Visit Blocked Sites check box.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

Step 4 Click **Apply** to save the settings.

8.9.2. Block Services

WNAP-1260 allows you to block the use of certain Internet services by computers on your network. Choose **Security Options** > **Block Services** and the **Block Services** page is displayed.

Block Services			
Services Blocking			
Never			
Black List Per Schedule			
Black List < Always			
Block Service Rules Table - Bla	ick List		
Max of rules: 32			
#	Service Name	Port	IP
	Add Edit Delete		
Block Service Rules Table - Wh	ite List		
Max of rules: 32			
#	Service Name	Port	IP
	Add Edit Delete		
	Apply Cancel		
	Figuro 8-14		

Figure 8-44

To specify a service for blocking:

Step 1 Select Per Schedule or Always to enable keyword blocking.

To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section 8.10.3. "Schedules".

- Black List: Indicates to prevent service that complies with the rule in the Block Service Rules Table-Black List area from being used.
- White List: Indicates to allow only service that complies with the rule in the Block Service Rules Table-White List area to be available for use.

Step 2 Click **Add** to specify a service for blocking. The **Block Services Setup** page is displayed:

Service TypeUser DefinedProtocolTCPStarting Port(1~65535)Ending Port(1~65535)Service Type/User Defined(1~65535)Fitter Service For:(1~65535)Only This IP Address:192, 168, 1IP Address Range:192, 168, 1to192, 168, 1SAll IP Address:(192, 168, 1)	nock services setup	
ProtocolTCPStarting Port(1~65535)Ending Port(1~65535)Service Type/User Defined(1~65535)Filter Service For:(1Only This IP Address:192.168.1.IP Address Range:192.168.1.to192.168.1.• All IP Address:(1	Service Type	User Defined 💌
Starting Port (1~65535) Ending Port (1~65535) Service Type/User Defined (1~65535) Filter Service For: (1~65535) Only This IP Address: 192, 168, 1 IP Address Range: 192, 168, 1 to 192, 168, 1 IP Address: (12, 168, 1)	Protocol	ТСР
Ending Port (1~65535) Service Type/User Defined Filter Service For: Only This IP Address: 192.168.1. IP Address Range: 192.168.1. to 192.168.1. IP Address: 192.168.1.	Starting Port	(1~65535)
Service Type/User Defined Filter Service For: Only This IP Address: 192.168.1. IP Address Range: 192.168.1. to 192.168.1. All IP Address:	Ending Port	(1~65535)
Filter Service For: Only This IP Address: IP Address Range:	Service Type/User Defined	
Only This IP Address: 192.168.1. IP Address Range: 192.168.1. to 192.168.1. All IP Address:	Filter Service For:	
 ○ IP Address Range: 192. 168. 1. to 192. 168. 1. O All IP Address: 400 - 1	Only This IP Address:	192. 168. 1.
to 192. 168. 1.	O IP Address Range:	192 . 168 . 1 .
All IP Address:	t	192 . 168 . 1 .
	All IP Address:	

Set the parameters in this page.

Step 3

Object	Description
	Select a service type. If your desired type is not in the list, select User defined.
Service Type:	Then, you need to select the protocol, enter the service name, and specify the port range. For services that exist in the drop-down list, the corresponding information is already preset.
Protocol:	Set the protocol used at service ports. If you are not sure about the protocol that the application uses, select TCP/UDP.
Starting Port/Ending Port:	The starting and ending ports of the port range where the specified service is blocked. If the application uses a single port number, enter the number in both fields
Service Type/User Defined:	Enter the service name
• Filter Service For:	You can block the specified service for a single computer, computers within an IP address range, or all computers

After finishing settings, click Add to add a new rule. Then, click Apply to save the settings.

8.9.3. Protection

Choose **Security Options > Protection** and the **Protection** page is displayed.

Protection	
Disable Port Scan and DOS Protection	
Respond to Ping on Internet Port	
NAT Filtering	
 Secured 	
◯ Open	
	Apply Cancel

Figure 8-46

Object	Description
 Disable port scan and DoS protection: 	Denial of service (DoS) protection protects your LAN against DOS attacks. Generally, please enable the port scanning and DOS protection function
Respond to Ping on Internet Port:	If enabled, the router responds to ping commands from the Internet. However, like the DMZ server, enabling this function can bring about security risks. Generally, please disable this function.
	NAT filtering determines the way that the router deals with incoming traffic.
NAT Filtering:	Secured: This option provides a secured firewall to protect PCs on LAN from attacks from the Internet, but it may not allow some Internet games, point-to-point applications, or multimedia applications to work.
	Open: This option provides a less secure firewall that allows almost all Internet applications to work.

After finishing the settings, click **Apply** to apply the settings.

8.10. Management Function

Click Management Function and the extended navigation menu is shown as follows.

Management Function
- Backup Settings
- Remote Management
- Schedules
- SNTP
- Reboot Device
- Set Password
- Upgrade

Click a submenu to perform specific parameter configurations.

8.10.1. Backup Settings

Choose Management Function > Backup Settings and the Backup Settings page is displayed.

Backup Settings	
Save a Copy of Current Settings	
	Васкир
Restore Saved Setting from a File	
	Browse
	Restore
Revert to Factory Default Settings	
	Erase

Figure 8-47

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

Backup

Click Backup and save configuration information of the router as a local file.



Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Restore

The Backup and Restore options in the Backup Settings page let you save and retrieve a file containing your router's configuration settings.

Click Browse... to select the configuration file restored in your computer and click Restore to load the file to the router.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click Erase to restore the factory default settings of the router. This operation has the same effect as pressing the Reset button on the side panel for 3-6 seconds.

8.10.2. Remote Management

The remote management function allows you to configure the router from the WAN through the Web browser. In this way, you can manage the router on a remote host.

Choose **Management Function > Remote Management** and the **Remote Management** page is displayed.

Remote Management				
Turn Remote Management On				
Remote I	Management Address :	http://0.0.0.0:8080		
Port Num	ber :	8080		
Allow Remote Access By :				
0	Only This Computer :			
	IP Address Range :	From		
0		To		
۲	Everyone	Everyone		
Apply Cancel				



Object	Description
Turn Remote Management On:	If selected, you can perform remote Web management for the router from the WAN
 Remote Management Address: 	IP address that is used to access the router from the Internet. The default is http://0.0.0.0:8080. When accessing the router, you need to enter an address in the form of "the WAN IP address of the router"+ ":" + "the port number" in the IE address bar.
	For example, if your external address is 10.0.0.123 and the used port number is 8080 , enter 10.0.0.123:8080 in your browser.
Port Number:	The port number for accessing the router through remote Web management.
	Set the IP address of the computer on which remote Web management is carried out to access the router.
Allow Remote	 Only This Computer: Only the specified IP address can access the router.
Access By:	IP Address Range: A range of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify a range.
	Everyone : Everyone on the Internet can access the router.

After finishing settings, click **Apply** to save the settings.

8.10.3. Schedules

Choose Management Function > Schedules and the Schedule page is displayed.

Schedule		
Days to Block:		
Every Day		
Sunday		
Monday		
✓ Tuesday		
✓ Wednesday		
Thursday		
Friday		
Saturday		
Time of day to Block:(use 24-ho	our clock)	
All Day		
Start Blocking	00 Hour 00 Minute	
End Blocking	23 Hour 59 Minute	
Apply Cancel		
Figure 8-49		

If you already set site filtering in the **Block Sites** page or set sevice filtering in the **Block Services** page, you can set a schedule to specify the time and mode of restricting Internet access.

Object	Description	
Days to Block:	Select days on which you want to apply blocking by selecting the appropriate check boxes. Select Every Day to select the check boxes for all days	
	All Day: To perform 24-hour blocking.	
 Time of Day to Block: 	Start Blocking/End Blocking: If you want to restrict access in a fixed period during the days you specify, enter the start and end time in 24-hour format.	

After finishing settings, click **Apply** to save the settings.
8.10.4. SNTP

Choose Management Function > SNTP and the SNTP page is displayed.

SNTP				
Time Setting				
Automatically synchronize with Intern	et time servers			
First NTP time server :	210.72.14	15.44		
Second NTP time server :				
Time Configuration				
Current Router Time :	1971-01-01	1971-01-01 08:35:31		
Time Zone :	(GMT-00:0	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 💌		
Enable Daylight Saving				
Daylight Saving Offset :	light Saving Offset : 0:00 💌			
Daylight Saving Dates :		Month	Week	Day
(Time interval must be greater	Start	Apr 👻	2nd 💌	Sun 💌
than the days of start month)	End	Sep 💌	2nd 💌	Sun 💌
Apply Cancel				

Figure 8-50

SNTP refers to **Simple Network Time Protocol**. In this page, you can set time information of your router. It is strongly recommended to set the correct time on the router first. This ensures proper functioning of log, site blocking, and schedule because their time settings are based on time information in this page.

Object	Description
Automatically synchronize with Internet time servers:	If selected automatic synchronization with the network time server is enabled
First NTP time server:	Enter the IP address of the primary NTP server. The NTP server is a network time server that is used to synchronize the time of computers on the Internet. When you set the first NTP time server, the router obtains GMT time from the specified NTP server with priority after it is connected to the Internet
Second NTP time server:	Enter the IP address of the secondary NTP server if available
Current Router Time:	Display the current system time of the router
• Time Zone:	Select the time zone where you are located.
 Enable Daylight Saving: 	Enable or disable daylight saving time (DST).
 Daylight Saving Offset: 	Select a proper offset. If it is set to +1:00, 10:00 in the morning in standard time becomes 11:00 in the morning in DST
Daylight Saving Dates:	Set the starting time and ending time of DST

After finishing settings, click **Apply** to save the settings.

8.10.5. Reboot Device

Choose Management Function > Reboot Device and the Reboot Device page is displayed.

Reboot Device			
Reboot Device			
Reboot			
Eiguno 9 54			

Figure	8-51
--------	------

Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

8.10.6. Set Password

Choose Management Function > Set Password and the Set Password page is displayed.

Set Password	
Set Password	
Old Password	
Set Password	
Repeat New Password	
	Apply Cancel
Web Idle Time Out Settings	
Web Idle Time Out	5 (5 ~ 30 minutes)
	Apply Cancel

Figure 8-52

In this page, you can change the password of the administrator and set the page timeout time.



For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

8.10.7. Upgrade

Choose Management Function > Upgrade and the Upgrade page is displayed.

Upgrade			
Locate and select the upgrade file from your hard disk:			
Browse	Clear Config		
Upload Cancel			

Figure 8-53

Upgrade the software of the router in the following steps:

- Step 1 Click Browse... to navigate to the latest software.
- **Step 2** Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.
- Step 3 Click Upload to start upgrade.

After the upgrade is completed, the router automatically reboots.

Chapter 9. Web Configuration for the WDS Mode

9.1. WDS Mode Topology

In the WDS mode, WNAP-1260 expands wireless coverage of the existing AP. Computers can connect to WNAP-1260 in either a wired or wireless way.



9.2. Hardware Setting

Set the three-way switch on the side panel to Repeater after WNAP-1260 is powered on.



9.3. Running Status

Log in to the configuration page after the system is started.

Click **Running Status** and the extended navigation menu is shown as follows:

Running Status	
- System Status	
- Clients List	

Click the submenu to enter a specific configuration page.

9.3.1. System Status

Choose Running Status > System Status and the System Status page is displayed.

System Status		
System Info		
Hardware Version	V1.0.0	
Firmware Version	V1.0.0	
Product Name	WiFi Repeater	
Work Mode	Repeater Mode	
Time and Date	1971-01-01 10:16:00	
LAN1 Port		
MAC Address	0	
IP Address	192.168.1.253	
IP Subnet Mask	255.255.255.0	
LAN2 Port		
DHCP	Enabled	
IP Address	192.168.1.126	
IP Subnet Mask	255.255.255.0	
Gateway IP Address	192.168.1.254	
Wireless Client		
Wireless Network Selected Name (SSID)	WiFi_Original	
Wireless Channel	2.412GHz- CH1	
Wi-Fi Protected Setup(WPS)	ON	

Figure 9-1

In this page, you can view information about the current running status of WNAP-1260, including system information, LAN port status, and wireless repeating information.

9.3.2. Clients List

Choose Running Status > Clients List and the Clients List page is displayed.

Clients List Wireless Devices(Wireless intruders also show up here)			
1	192.168.1.200	00:30:4F:19:9D:11	unknown
		Refresh	

This page displays information of devices connected to WNAP-1260, including the IP adress and MAC address of each device.

9.4. Setup Wizard

For settings, refer to section 5.2. "WDS Mode Configuration".

9.5. Mode Setting

Click **Mode Settings** and the **Mode Settings** page is displayed.

Figure 9-2

Repeater Mode Settings		
There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or UR Mode.		
Please choose your repeater mode as follows:		
WDS Mode		
O Wireless Universal Repeater Mode		
Apply Cancel		

Figure 9-3

Select **WDS Mode**. Note that WDS function cannot be used if the channel is set to **Auto**.

9.6. Network Settings

Click Wired Network Settings and the extended navigation menu is shown as follows:

Network Settings
- LAN Interface Settings
- DHCP Server

Click a submenu to perform specific parameter configurations.

9.6.1. LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings		
LAN TCP/IP Setup		
IP Address		192 . 168 . 1 . 253
IP Subnet Mask		255 . 255 . 255 . 0
Apply Cancel		



You can modify the IP address and IP subnet mask of the LAN port as required.



If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

9.6.2. DHCP Server

Choose **Network Settings > DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to **Dynamic Host Configuration Protocol**. If **Use Device as DHCP Service** is selected, WNAP-1260 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHC	DHCP Server			
🗌 U	Use Router as DHCP Server			
Starting IP Address		S		192 168 1 2
Ending IP Address		3		192 168 1 200
DHCP Lease Time(1 - 160 hours)		e(1 - 160 hours)		24
Addre	Address Reservation			
	#	IP Address	Device Name	MAC Address
			Add Edit Delete	
			Apply Cancel	

Figure 9-5

Using the Router as a DHCP Server

Object	Description
Use Router as DHCP Server:	If you select the Use Router as DHCP Server check box, WNAP-1260 serves as a DHCP server to automatically assign IP addresses to computers connected to it
 Starting IP Address/Ending IP Address: 	Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set Starting IP Address/Ending IP Address , hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses
DHCP Lease Time:	The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time

Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

Step 1 Click Add to enter the Address Reservation page.

	eservauori i	able		
	#	IP Address	Device Name	MAC Address
\circ	1	192.168.1.11	dW5rbm93bg==	00:01:6C:FC:F9:74
P Address				
MAC Address				
Device Name				



Step 2 Select one item from Address Reservation Table, or enter the IP address in the IP Address field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.1.x). Enter the MAC address and device name of the computer or server.

Step 3 Click Add to add a new item into Address Reservation.

Step 4 Click **Apply** to save the settings.

9.7. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:

🖻 Wireless Settings	
- WDS Function	
- Wireless Basic Settings	

Click a submenu to perform specific parameter configurations.

9.7.1. WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. Enable WDS if you want to use WDS to achieve wireless repeating or bridging.

Choose Wireless Settings > WDS Function and the WDS Function page is displayed.

WDS Function	
Disable Wireless Clients Association	
Wireless MAC of this router: 00:30:4F:91:1C:44	
Wireless Repeater	
Repeater IP Address:	192 . 168 . 1 . 1
Basic Station MAC Address:	00:30:4F:19:9D:11
	· · · · · · · · · · · · · · · · · · ·
	Apply Cancel

Figure 9-7

Object	Description
Disable Wireless Clients Association:	If selected, the repeater does not transmit any signals to clients that are connected to it. Generally, clear this check box. Generally, select this check box
 Repeater IP Address: 	Set the repeater's IP address different from the wireless basic station and other repeaters to avoid IP address conflict. We suggest setting IP addresses of the same network segment for the wireless basic station and repeaters
Basic Station MAC Address:	Enter the MAC address of the wireless basic station.

After finishing settings, click **Apply** to save the settings.

For WDS application description, refer to section 5.2.3. "WDS Application".

9.7.2. Wireless Basic Settings

Choose Wireless Settings > Wireless Basic Settings and the Wireless Basic Settings page is displayed.

Wireless Basic Settings			
Region Selection			
Region :	Europe 💌		
Wireless Network			
Enable SSID Broadcast			
Enable Wireless Isolation			
Name(SSID) :	PlanetAP		
Mode :	Mixed 802.11b/g/n 💌		
Channel:	1 💌		
Band Width :	Auto 💌		
Max Transmission Rate :	Auto 💌 Mbps		
Security Options			
Security Options :	None		
	Apply Cancel		

Figure 9-8

Object	Description
Region:	Select the region where you are located.
Enable SSID Broadcast:	If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.

Enable Wireless Isolation:	If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.
Name (SSID):	Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive
• Mode:	Select the wireless mode. Mixed 802.11b/g/n is recommended.
Channel:	The channel for transmitting wireless signals. When you select Auto, WNAP-1260 automatically selects the best channel from the available channels according to actual situations.
Band Width:	The bandwidth occupied for wireless signal transmission.
Max Transmission Rate:	The maximum transmission rate of WNAP-1260.
Security Options:	Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

- None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	none

Figure 9-9

WEP

Wired Equivalent Privacy. You can use WEP 64- or 128-bit encryption.

Security Options			
WEP 🗸			
Security Encryption(WEP)			
Automatic 💌			
ASCII 🗸			
64 bits 🗸			
Security Encryption(WEP) Key			
(5 ASCII characters)			

Figure 9-10

Object	Description
Authentication Type:	Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and
	Shared keys.

	Automatic:	
	If selected, the router uses an authentication type of Open or	
	Shared keys according to the request of the host.	
	■ Open:	
	If selected, hosts in the wireless network can pass the	
	authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.	
	■ Shared keys:	
	If selected, hosts in the wireless network can pass	
	authentication only when the correct password is entered.	
	Otherwise, the hosts cannot connect to the wireless network.	
	The type of the key to be set. Hexadecimal and ASCII code are available.	
Encryption Type:	■ Hex : Valid characters for keys contain 0–9 and A–F.	
	 ASCII: Valid characters for keys contain all characters of the key board. 	
	The encryption strength determines the length of the key.	
Encryption	If Encryption Strength is set to 64 bits, set the key to 10	
Strength:	hexadecimal digits or 5 ASCII characters.	
	■ If Encryption Strength is set to 128 bits, set the key to 26	
	Set the key based on the selected encryption type and encryption	
• Key 1/2/3/4:	strength.	

WPA-PSK[TKIP] or WPA2-PSK[TKIP]

_

- WPA-PSK: Preshared key Wi-Fi protection access
- WPA2-PSK: Preshared key Wi-Fi protection access version 2
- **TKIP**: Temporal Key Integrity Protocol

Security Options		
Security Options :	WPA-PSK[TKIP]	
Security Options(WPA-PSK)		
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)	



WPA2-PSK[TKIP]	
21 (8-63 characters or 64 hex digits)	

Figure 9-12

■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.



The 802.11n mode does not support the TKIP algorithm.

WPA-PSK[AES] or WPA2-PSK[AES]

- WPA-PSK: Preshared key Wi-Fi protection access.
- WPA2-PSK: Preshared key Wi-Fi protection access version 2.
- **AES:** Advanced Encryption Standard

Security Options		
Security Options :	WPA-PSK[AES]	
Security Options(WPA-PSK)		
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)	

Security Options		
Security Options :	WPA2-PSK[AES]	
Security Options(WPA2-PSK)		
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)	

Figure 9-13

■ **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.

– WPA-PSK/WPA2-PSK+[TKIP]/[AES]

It allows the client to use either WPA-PSK[TKIP]/[AES] or WPA2-PSK[TKIP]/[AES].

Security Options		
Security Options :	WPA-PSK/WPA2-PSK+[TKIP]/[AES]	
Security Options(WPA-PSK+WPA2-PSK)		
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)	



PassPhrase: Enter 8-63 ASCII characters or 64 hexadecimal digits.



- After you complete configuring wireless settings for WNAP-1260, only hosts that have the same wireless settings (for example, the SSID) as WNAP-1260 can connect to it.
- If you configure security settings for WNAP-1260, hosts must have the same security settings (for example, the password) as WNAP-1260 in order to connect to WNAP-1260.

9.8. Management Function

Click Management Function and the extended navigation menu is shown as follows.

Management Function
- Backup Settings
- Reboot Device
- Set Password
- Upgrade

Click a submenu to perform specific parameter configurations.

9.8.1. Backup Settings

Choose Management Function > Backup Settings and the Backup Settings page is displayed.

Backup Settings	
Save a Copy of Current Settings	
	Backup
Restore Saved Setting from a File	
	Browse
	Restore
Revert to Factory Default Settings	
	Erase

Figure 9-16

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

Backup

Click Backup and save configuration information of the router as a local file.



Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Restore

The Backup and Restore options in the Backup Settings page let you save and retrieve a file containing your router's configuration settings.

Click Browse... to select the configuration file restored in your computer and click Restore to load the file to the router.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click Erase to restore the factory default settings of the router. This operation has the same effect as pressing the Reset button on the side panel for 3-6 seconds.

9.8.2. Reboot Device

Choose Management Function > Reboot Device and the Reboot Device page is displayed.

Reboot Device
Reboot

Figure 9-17

Click Reboot to reboot the router. After the router is rebooted, the system jumps to the login page.

9.8.3. Set Password

Choose Management Function > Set Password and the Set Password page is displayed.

Set Password	
Set Password	
Old Password	
Set Password	
Repeat New Password	
	Apply Cancel
Web Idle Time Out Settings	
Web Idle Time Out	5 (5 ~ 30 minutes)
	Apply Cancel



In this page, you can change the password of the administrator and set the page timeout time.



For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

9.8.4. Upgrade

Choose Management Function > Upgrade and the Upgrade page is displayed.

Upgrade	
Locate and select the upgrade file from your hard disk:	
Browse	✓ Clear Config
Upload Cancel	
E ¹ 0.40	



Upgrade the software of the router in the following steps:

Step 1 Click Browse... to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click Upload to start upgrade.

After the upgrade is completed, the router automatically reboots.

Chapter 10. Web Configuration for the Client Mode

10.1. Client Mode Topology

In Client Mode, the WNAP-1260 is supposed to act as a wireless station for the PC or other wired-only network device. Users can site survey the available local AP and choose someone to connect with.



10.2. Hardware Setting

Set the three-way switch on the side panel to Client after WNAP-1260 is powered on.



10.3. Running Status

Log in to the configuration page after the system is started. Click **Running Status** and the extended navigation menu is shown as follows:

Running Status
- System Status
- Clients List

Click the submenu to enter a specific configuration page.

10.3.1. System Status

Choose Running Status > System Status and the System Status page is displayed.

System Status	
System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	WiFi Repeater
Work Mode	Client Mode
Time and Date	1971-01-01 08:55:02
LAN Port	
MAC Address	00:30:4F:91:1C:44
IP Address	192.168.1.253
IP Subnet Mask	255.255.255.0
Wireless Client	
Wireless Network Selected Name (SSID)	
Wireless Channel	Auto
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None
Connect Status	Disconnected

Figure 9-20

In this page, you can view information about the current running status of WNAP-1260, including system information, LAN port status, and wireless client status.

10.3.2. Clients List

Choose Running Status > Clients List and the Clients List page is displayed.

Vireless D	evices(Wireless intruders also sho	w up here)	
#	IP Address	MAC Address	Device Name
1	192.168.1.200	00:30:4F:19:9D:11	unknown
		Refresh	

Figure 9-21

This page displays information of wireless devices connected to WNAP-1260, including the IP adress and MAC address of each device.

10.4. Setup Wizard

For settings, refer to section 5.5. "Client Mode Configuration".

10.5. Network Settings

Click **Network Settings** and the extended navigation menu is shown as follows:

Network Settings	
- LAN Interface Settings	
- DHCP Server	

Click a submenu to perform specific parameter configurations.

10.5.1. LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page is displayed.

LAN Interface Settings		
LAN TCP/IP Setup		
IP Address		192 . 168 . 1 . 253
IP Subnet Mask		255 . 255 . 255 . 0
	Apply Cancel	
	Figure 9-22	

You can modify the IP address and IP subnet mask of the LAN port as required.



If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

10.5.2. DHCP Server

Choose Network Settings > DHCP Server and the DHCP Server page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, WNAP-1260 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHCP Server		
Use Router as DHCP Server		
Starting IP Address		192 168 1 2
Ending IP Address		192 168 1 200
DHCP Lease Time(1 - 160 hours)		24
Address Reservation		
# IP Address	Device Name	MAC Address
Add Edit Delete		
Apply Cancel		

Figure 9-23

Using the Router as a DHCP Server

Object	Description	
Use Router as DHCP Server:	If you select the Use Router as DHCP Server check box, WNAP-1260 serves as a DHCP server to automatically assign IP addresses to computers connected to it	

 Starting IP Address/Ending IP Address: 	Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set Starting IP Address/Ending IP Address , hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses
• DHCP Lease Time: The valid time for an IP address that is automatically assigned by DHCP server to a host. The DHCP server does not assign the address to other hosts within the specified time	

Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

Step 1	Click Add to er	ter the Address	Reservation page.
--------	-----------------	-----------------	-------------------

Address R	leservation T	able		
	#	IP Address	Device Name	MAC Address
\circ	1	192.168.1.11	dW5rbm93bg==	00:01:6C:FC:F9:74
P Address	3			
MAC Addre	ess	L		
Device Na	me			

Figure 9-24

Step 2 Select one item from Address Reservation Table, or enter the IP address in the IP Address field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.1.x). Enter the MAC address and device name of the computer or server.

Step 3 Click Add to add a new item into Address Reservation.

Step 4 Click **Apply** to save the settings.

10.6. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

10.6.1. WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

The following describes how to configure WPS for the Client mode.

Using the WPS Button

In the Client mode, WNAP-1260 can perform WPS encrypted connection to either the uplink AP or the repeater.

Using the Web Page

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

PBC mode

Step 1 Select Push Button and click Start PBC. WPS encrypted connection starts.

WPS Setup	
As Client, Select a setup method:	
 Push Button (recommended) 	
You can either press the Push Button physically on the router or press the Button below (soft Push Button).	Start PBC
O PIN (Personal Identification Number)	



Step 2 Start the WPS PBC process. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



Figure 10-2

• PIN mode

Step 1	Select PIN, click Generate New PIN	I, and click Start PIN to start WPS connection
--------	------------------------------------	--

WPS Setup	
As Client, Select a setup method:	
O Push Button (recommended)	
 PIN (Personal Identification Number) 	
If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.	Gernerate New PIN Client's PIN:12345670 Start PIN

Figure 10-3

Step 2 Start the WPS PBC process within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

ess	
The wirele Click	ess client has been added to the network successfully. K OK to go back to the Wi-Fi Protected Setup page
	OK

10.6.2. Wireless Client Function

Choose Wireless Settings > Wireless Client Function and the Wireless Client Function page is displayed.

This pa Step1: displat	Wireless Client Function This page help you to configure the wireless client. Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later you could select anyone to connect it manually. Then click "Next"					
Site Survey Number of Sites Scaned :8						
Site Su	urvey List					
#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	PlanetAP	00:30:4F:21:D4:37	1	100%	WPA2-PSK(AES)	۲
2	default_2.4G	00:30:4F:7C:84:50	11	100%	None	0
3	C3220	00:30:4F:81:86:34	11	86%	None	0
4	RTL8186-default	00:30:4F:55:AA:CC	1	60%	None	0
Next						

Figure 10-5

Step 1 Click Site Survey to search for the wireless network you want to connect.

Step 2 Enter encryption information of the selected wireless network. Configure the client with the same security settings as the selected network. Click Finish. Then, the client can communicate with the selected network.

Wireless Client Function				
Step2: You should configure your wireless client manually so it has the same wireless security settings as the network which you selected. T hen click "Next".				
Security Options				
Security Options :	WPA2-PSK[AES]			
Security Options(WPA2-PSK)				
PassPhrase :	0987654321 (8-63 characters or 64 hex digits)			
	Paale Mant			
	Dack			

Figure 10-6

10.7. Management Function

Click Management Function and the extended navigation menu is shown as follows.

Management Function	
- Backup Settings	
- Reboot Device	
- Set Password	
- Upgrade	

Click a submenu to perform specific parameter configurations.

10.7.1. Backup Settings

Choose Management Function > Backup Settings and the Backup Settings page is displayed.

Backup Settings	
Save a Copy of Current Settings	
	Backup
Restore Saved Setting from a File	
	Browse
	Restore
Revert to Factory Default Settings	
	Erase

Figure 10-7

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

Backup

Click Backup and save configuration information of the router as a local file.



Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

Restore

The Backup and Restore options in the Backup Settings page let you save and retrieve a file containing your router's configuration settings.

Click Browse... to select the configuration file restored in your computer and click Restore to load the file to the router.

Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click Erase to restore the factory default settings of the router. This operation has the same effect as pressing the Reset button on the side panel for 3-6 seconds.

10.7.2. Reboot Device

Choose Management Function > Reboot Device and the Reboot Device page is displayed.

Reboot Device	
Reboot Device	
	Reboot

Figure 10-8

Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

10.7.3. Set Password

Choose Management Function > Set Password and the Set Password page is displayed.

Set Password	
Set Password	
Old Password	
Set Password	
Repeat New Password	
	Appiy Cancel
Web Idle Time Out Settings	
Web Idle Time Out	5 (5 ~ 30 minutes)
	Apply Cancel

Figure 10-9

In this page, you can change the password of the administrator and set the page timeout time.



10.7.4. Upgrade

Choose Management Function > Upgrade and the Upgrade page is displayed.

Upgrade			
Locate and select the upgrade file from your hard disk:			
Browse	✓ Clear Config		
Upload Cancel			
Figure 40.40			

Figure 10-10

Upgrade the software of the router in the following steps:

Step 1 Click Browse... to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click Upload to start upgrade.

After the upgrade is completed, the router automatically reboots.

Chapter 11. Quick Connection to a Wireless Network

In the following sections, the default SSID of the WNAP-1260 is configured to "default".

Default SSID: default

11.1. Windows XP (Wireless Zero Configuration)

Step 1: Right-Click on the wireless network icon displayed in the system tray



Figure 11-1

Step 2: Select [View Available Wireless Networks]

Step 3: Highlight and select the wireless network (SSID) to connect

- (1) Select SSID [default]
- (2) Click the [Connect] button

(1	⁰ Wireless Network Connect	ion	×
	Network Tasks	Choose a wireless network	
	🚭 Refresh network list	Click an item in the list below to connect to a <u>w</u> ireless network in range or to ge information.	t more:
	Set up a wireless network for a home or small office	((က)) <u>Recurity-enabled wireless network (WPA)</u>	
	Related Tasks	((Q))	
	 Learn about wireless networking Change the order of preferred networks 	Security-enabled wireless network Comparison Security-enabled wireless network	
	Change advanced settings	(()) default Security-enabled wireless network (WPA) To connect to this network, click Connect. You might need to enter additional information.	antil '
		((o))	<u>_n v</u>

Figure 11-2

- (1) The Wireless Network Connection box will appear
- (2) Enter the encryption key that configured in section 7.7.1
- (3) Click the [Connect] button

Wireless Network Connection			
The network 'default' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.			
Type the key, and then click Connect.			
Network <u>k</u> ey:	•••••		
C <u>o</u> nfirm network key:	onfirm network key:		
	<u>C</u> onnect Cancel		

Figure 11-3



ነ ⁰ Wireless Network Connect	tion	X
Network Tasks	Choose a wireless network	
😴 Refresh network list	Click an item in the list below to connect to a <u>w</u> ireless network in range or to get more information.	
Set up a wireless network for a home or small office	((p)) default Connected 👷	
	Contract of the security-enabled wireless network (WPA)	
Related Tasks	((g))	
Learn about wireless petworking	Security-enabled wireless network (WPA)	≡
Change the order of	((o))	
preferred networks	Contract of the security-enabled wireless network	
Change advanced settings	((o))	
secongs	Contract Con	
	((p))	
	Unsecured wireless network	
	((p))	
	Unsecured wireless network	~
		:t

Figure 11-4



Some laptops are equipped with an "Wi-Fi ON/OFF" hardware switch for the internal wireless LAN. Make sure the it is switched to "ON" position.

11.2. Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 and can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

Step 1: Right-Click on the network icon displayed in the system tray





Step 2: Highlight and select the wireless network (SSID) to connect

- (1) Select SSID [default]
- (2) Click the [Connect] button

Not connected	÷3	•
Connecti	ons are available	
Dial-up and VPN	v ^	
Office VPN	×	=
Wireless Netwo	rk 🔨	
default	llte.	
Noni Annihushadan Dis-BARK	Name: default Signal Strength: Excellent Security Type: WPA-PSK Radio Type: 802.11n SSID: default	
- mage	301	
AUTUMIN	.ail	-
Open Net	work and Sharing Center	

Figure 11-6

Not connected	*
Connections are available	
Dial-up and VPN	
Office VPN 🗙	
Wireless Network	III
default	
Connect automatically	
the entertainty all	
and	
comean all	
an al	Ŧ
Open Network and Sharing Center	

Figure 11-7



If you want to connect to this Wireless Router in the future, please check the box of **[Connect automatically]**.

Step 3: Enter the encryption key of the Wireless Router

- (1) The [Connect to a Network] box will appear
- (2) Enter the encryption key that configured in section 7.7.1
- (3) Click the [OK] button

Connect to a Network	X
Type the network security key	
Security key:	
🕅 Hide characters	
You can also connect by pushing the button on the router.	
ОК	Cancel

Figure 11-8

Provide the second seco	×
Connecting to default	
	Cancel

Figure 11-9

```
Step 4: Check if "Connected" is displayed
```



Figure 11-10

11.3. Mac OS X





Figure 11-11

- Step 2: Highlight and select the wireless network (SSID) to connect
 - (1) Select and SSID [default]
 - (2) Double-click on the selected SSID



Figure 11-12

Step 3: Enter the encryption key of the Wireless Router

- (4) Enter the encryption key that configured in section 7.7.1
- (1) Click the [OK] button

assword	ork "default" requires a WPA I.
Passwo	ord: ••••••
	Show password Remember this network
	Remember this network

Figure 11-13



If you want to connect to this Wireless Router in the future, please check [Remember this network].

Step 4: Check if the AirPort is connect to the selected wireless network. If "Yes", then there will be a "check" symbol in front of the SSID.



Figure 11-14

There is another way to configure the MAC OS X Wireless settings:





Figure 11-15

Step 2: Open Network Preference by clicking on the [Network] icon

00			System I	Preferences			
	how All					Q	
Personal Appearance	Desktop &	Dock	Exposé &	Language &	Security	Q Spo:light	
Hardware CDs & DVDs	Displays	Energy Saver	Keyboard	Mouse	Trackpad	Print & Fax	Sound
Internet &	Wireless	Bluetooth	Sharing				
System	Date & Time	Parestal Controls	Software Update	Speech	Startup Disk	() Time Machine	Universa Access
Other MacFUSE							

Figure 11-16

Step 3: Check Wi-Fi setting and select the available wireless network

- (1) Choose the AirPort on the left-menu (make sure it is ON)
- (2) Select Network Name [default] here

If this is the first time to connect to the Wireless Router, it should shows "Not network selected".

00	Netwo	rk	
Show All			٩
	Location: Automatic		•
USB Ethernet Not Connected S02.11dapter	Statu:	s: On (AirPort is turned on but a network.	Turn AirPort Off t is not connected to
AirPort On	Network Name	e ✓ No network selecte	ed and a second
O Home VPN		default	₽ २
			(;-) (;-)
		The State of State	
		Join Other Network Create Network	<u>م</u> ج
+ - &-	Show AirPort sta	atus in menu bar	Advanced) ?
Click the lock to pr	event further changes.	Assist me	Revert Apply

Figure 11-17

11.4. iPhone / iPod Touch / iPad

Step 1: Tap the [Settings] icon displayed in the home screen



Figure 11-18

Step 2: Check Wi-Fi setting and select the available wireless network

- (3) Tap [General] \ [Network]
- (4) Tap [Wi-Fi]

If this is the first time to connect to the Wireless Router, it should appears "Not Connected".

iPad	10:35 AM	🕒 100% 🖃
Settings	General	
Airplane Mode		
S Wi-Fi Not Connected	About	>
Notifications On	Usage	>
Carrier	Sounds	>
🕎 Cellular Data		
🙀 Brightness & Wallpaper	Network	>
Picture Frame	Bluetooth	Off >
General	Location Services	On >
Salendars Mail, Contacts, Calendars	Spotlight Search	>
🧭 Safari		

Figure 11-19

Pad	10:35 AM	100%
Settings	General	Network
Airplane Mode OFF	10	
WI-FI Not Connected	VPN	Not Connected >
Notifications On	Wi-Fi	Not Connected >
Carrier		
🔀 Cellular Data		
Brightness & Wallpaper		
Picture Frame		
General		
📴 Mail, Contacts, Calendars		
Safari		

Figure 11-20

Step 3: Tap the target wireless network (SSID) in "Choose a Network..."

- (1) Turn on Wi-Fi by tapping "Wi-Fi"
- (2) Select SSID [default]

iPad	11:23 PM	@ 76% ■
Settings	Network Wi-Fi Network	S
Airplane Mode OFF	(
Wi-Fi Not Connected	Wi-Fi	ON
Notifications On	Choose a Network	
Location Services On	default	₽ 🗢 📀
🕎 Cellular Data	Other	>
🙀 Brightness & Wallpaper	Ask to Join Networks	ON
Picture Frame	Known networks will be joined aut	omatically. If no
🚳 General	before joining a new ne	twork.



Step 4: Enter the encryption key of the Wireless Router

- (1) The password input screen will be displayed
- (2) Enter the encryption key that configured in section 7.7.1
- (3) Tap the [Join] button

iPad 🗇	11:20 PM		@ 76% ID
Settings	(maxim)	Wi-Fi Networ	ks
Airplane Mode OFF	- Ale		_
WI-FI CA8-1	Wi-Fi		ON
Notifications On	Choose a Ne	lwork	
Location	rier the password for "d	etaut:"	
Cellular Cancel	Enter Passwor	d	
Brightne			-
Picture Password			DN
General			e. Il no askat
📑 Mail, Co			
Satari			_
iPod			_
Video Video			_
Photos			
T Notes			_
Store			_
Apps			
1 2 3 4	5 6	7 8	9 0 43
• / : :	()	\$&	@ Join
#+- undo ,	, ? !	•	Ø1-
ABC			ABC

Figure 11-22



iPad	11:25 PM	₹75% 🔳
Settings	Network Wi-Fi Networks	
Airplane Mode OFF		
S Wi-Fi default	Wi-Fi ON	
Notifications On	Choose a Network	
Location Services On	✓ default 🔒 🗢	٥
🕎 Cellular Data	Other	>
🙀 Brightness & Wallpaper	Ask to Join Networks ON	
Picture Frame	Known networks will be joined automatically. If no	
Seneral	before joining a new network.	

Figure 11-23
Appendix A. Planet Smart Discovery Utility

For easily list the WNAP-1260 in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution.

The following install instructions guiding you for run the Planet Smart Discovery Utility.

Step 1: Deposit the Planet Smart Discovery Utility in administrator PC.

Step 2: Run this utility and the following screen appears.

Step 3: Press **"Refresh"** button for list current connected devices in the discovery list, the screen is shown as follow.

		Ú Re	fresh	🖹 Exit				PLANE
MAC Address	Device Name	Version	DevicelP	NewPassword	IP Address	NetMask	Gateway	Description
00-30-4F-91-1C-4B	WNAP-1260	V1.0.0	192.168.1.253		192 158 1 253	255.255.255.	0.0.0.0	WiFi Repeater
Select Adap	ter: 0.0.0.0(0	0:136867.08	13)			Control Pa	cket Force Br	roadcast

Step 3: Press "Connect to Device" button then the Web login screen appears.

1. In Repeater Mode, the IP address of LAN 2 (DHCP) assigned by DHCP server will be listed in the table.



- 2. The LAN 2 (DHCP) only supported in Repeater Mode.
- 3. If cannot get the IP address from DHCP server or DHCP server is not existed, it will displayed the LAN 1 (Static IP address).
- 4. In other Modes, WNAP-1260 only supported LAN 1 (Static IP address).

Appendix B. FAQ

Malfunction	Solution
The WNAP-1260 is not responding to me when I want to access it via web browser	a. Please check the connection of power cord and network cable of the WNAP-1260. All cords and cables should be correctly and firmly inserted to the device.
	 b. If all LEDs on the WNAP-1260 are off, please check the status of power adapter, and make sure it is correctly powered.
	c. You must configure your PC as the same IP address section with the WNAP-1260.
	d. Are you using MAC or IP address filter? Try to connect the WNAP-1260 by another computer and see if it works; if not, please restore the WNAP-1260 to factory default settings (Press "reset" button for over 10 seconds).
	 e. Shift the hardware switch to Router Mode, and set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.
	 If you just did firmware upgrade and this happens, contact the dealer of purchase for help.
	a. If all above solutions don't work, contact the dealer of purchase for help.
Unable to get connected with the Internet	 Go to "Management → Status" submenu, and check the WAN configuration status.
	Please be patient, sometime Internet is just that slow.
	b. If you connect your computer to the Internet directly before, try to do that again. And check if you can get connected to the Internet with your computer directly via the device provided by your local Internet service provider.
	c. Check the WAN access type (Static IP / Dynamic IP / PPPoE / PPTP / L2TP), user name, password, and the other parameters provided by your local ISP again.
	 Call your Internet service provider and check if there is something wrong with their service.
	e. If you just can't connect to one or more website, but you can still use other internet services, please check URL filter in the web UI.
	f. Reset the WNAP-1260 to the factory default settings and try again later.
	 Reset the device provided by your Internet service provider as well.
	h. Try to use IP address instead of hostname. If you can

	access a remote server by an IP address but not by a hostname, please check the DNS setting.			
Unable to be found by the	a. Check if the "Broadcast SSID" is disabled.			
wireless clients	b. Are you too far from the WNAP-1260? Try to get closer.			
	c. Please remember that you have to enter SSID to your wireless client device manually, if SSID broadcast is disabled.			
File download is very slow or breaks frequently	a. Are you using QoS function? Please disable it and try again.			
	Please be patient, sometime Internet is just that slow.			
	b. Reset the WNAP-1260 to the factory default settings and see if it is better after that.			
	c. Try to know what are other computers doing in your local area network. If someone is transferring big files, other people will think Internet is really slow.			
	d. If this never happens before, call you Internet service provider to check if there is something wrong with their network.			
Unable to login the web management UI: password is	a. Make sure you are connecting to the correct IP address of the WNAP-1260.			
wrong	b. Password is case-sensitive. Make sure the "Caps Lock" light is not illuminated.			
	c. If you really forget the password, please do hardware reset.			
The device is getting hot.	a. This is not a malfunction if you can keep your hand on the case of the WNAP-1260.			
	b. If you smell something wrong or see the smoke coming out from the WNAP-1260 or power adapter, please disconnect the device and power adapter from power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.			
The date and time of all event logs are wrong	a. Adjust the internal clock of the WNAP-1260.			



EC Declaration of Conformity

For the following equipment:

*Type of Product	:	Wall Plug 300Mbps Universal WiFi Repeater (EU Type)
*Model Number	:	WNAP-1260
* Produced by:		
Manufacturer's Nam	e :	Planet Technology Corp.
Manufacturer's Addr	ess:	10F., No.96, Minquan Rd., Xindian Dist.,
		New Taipei City 231, Taiwan (R.O.C.)

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE. For the evaluation regarding the R&TTE the following standards were applied:

(2005 + A1:2009)
(2006)
(2008)
(2009)
(2008)

Responsible for marking this declaration if the:

⊠ Manufacturer **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: Planet Technology Corp.

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.) **Company Address:**

Person responsible for making this declaration

Name, Surname Kent Kang

Position / Title : Product Manager

Taiwan Place

22th June, 2012 Date

Kent Long Legal Signature

PLANET TECHNOLOGY CORPORATION

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation , declares that this 802.11n Wall Plug Universal WiFi Repeater is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	Lietuviškai	Šiuo PLANET Technology Corporation ,, skelbia, kad 802.11n Wall Plug Universal WiFi Repeater tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation, tímto prohlašuje, že tato 802.11n Wall Plug Universal WiFi Repeater splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	Magyar	A gyártó PLANET Technology Corporation, kijelenti, hogy ez a 802.11n Wall Plug Universal WiFi Repeater megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation, erklærer herved, at følgende udstyr 802.11n Wall Plug Universal WiFi Repeater overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	Malti	Hawnhekk, PLANET Technology Corporation , jiddikjara li dan 802.11n Wall Plug Universal WiFi Repeater jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt PLANET Technology Corporation, dass sich dieses Gerät 802.11n Wall Plug Universal WiFi Repeater in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)	Nederlands	Hierbij verklaart , PLANET Technology orporation, dat 802.11n Wall Plug Universal WiFi Repeater in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eesti keeles	Käesolevaga kinnitab PLANET Technology Corporation, et see 802.11n Wall Plug Universal WiFi Repeater vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation, oświadcza, że 802.11n Wall Plug Universal WiFi Repeater spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie "Directive 1999/5/EC".
Ελληνικά		Português	PLANET Technology Corporation , declara que este 802.11n Wall Plug Universal WiFi Repeater está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, PLANET Technology Corporation , declara que 802.11n Wall Plug Universal WiFi Repeater cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	Slovensky	Výrobca PLANET Technology Corporation, týmto deklaruje, že táto 802.11n Wall Plug Universal WiFi Repeater je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, PLANET Technology Corporation , déclare que les appareils du 802.11n Wall Plug Universal WiFi Repeater sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	Slovensko	PLANET Technology Corporation, s tem potrjuje, da je ta 802.11n Wall Plug Universal WiFi Repeater skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , PLANET Technology Corporation , dichiara che questo 802.11n Wall Plug Universal WiFi Repeater è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva. 1999/5/CE.	Suomi	PLANET Technology Corporation , vakuuttaa täten että 802.11n Wall Plug Universal WiFi Repeater tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo PLANET Technology Corporation , apliecina, ka šī 802.11n Wall Plug Universal WiFi Repeater atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation, att denna 802.11n Wall Plug Universal WiFi Repeater står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.