

User's Manual

802.11b/g/n Wireless Outdoor Access Point

WNAP-6308





www.PLANET.com.tw

Copyright

Copyright © 2014 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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense. Any changes or modifications not expressly approved by PLANET could void the user's authority to operate this equipment under the rules and regulations of the FCC.

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.

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.

CE CE Mark Warning

This is a Class B product. 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 Standby mode operation.

For energy saving, please remove the DC-plug to disconnect the device from the power circuit. Without remove the DC-plug, the device 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 remove the DC-plug for 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.

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 802.11b/g/n Wireless Outdoor Access Point

Model: WNAP-6308

Rev: 1.0 (February, 2014)

Part No. EM-WNAP-6308_v1.0 (2081-E10570-000)

CONTENTS

Chapter 1	. Product I	Introduction	1
1.1	Package Contents1		
1.2	Product Description2		
1.3	Product Features5		
1.4	Product S	Specifications	6
Chapter 2	2. Hardware	e Installation	9
2.1	Hardware	Description	9
	2.1.1 Th	ie Top/Bottom Panel	9
	2.1.2 Th	ne Side Panel	10
Chapter 3	8. Connecti	ng to the AP	11
3.1	Preparati	on before Installation	11
	3.1.1 Pr	ofessional Installation Required	11
	3.1.2 Sa	afety Precautions	11
3.2	Installatio	on Precautions	11
3.3	Installing	the AP	13
Chapter 4	. Quick Ins	stallation Guide	15
4.1	Manual N	etwork Setup - TCP/IP Configuration	15
	4.1.1 Co	onfiguring the IP Address Manually	15
	Starting Setup in the Web UI		
4.2	Starting S	Setup in the Web UI	18
4.2 Chapter 5	Starting S 5.'Configur	Setup in the Web UI	18 21
4.2 Chapter 5 5.1	Starting S 5.'Configur Status	Setup in the Web UI	18 21 21
4.2 Chapter 5 5.1 5.2	Starting S 5.'Configur Status Easy Setu	Setup in the Web UI	18 21 21 25
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced	Setup in the Web UI ing the AP	18 21 21 25 25
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced 5.3.1 Ac	Setup in the Web UI ing the AP up d dvanced - Management	18 21 21 25 25 26
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1.	Setup in the Web UI ing the AP Jp d dvanced - Management	18 21 21 25 25 26 26
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2.	Setup in the Web UI ing the AP Jp d. dvanced - Management Web Interface Settings (Password) Firmware Upgrade	 18 21 21 25 26 .26 .27
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3.	Setup in the Web UI ing the AP up d dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration	 18 21 25 26 .26 .27 .28
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4.	Setup in the Web UI ing the AP up d dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults	 18 21 25 25 26 27 28 28
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5.'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5.	Setup in the Web UI ing the AP Jp d. dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults Reboot System	 18 21 25 26 .26 .27 .28 .28 .29
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6.	Setup in the Web UI ing the AP Jp d. dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults Reboot System Scheduling Reboot	 18 21 21 25 25 26 27 28 28 29 29
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac	Setup in the Web UI ing the AP Jp d dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults Reboot System Scheduling Reboot dvanced – Advanced Settings	 18 21 21 25 25 26 27 28 29 29 30
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac 5.3.2.1.	Setup in the Web UI ing the AP up d dvanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults Reboot System Scheduling Reboot dvanced – Advanced Settings Time Zone Settings	 18 21 21 25 25 26 27 28 29 29 30 30 31
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac 5.3.2.1. 5.3.2.1. 5.3.2.2.	Setup in the Web UI ing the AP J. J. J. J. J. J. J. J. J	 18 21 21 25 26 26 27 28 29 29 30 31 22
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac 5.3.2.1. 5.3.2.3. 5.3.2.3. 5.3.2.4	Setup in the Web UI ing the AP up duanced - Management Web Interface Settings (Password) Firmware Upgrade Configuration Load Factory Defaults Reboot System Scheduling Reboot dvanced – Advanced Settings Time Zone Settings DDNS Settings UPNP Settings SNMP Settings	 18 21 25 26 26 27 28 29 29 30 31 33 34
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac 5.3.2.1. 5.3.2.1. 5.3.2.2. 5.3.2.3. 5.3.2.4. 5.3.3 Ac	Setup in the Web UI ing the AP	 18 21 21 25 26 26 27 28 29 29 30 31 33 34 35
4.2 Chapter 5 5.1 5.2 5.3	Starting S 5. 'Configur Status Easy Setu Advanced 5.3.1 Ac 5.3.1.1. 5.3.1.2. 5.3.1.3. 5.3.1.4. 5.3.1.5. 5.3.1.6. 5.3.2 Ac 5.3.2.1. 5.3.2.2. 5.3.2.3. 5.3.2.4. 5.3.3 Ac 5.3.3.1.	Setup in the Web UI ing the AP up duanced - Management. Web Interface Settings (Password). Firmware Upgrade Configuration. Load Factory Defaults. Reboot System Scheduling Reboot. dvanced – Advanced Settings. Time Zone Settings. DDNS Settings. UPNP Settings. SNMP Settings. SNMP Settings. AP Router (AP+Router)	18 21 25 26 .27 .28 .29 .30 .31 .33 .34 .35

	5.3.3.3.	Client Router (WISP)	
	5.3.3.4.	Client Bridge (Slave AP Bridge)	41
	5.3.4 A	dvanced – System Log	41
	5.3.5 A	dvanced – Tools	42
	5.3.5.1.	Ping	42
	5.3.5.2.	Traceroute	
	5.3.5.3.	Throughput	44
5.4	Firewall	Settings	
	5.4.1 M	IAC/IP/Port Filtering	
	5.4.2 V	/irtual Server	46
	5.4.3 D)MZ	47
	5.4.4 F	irewall	48
	5.4.5 Q	20S	
	5.4.6 C	Content Filtering	
	5.4.6.1.	Webs URL Filter Settings	51
	5.4.6.2.	Web Host Filter Settings	51
5.5	Network	Settings	51
	5.5.1 W	VAN	
	5.5.1.1.	Static (Fixed IP)	
	5.5.1.2.	Cable/Dynamic IP (DHCP)	53
	5.5.1.3.	PPPoE (ADSL)	54
	5.5.1.4.	IPSEC	54
	5.5.1.5.	PPTP	58
	5.5.1.6.	L2TP	
	5.5.2 L	AN	60
	5.5.2.1.	DHCP Server	61
	5.5.2.2.	DHCP Relay	61
	5.5.3 V	/LAN	62
	5.5.4 A	dvanced Routing	63
	5.5.5 IF	Pv6	64
5.6	Wireless	s Settings	65
	5.6.1 B	Basic	65
	5.6.1.1.	Wireless Mode – Access Point	66
	5.6.1.2.	Wireless Mode – WDS Access Point	
	5.6.1.3.	Wireless Mode – WDS Repeater	70
	5.6.1.4.	Wireless Mode – WDS Client	72
	5.6.2 P	Profile Settings	74
	5.6.3 A	dvanced	76
	5.6.4 A	Access Control	77
5.7	Logout		78
Chapter 6	6. Quick C	onnection to a Wireless Network	

	6.1	Windows XP (Wireless Zero Configuration)	79
	6.2	Windows 7 (WLAN AutoConfig)	81
	6.3	Mac OS X 10.x	84
	6.4	iPhone / iPod Touch / iPad	86
Арр	endix	A: Planet Smart Discovery Utility	90
Арр	endix	B: Troubleshooting	91
Арр	endix	C: Specifications	93

FIGURE 2-1 APPEARANCE	9
FIGURE 2-2 TOP / BOTTOM PANEL	9
FIGURE 2-3 THE LED INDICATOR	10
FIGURE 3-1 CONNECT THE ANTENNA	13
FIGURE 3-2 CONNECT THE ETHERNET CABLE	13
FIGURE 3-3 CONNECT THE POE INJECTOR	14
FIGURE 3-4 POLE MOUNTING	14
FIGURE 4-1 TCP/IP SETTING	16
FIGURE 4-2 WINDOWS START MENU	17
FIGURE 4-3 SUCCESSFUL RESULT OF PING COMMAND	17
FIGURE 4-4 FAILED RESULT OF PING COMMAND	18
FIGURE 4-5 LOGIN BY DEFAULT IP ADDRESS	18
FIGURE 4-6 LOGIN WINDOW	19
FIGURE 4-7 WNAP-6308 WEB UI SCREENSHOT	19
FIGURE 4-8 CHOOSE OPERATION MODE	20
FIGURE 4-9 CONFIGURE WIRELESS SETTINGS	20
FIGURE 5-1 MAIN MENU	21
FIGURE 5-2 STATUS	21
FIGURE 5-3 STATISTICS	23
FIGURE 5-4 DHCP CLIENT LIST	24
FIGURE 5-5 STATION LIST	24
FIGURE 5-6 EASY SETUP	25
FIGURE 5-7 ADVANCED MENU	25
FIGURE 5-8 WEB INTERFACE SETTINGS	26
FIGURE 5-9 FIRMWARE UPGRADE	27
FIGURE 5-10 CONFIGURATION BACKUP/RESTORE	28
FIGURE 5-11 LOAD FACTORY DEFAULTS	28
FIGURE 5-12 REBOOT SYSTEM	29
FIGURE 5-13 SCHEDULING REBOOT	29
FIGURE 5-14 TIME ZONE SETTINGS	30
FIGURE 5-15 DDNS SETTINGS	31
FIGURE 5-16 PLANET DDNS SETTINGS	32
FIGURE 5-17 REMOTE MANAGEMENT ACCESS SETTING	32
FIGURE 5-18 WAN - STATIC	32
FIGURE 5-19 REMOTE LOGIN THROUGH DDNS DOMAIN	32
FIGURE 5-20 PLANET DDNS – MY DEVICE	33
FIGURE 5-21 UPNP SETTINGS	33
FIGURE 5-22 UPNP – NETWORK LOCATION	34
FIGURE 5-23 SNMP SETTINGS	34
FIGURE 5-24 TOPOLOGY – AP ROUTER MODE	35
FIGURE 5-25 OPERATION MODE – AP ROUTER	36
FIGURE 5-26 TOPOLOGY – WDS REPEATER MODE	36
FIGURE 5-27 OPERATION MODE – AP BRIDGE	37

FIGURE

FIGURE 5-28 TOPOLOGY - CLIENT ROUTER (WISP) MODE	37
FIGURE 5-29 OPERATION MODE – CLIENT ROUTER	37
FIGURE 5-30 WISP STEP-1	38
FIGURE 5-31 WISP STEP-2	38
FIGURE 5-32 WISP STEP-3	39
FIGURE 5-33 WISP STEP-4	39
FIGURE 5-34 WISP STEP-5	40
FIGURE 5-35 WISP STEP-6	40
FIGURE 5-36 WISP STEP-7	40
FIGURE 5-37 TOPOLOGY – CLIENT BRIDGE MODE	41
FIGURE 5-38 OPERATION MODE – CLIENT BRIDGE	41
FIGURE 5-39 SYSTEM LOG	42
FIGURE 5-40 PING	43
FIGURE 5-41 TRACEROUTE	43
FIGURE 5-42 SPEED TEST	44
FIGURE 5-43 MAC/IP/PORT FILTERING	45
FIGURE 5-44 VIRTUAL SERVER	46
FIGURE 5-45 DMZ	47
FIGURE 5-46 NAT OPTION	48
FIGURE 5-47 QOS	49
FIGURE 5-48 WEBS URL FILTER SETTINGS	51
FIGURE 5-49 WEBS HOST FILTER SETTINGS	51
FIGURE 5-50 WAN - STATIC IP	52
FIGURE 5-51 WAN - DYNAMIC IP	53
FIGURE 5-52 WAN - PPPOE	54
FIGURE 5-53 WAN - IPSEC	55
FIGURE 5-54 WAN – IPv4 (IPSEC CONNECTION TYPE)	55
FIGURE 5-55 WAN – PPTP	58
FIGURE 5-56 WAN – L2TP	59
FIGURE 5-57 LAN SETUP	60
FIGURE 5-58 DHCP SERVER	61
FIGURE 5-59 DHCP RELAY	61
FIGURE 5-60 VLAN	62
FIGURE 5-61 ADVANCED ROUTING	63
FIGURE 5-62 IPv6	64
FIGURE 5-63 WIRELESS MODE - AP	66
FIGURE 5-64 WIRELESS MODE – WDS AP	68
FIGURE 5-65 WIRELESS MODE – WDS REPEATER	70
FIGURE 5-66 WIRELESS MODE – WDS CLIENT	72
FIGURE 5-67 CLIENT BRIDGE – PROFILE SETTINGS	74
FIGURE 5-68 WIRELESS SETTINGS – ADVANCED	76
FIGURE 5-69 WIRELESS SETTINGS – ACCESS CONTROL	78
FIGURE 5-70 LOGOUT	78
FIGURE 6-1 WIRELESS ZERO CONFIGURATION	79
FIGURE 6-2 VIEW AVAILABLE WIRELESS NETWORKS	79

FIGURE 6-3 CHOOSE A WIRELESS NETWORK	80
FIGURE 6-4 ENTER THE ENCRYPTION KEY	80
FIGURE 6-5 WIRELESS NETWORK CONNECTED	81
FIGURE 6-6 WLAN AUTOCONFIG	81
FIGURE 6-7 WLAN AUTOCONFIG WINDOW	82
FIGURE 6-8 WLAN AUTOCONFIG - TYPE THE NETWORK SECURITY KEY	83
FIGURE 6-9 WLAN AUTOCONFIG – CONNECTING	83
FIGURE 6-10 WLAN AUTOCONFIG – CONNECTED	84
FIGURE 6-11 THE AIRPORT NETWORK CONNECTION ICON	84
FIGURE 6-12 THE AIRPORT NETWORK CONNECTION MENU	85
FIGURE 6-13 THE AIRPORT NETWORK CONNECTION – ENTER PASSWORD	85
FIGURE 6-14 THE AIRPORT NETWORK CONNECTION – CONNECTED	86
FIGURE 6-15 THE WI-FI SETTINGS IN IPHONE/IPOD TOUCH/IPAD	86
FIGURE 6-16 GENERAL SETTINGS	87
FIGURE 6-17 GENERAL SETTINGS – NOT CONNECTED	87
FIGURE 6-18 GENERAL SETTINGS – WI-FI ON	88
FIGURE 6-19 GENERAL SETTINGS – ENTER PASSWORD	88
FIGURE 6-20 GENERAL SETTINGS – WI-FI NETWORK CONNECTED	

1.1 Package Contents

Thank you for choosing PLANET WNAP-6308. Before installing the AP, please verify the contents inside the package box.





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

1.2 Product Description

High Power Outdoor Wireless Coverage

PLANET Technology Corp. provides a wireless solution that can be easily attached directly to the antenna, which has more flexibility to extending outdoor wireless coverage, the Wireless Outdoor Access Point -- WNAP-6308. Adopting the IEEE 802.11n advanced MIMO technology, it provides reliable wireless network coverage, and incredible improvement in the wireless performance. As an IEEE 802.11b/g/n compliant wireless device, the WNAP-6308 is able to give stable and efficient wireless performance for outdoor application, while designed with IEEE 802.11n standard and 1T1R MIMO technology, it makes it possible to deliver three times faster data rate up to 150Mbps than the normal 802.11g wireless device. With the built-in N-type antenna connector, it can directly connect with various and high gain antennas, thus it can easily cover widely range and deliver much farther wireless connection over 10Km. For WNAP-6308 is optionally following products available: ANT-OM8, ANT-OM15, ANT-FP18, ANT-SE18, ANT-YG13, ANT-YG20, and ANT-GR21.



Multiple Operating & Wireless Modes

The WNAP-6308 supports multiple types of wireless communication connectivity (AP, Client CPE, WDS PtP, WDS PtMP and Repeater) allowing for various application requirements and thus it gives users more comprehensive experience when accessing through Wireless LAN. It helps users to easily build a wireless



network and extend the wireless range of the existing wireless network. The WNAP-6308 also supports WISP mode, so CPE users could easily connect to Internet via WISP provider or connect to a wired network.

Advanced Security and Management

In aspect of security, besides 64/128- bit WEP encryption, the WNAP-6308 integrates WPA / WPA2, WPA-PSK / WPA2-PSK and 802.1x authority to secure and protect your wireless LAN. The wireless MAC filtering and SSID broadcast control consolidate the wireless network security and prevent unauthorized wireless connection. Furthermore, with the Dual-SSID feature you can set up two different wireless networks, the WNAP-6308 can therefore serve as a virtual access point for segmented networks tailored to any office or industrial need. With the SNMP-based management interface, the WNAP-6308 is convenient to be managed and configured remotely.

Highly Reliable Outdoor Device

The WNAP-6308 is perfectly suitable to be installed in outdoor environments and exposed locations. Rated to operate at the temperature from -35 to 65 degrees C and adopted IP55 and outdoor UV Stabilized Enclosure, the WNAP-6308 can perform normally under rigorous weather conditions including heavy rain and wind. With

the proprietary Power over Ethernet (PoE) design, the WNAP-6308 can be easily installed in the areas where power outlets are not available. It is the best way to use the WNAP-6308 to build outdoor wireless access applications between buildings on campuses, business, rural areas, etc.



Easy Plug-n-Link

To accomplish the concept of Plug-n-Link through an easy way for outdoor wireless network deployment, the WNAP-6308 comes with a built-in N-Type antenna connector, which is most commonly adapted with outdoor antenna. Therefore, it is easier to install via directly plugging into the mounted antenna, faster than constructing the wireless link even though a user who has never experienced in deploying a wireless network. Moreover, by using the straps through the extra ring design on the casing can fasten the WNAP-6308 to prevent from shaking or dropping caused by strong winds and earthquakes.

1.3 Product Features

Industrial Compliant Wireless LAN & LAN

- Compliant with IEEE 802.11n wireless technology capable of up to 150Mbps 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 / IPSec
- Supports Virtual Server, DMZ for various networking applications
- Supports DHCP Server, UPnP, Dynamic DNS

RF Interface Characteristics

- Built-in N-Type Male Antenna Connector
- High Output Power Up to 200mW with multiple adjustable transmit power control

Outdoor Environmental Characteristics

- IP55 Enclosure, UV resistance
- Passive Power Over Ethernet Design
- Operating Temperature: -35~65 degrees C

Multiple Operation & Wireless Mode

- Multiple Operation Modes: Bridge, Gateway, WISP
- Multiple Wireless Modes: AP, Client CPE(WISP), WDS PtP, WDS PtMP, Repeater
- Supports Dual-SSID to allow users to access different networks through a single AP
- Supports WMM (Wi-Fi Multimedia)

Secure Network Connection

- Supports Software Wi-Fi Protected Setup (WPS)
- Advanced security: 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK(TKIP/AES), and 802.1x Authentication
- Supports NAT firewall features, with SPI function to protect against DoS attacks.
- Supports IP / Protocol-based access control and MAC Filtering

Easy Installation & Management

- Web-based UI and Quick Setup Wizard for easy configuration
- Remote Management allows configuration from a remote site
- SNMP-based management interface
- System status monitoring includes DHCP Client, System Log

1.4 Product Specifications

Product	WNAP-6308	
Troduct	2.4GHz 150Mbps 802.11n Wireless Outdoor Access Point	
Hardware Specifications		
Standard	IEEE 802.11b/g/n Wireless LAN IEEE 802.11i Wireless Security IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Ethernet IEEE 802.3x Flow Control	
Memory	32 Mbytes DDR SDRAM 8 Mbytes Flash	
Interface	Wireless IEEE 802.11b/g/n, 1T1R LAN/WAN: 1 x 10/100Base-TX, Auto-MDI / MDIX	
Antenna	Built-in N-Type (Male) Antenna Connector	
Wireless RF Specification	s	
Wireless Technology	IEEE 802.11b/g IEEE 802.11n	
Data Rate	IEEE 802.11b: 11, 5.5, 2 and 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps IEEE 802.11n (20MHz): up to 72Mbps IEEE 802.11n (40MHz): up to 150Mbps	
Media Access Control CSMA / CA		
Modulation	Transmission/Emission Type: DSSS / OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK, CCK	
Frequency Band	2.412GHz ~ 2.484GHz	
Operating ChannelAmerica/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels) Japan/ TELEC: 2.412~2.484GHz (14 Channels)		
RF Output Power (Max.)	IEEE 802.11b/g: 23 ± 1.5dBm IEEE 802.11n: 23 ± 1.5dBm	
Receiver Sensitivity	IEEE 802.11b/g: -95dBm IEEE 802.11n: -91dBm	
Output Power Control	3~23dBm	
Software Features		
LAN	Built-in DHCP server supporting static IP address distributing Supports 802.1d STP (Spanning Tree)	
WAN	 Static IP Dynamic IP PPPoE PPTP L2TP 	

	- 150		
	■ IPSec		
	■ Bridge		
Operating Mode			
	■ WISP		
	NAT firewall with SPI (Stateful Packet Inspection)		
Firewall	Built-in NAT server supporting Virtual Server and DMZ		
	Built-in firewal	I with Port / IP address / MAC / URL filtering	
	■ AP		
	■ Client		
Wireless Mode	WDS PTI	D	
	WDS PTI	MP	
	WDS Rep	peater (AP+WDS)	
Channel Width	20MHz / 40MH	Hz	
Wireless Isolation	Enables isolat	tion of each connected wireless client from communicating with	
	each other mutually.		
Encryption Type	64/128-bits W	EP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X	
	Provides wireless LAN ACL (Access Control List) filtering		
Wireless Security	Wireless MAC address filtering		
Wheless Security	Supports WPS (Wi-Fi Protected Setup)		
	Enable / Disable SSID Broadcast		
Multiple SSID	Up to 2		
Max. Wireless Client	20		
Max. WDS AP	8		
Max. Wired Client	30		
WMM	Supports Wi-Fi Multimedia		
QoS	Supports Quality of Service for bandwidth control		
NTP	Network Time Management		
Management	Web UI, DHCP Client, Configuration Backup & Restore. Dvnamic DNS. SNMP		
Diagnostic tool	System Log, Ping Watchdog		
Mechanical & Power			
IP Rate	IP55		
Material	Outdoor UV Stabilized Enclosure		
Dimensions (Φ x H)	45 x 169 mm		
Weight	128kg		
Installation	Pole mounting		
	LAN 1	2~24V DC, Passive PoE	
Power Requirements	F	Pin 4,5 VDC+	
	F	Pin 7,8 VDC-	
Power Consumption	1.5W		
Environment & Certificati	on		
Operation Temperature	-35 ~ 65 degre	ees C	
Operating Humidity	5 ~ 90% non-condensing		

Regulatory	CE / FCC/ RoHS			
Accessory				
Standard Accessories	 Passive PoE injector & Power Cord x 1 Plastic Strap x 2 Quick Installation Guide x 1 CD (User's Manual, Quick Installation Guide) x 1 			

Chapter 2. Hardware Installation

Please follow the instructions below to connect the WNAP-6308 to the existing network devices and your computers.

2.1 Hardware Description

Dimensions: 45 x 169 mm (Φ x H)



Figure 2-1 Appearance

2.1.1 The Top / Bottom Panel

The top and the bottom panels provide the physical connectors connected to the antenna, power injector and any other network device. Figure 2-2 shows the top and the bottom panels of the WNAP-6308.



Figure 2-2 Top / Bottom Panel

Object	Description		
PoE (LAN Port)	10/100Mbps RJ-45 port , Auto MDI/ MDI-X & Passive PoE supported.		
	(Pin 4,5 VDC+; Pin 7,8 VDC-)		

Top & Bottom Panel

	Connect this port to the xDSL modem in router mode.		
	Connect this port to the network equipment in bridge mode.		
	N-Type Male Antenna Connector.		
N-Type (Male) Antenna Connector	Connect N-Type (M) Antenna Connector with 2.4GHz Outdoor Antenna directly or through the N-male (male pin) to N-female (female pin) cable.		
	Planet supplied RF cable Model No.: WL-MF-0.6 or WL-N-10.		
Reset	Push continually the reset button about 15 seconds to reset the configuration parameters to factory defaults.		

2.1.2 The Side Panel

The side panel provides the LED indicators of system status and signal strength when connected to the remote AP. Figure 2-3 shows the side panel of the WNAP-6308.

LED Indicator

802.11 b/g/n Access Point	
PLANET Hetworking & Communication	

Figure 2-3 The LED Indicator

LED		Status	Indication	
Power		On	System On	
		Off	System Off	
LAN		On	Port linked.	
		Off	No link.	
		Blinking	Data is transmitting or receiving on the LAN interface.	
Signal Indicator LED1		On	The Signal Strength reaches the value	
LED2		On	The Signal Strength reaches the value	
LED3 (On	The Signal Strength reaches the value	
LED4 On		On	The Signal Strength reaches the value	

Chapter 3. Connecting to the AP

3.1 Preparation before Installation

3.1.1 Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

3.1.2 Safety Precautions

- 1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
- 2. If you are installing the WNAP-6308 for the first time, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved.
- 3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
- 4. When installing the WNAP-6308, please note the following things:
 - Do not use a metal ladder;
 - Do not work on a wet or windy day;
 - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- 5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

3.2 Installation Precautions

- Users MUST use a proper and well-installed surge arrestor and grounding kit with the WNAP-6308; otherwise, a random lightning could easily cause fatal damage to the WNAP-6308. EMD (Lightning)
 DAMAGE IS NOT COVERED UNDER WARRANTY.
- Users MUST use the "Power cord and PoE Injector" shipped in the box with the WNAP-6308. Use of other options will cause damage to the WNAP-6308.
- Users MUST power off the WNAP-6308 first before connecting the external antennas to it; otherwise, damage might be caused to the WNAP-6308 itself.
- The Antenna is required, and must be purchased separately.



OUTDOOR INSTALLATION WARNING

IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK! Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

CONTACTING POWER LINES CAN BE LETHAL. Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these lines. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure there is NO possibility that equipment or personnel can come in contact directly or indirectly with power lines.



Assume all overhead lines are power lines.

The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination. This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

- Select equipment locations that will allow safe, simple equipment installation.
- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Use approved non-conducting lasers and other safety equipment. Make sure all equipment is in good repair.
- If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or mast does come in contact with a power line, DON'T TOUCH IT OR ATTEMPT TO MOVE IT. Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED

TO ANTENNAS HAVE LIGHTNING ARRESTORS. This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

- The base of the antenna mast or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 10 AWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE:

- DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.
- Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.

Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

3.3 Installing the AP

Please install the AP according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

Step 1. Connect the Antenna to the top of the WNAP-6308.



Figure 3-1 Connect the Antenna

Step 2. (1) Open the bottom of the WNAP-6308.
(2) Plug the RJ-45 Ethernet cable into the LAN port through the Cap and Gasket. Then seal the bottom of the WNAP-6308 with the Cap and Gasket.



Figure 3-2 Connect the Ethernet cable

Step 3. Take out the power cord and PoE injector. Plug the power cord into the DC port and plug the other side of the RJ-45 cable like Step 2 into the POE port of the PoE injector.



Figure 3-3 Connect the PoE injector

Step 4. Pole Mounting:

Place the straps through the slots on the sides of the WNAP-6308 and then around the pole. Tighten the straps to secure the WNAP-6308.



Figure 3-4 Pole Mounting

Chapter 4. Quick Installation Guide

This chapter shows you how to configure the basic functions of your AP using **Easy Setup** within minutes.



A computer with wired Ethernet connection to the Wireless AP is required for the first-time configuration.

4.1 Manual Network Setup - TCP/IP Configuration

The default IP address of the WNAP-6308 is **192.168.1.1**. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the WNAP-6308 with your PC by an Ethernet cable plugging in the LAN port of the PoE injector on one side and in the LAN port of the PC on the other side. Please power on the WNAP-6308 by PoE from PoE injector or PoE switch.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 7**. And the procedures in other operating systems are similar. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter manual if needed.

4.1.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The AP's default IP address)
- 1 Select Use the following IP address radio button.
- 2 If the AP's LAN IP address is 192.168.1.1, enter IP address 192.168.1.x (x is from 2 to 254), and **Subnet** mask 255.255.255.0.
- 3 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field, you can enter the DNS server IP address which has been provided by your ISP

eneral	
You can get IP settings assigned this capability. Otherwise, you no for the appropriate IP settings.	automatically if your network supports eed to ask your network administrator
Obtain an IP address autor	natically
• Use the following IP addres	s:
IP address:	192 . 168 . 1 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	1 11 11
Obtain DNS server address	automatically
Ose the following DNS serve	er addresses:
Preferred DNS server:	D 13 14
Alternate DNS server:	
	Advanced

Figure 4-1 TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 7** OS. Please follow the steps below:

- 1. Click on **Start > Run**.
- 2. Type "**cmd**" in the Search box.

Files (1)				
History				
P See more res	ults			
cmd		×	Shut down	n 🕨

- 3. Open a command prompt, and type ping **192.168.1.1**, and then press **Enter**.
 - If the result displayed is similar to Figure 4-3, it means the connection between your PC and the AP has been established well.



Figure 4-3 Successful result of Ping command

If the result displayed is similar to Figure 4-4, it means the connection between your PC and the AP has failed.



Figure 4-4 Failed result of Ping command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

4.2 Starting Setup in the Web UI

It is easy to configure and manage the WNAP-6308 with the web browser.





Figure 4-5 Login by default IP address

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 4-6 Login Window

Default IP Address: 192.168.1.1

Default User name: admin

Default Password: admin

Note

If the above screen does not pop up, it may mean that your web-browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

After entering the username and password, the Status page screen appears as Figure 4-8

PLANET Networking & Communication		WNAP-6308 802.11b/g/n Wireless Outdoor Access Poin		
Status	Easy Setup	Advanced	Language English 🝸	
LAN Configuration				
LAN IP A	LAN IP Address 192.168.2.1 MAC Address 00:30:4F:61:1A:58		.255.255.0	
System Info				
Firmware V	Firmware Version V2.6 2013-08-16-10:30		n, 01 Jan 2012 12:01:06	
Operation	n Mode AP Bridge mode	Wireless MAC Address 00:	30:4F:61:1A:5A	



Step 2. Go to "**Easy Setup**" to choose an Operation Mode. Please refer to the instructions in the next chapter for configuring the other Operation Mode.



Figure 4-8 Choose Operation Mode

Step 3. Please enter the SSID, configure your Encryption Settings, Pre-Shared Key, etc. Then click **Done** button to make the configuration take effect immediately.

SSID I Security Settings	
Network Name (SSID)	WNAP-6308
WPS Choice	
Encryption Settings	WPA2-PSK
WPA Algorithms	● TKIP [?] ● CCMP(AES) ● Auto
Key Renewal Interval(Secconds)	60
Pre-Shared Key	12345678 Generator
Done	Back

Figure 4-9 Configure Wireless Settings

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and features under 3 main menus (**Status**, **Easy Setup**, and **Advanced**) below, allowing you to manage the AP with ease.

PLANET Networking & Communication		802.11b/g/n Wirele	Logout WNAP-6308 ss Outdoor Access Point
Status	Easy Setup	Advanced	Language English 💙



5.1 Status

On this page, you can view information about the current running status of the WNAP-6308, including WAN interface, LAN interface, wireless interface, and firmware version information.

Status
Status
Statistics
DHCP Clients
Station List

Status



This section allows you to view the AP's system info listed below:

Internet Configuration			
Connected Type	онср	Connected Status	
WAN IP Address		Subnet Mask	
Default Gateway		Primary Domain Name Server	
Secondary Domain Name Server		MAC Address	00:30:4F:60:37:91
LAN Configuration			
LAN IP Address 1	192.168.1.1	LAN Netmask	255.255.255.0
MAC Address 0	00:30:4F:60:37:90		
System Info			
Firmware Version V	/2.6 2012-10-23-15:12	System Time	Sun, 01 Jan 2012 12:02:42
Operation Mode A	AP Router mode	Wireless MAC Address	00:30:4F:60:37:92

Figure 5-2 Status

Object	Description
Internet Configuration	
Connected Type	Displays current Internet connection type.
Connected Status	 Disconnected: Indicates that the Ethernet cable from your ISP side is / is not correctly connected to the WAN port on the AP or the AP is not logically connected to your ISP. Connecting: Indicates that the WAN port is correctly connected and is requesting an IP address from your ISP. Connected: Indicates that the AP has been connected to your ISP.
• WAN IP	Displays WAN IP address.
Subnet Mask	Displays WAN subnet mask.
Default Gateway	Displays WAN gateway address.
Primary Domain Name Server	Displays WAN DNS address.
Secondary Domain Name Server	Displays WAN DNS address.
MAC Address	Displays AP's WAN MAC address.
LAN Configuration	
LAN IP Address	Displays LAN IP address.
LAN Netmask	Displays LAN subnet mask.
MAC Address	Displays AP's LAN MAC address.
System Info	
• Firmware Version	Displays current F/W version.
System Time	Displays the System Time.
Operation Mode	Displays current Operation Mode.
Wireless MAC Address	Displays AP's Wireless MAC address.

Statistics

Status	
Status	
Statistics	ĥ
DHCP Clients	1
Station List	

This section allows you to view the AP's statistics listed below:

Memory				
Memory Left/Memory Total 1	3776 kB /28436 kB			48.4%
WAN/LAN				
WAN Rx packets 2	3182		WAN Rx bytes	2035659
WAN Tx packets 4	65		WAN Tx bytes	45355
LAN Rx packets 4	101		LAN Rx bytes	478060
LAN Tx packets 3	577		LAN Tx bytes	698397
	All interfaces	Clear Statistics		



Object	Description
Memory	
 Memory Left/ Memory Total 	Displays the retain memory and total memory.
WAN/LAN	
WAN Rx packets	Displays the real-time packets received from WAN port.
WAN Rx bytes	Displays the real-time bytes received from WAN port.
WAN Tx packets	Displays the real-time packets transmitted from WAN port.
WAN Tx bytes	Displays the real-time bytes transmitted from WAN port.
LAN Rx packets	Displays the real-time packets received from LAN port.
LAN Rx bytes	Displays the real-time bytes received from LAN port.
LAN Tx packets	Displays the real-time packets transmitted from LAN port.
LAN Tx bytes	Displays the real-time bytes transmitted from LAN port.

DHCP Clients

Status	
Status	
Statistics	
DHCP Clients	վել
Station List	

This section displays a DHCP dynamic client list, which includes MAC address, IP address, and lease time info.

DHCP Clients		
MAC Address	IP Address	Expires in
00:26:66:46:cb:cf	192.168.1.195	23:27:35
	Refresh	

Figure 5-4 DHCP Client List

Object	Description
MAC address	Displays MAC address of a given host.
IP Address	Displays IP address(es) that client(s) obtained from the DHCP server.
• Expires in	Remaining time for a corresponding IP address lease.

Station List

Status	
Status	
Statistics	
DHCP Clients	
Station List	Ś

This section allows you to view the Station List. The Station List submenu is only available in AP mode.

Internet Configuration			
Connected Ty	pe DHCP	Connected Status	
WAN IP Addre	ss	Subnet Mask e	th0
Default Gatew	ay	Primary Domain Name Server	
Secondary Domain Name Serv		MAC Address 0	0:30:4F:61:1A:59
LAN Configuration			
LAN IP Addre	ss 192.168.2.253	LAN Netmask 2	55.255.255.0
MAC Addre	ss 00:30:4F:61:1A:58		
System Info			
Firmware Versi	on V3.0b 2013-12-06-11:33	System Time S	un, 01 Jan 2012 20:39:23
Operation Mo	de AP Router mode	Wireless MAC Address 0	0:30:4F:61:1A:5A
Station List			
MAC Address	RATE	RSSI	RSSI(dB)
00:30:4f:a8:ff:ff	149M	28%	-67

Figure 5-5 Station List

Object	Description
MAC address	Displays MAC address of a connected client.
Rate	Displays connection speed of a connected client.
Expires in	Displays the signal strength of a connected client.

5.2 Easy Setup

The Easy Setup helps you configure the basic functions of your AP within minutes.

Please refer to the Step 2 in the section "4.2 Starting Setup in the Web UI" for the detailed procedure.

Status	Easy Setup	Advanced	Language English 👻
Operation Mode Setup			
	Please select an Operation	on Mode Please select an Operation Mod	e 💙
		Next	

Figure 5-6 Easy Setup

5.3 Advanced

"Advanced" includes the following four submenus (Advanced, Firewall Settings, Network Settings, and Wireless Settings). Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



Figure 5-7 Advanced Menu

5.3.1 Advanced - Management



This section allows you to manage the Wireless AP.

5.3.1.1. Web Interface Settings (Password)

System Management					
Web Interface Se	ttings	Firmware Upgrade	Configuration	Load Factory Defaults	
Reboot System	Schee	uling Reboot			
	User Name admin				
		Pass	word		
		Re-enter to con	nfirm		
			Apply		
			11.7		

Figure 5-8 Web Interface Settings

Object	Description
User Name	Display the User Name info.
Password	Enter the new password that you prefer for login.
Re-enter to confirm	Re-enter the new password to confirm.



If you change the login password, you must enter the new one in the next login.
5.3.1.2. Firmware Upgrade

System Management	2				
Web Interface Se	ttings Firmware Upgrade	Configuration	Load Factory Defaults		
Reboot System Scheduling Reboot					
	Software Ve Loc Warning Upgrading firmw Do not turn off the	are may take a f	-10-23-15:12 Browse ew minutes. the browser!		

Figure 5-9 Firmware Upgrade

Click the "**Browse...**" button to select the new firmware for upgrading.

Object	Description
Software Version	Display the current Software Version info.
Location	Click the "Browse" button to select the new firmware in this field.
• Upload	Click the "Upload" button to upgrade the new firmware.



5.3.1.3. Configuration

vstem Management					
Web Interface Set	ttings	Firmware Upgrade	Configuration	Load Factory Defaults	
Reboot System	Schedu	ling Reboot			
		Export Configuration	File Export]	
	1	mport Configuration	n File Import	Browse	
Conly	Warning upload f Do not	iles backed up using upload any files th	g this firmware a router. at were not creat	nd from the same model of ed by this interface!	ī

Figure 5-10 Configuration Backup/Restore

Click the "**Export**" button to back up the configuration of the Wireless AP, and click "**Import**" to restore the configuration.

Object	Description	
• Export	Click the "Export" button to back up the configuration.	
Browse	Click the "Browse" button to select the configuration file in this field for restoring settings.	
Import Click the "Import" button to restore the configuration.		

5.3.1.4. Load Factory Defaults

System Management					
Web Interface Set	ttings	Firmware Upgrade	Configuration	Load Factory Defaults	
Reboot System	Schee	luling Reboot			
Res	store Se	ettings To Factory De	fault Load Def	ault	

Figure 5-11 Load Factory Defaults

Click the "Load Default" button to reset it to factory default settings.

5.3.1.5. Reboot System

System Management					
Web Interface Set	ttings	Firmware Upgrade	Configuration	Load Factory Defaults	
Reboot System	Schee	luling Reboot			
		Reboot Sy	stem Reboot N	low!	

Figure 5-12 Reboot System

Click the "Reboot Now!" button to restart the Wireless AP.

5.3.1.6. Scheduling Reboot

System Management	
Web Interface Settings Firmware Upgrade Configuration Load Factory Defaults	
Reboot System Scheduling Reboot	
Enable Scheduling Reboot Disable	
Apply Cancel	

Figure 5-13 Scheduling Reboot

Select "Enable" to configure the system auto reboot according to the Duration Time (Time interval).

Object	Description	
Enable Scheduling	Enable: select it to enable the Scheduling Reboot.	
Reboot	Disable: select it to disable the Scheduling Reboot.	
Den time Time	Configure the particular time interval for the system auto reboot.	
Duration Time (bb:mm)	hh: means hours	
()	mm: means minutes	

5.3.2 Advanced – Advanced Settings

Advanced	
Management	
Advanced Settings	վեղ
Operation Mode	U
System Log	
Tools	

This section allows you to configure advanced settings of the Wireless AP.

5.3.2.1. Time Zone Settings

Advanced	Settings					
Time Zone Settings	DDNS Settings	UPNP Settings	SNMP Settings		_	
	Current Time <mark>Su</mark>	n, 01 Jan 2012 14:50	Sync with host			
	Time Zone Pl	ease select your	Time Zone setti	ngs.	~	
	SNTP Server		[?]			
SNTP synchroniza	tion (minutes)					
		App	Cano	el		

Figure 5-14 Time Zone Settings

Object	Description
Current Time	Display the current time.
Sync with host	Click it to sync your PC's time to the device.
Time Zone	Select your current time zone.
SNTP Server	Configure your SNTP Server.
SNTP Synchronization (minutes)	Determines a time length when device periodically updates its time and date info from Internet.

5.3.2.2. DDNS Settings

Advanced Settings			
Time Zone Settings DDNS Settings	UPNP Settings	SNMP Settings	
Dynamic DNS Provider None	~		
HostName			
	Арр	ly Cancel	



The page includes the following fields:

Object	Description
Dynamic DNS Provider	Select your Dynamic DNS 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	Password: Enter the password of the DDNS account.

Example of Planet DDNS Settings:

Note

Please go to http://www.planetddns.com/ to register a Planet DDNS account.

Please refer to the FAQ (http://www.planetddns.com/index.php/faq) on how to register a free account.

Please refer to the procedure listed as follows to configure using Planet DDNS service.

Step 1. Select "planetddns.com" to choose Planet DDNS service.

Step 2. Configure the DDNS account that has been registered on Planet DDNS website.

Host Name: Enter your DDNS host (format: xxx.planetddns.com, xxx is the registered domain name)

User Name: Enter your DDNS account

Password: Enter your DDNS account's password

Advanced Settings					
Time Zone Settings DDNS Settings	UPNP Settings	SNMP Settings		_	
Dynamic DNS Provider planetddns	.com 💙		ne <mark>test12</mark>		
HostName test12.plan	etddns.		rd •••••		
	Арр	oly Canc	el		

Figure 5-16 Planet DDNS Settings

Step 3. Go to "Advanced-> Firewall Settings-> Firewall" to allow remote access from WAN port.

Remote Management Access	
	Remote Management (via WAN) Allow ⊻
	Remote Management Port 2020

Figure 5-17 Remote Management Access Setting

Step 4. Go to "Advanced-> Network Settings-> WAN" to configure WAN Connection using Static (Fixed IP).

Wide Area Network (WAN) Settings			
	WAN Connections	Static (Fixed IP)	✓
Static Mode			
	IP Address	210.66.155.70	
	Subnet Mask	255.255.255.0	
	Default Gateway	210.66.155.94	
DNS Settings			
Primary DNS Server 8.8.8.8		Secondary	DNS Server 168.95.1.1
	Apply	ancel	

Figure 5-18 WAN - Static

Step 5. Apply the settings, and connect your WAN port of the Wireless AP to the internet by Ethernet cable.

Step 6. In a remote computer, enter the DDNS host name as the figure is shown below. Then, you should be able to login the WNAP-6308 remotely.

Please remember to enter the remote management port number that you have configured in Step 3.



Figure 5-19 Remote Login through DDNS domain

You can go to **My Devices** page of Planet DDNS website to check if the "**Last Connection IP**" is displayed. This indicates your DDNS service is working properly.



Figure 5-20 Planet DDNS – My Device

5.3.2.3. UPNP Settings

Select "Enable" to enable the UPNP function.

Advanced S	Settings
Time Zone Settings	DDNS Settings UPNP Settings SNMP Settings
	UPNP Settings Enable
	Apply Cancel

Figure 5-21 UPnP Settings

In the computer connected with the WNAP-6308, go to "**Network**" to check whether the WNAP-6308 is displayed on the list.

Double-click it to logon the Web UI of the WNAP-6308.



Figure 5-22 UPnP - Network Location

5.3.2.4. SNMP Settings

Enabling **SNMP** function will allow the network management station to retrieve statistics and status from the SNMP Agent in the device.

Advanced Settings	
Time Zone Settings DDNS Settings UPNP Settings SNMP Settings	
SNMD Sattings Enable w	
Get Community public	
Set Community private	
Apply Cancel	

Figure 5-23 SNMP Settings

Object	Description
• SNMD Sottingo	Choose Enable to open this function if you want to have
• Siving Settings	remote control through SNMPv1/v2 agent.

	Choose Disable to close this function.
	Enter the community name that allows Read-Only access to
Get Community	the Device's SNMP information. The community name can be
	considered a group password. The default setting is public.
	Enter the community name that allows Read/Write access to
Set Community	the Device's SNMP information. The community name can be
	considered a group password. The default setting is private.

5.3.3 Advanced – Operation Mode



There are 4 operation modes (**AP Router**, **AP Bridge**, **Client Router**, **Client Bridge**) that can be configured to meet various applications.

5.3.3.1. AP Router (AP+Router)

In the Access Point Mode with Router Function, the **WNAP-6308** acts as a central connection point, which wireless clients can connect to. The DHCP & NAT is enabled, so the clients are wirelessly connected to the WNAP-6308 that can share the internet connection by connecting the WNAP-6308 to a DSL/cable modem.



Figure 5-24 Topology – AP Router Mode

- 1. Connect the LAN port of the WNAP-6308 to the POE port of the PoE Injector over an Ethernet cable.
- 2. Connect the DSL/cable modem to the WAN port of the WNAP-6308.

- 3. Plug one end of the power cord into the PoE Injector, and the other end in electrical socket.
- 4. Go to "Advanced-> Operation Mode" to configure it in AP Router Mode.

Operation Mode Configuration					
Oper	ation Mode	AP Router	*		
	Apply	Cancel			





To configure the Wireless Settings of AP Router Mode, please refer to the section 5.6 Wireless Settings.

5.3.3.2. AP Bridge (AP+WDS)

In the Access Point mode with WDS function, the **WNAP-6308** functions like a central connection for any stations or clients. Stations and clients must configure the same SSID and Security Password to associate within the range. The WNAP-6308 supports 2 different SSIDs to separate different clients at the same time.



Figure 5-26 Topology – WDS Repeater Mode

- 1. Connect the LAN port of the WNAP-6308 to the POE port of the PoE Injector over an Ethernet cable.
- 2. Connect the PC to the LAN port of the PoE Injector over an Ethernet cable.
- 3. Plug one end of the power cord into the PoE Injector, and the other end in electrical socket.
- 4. Go to "Advanced-> Operation Mode" to configure it to AP Bridge mode.





To configure the Wireless Settings of AP Bridge Mode, please refer to the section 5.6 Wireless Settings.

5.3.3.3. Client Router (WISP)

In the Client Router mode, the WNAP-6308 has DHCP Server built inside that allows many LANs automatically generate an IP address to share the same Internet. Connect an AP/WISP wirelessly and connect to LANs via wired. The Client Router mode acts completely opposite to the AP Router mode.



Figure 5-28 Topology – Client Router (WISP) Mode

- 1. Connect the LAN port of WNAP-6308 to the POE port of the PoE Injector over an Ethernet cable.
- 2. Connect the PC to the LAN port of the PoE Injector over an Ethernet cable.
- 3. Plug one end of the power cord into the PoE Injector, and the other end in electrical socket.
- 4. Go to "Advanced-> Operation Mode" to configure it to Client Router mode.

Operation Mode Configuration		
Operation	n Mode Client Router 🛩	
App	pply Cancel	

Figure 5-29 Operation Mode - Client Router

WISP Setup Procedure:



Figure 5-30 WISP Step-1

Step 2. Click "Site Survey" to discover the Wireless Internet Service Provider.

Step 3.	Select the WISP's AP, and the click "Select".
---------	---

O WNAP-6350 00:30:4F:60:37:92 54 Mb/s 82/94(-66 dBm) 6 WPA2-Personal CCMP Infr	INTE TYP
	rastructur
WNAP-6350 00:30:4F:60:EF:F6 54 Mb/s 93/94(-55 dBm) 6 WPA2-Personal CCMP Infr	rastructur

Figure 5-31 WISP Step-2

Step 4. Enter the Passphrase, and then click "Add" to add this setting to the profile.

Currently	Used Profile					
SSI						
Profile L	list					
Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
-						No Wirelėss Profile Rulesi
Profile Se	tup					
	Profile Name	WNAP-6	350		Network Type Infrast	ructure 🜱 Site Survey
	SSIC	WNAP-6	350		BSSID(optional) 00:30	4F:60:AF:7A
	Encryption Settings	WPA2-PS	к 🗹		Encryption CCMF	
	Passphrase	•••••	•			
Ack Time	out Settings					
	Distance	_	0.6	miles (1.0 km)		
	ACK/CTS Timeout	41				
	RTS/CTS		Bytes			
Fragn	nentation Threshold	-	Bytes			
			Activate	Add Delet	ę	

Figure 5-32 WISP Step-3

Step 5. The profile should be listed on the Profile List as the figure is shown below.





Step 6. Go to "Advanced-> Network Settings-> LAN" to enable DHCP Server.

LAN Setup	
MAC Address	00:30:4F:60:37:90
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Setup	
DHCP Server	DHCP Server 💌
Local Domain Name (Optional)	
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Lease Time	One day 💌
Apply	Cancel

Figure 5-34 WISP Step-5

Step 7. Go to "Advanced-> Network Settings-> WAN" to configure the WAN Connection.

Wide Area Network (WAN) Settings		
	WAN Connections Cable/Dynamic IP (DHCP) 💌	
DHCP Mode		
	Hostname planet	
DNS Settings (Optional)		
Primary DNS Server 8.8.8.8	Secondary DNS Server 168.95.1.1	
	Apply Cancel	

Figure 5-35 WISP Step-6

Step 8. Configure the wired client's TCP/IP setting to "Obtain an IP address automatically".

ieneral	Alternate Configuration	
You ca this cap the app	n get IP settings assigned ability. Otherwise, you ne ropriate IP settings.	d automatically if your network supports sed to ask your network administrator for
00	otain an IP address autor	natically
OU	se the following IP addres	и
JP a	Idress:	
Syb	net mask:	
Defa	ult gateway.	
0	btain DNS server address	s automatically
OU	se the following DNS serv	ver addresses;
Eref	erred DNS server.	
Alter	nate DNS server.	
		Advanced
_		OK Ca

Figure 5-36 WISP Step-7

After getting the IP assigned by the WNAP-6308, ping the DNS server to check whether internet connection is reachable.

5.3.3.4. Client Bridge (Slave AP Bridge)

In the Client Bridge mode, the WNAP-6308 functions like a wireless adapter. Connect to an Access Point wirelessly and surf Internet whenever you want. Using Site Survey to scan all the Access Points within the range and configure its SSID and Security Password to associate with it.



Figure 5-37 Topology - Client Bridge Mode

- 1. Connect the LAN port of WNAP-6308 to the POE port of the PoE Injector over an Ethernet cable.
- 2. Connect the PC to the LAN port of the PoE Injector over an Ethernet cable.
- 3. Plug one end of the power cord into the PoE Injector, and the other end in electrical socket.
- 4. Go to "Advanced-> Operation Mode" to configure it to Client Bridge mode.



Figure 5-38 Operation Mode – Client Bridge

To configure the Wireless Settings of Client Bridge Mode, please refer to the section 5.6 Wireless Settings.

5.3.4 Advanced – System Log

Choose menu "Advanced-> System Log" to view the logs of the Wireless AP.

Advanced	
Management	
Advanced Settings	
Operation Mode	
System Log	վեր
Tools	Ú

Click "Refresh" to update the system log.

Click "Clear" to erase the current system log.



Figure 5-39 System Log

5.3.5 Advanced – Tools

The Tools included **Ping**, **Traceroute**, **and Throughput** can help user diagnostic the network connection.



5.3.5.1. Ping

Ping is a network tool used to test whether a particular host is reachable across an IP network. Enter the IP, Ping Count, and click "**Start**" to diagnostic your internet connection.



Figure 5-40 Ping

5.3.5.2. Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. It can help identify connection problems.

Enter the IP or Host Name, and click "Start" to diagnostic your internet connection.

Tools				
	Ping	Traceroute	Throughput	
			URL http:// www.google.com	
			Arraceroute Start raceroute Start raceroute to www.google.com (173.194.72.103), 30 hops max, 38 byte packets 1 h94-210-66-155.seed.net.tw (210.66.155.94) 167.541 ms 0.703 ms 0.712 ms 2 172.26.9.149 (172.26.9.149) 35.986 ms 35.667 ms 35.790 ms 3 139.175.70.2 (139.175.70.2) 35.920 ms 35.636 ms 35.772 ms 4 R56-30.seed.net.tw (139.175.56.30) 38.422 ms 36.108 ms 35.989 ms 5 R58-193.seed.net.tw (139.175.58.193) 36.235 ms 35.875 ms 35.641 ms 6 R59-194.seed.net.tw (139.175.59.194) 36.534 ms 35.308 ms 37.878 ms 7 h33-192-72-123.seed.net.tw (192.72.123.33) 37.694 ms 35.537 ms 35.822 ms 8 209.85.243.26 (209.85.243.26) 35.861 ms 35.699 ms 37.755 ms 9 209.85.250.103 (209.85.250.103) 37.894 ms 37.706 ms 209.85.250.101 (209.85.250.101) 39.776 ms	
			Start Stop	

Figure 5-41 Traceroute

5.3.5.3. Throughput

Click "VISIT THE SITE TO TEST SPEED" button to go to <u>http://www.speedtest.net/</u> to test the Internet connection speed.

Tools						
	Ping	raceroute	Throughput		_	
	Speed Testing Test the speed to the internet. Before visit the site to test the speed, The client need to be installed the Adobe Flash Player 10 or newer version first.					
				VISIT THE SITE TO TEST SPEED		

Figure 5-42 Speed Test

5.4 Firewall Settings

5.4.1 MAC/IP/Port Filtering



Basic Settings	
MAC/IP/Port Filtering Enable 🜱	Default Policy: Describes how packets not matching any rules will Accepted Y be handled
	Apply Reset
MAC/IP/Port Filter Settings	
MAC address	
Destination IP address (DIP)	Source IP address (SIP)
Protocol None 💌	
Destination Port Range (DPR)	Source Port Range (SPR)
Action Drop 💌	
Comment	
	(The maximum rule count is 32.)
	Apply Reset
Current MAC/IP/Port filtering rules in system	
No. MAC address DIP	SIP Protocol DPR SPR Action Comment
	Others would be accepted
	Delete Selected Reset

Figure 5-43 MAC/IP/Port Filtering

Object	Description		
MAC/IP/Port Filtering	Select Enable to enable the MAC/IP/Port Filtering function.		
Default Policy	Select a policy for filtering rule.		
MAC Address	Fill in the MAC address of source NIC, to restrict data transmission.		
Destination IP address (DIP)	Fill in the IP address of destination, to restrict data transmission.		
Source IP address (SIP)	Fill in the IP address of source, to restrict data transmission.		
Protocol	Select the protocol that you want to restrict. There are four options: None, TCP, UDP and ICMP.		
Destination Port Range	Fill in the start-port and end-port number of destination, to restrict data transmission.		
Source Port Range	Fill in the start-port and end-port number of source, to restrict data transmission.		
Action	Select Accept or Drop to specify the action of filtering policies.		
Comment	Make a comment for the filtering policy.		

5.4.2 Virtual Server

Firewall Settings			
MAC/IP/Port Filtering			
Virtual Server 🔬			
DMZ			
Firewall			
QoS			
Content Filtering			
Virtual Conver			
	Virtual Server Fnable V		
	Apply		
	ID Address		
	Driveto Port		
	Comment		
		(The maximun	n rule count is 32.)
	Apply Reset		
Current Virtual Servers in system			
No. IP Address	Port Mapping	Protocol	Comment
	Delete Selected Reset		

Figure 5-44 Virtual Server

Object	Description
Virtual Server	Select Enable to enable the Virtual Server function.
• IP address	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address.
Private Port	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the private port.
Public Port	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the public port.
Protocol	The protocol used for this application, either TCP, UDP, or TCP&UDP (all protocols are supported by the Device.).
Comment	Make a comment to help identify the setting.

5.4.3 DMZ

Firewall Setting	S	
MAC/IP/Port Filterin	ıg	
Virtual Server		
DMZ	d b	
Firewall		
QoS		
Content Filtering		
DMZ Settings		
		DMZ Settings Enable 💌
		DMZ IP Address 192.168.1.100
		Apply Reset

Figure 5-45 DMZ

Object	Description	
DMZ Settings	Select Enable to enable the DMZ function.	
DMZ IP Address	To support DMZ in your firewall design, fill in the IP address of	
	DMZ host that can be accessed from the WAN interface.	

5.4.4 Firewall

Firewall Settings	
MAC/IP/Port Filtering	
Virtual Server	
DMZ	
Firewall	շխ
QoS	
Content Filtering	

Remote Management Access			
Remote Management (via WAN)	Allow 🔽		
Remote Management Port	2020		
Ping from WAN Flitter			
Ping from WAN Filter	Allow 🛩		
Stateful Packet Inspection (SPI)			
SPI Firewall	Disable 💌		
Network Address Translation Settings			
Network Address Translation	Enable 🔽 😭	Note:	
	V	In the second se	
		If it is enabled, the LAN	
PPPoE Passthrough Setup		devices will connect to	
PPPoE Passthrough	Disable 💌	the Internet.	
Apply	Reset		

Figure 5-46 NAT Option

Object	Description	
Remote Management (via WAN)	Select Deny or Allow for remote management function.	
Remote Management Port	Configure the port for remote management.	
• Ping from WAN Filter	Select Deny or Allow for Ping permit from WAN.	
SPI Firewall	Select Disable or Enable for SPI firewall function.	
Network Address Translation	Enable it to let the LAN devices connect to the Internet. All computers must be assigned with a public IP address to get connected to the Internet without NAT. However, Internet Service Providers only provide very few IP addresses to every user. Therefore it is necessary to use NAT to share a single public IP address to multiple computers on local network, so everyone can get	

	connected to the Internet.
PPPoE Passthrough	Enable it to allow Multiple PPP connections on remote hosts.

5.4.5 QoS

Quality of Service provides an efficient way for clients on the network to share the bandwidth with a promised quality of Internet service. Without QoS, all computers and devices on the network will compete with each other to get the bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected. With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth for a specific computer, to avoid such unpleasing result from happening.



Figure 5-47 QoS

Object	Description	
QoS Setup	Select Enable to enable the QoS function.	
Upload Bandwidth	Set the limit of total upload bandwidth in kbits. To disable upload bandwidth limitation, input '0' here.	
Download Bandwidth	Set the limit of total download bandwidth in kbits. To disable download bandwidth limitation, input '0' here.	
• Target	Set the target of QoS rule.	
Source IP	Specify the local (source) IP address that will be affected by this rule. Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.	
Destination IP	Specify the remote (destination) IP address that will be affected by this rule. Please input the starting IP address in the left field and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.	
Application	Select the pre-defined application for this rule.	
Protocol	Please select the protocol type of this rule. If you don't know what protocol your application uses, please try ' TCP ' first, and switch to ' UDP ' if this rule doesn't seems to work.	
Ports	Fill out the ports for this rule.	
Number of Bytes	Fill out the maximum number of bytes for this rule.	

5.4.6 Content Filtering

Firewall Settings	
MAC/IP/Port Filtering	
Virtual Server	
DMZ	
Firewall	
QoS	
Content Filtering	d۳)

There are two types (Webs URL Filter Settings and Web Host Filter Settings) of content filtering.

5.4.6.1. Webs URL Filter Settings

The Webs URL Filter option allows you to set up a list of Web sites you would like to deny through your network. Please enter a URL for filtering.

Content Filter Settings			
	Webs URL Filter Settings	Webs Host Filter Settings	
	Current Web URL Filters	5	
	No	URL	
		Delete Reset	
	Add	a URL filter Http(s)://	
		Add Reset	

Figure 5-48 Webs URL Filter Settings

5.4.6.2. Web Host Filter Settings

The Web Host Filter option allows you to set up a list of keywords you would like to deny through your network. Please enter a Host (keyword) for filtering.

Content Filter Settings			
	Webs URL Filter Settings	Webs Host Filter Settings	
	Current Website Host	Filters Host (Keyword)	
		Delete Reset	
	Add a Host (ke	eyword) Filter	
		Add Reset	

Figure 5-49 Webs Host Filter Settings

5.5 Network Settings

5.5.1 WAN

There are 5 submenus under the Network menu: WAN, LAN, VLAN, Advanced Routing and IPv6. Click any of them, and you will be able to configure the corresponding function.

Network Settings	
WAN	վեր
LAN	
VLAN	
Advanced Routing	
IPv6	

WAN Connection Types:

Cable/Dynamic IP (DHCP) 🔽
Static (Fixed IP)
Cable/Dynamic IP (DHCP)
PPPoE (ADSL)
IPSEC
PPTP
L2TP

5.5.1.1. Static (Fixed IP)

If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static (Fixed IP)**. The Static IP settings page will appear as the figure is shown below.

Wide Area Network (WAN) Settings	
WAN Connections	Static (Fixed IP)
Static Mode	
IP Address	210.66.155.70
Subnet Mask	255.255.255.0
Default Gateway	210.66.155.94
DNS Settings	
Primary DNS Server 8.8.8.8	Secondary DNS Server 168.95.1.1
Apply Cano	cel

Figure 5-50 WAN - Static IP

Object	Description	
WAN Connections	Select Static (Fixed IP) from the list.	
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.	
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0	
Default Gateway	(Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.	

Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation
	provided by your ISP.
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal
	notation provided by your ISP.

5.5.1.2. Cable/Dynamic IP (DHCP)

If your ISP provides the DHCP service, please choose **Cable/Dynamic IP (DHCP)** type, and the AP Router will automatically obtain IP parameters from your ISP. You can see the page as shown below.

Wide Area Network (WAN) Settings			
		WAN Connections Cable/Dynamic IP (DHCP)	
DHCP Mode			
		Hostname planet	
		house	
DNS Settings (Optional)			
Primary DNS Ser	ver 8.8.8.8	Secondary Di	IS Server 168.95.1.1
		Apply Cancel	
Internet Configuration		<u> </u>	
Connected Type	DHCP	Connected Status	Connected
WAN IP Address	192.168.2.150	Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1	Primary Domain Name Server	8.8.8
Secondary Domain Name Server	168.95.1.1	MAC Address	00:30:4F:60:37:91
LAN Configuration			
LAN IP Address	192.168.1.1	LAN Netmask	255.255.255.0
MAC Address	00:30:4F:60:37:90		
System Info			
Firmware Version	V2.6 2012-10-23-15:12	System Time	Sun, 01 Jan 2012 12:03:11
Operation Mode	AP Router mode	Wireless MAC Address	00:30:4F:60:37:92

Figure 5-51 WAN - Dynamic IP

Object	Description	
WAN Connections	Select Cable/Dynamic IP (DHCP) from the list.	
Host Name	This option specifies the Host Name of the AP Router.	
Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation	
	provided by your ISP.	
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal	
	notation provided by your ISP.	

5.5.1.3. PPPoE (ADSL)

If local ISP provides a PPPoE connection, choose PPPoE (ADSL) and fill the necessary parameters below.

Wide Area Network (WAN) Settings	
WAN Co	onnections PPPoE (ADSL)
PPPoE Mode	
User Name pppoe_user	
Password	Verify Password
Operation Mode Keep Alive 💌	Keep Alive Mode: Redial Period 60 Seconds
MTU 1492 bytes (Default=1492)	
DNS Settings (Optional)	
Primary DNS Server 8.8.8.8	Secondary DHS Server 168.95.1.1
A	Apply Cancel

Figure 5-52 WAN - PPPoE

The page includes the following fields:

Object	Description	
WAN Connections	Select PPPoE (ADSL) from the list.	
Host Name	This option specifies the Host Name of the AP Router.	
User Name / Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.	
Verify Password	Enter the same password entered above for the confirmation.	
Operation Mode	Keep Alive: Being constantly connected.	
Keep Alive Mode	Set up the redial period after the disconnection. The default setting is " 60 seconds ".	
• MTU	Please input the MTU value of your network connection here. If you don't know, please keep the default value.	
Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.	
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.	

5.5.1.4. IPSEC

If your ISP provides IPSEC connection, please select IPSEC. And enter the following parameters.

Wide Area Network (WAN) Settings			
	WAN Connections	EC 💌	
DNS Settings (Optional)			
Primary DNS Server 8.8.8.	8	Secondary DNS Server	168.95.1.1
	Apply Cancel		
wan ipsec mode			
Connection addrress family IPv4	<u>×</u>	IPSec Operation Mode	add 🔽
IPSec Connection Type Road	Warrior Tunnel 💽	PFS DH Group	modp1024 💌
IPSec Authentication SHA-	1 🔽	IPSec Encryption	AES 💌
SA connection Life Time	hours	IKE Key Tries	3 times
Local IP Address		Peer IP Address	
Local Subnet		Peer Subnet	
Local Gateway		Peer Gateway	
IPSec Tunnel Name	NNC	IPSec Secret Key	PSK 💌
IPSec Key Life time 12h	hours		
NAT Transversal		Perfect Forward Secrets	
IPSec Compression		IPSec Conn. Keep Alive	
	IPSec Tunnel UP		

Figure 5-53 WAN - IPSec

wan ipsec mode			L			
Connection addrress family	IPv4 💌	IPSe	ec Operation Mode	add 🛛 💌		
IPSec Connection Type	Road Warrior Tunnel 🛛 💌		PFS DH Group	modp1024 🔽		
IPSec Authentication	Road Warrior Tunnel		IPSec Encryption	AES 💌		
SA connection Life Time	Subnet to Subnet Tunnel		IKE Key Tries	3	times	
Local IP Address	Host to Host Transport Passthrugh		Peer IP Address			
Local Subnet	Drop		Peer Subnet			
Local Gateway	Reject		Peer Gateway			
IPSec Tunnel Name	accCONN		IPSec Secret Key	PSK 🔽		
IPSec Key Life time	12h hours					
NAT Transversal		Perfec	t Forward Secrets			
IPSec Compression		IPSec	c Conn. Keep Alive			
	IPSec Tu	Innel UP UP				

Figure 5-54 WAN – IPv4 (IPSec Connection Type)

Object	Description
WAN Connections	Select IPSEC from the list.
Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation provided
	by your ISP.
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal notation
	provided by your ISP.

Connection address	For an IPSec connectior	n, all host addresses must be	e of the same
family	Address Family (IPv4 and IPv6 use different Address Families).		
IPSec Operation Mode	Select the IPSec Operation mode from the drop-down list.		
	This field allows you to set Select Tunnel to specify Warrior) , or Subnet to Su connection type.	the connection type to any of the connection type to any of the any the an	he following: Subnet (Road e most common
• IPSec Connection Type	Select Transport to specif connection type is much le if you are attempting to es which specifically requires	y a Host to Host Transport mo ess common, and would genera stablish and IPSec connection this mode.	ode tunnel. This Ily only be used to another host
	Select Passthrough to disable IPSec processing on packets associated with the tunnel. We can't imagine a scenario where you would use this connection type. I mean seriously, if you don't allow IPSec to process the packets then you don't really have a tunnel, right? Still, the underlying protocol supports this mode, and so here we are.		
	Select Drop to cause the the tunnel. Select Reject to cause the	kernel to drop IPSec packets	associated with associated with
	the tunnel.		
• PFS DH Group	Perfect Forward Secrecy (PFS)—PFS ensures that a given IPSec SA key was not derived from any other secret, like some other keys. In other words, if someone breaks a key, PFS ensures that the attacker is not able to derive any other key. If PFS is not enabled, someone can potentially break the IKE SA secret key, copy all the IPSec protected data, and then use knowledge of the IKE SA secret in order to compromise the IPSec SAs setup by this IKE SA. With PFS, breaking IKE does not give an attacker immediate access to IPSec. The attacker needs to break each IPSec SA individually. Diffie-Hellman (DH) key exchange protocol allows two parties without any initial shared secret to create one securely. The following Modular Exponential (MODP) and Elliptic Curve (EC2N) Diffie-Hellman (also known as "Oakley") Groups are supported: Diffie-Hellman Group Name		
	Group 1	768 bit MODP group	RFC 2409

	Group 2	1024 bits MODP group	RFC 2409	
	Group 3	EC2N group on GP(2^155)	RFC 2409	
	Group 4	EC2N group on GP(2^185)	RFC 2409	
	Group 5	1536 bits MODP group	RFC 3526	
IPSec Authentication	The AP supports SHA1 &	MD5 authentication algorithms		
	The AP supports DES ,	3DES, AES, Blowfish, Two	ofish, Camellia	
	Encryption methods.			
	DES - 56-bit DES-CBC er	cryption algorithm		
	3DES - 168-bit DES encry	ption algorithm		
IPSec Encryption	AES - 128, 192 and 256-b	it key AES-CBC encryption al	gorithm	
	Blowfish - a symmetric	block cipher that can be use	ed as a drop-in	
	replacement for DES or ID	EA. It takes a variable-length	key, from 32 bits	
	to 448 bits.			
	Twofish - Twofish has a 12	28-bit block size, a key size ran	ging from 128 to	
	256 bits, and is optimized	for 32-bit CPUs.		
	Camellia - 128, 192 and 256-bit key Camellia encryption algorithm			
SA connection Life	This value describes the timeframe in hours for which the IKE SA is valid			
Time	and when the next rekeyin	g should take place.		
IKE Key Tries	The field is used to specify the retry times of IKE Key.			
	This field is used to configure the IP address of the Untangle server on			
	the network configured in the Local Network field.			
Peer IP Address	This field should contain the public IP address of the host to which the			
	IPSec VPN will be connected.			
Local Subnet	This field is used to confi	gure the local network that w	ill be reachable	
	from hosts on the other side of the IPSec VPN.			
Peer Subnet	This field is used to configure the remote network that will be reachable			
	from hosts on the local side of the IPSec VPN.			
Local Gateway	This field is used to configure the Gateway of the Untangle server on the			
	network configured in the Local Network field.			
Peer Gateway	This field should contain the public Gateway of the host to which the			
	IPSec VPN will be connec	ted.		
IPSec Tunnel Name	This field should contain a	short name or description.		
	This field should contain th	ne shared secret or PSK (pre-s	shared key) that	
	is used to authenticate the connection, and must be the same on both			
IPSec Secret Key	sides of the tunnel for the connection to be successful. Because the PSK			
	is actually used as the encryption key for the session, using long strings			
	of a random nature will provide the highest level of security.			

	Lifetime settings determine when a new key is generated. Any time a key
	lifetime is reached, the associated SA is also renegotiated. The process
	of generating new keys at intervals is called dynamic rekeying or key
IPSec Key Life time	regeneration. Lifetimes allow you to force the generation of a new key
	after a specific interval. For example, if the communication takes 12
	hours and you specify the key lifetime as 1 hour, 12 keys will be
	generated (one every 1 hour) during the exchange.
	NAT Traversal also known as UDP encapsulation allows traffic to get to
NAT Traversal	the specified destination when a device does not have a public address.
	This is usually the case if your ISP is doing NAT, or the external interface
	of your firewall is connected to a device that has NAT enabled.
Perfect Forward Secrets	Select the checkbox to enable PFS (Perfect Forward Secrets).
IPSec Compression	Select the checkbox to enable compression of content on the connection.
	When the firewall is located behind a NAT device, it sends keep alive
IPSec Conn. Keep	packets to maintain the connection. You can also force it to send keep
	alive packets for all NAT-T connections.
IPSec Tunnel UP	This field indicates the IPSec Tunnel is UP and running.

5.5.1.5. PPTP

If your ISP provides PPTP connection, please select **PPTP**. And enter the following parameters.

Wide Area Network (WAN) Settings			
	WAN Connections	PPTP	*
PPTP Mode			
Server IP pptp_server			
User Name pptp_user		I	Password ••••••••
Address Mode Static IP 💌			
IP Address			
Subnet Mask			
Operation Mode Keep Alive 💌			Keep Alive Mode: Redial Period 60
DNS Settings (Optional)			
Primary DNS Server 8.8.8.8		Secondary	DNS Server 168.95.1.1
	Apply Canc	el	

Figure 5-55 WAN – PPTP

Object	Description
WAN Connections	Select PPTP from the list.
Server IP	Enter the IP address of the PPTP server.
User Name / Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Address Mode	Static IP/ Dynamic IP : Choose either as you are given by your ISP and If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the Save button.
IP Address	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Operation Mode	Keep Alive: Being constantly connected.
Keep Alive Mode	Set up the redial period after the disconnection. The default setting is " 60 seconds ".
Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

5.5.1.6. L2TP

If your ISP provides L2TP connection, please select L2TP and enter the following parameters.

Wide Area Network (WAN) Settings		
	WAN Connections L2TP	~
L2TP Mode		
Server IP I2tp_server		
User Name <mark>I2tp_user</mark>		Password
Address Mode Static IP 💉		
IP Address		
Subnet Mask		
Operation Mode Keep Alive 💌		Keep Alive Mode: Redial Period 60
DNS Settings (Optional)		
Primary DNS Server 8.8.8.8		Secondary DNS Server 168.95.1.1
	Apply Cancel	

Figure 5-56 WAN – L2TP

Object	Description
WAN Connections	Select L2TP from the list.
Server IP	Enter the IP address of the L2TP server.
User Name / Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Address Mode	Static IP/ Dynamic IP : Choose either as you are given by your ISP and If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the Save button.
IP Address	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Operation Mode	Keep Alive: Being constantly connected.
Keep Alive Mode	Set up the redial period after the disconnection. The default setting is " 60 seconds ".
Primary DNS Server	(Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
Secondary DNS Server	(Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

5.5.2 LAN

Net	work Settings					
	WAN					
	LAN	ζ ^h η				
	VLAN					
Ad	vanced Routing					
	IPv6					
LAN Setup						
			MAC Address	00:30:4F:60:37:90		
			IP Address	192.168.1.1		
			Subnet Mask	255.255.255.0		



	Object	Description
--	--------	-------------

MAC Address	Display the LAN port MAC address of the Wireless AP.
	The Wireless AP's LAN IP.
• IF Address	The default is 192.168.1.1 . You can change it according to your need.
Subnet Mask	Enter the subnet mask of the LAN IP.

5.5.2.1. DHCP Server

DHCP Setup	
DHCP Server	DHCP Server
Local Domain Name (Optional)	
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Lease Time	One day 💌
Apply	Cancel

Figure 5-58 DHCP Server

The page includes the following fields:

Object	Description
DHCP Server	Select DHCP Server to enable DHCP server feature.
Local Domain Name (Optional)	(Optional) Input the domain name of your network.
Start IP Address	Enter the starting IP address for the DHCP server's IP assignment.
End IP Address	Enter the ending IP address for the DHCP server's IP assignment.
	The length of time for the IP address lease. Configuring a proper
Lease Time	lease time improves the efficiency for the DHCP server to reclaim
	disused IP addresses.

To benefit from the DHCP server feature, you must set all LAN PCs to DHCP clients by selecting the "Obtain an IP Address Automatically" radio buttons thereon.

5.5.2.2. DHCP Relay

DHCP Setup	
DHCP Server	DHCP Relay 💙
DHCP Relay	192.168.23.168
Apply	Cancel

Figure 5-59 DHCP Relay

Object	Description		
DHCP Server	Select DHCP Relay to enable DHCP relay feature.		
	A DHCP relay agent is any host that forwards DHCP packets		
DHCP Relay	between clients and servers.		
	Configure the IP address of DHCP Relay host.		

5.5.3 VLAN



Figure 5-60 VLAN

Object	Description
VLAN Setup	Check this box to enable the VLAN function.
Management VLAN ID	Configure a specified VLAN to be the management VLAN.
Enable Management VLAN ID	Check this box to enable the Management VLAN function.
-------------------------------	--
• VLAN ID	The ID of a VLAN. Only in the same VLAN can a wireless PC and a
	wired PC communicate with each other. The value can be between 1
	and 4095. If the VLAN function is enabled, when AP forwards
	packets, the packets out from the LAN port will be added with an
	IEEE 802.1Q VLAN Tag, whose VLAN ID is just the ID of the VLAN
	where the sender belongs.

5.5.4 Advanced Routing

-

	Network Set	tings							
	WAN								
	LAN								
	VLAN								
	Advanced Ro	uting 🖓							
	IPv6								
Advan	red Routing Settings								
	ou nouting octaings								
Add a i	routing rule								
			Destination						
			Туре	Host 💌					
			Gateway						
			Interface	LAN 🔽					
			Comment						
			Apply	Reset					
			Арріу	Reser					
Curren	nt Routing table in the sys	stem							
No.	Destination	Netmask	Gatew	ay Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.	0.0 5	0	0	0	LAN(br0)	
2	210.66.155.0	255.255.255.0	0.0.	0.0 1	0		0	eth0(eth0)	
	192.168.1.0	255.255.255.0	0.0.	0.0 1	0		0	LAN(br0)	
4	0.0.0.0	0.0.0.0	210.66.155	.94 3	0		0	eth0(eth0)	
			Delete	Reset					
Dynam	ic Routing Protocol								
			RIP	Disable 💌					
			Apply	Reset					

Figure 5-61 Advanced Routing

The page includes the following fields:

Object	Description
Destination	The IP address of packets that can be routed.
• Туре	Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)
Gateway	Defines the packets destination next hop
Interface	Select interface to which a static routing subnet is to be applied
Comment	Help identify the routing
Dynamic Routing Protocol	Enable or disable the RIP (Routing Information Protocol) for the WAN or LAN interface. It supports RIP v1 and v2.

5.5.5 IPv6

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.



IPv6 Connection Mode	
IPv6 Connection	DHCPv6
DNS Address Server Setting	
IPv6 Primary DNS	
IPv6 Secondary DNS	
Prefix Delegation Setting	
Enable DHCP-PD	
SLD ID	0
SLA Length	16
Lan IPv6 Address Setting	
Lan IPv6 Address	2001:db8:1:2::1 / 64
Lan IPv6 Link-Local Address	/64
Lan Address Autoconfiguration	
IPv6 Autoconfiguration	Stateless(RADVD) 💌
IPv6 Address Lifetime	1800
Apply	Cancel

Figure 5-62 IPv6

The page includes the following fields:

Object	Description
	Choose the mode to be used by the AP/Router to the IPv6 Internet.
. IPv6 Connection Mode	There are 7 connection modes available:
IPv6 Connection Mode	Static, SLAAC, DHCPv6, 6to4 Tunnel, 6in4 Tunnel, PPPoE, and
	Pass Through.
DNS Address Server Setting	Enter the IPv6 Primary DNS & IPv6 Secondary DNS to this section.
Prefix Delegation	Enter the IPv6 Prefix Delegation information provided by your
Setting	Internet Service Provider (ISP).
	Use this section to configure the internal network settings of your
LAN IPv6 Address	AP/Router. If you change the LAN IPv6 Address here, you may need
Oetting	to adjust your PC network settings to access the network again.
	IPv6 offers two types of autoconfiguration: Stateful (DHCPv6) &
	Stateless (RADVD).
	Stateful (DHCPv6):
	This type of configuration is suitable for small organizations and
	individuals. It allows each host to determine its address from the
LAN Address Auto configuration	contents of received user advertisements. It makes use of the IEEE
comguration	EUI-64 standard to define the network ID portion of the address.
	Stateless(RADVD):
	With Stateless Autoconfiguration, a host gains an address via an
	interface automatically "leasing" an address and does not require the
	establishment of a server to delve out address space.

5.6 Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

5.6.1 Basic





5.6.1.1. Wireless Mode – Access Point

Figure 5-63 Wireless Mode - AP

Object	Description
	Click to select Wireless Mode from pull down menu.
	There are 4 options available:
	Access Point:
	This mode allows wireless clients or Stations(STA) to access
	WDS Access Point:
	This mode enables the wireless interconnection of Access Point in an
Wireless Mode	IEEE802.11 network .and accept wireless clients at the same time.
	■ WDS Repeater:
	Set to this mode to enable the wireless access point repeat the signal
	of root access point using WDS.
	WDS Client:
	Set to this mode to enable wireless client using WDS to connect to
	the WDS Access Point.
Multiple SSID	There is one more SSID available. Select the checkbox to enable it,

	enter the descriptive names that you want to use.
Country Code	Set your country code by clicking the "Set Country Code".
• Frequency (Channel)	Set the channel you would like to use. The channel range will be changed by selecting different domain.
Site Survey	Click "Site Survey" button to observe the signal of remote sites.
Network Mode	Select the operating channel width to WiFi 11gn (mixed), HT20 or HT40MHz.
Extension Channel	An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz. Bonded channels allow for greater bandwidth on the local network.
Distance	To decrease the chances of data retransmission at long distance, the IEEE 802.11b/g/n Wireless Outdoor CPE can automatically adjust proper ACK timeout value by specifying distance of the two nodes.
ACK/CTS Timeout	ACK/CTS Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement. The device's default settings should be sufficient for most applications. The value is auto determined by distance between the radios, data rate of average environment.
Network Name (SSID)	It is the wireless network name. The SSID can be 32 bytes long. User can use the default SSID or change it. The default SSID is WNAP-6308 .
WPS Choice	Enable it to use WPS associating with AP or Client device.
Encryption Settings	Select the encryption type that you would like to use.
WPA Algorithms	Select the WPA Algorithms that you would like to use.
Key Renewal Interval (Seconds)	The key renewal time is the period of time that the AP uses the same key before a new one is generated.
Pre-Shared Key	Data encryption and key are required for wireless authentication.





Figure 5-64 Wireless Mode - WDS AP

Object	Description
	Click to select Wireless Mode from pull down menu.
	There are 4 options available:
	Access Point:
	This mode allows wireless clients or Stations(STA) to access
	WDS Access Point:
	This mode enables the wireless interconnection of Access Point in an
Wireless Mode	IEEE802.11 network .and accept wireless clients at the same time.
	WDS Repeater:
	Set to this mode to enable the wireless access point repeat the signal
	of root access point using WDS.
	WDS Client:
	Set to this mode to enable wireless client using WDS to connect to
	the WDS Access Point.
Country Code	Set your country code by clicking the "Set Country Code".
	Set the channel you would like to use. The channel range will be
• Frequency (Channel)	changed by selecting different domain.

Site Survey	Click "Site Survey" button to observe the signal of remote sites.		
Network Mode	Select the operating channel width to WiFi 11gn (mixed), HT20 or		
	HT40MHz.		
	An extension channel is a secondary channel used to bond with the		
Extension Channel	primary channel to increase this range to 40MHz. Bonded channels		
	allow for greater bandwidth on the local network.		
	To decrease the chances of data retransmission at long distance, the		
Distance	IEEE 802.11b/g/n Wireless Outdoor CPE can automatically adjust		
	proper ACK timeout value by specifying distance of the two nodes.		
	ACK/CTS Timeout settings are for long distance links. It is important		
	to tweak settings to achieve the optimal result based on requirement.		
ACK/CTS Timeout	The device's default settings should be sufficient for most		
• ACK/CTS Timeout	applications.		
	The value is auto determined by distance between the radios, data		
	rate of average environment.		
	It is the wireless network name. The SSID can be 32 bytes long.		
Network Name (SSID)	User can use the default SSID or change it.		
	The default SSID is WNAP-6308 .		
Encryption Settings	Select the encryption type that you would like to use.		
WPA Algorithms	Select the WPA Algorithms that you would like to use.		
Key Renewal Interval	The key renewal time is the period of time that the AP uses the same		
(Seconds)	key before a new one is generated.		
Pre-Shared Key	Data encryption and key are required for wireless authentication.		



Basic Wireless Settings			
	Wireless Mode	WDS Repeater	
Ro	ot AP MAC Address (optional)		
	Country Code:	United Kingdom Set Country Code	
	Frequency (Channel)	2412 MHz (Channel 1) 💌	
	Site Survey	Site Survey	
	Network Mode	WiFi 11gn HT40 🔽	
	Extension Channel	Upper Channel 💌	
	Distance	0.6	miles (1.0 km)
	ACK/CTS Timeout	41	
SSID I Security Settings		SSID II Security Settings	
Network Name (SSID) WNAP-63	308 🗖 Hide	Root AP S	SID Hide
		Encryption Settin	gs Disable 💌
Encryption Settings WPA2-PS	SK 🔽		
WPA Algorithms 🛛 TKIP 🛛	🛛 오 CCMP(AES) 🔍 Auto		
Key Renewal Interval(Secconds) 60			
Pre-Shared Key 12345678	Generator		
	Apply	ancel	

Figure 5-65 Wireless Mode – WDS Repeater

Object	Description
	Click to select Wireless Mode from pull down menu.
	There are 4 options available:
	Access Point:
	This mode allows wireless clients or Stations(STA) to access
	WDS Access Point:
	This mode enables the wireless interconnection of Access Point in an
Wireless Mode	IEEE802.11 network .and accept wireless clients at the same time.
	WDS Repeater:
	Set to this mode to enable the wireless access point repeat the signal
	of root access point using WDS.
	WDS Client:
	Set to this mode to enable wireless client using WDS to connect to
	the WDS Access Point.
Root AP MAC Address	Fill out the Root AP's MAC Address enable it to connect to the Root
(optional)	AP using WDS.
Country Code	Set your country code by clicking the "Set Country Code".

• Frequency (Channel)	requency (Channel)	
- Sito Survov	Click "Site Survey" button to observe the signal of remote sites	
	Click Site Survey button to observe the signal of remote sites.	
Network Mode	Select the operating channel width to WiFi 11gn (mixed), HT20 or HT40MHz.	
	An extension channel is a secondary channel used to bond with the	
Extension Channel	primary channel to increase this range to 40MHz. Bonded channels	
	allow for greater bandwidth on the local network.	
	To decrease the chances of data retransmission at long distance, the	
Distance	IEEE 802.11b/g/n Wireless Outdoor CPE can automatically adjust	
	proper ACK timeout value by specifying distance of the two nodes.	
	ACK/CTS Timeout settings are for long distance links. It is important	
	to tweak settings to achieve the optimal result based on requirement.	
	The device's default settings should be sufficient for most	
ACK/CTS Timeout	applications.	
	The value is auto determined by distance between the radios, data	
	rate of average environment.	
	It is the wireless network name of itself. The SSID can be 32 bytes	
Notwork Name (CCID)	long.	
• Network Name (SSID)	User can use the default SSID or change it.	
	The default SSID is WNAP-6308 .	
	It is the wireless network name of Root AP.	
Root AP SSID	The SSID must be the same with Root AP so that the connection can	
	be established successfully.	
Encryption Settings	Select the encryption type that you would like to use.	
WPA Algorithms	Select the WPA Algorithms that you would like to use.	
Key Renewal Interval	The key renewal time is the period of time that the AP uses the same	
(Seconds)	key before a new one is generated.	
Pre-Shared Key	Data encryption and key are required for wireless authentication.	

5.6.1.4. Wireless Mode – WDS Client



Figure 5-66 Wireless Mode - WDS Client

Object	Description	
	Click to select Wireless Mode from pull down menu.	
	There are 4 options available:	
	Access Point:	
	This mode allows wireless clients or Stations(STA) to access	
	WDS Access Point:	
	This mode enables the wireless interconnection of Access Point in an	
Wireless Mode	IEEE802.11 network .and accept wireless clients at the same time.	
	WDS Repeater:	
	Set to this mode to enable the wireless access point repeat the signal	
	of root access point using WDS.	
	WDS Client:	
	Set to this mode to enable wireless client using WDS to connect to	
	the WDS Access Point.	
Root AP MAC Address (optional)	Fill out the Root AP's MAC Address enable it to connect to the Root	
	AP using WDS.	
Country Code	Set your country code by clicking the "Set Country Code".	

- Fragueney (Channel)	Set the channel you would like to use. The channel range will be		
• Frequency (Channel)	changed by selecting different domain.		
No formalis Billio al s	Select the operating channel width to WiFi 11gn (mixed), HT20 or		
Network Mode	HT40MHz.		
	An extension channel is a secondary channel used to bond with the		
Extension Channel	primary channel to increase this range to 40MHz. Bonded channels		
	allow for greater bandwidth on the local network.		
	To decrease the chances of data retransmission at long distance, the		
Distance	IEEE 802.11b/g/n Wireless Outdoor CPE can automatically adjust		
	proper ACK timeout value by specifying distance of the two nodes.		
	ACK/CTS Timeout settings are for long distance links. It is important		
	to tweak settings to achieve the optimal result based on requirement.		
	The device's default settings should be sufficient for most		
ACK/CTS Timeout	applications.		
	The value is auto determined by distance between the radios, data		
	rate of average environment.		
	It is the wireless network name of Root AP.		
	The SSID must be the same with Root AP so that the connection can		
ROOT AP SSID	be established successfully.		
	Click " Scan " to site survey the Root AP.		
Encryption Settings	Select the encryption type that you would like to use.		
WPA Algorithms	Select the WPA Algorithms that you would like to use.		
Key Renewal Interval	The key renewal time is the period of time that the AP uses the same		
(Seconds)	key before a new one is generated.		
Pre-Shared Key	Data encryption and key are required for wireless authentication.		

-

5.6.2 Profile Settings

In **Client Bridge** and **Client Router** operation modes, please go to "Advanced-> Wireless Settings-> Profile Settings" to configure the wireless client function to connect with the wireless AP.

Wireless Settings	
Profile Settings	

Curren	tly Used Profile					
Profile	e List					
Select	Profile	SSID	BSSID	Authentication	Encryption	Network Type
	WNAP-6308	WNAP-6308	00:30:4F:60:AF:7A	WPA2-Personal	ССМР	Infrastructure
Profile	Setup					
	Profile Na	me		Network T	ype Infrastructure	Site Survey
	s	SID		BSSID(optio	nal)	
	Encryption Settings Disabled					
Ack Tir	Ack Timeout Settings					
	Distar	nce	0.6 mil	es (1.0 km)		
	ACK/CTS Time	out <mark>41</mark>				
	RT S/C	ITS 🔲 📃	Bytes			
Fra	gmentation Thresh	old 🔲 📰 E	lytes			
	Activate Add Delete					

Figure 5-67 Client Bridge – Profile Settings

Object	Description	
Profile Name	Fill out the Root AP's MAC Address enabling it to connect to the Root	
	AP using WDS.	
	Set the Network Type that you would like to use.	
	Infrastructure:	
	Infrastructure networks consist of the networked devices and the	
	wireless access point or wireless router. Each device must connect to	
Network Type	the access point before having access to other computers on the	
	network.	
	Ad-hoc:	
	In an ad hoc network, each device's network adapter directly	
	communicates with other devices.	

• SSID	It is the wireless network name of Root AP.		
BSSID (optional)	Indicate the Basic Service Set ID of the associated AP		
Encryption Settings	Select the encryption type that you would like to use.		
Distance	To decrease the chances of data retransmission at long distance, the IEEE 802.11b/g/n Wireless Outdoor CPE can automatically adjust proper ACK timeout value by specifying distance of the two nodes.		
ACK/CTS Timeout	 ACK/CTS Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement. The device's default settings should be sufficient for most applications. The value is auto determined by distance between the radios, data rate of average environment. 		
RTS/CTS (Request to Send / Clear to Send) is the option mechanism used by the 802.11 wireless networking protoco reduce frame collisions introduced by the hidden node problem. You can enter a setting ranging from 0 to 2347 bytes.			
 Fragmentation Threshold The fragmentation threshold determines the size at which pack are fragmented (sent as several pieces instead of as one block). U a low setting in areas where communication is poor or where there			
WDS Client	Check it to enable WDS Client function.		

5.6.3 Advanced

Wireless Settings	
Basic	
Advanced	շ(հոյ
Access Control	

Turn Off
00:30:4F:66:E6:8A
Enable Disable
🗢 Enable 🕒 Disable
100 ms
1
Bytes
Bytes
127
Disable
LED1:-94 LED2:-80 LED3:-73 LED4:-65

Figure 5-68 Wireless Settings – Advanced

Object	Description		
Wireless On/Off	Click this button to switch the Wireless Radio On or Off.		
AP MAC Address	Display the AP MAC Address of wireless interface.		
Packet Aggregate	In a packet-based communications network, packet aggregation is the process of joining multiple packets together into a single transmission unit, in order to reduce the overhead associated with each transmission.		
• WMM	WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.		
• TX Power	You can limit the Transmit Power of the Device through this field. The default value is 23dBm, and the minimum TX Power is 3dBm.		
Beacon Interval	The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time		

	interval of the beacons. You can specify a value between 20-1000		
	milliseconds. The default value is 100 .		
• DTIM	This value determines the interval of the Delivery Traffic Indication		
	Message (DTIM). You can specify the value between 1-255		
	Beacon Intervals. The default value is 1, which indicates the DTIM		
	Interval is the same as Beacon Interval.		
	The RTS/CTS mechanism is widely used in wireless networks in		
• RTS/CTS	order to avoid packet collisions and, thus, achieve high		
	throughput.		
	This value is the maximum size determining whether packets will		
- Exampletion Threshold	be fragmented. Setting the Fragmentation Threshold too low may		
• Fragmentation Threshold	result in poor network performance since excessive packets. 2346		
	is the default setting and is recommended.		
• Station Control (SSID I)	Fill out the Station Control value of SSID I.		
Station Control (SSID II)	Fill out the Station Control value of SSID II.		
	Isolate all connected wireless stations so that wireless stations		
Wireless Isolate	cannot access each other through WLAN. This function will be		
	disabled if WDS/Bridge is enabled.		
	Set the AP to the external LED lights and wireless signal strength		
• Thresholds, dbm	received correspondence, when the AP receives the wireless		
	signal, according to the wireless signal strength, the		
	corresponding LED will be lit.		

5.6.4 Access Control

Choose menu "Advanced-> Wireless Settings-> Access Control" to configure the filtering rules for the clients who would like to associate with Wireless AP.



Basic Settings		
		SSID WNAP-6308 💌
	Acces	ss Control Mode Allow Listed 💌
		Apply Reset
Wireless Acce	ss Control	
		MAC Address 00:30:4F:11:22:33
		(content filter message 32.)
		Apply Reset
Current Acces	s Control List	
No.	Action	MAC Address
1	ALLOW	/ 00:30:4F:11:22:33
		Delete Reset

Figure 5-69 Wireless Settings – Access Control

The page includes the following fields:

Object	Description
• SSID	Select the SSID which you would like to configure access
	control.
Access Control Mode	Allow Listed: allow the packets not specified by any access
	control policy to pass through the AP Router.
	Deny Listed: deny the packets not specified by any access
	control policy to pass through the AP Router.
MAC Address Configure the MAC Address to apply the access contro	
Current Access	Display the current Access Control List
Control List	Display the current Access Control List.

5.7 Logout

Select "Logout", and then click "Yes" to logout the system.

PLANET Networking & Communication	Logout WNAP-6308 802.11b/g/n Wireless Outdoor Access Point
Logout	Do you want to logout? Yes

Figure 5-70 Logout

Chapter 6. Quick Connection to a Wireless Network

6.1 Windows XP (Wireless Zero Configuration)

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





Step 2: Select [View Available Wireless Networks]



Figure 6-2 View Available Wireless Networks

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

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



Figure 6-3 Choose a wireless network

Step 4: Enter the encryption key of the Wireless AP

- (1) The Wireless Network Connection box will appear
- (2) Enter the encryption key that is configured in Section 5.6.2
- (3) Click the [Connect] button

Wireless Network Connection						
The network 'PLANET' 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.						
rype are rey, and aren clerk						
Network <u>k</u> ey:	•••••					
C <u>o</u> nfirm network key:	Confirm network key:					
	Cancel					

Figure 6-4 Enter the encryption key

Step 5: Check if "Connected" is displayed



Figure 6-5 Wireless Network Connected



Some laptops are equipped with a "Wireless ON/OFF" switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to "ON" position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that 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 2: Highlight and select the wireless network (SSID) to connect

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

Not connected	47	-
Connections are available		ш
Dial-up and VPN	^	
Office VPN	×	
Wireless Network	^	
	lite	
	Itee	
PLANET	lte.	
Connect automatically	<u>Connect</u>	
aiiiyo .	lte.	
	(B_a)	-

Figure 6-7 WLAN AutoConfig window



Step 4: Enter the encryption key of the Wireless AP

- (1) The Connect to a Network box will appear
- (2) Enter the encryption key that is configured in Section 5.6.2
- (3) Click the [OK] button

😰 Connect to a Network	X
Type the network see	curity key
Security key:	
	Hide characters
You o butto	an also connect by pushing the n on the router.
	OK Cancel

Figure 6-8 WLAN AutoConfig - type the network security key

Connect to a Network	X
Getting information from PLANET	
	Cancel

Figure 6-9 WLAN AutoConfig - connecting

Step 5: Check if "Connected" is displayed

Currently connected to: PLANET Internet access	43	11 ×
Dial-up and VPN	^	
Office VPN		
Wireless Network	^	
PLANET	Connected	
<u> </u>		
		-
Open Network and	I Sharing Center	

Figure 6-10 WLAN AutoConfig - Connected

6.3 Mac OS X 10.x





Figure 6-11 The AirPort Network Connection icon

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

- (1) Select and SSID [PLANET]
- (2) Double-click on the selected SSID



Figure 6-12 The AirPort Network Connection menu

Step 4: Enter the encryption key of the Wireless AP

- (1) Enter the encryption key that is configured in Section 5.6.2
- (2) Click the [OK] button

1	The network "PLANET" requires a WPA password
	Password:
	Show password
	Remember this network
	Cancel OK

Figure 6-13 The AirPort Network Connection - enter password



If you will connect this Wireless AP in the future, check [Remember this network].

Step 5: Check if the AirPort is connected to the selected wireless network.If "Yes", then there will be a "check" symbol in the front of the SSID.



Figure 6-14 The AirPort Network Connection - connected

6.4 iPhone / iPod Touch / iPad

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



Figure 6-15 The Wi-Fi Settings in iPhone/iPod Touch/iPad

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

- (1) Tap [General] \ [Network]
- (2) Tap [Wi-Fi]

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

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

Figure 6-16 General Settings

iPad	10:35 AM 🕒 100% 📼
Settings	General Network
Airplane Mode OFF	
S Wi-Fi Not Connected	VPN Not Connected >
Notifications On	Wi-Fi Not Connected >
Carrier	
🕅 Cellular Data	
🙀 Brightness & Wallpaper	
Picture Frame	
Seneral General	
Mail, Contacts, Calendars	
Mafari Safari	

Figure 6-17 General Settings – Not Connected

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

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

iPad	10:35 AM 🕒 100% 📟		
Settings	Wi-Fi Networks		
Airplane Mode OFF Wi-Fi Not Connected	Wi-Fi ON		
Notifications On	Choose a Network		
Carrier	PLANET 🔒 🗢 🧿		
🔀 Cellular Data	Other >		
🛃 Brightness & Wallpaper	Ask to Join Networks		
Picture Frame	Known networks will be joined automatically. If no known networks are available, you will be asked		
General	before joining a new network.		
Mail, Contacts, Calendars			

Figure 6-18 General Settings – Wi-Fi On

Step 4: Enter the encryption key of the Wireless AP

- (1) The password input screen will be displayed
- (2) Enter the encryption key that is configured in Section 5.6.2
- (3) Tap the [Join] button



Figure 6-19 General Settings – Enter password

Step 5: Check if the iDevice is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in the front of the SSID.

iPad 🤶	10:36 AM	@ 100%		
Settings	Network Wi-F	i Networks		
Mirplane Mode OFF Wi-Fi PLANET_WNRT-617	Wi-Fi			
Notifications On	Choose a Network			
Carrier	✓ PLANET	≙ 중 🧕		
Cellular Data	Other	>		
🙀 Brightness & Wallpaper	Ask to Join Network	s ON		
Picture Frame	Known networks will be joined automatically. If no			
General	before joining a new network.			
Mail, Contacts, Calendars				

Figure 6-20 General Settings - Wi-Fi Network Connected

Appendix A: Planet Smart Discovery Utility

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

The following installation instructions guide you to running the Smart Discovery Utility.

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

Step 2: Run this utility.



Step 3: Click "Refresh" button for current connected devices in the discovery list as shown in the following screen.

3	PLANET Smart	Discovery Lite	3						
Fi	e <u>O</u> ption <u>H</u> elp								
			Ú Ref	esh	🖹 Exit			9	PLANET Networking & Communication
Γ	MAC Address	Device Name	Version	DevicelP	NewPassword	IP Address	NetMask	Gateway	Description
1	00-30-4F-61-1A-58	WNAP-6308	V 3.0b	192.168.1.1		192.168.1.1	255.255.255.0	192.168.1.1	WNAP-6308
	Select Adapter : 192.168.1.11 (EC:A8:6B:D6:99:C4) Control Packet Force Broadcast Update D evice Update Multi Update All Connect to Device 								
De	vice : WNAP-6308	(00-30-4F-61-17	A-58) Ge	t Device Informat	tion done.				

Step 4: Navigate to the device, and then click **"Connect to Device"** button to connect to its Web configuration page.



1. Before connecting to device, please ensure your network adapter has been configured to the IP address in the same subnet.

2. The fields in white background can be modified directly, and then you can apply the new setting by clicking the "**Update Device**" button.

Appendix B: Troubleshooting

If you found the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the Planet Tech Support for help,. Some problems can be solved by yourself within very short time.

Scenario	Solution		
The AP is not responding to me when	a. Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be		
I want to access it by web blowser.	correctly and firmly inserted to the AP.		
	b. If all LEDs on this AP are off, please check the status of		
	power adapter, and make sure it is correctly powered.		
	c. You must use the same IP address section which AP		
	uses.		
	d. Are you using MAC or IP address filter? Try to connect		
	the AP by another computer and see if it works; if not,		
	please reset the AP to the factory default settings		
	(pressing 'reset' button for over 10 seconds).		
	e. Set your computer to static IP address, and see if the		
	Planet Smart Discovery can find the AP or not.		
	f. If you did a firmware upgrade and this happens, contact		
	the Planet Tech Support for help.		
	g. If all the solutions above don't work, contact the Planet		
	Tech Support for help.		
I can't get connected to the Internet.	a. Check the Internet connection status from the router that		
	connected with the AP.		
	b. Please be patient, sometimes Internet is just that slow.		
	c. If you connect a computer to Internet directly before, try		
	to do that again, and check if you can get connected to		
	Internet with your computer directly attached to the		
	device provided by your Internet service provider.		
	d. Check PPPOE / L2TP / PPTP user ID and password in		
	your router again.		
	e. Call your internet service provider and check if there's		
	f If you just cap't connect to one or more website, but you		
	can still use other internet services, please check		
	a Try to reset the AP and try again later		
	 Beset the device provided by your Internet service 		
	provider, too.		
	i. Try to use IP address instead of hostname. If you can		
	use IP address to communicate with a remote server.		
	but can't use hostname, please check DNS setting.		
I can't locate my AP by my wireless	a. 'Broadcast ESSID' set to off?		

device	b.	The antenna is properly secured.			
		Are you too far from your AP? Try to get closer			
	d.	Please remember that you have to input ESSID on your			
	u.	wireless client manually if ESSID breadcast is disabled			
File download is very slow or breaks	a.	Are you using QoS function? Try to disable it and try			
frequently.		again.			
		Internet is slow sometimes, being patient.			
	C.	Try to reset the AP and see if it's better after that.			
	d.	Try to know what computers do on your local network. If			
		someone's transferring big files, other people will think			
		Internet is really slow.			
	e.	If this never happens before, call you Internet service			
		provider to know if there is something wrong with their			
		network.			
I can't log into the web management	a.	Make sure you're connecting to the correct IP address of			
interface; the password is wrong.		the AP!			
	b.	Password is case-sensitive. Make sure the 'Caps Lock'			
		light is not illuminated.			
	c.	If you really forget the password, do a hard reset.			
The AP becomes hot	a.	This is not a malfunction, if you can keep your hand on			
		the AP's case.			
	b.	If you smell something wrong or see the smoke coming			
		out from AP or A/C power adapter, please disconnect			
		the AP and A/C power adapter from utility power (make			
		sure it's safe before you're doing this!), and call your			
		dealer of purchase for help.			

Appendix C: Specifications

Draduet	WNAP-6308		
Product	2.4GHz 150Mbps 802.11n Wireless Outdoor Access Point		
Hardware Specifications			
Standard	IEEE 802.11b/g/n Wireless LAN IEEE 802.11i Wireless Security IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Ethernet IEEE 802.3x Flow Control		
Memory	32 Mbytes DDR SDRAM 8 Mbytes Flash		
Interface	Wireless IEEE 802.11b/g/n, 1T1R LAN/WAN: 1 x 10/100Base-TX, Auto-MDI / MDIX		
Antenna	Built-in N-Type (Male) Antenna Connector		
Wireless RF Specification	ls		
Wireless Technology	IEEE 802.11b/g IEEE 802.11n		
Data Rate	IEEE 802.11b: 11, 5.5, 2 and 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6Mbps IEEE 802.11n (20MHz): up to 72Mbps IEEE 802.11n (40MHz): up to 150Mbps		
Media Access Control	CSMA / CA		
Modulation	Transmission/Emission Type: DSSS / OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK, CCK		
Frequency Band	2.412GHz ~ 2.484GHz		
Operating Channel	America/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels) Japan/ TELEC: 2.412~2.484GHz (14 Channels)		
RF Output Power (Max.)	Itput Power (Max.) IEEE 802.11b/g: 23 ± 1.5dBm IEEE 802.11n: 23 ± 1.5dBm		
Receiver Sensitivity	IEEE 802.11b/g: -95dBm IEEE 802.11n: -91dBm		
Output Power Control	3~23dBm		
Software Features			
LAN	Built-in DHCP server supporting static IP address distributing Supports 802 1d STP (Spanning Tree)		
WAN	 Static IP Dynamic IP PPPoE 		

	■ PPTP ■ L2TP			
	■ Bridge			
Operating Mode	■ Gatewa	γ		
	■ WISP			
	NAT firewall with SPI (Stateful Packet Inspection)			
Firewall	Built-in NAT server supporting Virtual Server and DMZ			
	Built-in firewall with Port / IP address / MAC / URL filtering			
	■ AP			
	■ Client			
Wireless Mode	■ WDS PTP			
	■ WDS PTMP			
	WDS Repeater (AP+WDS)			
Channel Width	20MHz / 40MHz			
Wireless Isolation	Enables iso	Enables isolation of each connected wireless client from communicating with		
	each other mutually.			
Encryption Type	64/128-bits WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X			
	Provides wireless LAN ACL (Access Control List) filtering			
Wireless Security	Wireless MAC address filtering			
	Supports WPS (Wi-Fi Protected Setup)			
	Enable / Disable SSID Broadcast			
Multiple SSID	Up to 2			
Max. Wireless Client	20			
Max. WDS AP	8			
Max. Wired Client	30			
WMM	Supports Wi-Fi Multimedia			
QoS	Supports Quality of Service for bandwidth control			
NTP	Network Time Management			
Management	Web UI, DHCP Client, Configuration Backup & Restore, Dynamic DNS, SNMP			
Diagnostic Tool	System Log, Ping Watchdog			
Mechanical & Power				
IP Rate	IP55			
Material	Outdoor UV Stabilized Enclosure			
Dimensions (Φ x H)	45 x 169 mm			
Weight	128kg			
Installation	Pole mounting			
	LAN	12~24V DC, Passive PoE		
Power Requirements		Pin 4,5 VDC+		
		Pin 7,8 VDC-		
Power Consumption	1.5W			
Environment & Certificati	on			

Operation Temperature	-35 ~ 65 degrees C	
Operating Humidity	5 ~ 90% non-condensing	
Regulatory	CE / FCC/ RoHS	
Accessory		
Standard Accessories	Passive PoE Injector & Power Cord x 1	
	Plastic Strap x 2	
	Quick Installation Guide x 1	
	CD (User's Manual, Quick Installation Guide) x 1	



EC Declaration of Conformity

For the following equipment:

*Type of Product :		2.4GHz 802.11n Wireless Outdoor Access Point
*Model Number :		WNAP-6308
* Produced by: Manufacturer's Name Manufacturer's Addres	: ss:	Planet Technology Corp. 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:

EN 60950-1 EN 300 328 V1.8.1 EN 301 489-1 V1.9.2 EN 301 489-17 V2.2.1 (2006 + A11: 2009 + A1:2010+A12:2011) (2014-12-31) (2011-09) (2012-09)

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.

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

Person responsible for making this declaration

Name, Surname <u>Kent Kang</u>

Position / Title : <u>Product Manager</u>

Taiwan Place

28th Feb., 2014 *Date*

legal Signature

PLANET TECHNOLOGY CORPORATION

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation , declares that this 802.11b/g/n Wireless Outdoor Access Point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	Lietuviškai	Šiuo PLANET Technology Corporation ,, skelbia, kad 802.11b/g/n Wireless Outdoor Access Point tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation, tímto prohlašuje, že tato 802.11b/g/n Wireless Outdoor Access Point splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	Magyar	A gyártó PLANET Technology Corporation , kijelenti, hogy ez a 802.11b/g/n Wireless Outdoor Access Point megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation, erklærer herved, at følgende udstyr 802.11b/g/n Wireless Outdoor Access Point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	Malti	Hawnhekk, PLANET Technology Corporation, jiddikjara li dan 802.11b/g/n Wireless Outdoor Access Point jikkonforma mal-ħtiģijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt PLANET Technology Corporation , dass sich dieses Gerät 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eestikeeles	Käesolevaga kinnitab PLANET Technology Corporation, et see 802.11b/g/n Wireless Outdoor Access Point vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation, oświadcza, że 802.11b/g/n Wireless Outdoor Access Point spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie "Directive 1999/5/EC".
Ελληνικά	ME THN ΠΑΡΟΥΣΑ , PLANET Technology Corporation, $\Delta H \land \Omega N E I OT I A Y TO 802.11b/g/nWireless Outdoor Access Point\Sigma Y M M OP \Phi \Omega N E TA I ΠΡΟΣ ΤΙΣ ΟΥΣΙ Ω ΔΕ ΙΣΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙ ΠΕΣΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ$	Português	PLANET Technology Corporation, declara que este 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , PLANET Technology Corporation, dichiara che questo 802.11b/g/n Wireless Outdoor Access Point è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	Suomi	PLANET Technology Corporation, vakuuttaa täten että 802.11b/g/n Wireless Outdoor Access Point 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 802.11b/g/n Wireless Outdoor Access Point atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation , att denna 802.11b/g/n Wireless Outdoor Access Point står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.