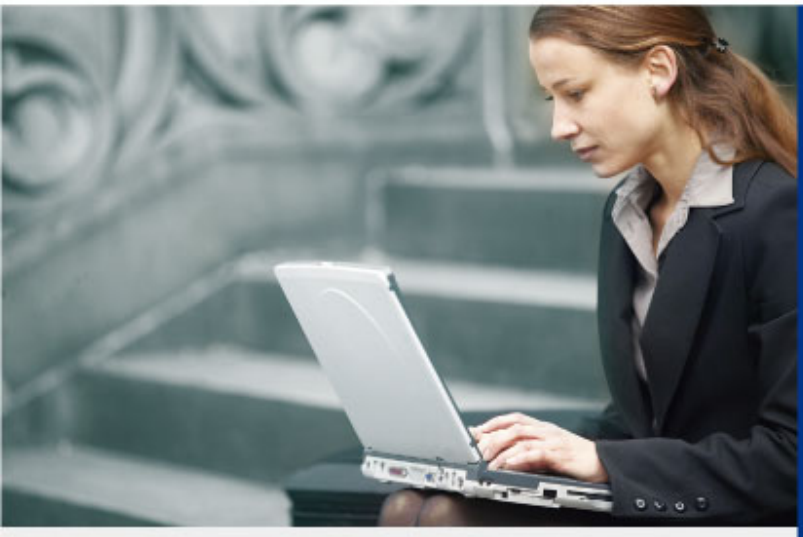
PLANET
Networking & Communication

User's Manual

5GHz 802.11a/n Wireless Outdoor AP

- WNAP-7206



www.PLANET.com.tw

Copyright

Copyright © 2013 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 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 802.11a/n Wireless Outdoor Access Point

Model: WNAP-7206

Rev: 1.0 (January, 2013)

Part No. EM-WNAP-7206_v1.0 (**2081-E10490-000**)

CONTENTS

Chapter 1.Product Introduction 1

1.1 Package Contents 1

1.2 Product Description 2

1.3 Product Features 4

1.4 Product Specification 5

Chapter 2.Hardware Installation 8

2.1 Hardware Description 8

2.1.1 The Rear Panel 8

2.1.2 The Bottom Panel 9

2.1.3 PoE Injector 10

Chapter 3.Connecting to the AP 12

3.1 Preparation before Installation 12

3.1.1 Professional Installation Required 12

3.1.2 Safety Precautions 12

3.2 Installation Precautions 12

3.3 Hardware Installation 14

3.4 Pole Mounting 16

3.4.1 Using the External Antenna 16

Chapter 4.Quick Installation Guide 17

4.1 Manual Network Setup - TCP/IP Configuration 17

4.1.1 Configure the IP Address Manually 17

4.2 Starting Setup in the Web UI 21

Chapter 5.Configuring the AP 25

5.1 Status 25

5.2 Quick Setup 28

5.3 WPS 28

5.3.1 Push Button Config (PBC) 29

5.3.2 PIN Input Config (PIN) 32

5.4 Operation Mode 36

5.5 Network 37

5.5.1 LAN 37

5.5.2 WAN 38

5.5.2.1. Dynamic IP 39

5.5.2.2. Static IP 40

5.5.2.3. PPPoE/Russia PPPoE 42

5.5.2.4. L2TP/Russia L2TP 45

5.5.2.5. PPTP/Russia PPTP 48

5.5.2.6. BigPond Cable 50

5.5.3 MAC Clone 52
5.6 Wireless 53
5.6.1 Wireless Settings 53
5.6.1.1. Access Point Mode 53
5.6.1.2. Multi-SSID Mode 55
5.6.1.3. Client Mode (Client Bridge) 58
5.6.1.4. Repeater Mode 61
5.6.1.5. Universal Repeater Mode 63
5.6.1.6. Bridge with AP Mode (PtP & PtMP) 65
5.6.1.7. AP Router Mode 68
5.6.1.8. AP Client Router Mode (WISP+AP) 70
5.6.2 Wireless Security 74
5.6.2.1. Operation Mode – Access Point 75
5.6.2.2. Operation Mode – Multi-SSID 78
5.6.2.3. Operation Mode – Client 80
5.6.2.4. Operation Mode – Repeater 82
5.6.2.5. Operation Mode – Universal Repeater 84
5.6.2.6. Operation Mode – Bridge with AP 86
5.6.2.7. Operation Mode – AP Router 88
5.6.2.8. Operation Mode – AP Client Router 91
5.6.3 Wireless MAC Filtering 93
5.6.4 Wireless Advanced 94
5.6.5 Antenna Alignment 96
5.6.6 Distance Setting 96
5.6.7 Throughput Monitor 98
5.6.8 Wireless Statistics 99
5.7 DHCP 99
5.7.1 DHCP Settings 100
5.7.2 DHCP Clients List 101
5.7.3 Address Reservation 102
5.8 Forwarding 103
5.8.1 Virtual Servers 103
5.8.2 Port Triggering 105
5.8.3 DMZ 108
5.8.4 UPnP 108
5.9 Security 111
5.9.1 Basic Security 111
5.9.2 Advanced Security 113
5.9.3 Local Management 115
5.9.4 Remote Management 116
5.10 Parental Control 117
5.11 Access Control 118

5.11.1 Rule 119
5.11.2 Host 121
5.11.3 Target 122
5.11.4 Schedule 123
5.12 Static Routing 125
5.13 Bandwidth Control 126
5.13.1 Control Settings 126
5.13.2 Rules List 127
5.14 IP & MAC Binding 129
5.14.1 Binding Settings 129
5.14.2 ARP List 130
5.15 Dynamic DNS 131
5.16 System Tools 134
5.16.1 Time Settings 134
5.16.2 Diagnostic 135
5.16.3 Ping Watch Dog 137
5.16.4 Speed Test 138
5.16.5 Firmware Upgrade 139
5.16.6 Factory Defaults 140
5.16.7 Backup & Restore 140
5.16.8 Reboot 141
5.16.9 Password 141
5.16.10 System Log 142
5.16.11 Statistics 145
Appendix A: FAQ 147
A.1 What and how to find my PC's IP and MAC address? 147
A.2 What is Wireless LAN? 147
A.3 What are ISM bands? 147
A.4 How does wireless networking work? 147
A.5 What is BSSID? 148
A.6 What is ESSID? 148
A.7 What are potential factors that may causes interference? 148
A.8 What are the Open System and Shared Key authentications? 149
A.9 What is WEP? 149
A.10 What is Fragment Threshold? 149
A.11 What is RTS (Request to Send) Threshold? 150
A.12 What is Beacon Interval? 150
A.13 What is Preamble Type? 150
A.14 What is SSID Broadcast? 150
A.15 What is Wi-Fi Protected Access (WPA)? 151

A.16 What is WPA2? 151
A.17 What is 802.1x Authentication? 151
A.18 What is Temporal Key Integrity Protocol (TKIP)? 151
A.19 What is Advanced Encryption Standard (AES)? 151
A.20 What is Inter-Access Point Protocol (IAPP)? 152
A.21 What is Wireless Distribution System (WDS)? 152
A.22 What is Universal Plug and Play (UPnP)? 152
A.23 What is Maximum Transmission Unit (MTU) Size? 152
A.24 What is Clone MAC Address? 152
A.25 What is DDNS? 152
A.26 What is NTP Client? 152
A.27 What is VPN? 153
A.28 What is IPSEC? 153
A.29 What is WLAN Block Relay between Clients? 153
A.30 What is WMM? 153
A.31 What is WLAN ACK TIMEOUT? 153
A.32 What is Modulation Coding Scheme (MCS)? 153
A.33 What is Frame Aggregation? 153
A.34 What is Guard Intervals (GI)? 154
Appendix B: Configuring the PC in Windows 7 155
Appendix C: Specifications 158
Appendix D: Factory Default Settings 161

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WNAP-7206. Before installing the AP, please verify the contents inside the package box.

WNAP-7206 Wireless AP

Quick Installation Guide

CD-ROM

(User Manual included)

Power Adapter

PoE Injector

Mounting Tie x 2

Note

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

1.2 Product Description

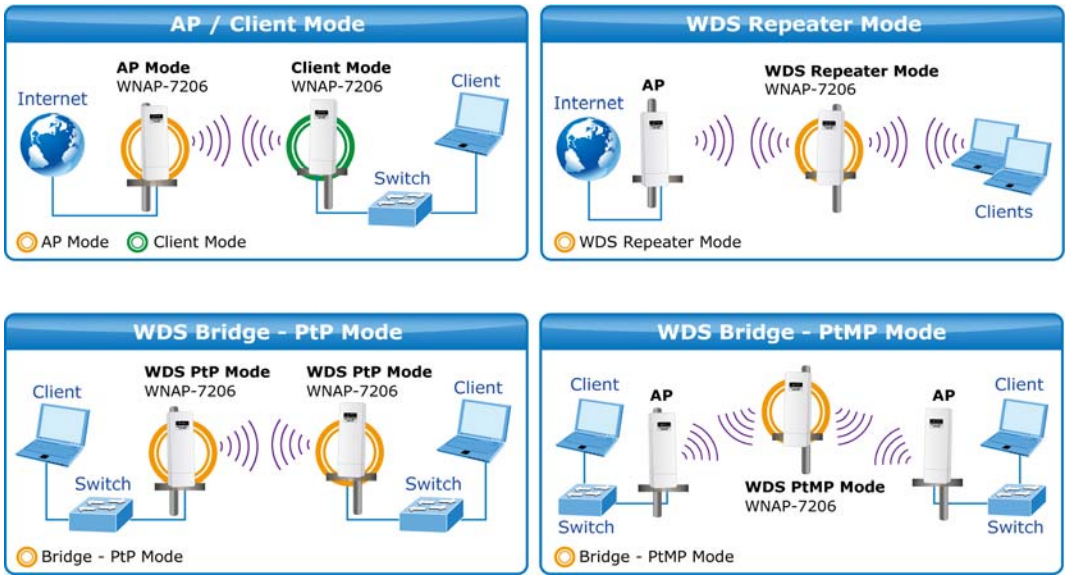
High Power Outdoor Wireless Coverage

PLANET Technology introduces the latest high power outdoor wireless LAN solution - the outdoor wireless AP, WNAP-7206. It provides higher transmit power, better performance, and widely coverage than standard outdoor wireless AP. The WNAP-7206 is compatible with IEEE 802.11a/n standard supporting the data rate up to 150Mbps in 802.11n mode. The WNAP-7206 not only has built-in 15dBi panel Antenna but also reserves one RP-SMA Type Antenna Connector to allow versatile antenna installations and multiple adjustable transmit output power controller. Therefore, the WNAP-7206 is quite suitable for widely open space applications.

Multiple Operating & Wireless Modes

The WNAP-7206 supports multiple wireless communication connectivity (AP / Client CPE / WDS PtP / WDS PtMP / Repeater / Universal Repeater) allowing for various application requirements and thus it gives users more comprehensive experience when using the WNAP-7206. It helps users to easily build a wireless network and extend the wireless range of existing wireless network.

The WNAP-7206 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 64/128/152-bit WEP encryption, the WNAP-7206 integrates WPA / WPA2, WPA-PSK / WPA2-PSK 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. To fulfill enterprise and various applications demand, the WNAP-7206 enhances security and management features such as multiple SSID support. It can create up to 4 virtual standalone AP with 4 different SSID according to individual security level and encryption scheme of various wireless devices.

Highly Reliable Outdoor Device

The WNAP-7206 is perfectly suitable to be installed in outdoor environments and exposed locations. Its built-in 15KV ESD and 4000V lightning protection can withstand storm and prevent damage from lightning surges. Furthermore, the WNAP-7206 can perform stably under rigorous weather conditions including heavy rain and wind by its Outdoor Weatherproof case protection. With the proprietary Power over Ethernet (PoE) design, the WNAP-7206 can be easily applied in any area where power outlets are not available. It is the best way using the WNAP-7206 to build outdoor wireless access applications between buildings on campuses, business, rural areas and etc.

Easy Installation & Management

With User-friendly Web UI and step by step Setup Wizard, the WNAP-7206 is easier to install, even for users who never experience setting up a wireless network. Furthermore, with SNMP-Based management interface, the WNAP-7206 is convenient to be managed and configured remotely.

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 802.11a standard
  - Equipped with 10/100Mbps RJ-45 Ports for LAN & WAN, Auto MDI/ MDI-X supported
- **RF Interface Characteristics**
  - Built-in 15dBi directional antenna
  - High Output Power up to 500mW with multiple adjustable transmit power control
  - Reserve RP-SMA Type Connector
- **Outdoor Environmental Characteristics**
  - Outdoor weatherproof enclosure, with built-in 15KV ESD and 4000V lightning protection
  - Passive Power over Ethernet design
  - Operating temperature: -30~70 Degree C
- **Multiple Operation & Wireless Mode**
  - Multiple Operation Modes: Bridge, Gateway, Ethernet Converter
  - Multiple Wireless Modes: AP, Client CPE (WISP), WDS PtP, WDS PtMP, Repeater, Universal Repeater
  - Supports Multiple SSID allowing users to access different networks through one single AP
  - Supports WMM (Wi-Fi Multimedia)
- **Secure Network Connection**
  - Advanced security: 64/128/152-bit WEP, WPA / WPA2, and WPA-PSK / WPA2-PSK (TKIP/AES)
  - Supports NAT firewall features, with SPI function to protect against DoS attacks
  - Supports IP / Protocol-based access control and MAC Filtering
- **Fixed-network Broadband Router**
  - Supported connection types: Dynamic / Static IP / PPPoE / PPTP / L2TP / Russia Dual-Access
  - Supports multiple sessions IPSec, L2TP and PPTP VPN pass-through
  - Supports Virtual Server, DMZ and Port Triggering for various networking applications
  - Supports DHCP Server, UPnP, Dynamic DNS
- **Easy Installation & Management**
  - User-friendly Web-Based UI and SNMP-Based management
  - Quick Setup Wizard for easy configuration
  - Remote Management allows configuration from a remote site
  - Intelligent Antenna Alignment tool speeds up field deployment
  - System status monitoring includes DHCP Client, System Log

1.4 Product Specification

Product	**WNAP-7206** 150Mbps 802.11a/n Wireless Outdoor Access Point
Hardware	
Standard compliance	IEEE 802.11a/n IEEE 802.3 IEEE 802.3u IEEE 802.3x
Memory	32 Mbytes DDR SDRAM 4 Mbytes Flash
Button	Reset Button x 1
LED	Provides 4-Level signal LED indicator
PoE	Passive PoE (Up to 60 meters)
Interface	Wireless IEEE 802.11a/n LAN / WAN: 10/100Base-TX, Auto-MDI/MDIX x 1 Grounding Terminal x 1
Antenna	Internal (Default): 15dBi directional antenna (Dual-Polarization) ■ Horizontal: 60 degree ■ Vertical: 14 degree External (Option): RP-SMA Female type Connector ■ Switchable by Software ■ For External Antenna Mode, attach antenna before power on.
Data Rate	802.11a: 54, 48, 36, 24, 18, 12, 9 and 6Mbps 802.11n (20MHz): up to 72Mbps 802.11n (40MHz): up to 150Mbp
Media Access Control	CSMA/CA
Modulation	Transmission / Emission Type: OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM
Frequency Band	5.180-5.240GHz; 5.745-5.825GHz
Operating Channel	5.180GHz-CH36 5.200GHz-CH40 5.220GHz-CH44 5.240GHz-CH48 5.745GHz-CH149 5.765GHz-CH153 5.785GHz-CH157 5.805GHz-CH161 5.825GHz-CH165 *The actual channels will vary depends on the regulation in different regions and countries.

RF Output Power	802.11a: 27 ± 1dBm 802.11n: 24 ± 1dBm	
Receiver Sensitivity	**802.11a:** 54M: -77dBm 48M: -79dBm 36M: -83dBm 24M: -86dBm 18M: -91dBm 12M: -92dBm 9M: -93dBm 6M: -94dBm	**802.11n:** 150M: -73dBm 121.5M: -76dBm 108M: -77dBm 81M: -81dBm 54M: -84dBm 40.5M: -88dBm 27M: -91dBm 13.5M: -93dBm
Output Power Control	High (default) Middle Low	
Power Requirements	Passive PoE 12V Pin 4,5 VDC+ Pin 7,8 VDC-	
Power Adapter	12V DC, 1A (switching)	
Environment & Certification		
Operation	Temperature: -30~70 Degree C, Humidity: 10~90% non-condensing	
Storage	Temperature: -40~70 Degree C, Humidity: 5~95% non-condensing	
Enclosure	Outdoor Weatherproof design 15KV ESD & 4000V Lightning Protection Grounding Terminal Integrated	
Regulatory	CE / FCC / RoHS	
Software		
LAN	Built-in DHCP server supporting static IP address distributing	
	Supports UPnP, Dynamic DNS	
	Supports Flow Statistics	
	IP & MAC Binding	
	IP / Protocol-based Bandwidth Control	
WAN	■ Static IP ■ Dynamic IP ■ PPPoE / Russia PPPoE ■ PPTP / Russia PPTP ■ L2TP / Russia L2TP ■ BigPond Cable	
VPN Passthrough	■ PPTP ■ L2TP ■ IPSec	
Operating Mode	■ Standard AP (Wireless AP) ■ AP Router (Wireless Broadband Router) ■ AP Client Router (WISP Client Router)	

Firewall	NAT firewall with SPI (Stateful Packet Inspection)
	NAT with ALG (Application Layer Gateway)
	Built-in NAT server supporting Port Triggering, Virtual Server, and DMZ
	Built-in firewall with IP address / MAC / DNS filtering
	Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter, DoS protection
Wireless Mode	■ AP ■ Client ■ WDS PTP ■ WDS PTMP ■ WDS Repeater (AP+WDS) ■ Universal Repeater (AP+Client)
Channel Width	20MHz / 40MHz
Wireless Isolation	Enable to isolate each connected wireless clients
Wireless Security	64/128/152-bits WEP, WPA, WPA-PSK, WPA2, WPA2-PSK
	Wireless MAC address filtering
	Enable/Disable SSID Broadcast
Multiple SSID	Up to 3
Max. Wireless Client	25
Max. WDS AP	4
Max. Wired Client	60
WMM	Supports Wi-Fi Multimedia
NTP	Network Time Management
Management	Web-Based (HTTP) management interface
	Supports SNMP v1/v2 agent with MIB-II
	Remote management
	SNTP time synchronize
	Easy firmware upgrade
	Configuration Backup & Restore
	DHCP Client List
Diagnostic tool	System Log supports auto mail and save to local host
	Ping Watch Dog allows you to continuously monitor the particular connection between the device and a remote host.
	Throughput Monitor provides real-time wireless throughput information
	Speed Test helps to test the connection speed

Chapter 2. Hardware Installation

Please follow the instructions below to connect WNAP-7206 to the existing network devices and your computers.

2.1 Hardware Description

- **Dimension**: 250 x 85 x 60.5 mm (W x D x H)

Figure 2-1 Three-way View

2.1.1 The Rear Panel

Rear Panel - LED

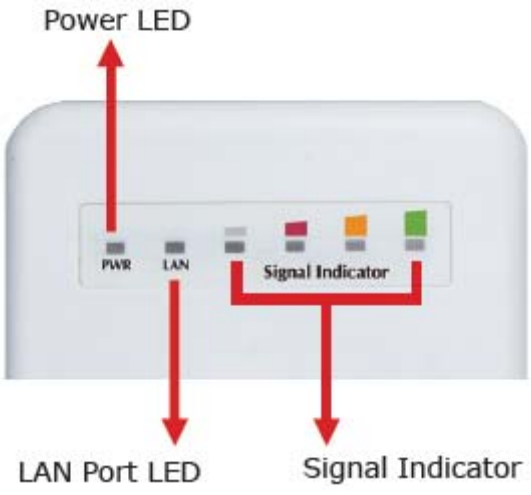


Figure 2-2 LED

LED definition

LED	State	Meaning
Power	On	System On
	Off	System Off
Signal Indicator (Client/Repeater Mode)	On	Indicates the wireless signal strength of remote AP
	Off	No remote wireless signal
WAN	On	Port linked.
	Off	No link.
	Blinking	Data is transmitting or receiving on the WAN interface.
LAN	On	Port linked.
	Off	No link.
	Blinking	Data is transmitting or receiving on the LAN interface.

2.1.2 The Bottom Panel

The Bottom panel provides the physical connectors connected to the antenna and any other network devices. **Figure 2-3** shows the Bottom panel of WNAP-7206, and the **Figure 2-4** shows the power warning of WNAP-7206.

Bottom Panel – Port & Connector

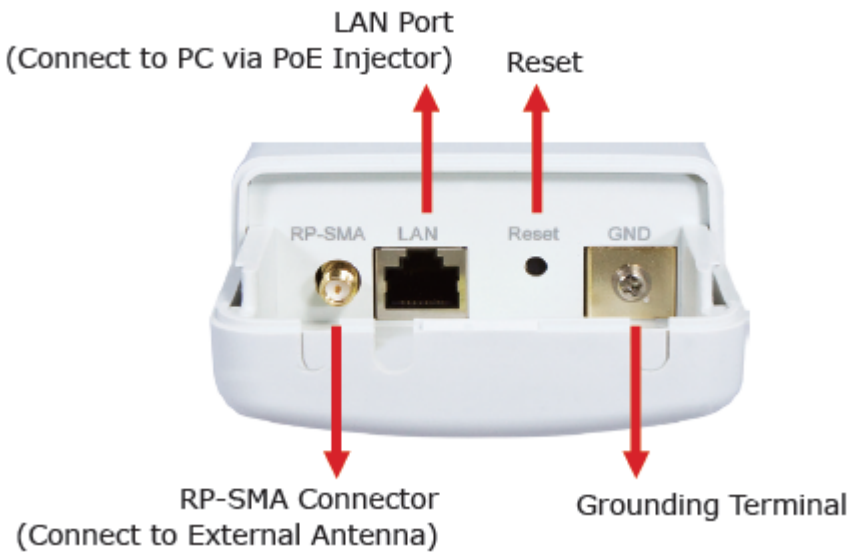


Figure 2-3 Port & Connector

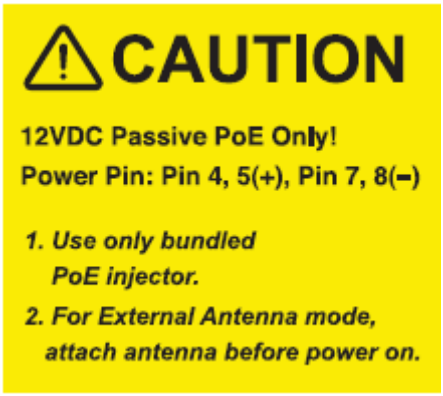


Figure 2-4 Warning label

Interface	Function
RP-SMA Connector	For external antenna. You can use the RP-SMA connector to connect with 5GHz external antenna.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
Reset	There are two ways to reset the AP's factory defaults: ◆ **Use the Factory Defaults function:** on **System Tools -> Factory Defaults** page in the AP's Web-based Utility. ◆ **Use the Factory Default Reset button:** Press and hold the Reset button until Wireless Signal Strength LEDs flash, and then the AP will reboot.

1. For External Antenna Mode, you MUST physically attach antenna before power on.
2. For using external antenna, you should configure the **Antenna Switch** from "**Internal**" to "**External**" via Web UI.

2.1.3 PoE Injector

Figure 2-5 Top view of PoE Injector

Figure 2-6 Warning Label of PoE Injector

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 WNAP-7206 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 WNAP-7206, 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 WNAP-7206; otherwise, a random lightening could easily cause fatal damage to WNAP-7206. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
- Users **MUST** use the "Power cord & PoE Injector" shipped in the box with the WNAP-7206. Use of other options will cause damage to the WNAP-7206.
- Users **MUST** power off the WNAP-7206 first before connecting the external antennas to it; otherwise, damage might be caused to the WNAP-7206 itself.

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 limes. 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 1 OAWG 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 Hardware Installation

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. Push the latch in the bottom of WNAP-7206 to remove the sliding cover.

Figure 3-1

Step 2. Plug the RJ-45 Ethernet cable into the LAN Port of WNAP-7206.

Figure 3-2

Note

RJ-45 8P8C Ethernet cable is required.

Step 3. Slide the cover back to seal the bottom of the WNAP-7206.

Figure 3-3

Step 4. 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 in the STEP 2 into the POE port of the PoE injector.

Figure 3-4

DC: Insert adapter

POE: This hole is linked to LAN port of the WNAP-7206 with RJ-45 Ethernet cable.

LAN: This hole is linked to LAN port of PC/Hub or Router/xDSL modem device with RJ-45 Ethernet cable.

Step 5. Successful installation.

Figure 3-5

Note

It will take about 50 seconds to complete the boot up sequence after powered on the Outdoor AP/Router; Power LED will be active, and after that the LAN Activity LED will be flashing to show the LAN interface is enabled and working now.

Note

To avoid thunder strike, consider to install ELA-100, thunder arrester toward the CPE AP and the PoE injector.

3.4 Pole Mounting

Step 1. Turn the WNAP-7206 over. Put the pole mounting tie through the middle hole of it.

Step 2. Mount WNAP-7206 steadily to the pole by fastening the mounting tie tightly.

Step 3. Now you have completed the hardware installation of WNAP-7206 as figure below.

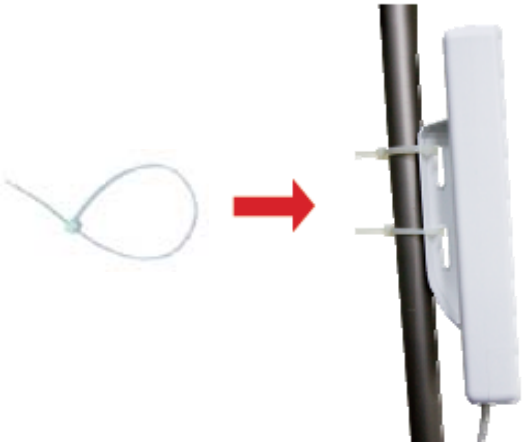


Figure 3-6 Pole Mounting

3.4.1 Using the External Antenna

If you prefer to use the external antenna with RP-SMA Type connector for your application instead of the built-in directional antenna, please follow the steps below.

Step 1. Connect your antenna with the RP-SMA Type connector on the bottom of WNAP-7206.

Step 2. Power on the WNAP-7206, and then go to **Wireless -> Wireless Advanced** to configure the **Antenna Setting** to "**External Antenna**".

1. If you are going to use an external antenna on WNAP-7206, get some cable in advance.
1. Users MUST power off the WNAP-7206 first before connecting the external antenna to it. **Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the WNAP-7206**; otherwise, damage might be caused to the WNAP-7206 itself.

Chapter 4. Quick Installation Guide

This chapter will show you how to configure the basic functions of your Wireless AP using **Quick 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-7206 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-7206 with your PC by an Ethernet cable plugging in LAN port of PoE injector in one side and in LAN port of PC in the other side. Please power on the WNAP-7206 by the PoE injector shipping with WNAP-7206.

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

4.1.1 Configure 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

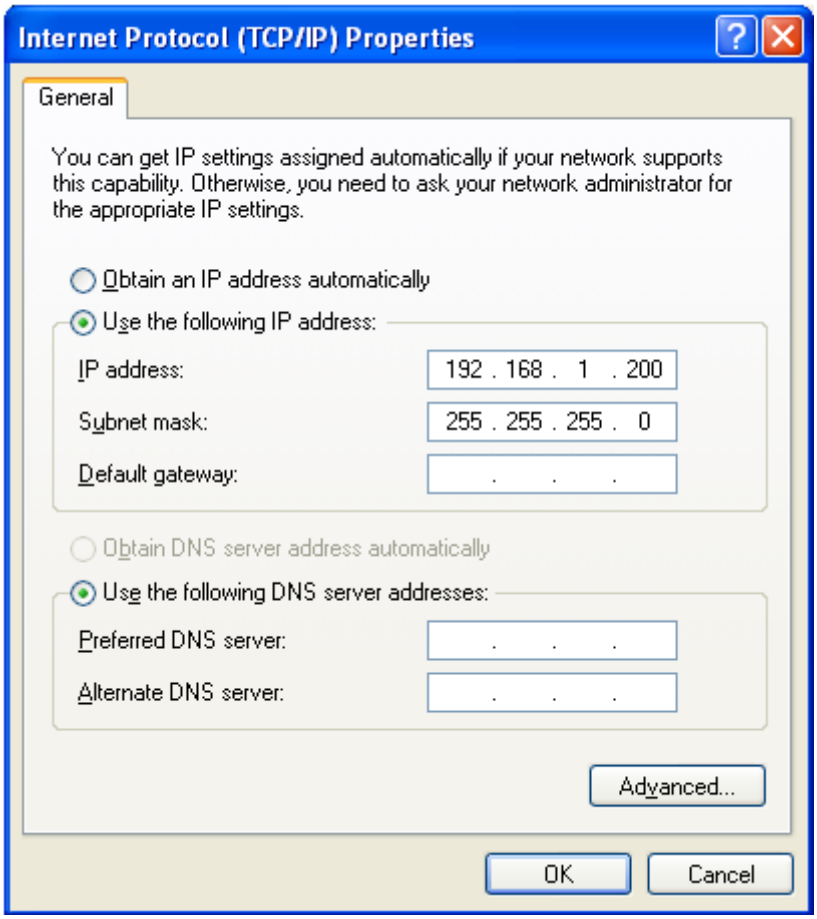


Figure 4-1

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 XP** OS. Please follow the steps below:

1. Click on **Start > Run**.

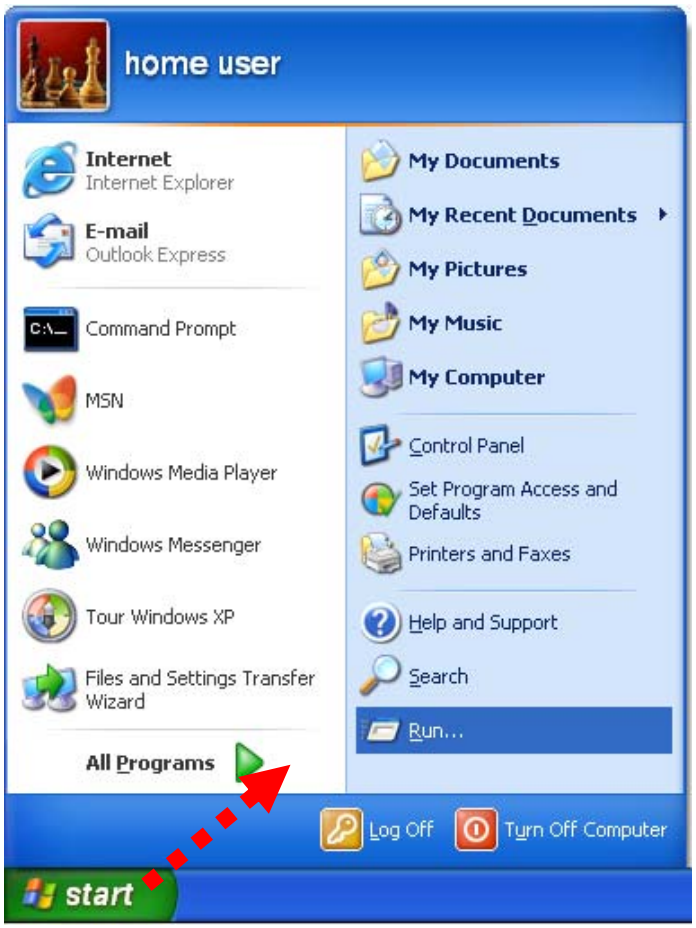


Figure 4-2

2. In the run box type "**cmd**" and click OK. (Windows Vista users type "**cmd**" in the Start .Search box.)At the prompt.

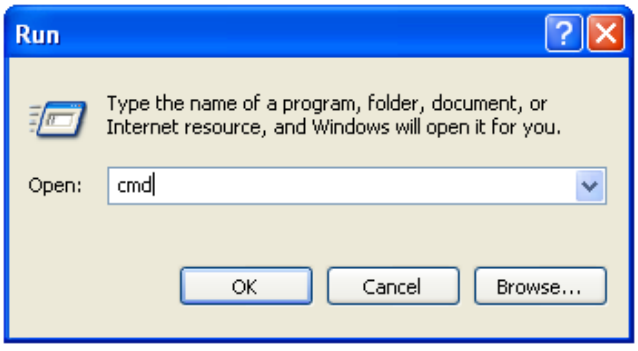


Figure 4-3

Open a command prompt, and type ***ping 192.168.1.1***, and then press **Enter**.

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

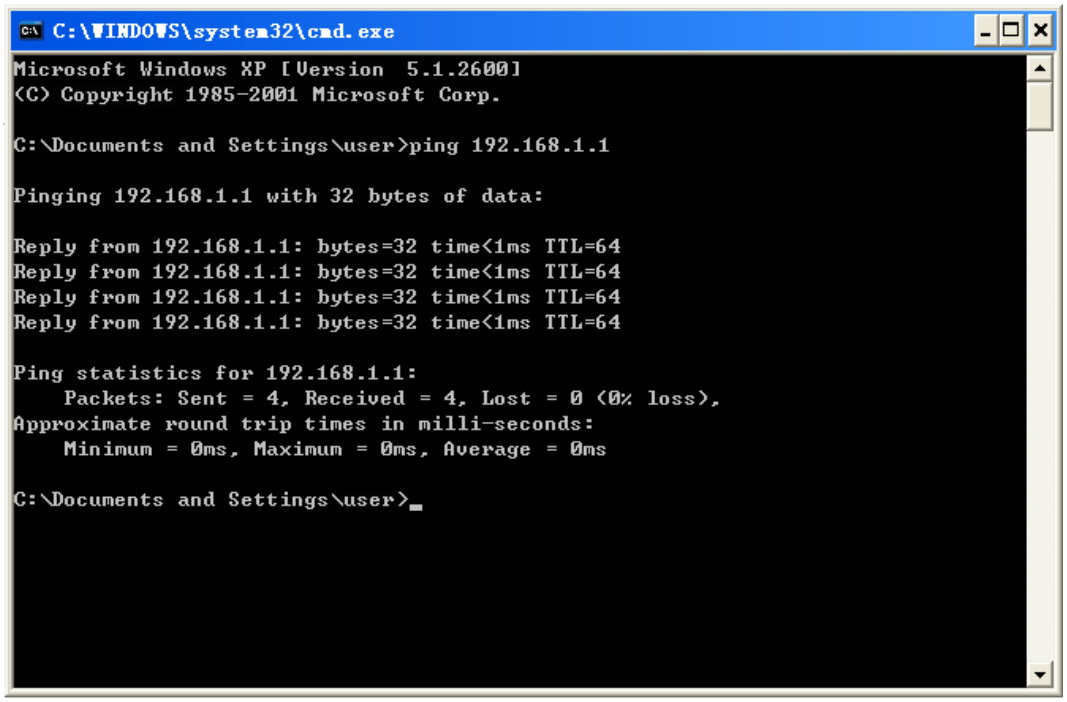


Figure 4-4 Success result of Ping command

If the result displayed is similar to **Figure 4-5**, it means the connection between your PC and the AP has failed.

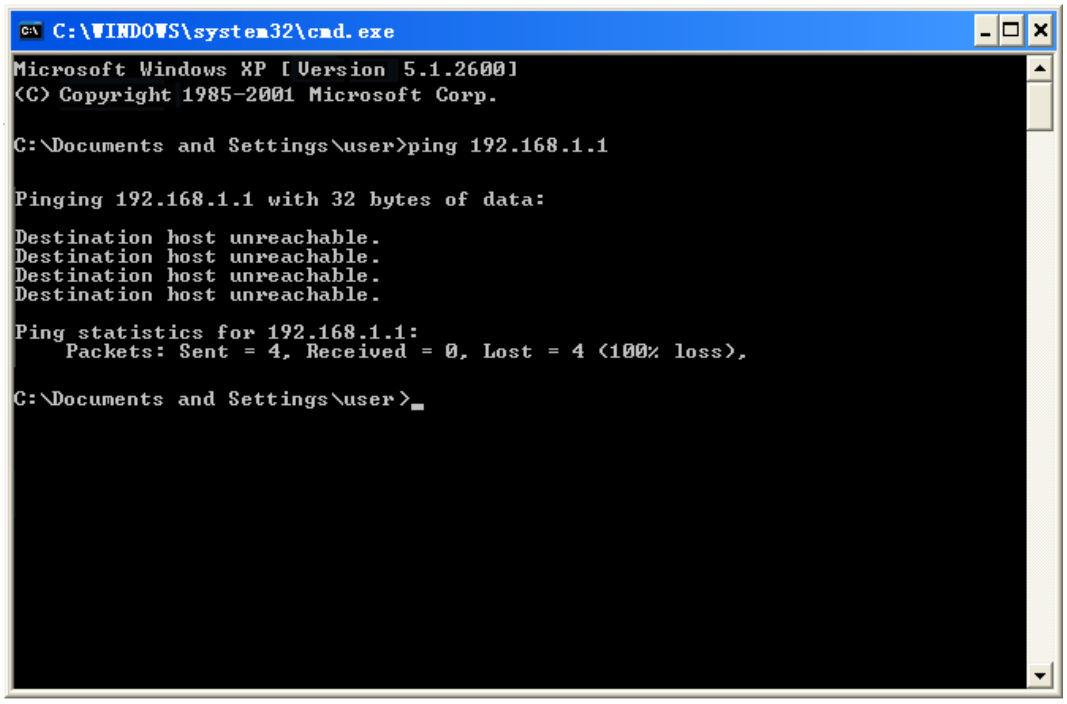


Figure 4-5 Failure result of Ping command

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-7206 with the web browser.

Step 1. To access the configuration page, open a web-browser and enter the default IP address http://192.168.1.1 in the web address field of the browser.

Figure 4-6 Login the AP

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 4-7 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 **Welcome** message screen appears as **Figure 4-8**.

Check "**I agree to these terms of use**" and click **Login** button to login WNAP-7206.

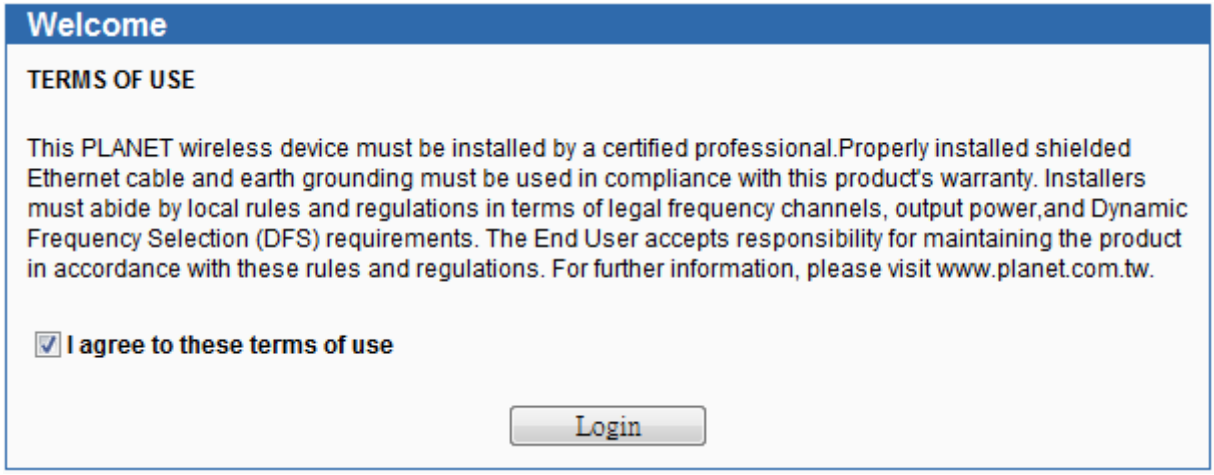


Figure 4-8 WNAP-7206 Login Welcome Screen

Step 2. The **Quick Setup** page appears as **Figure 4-9**.

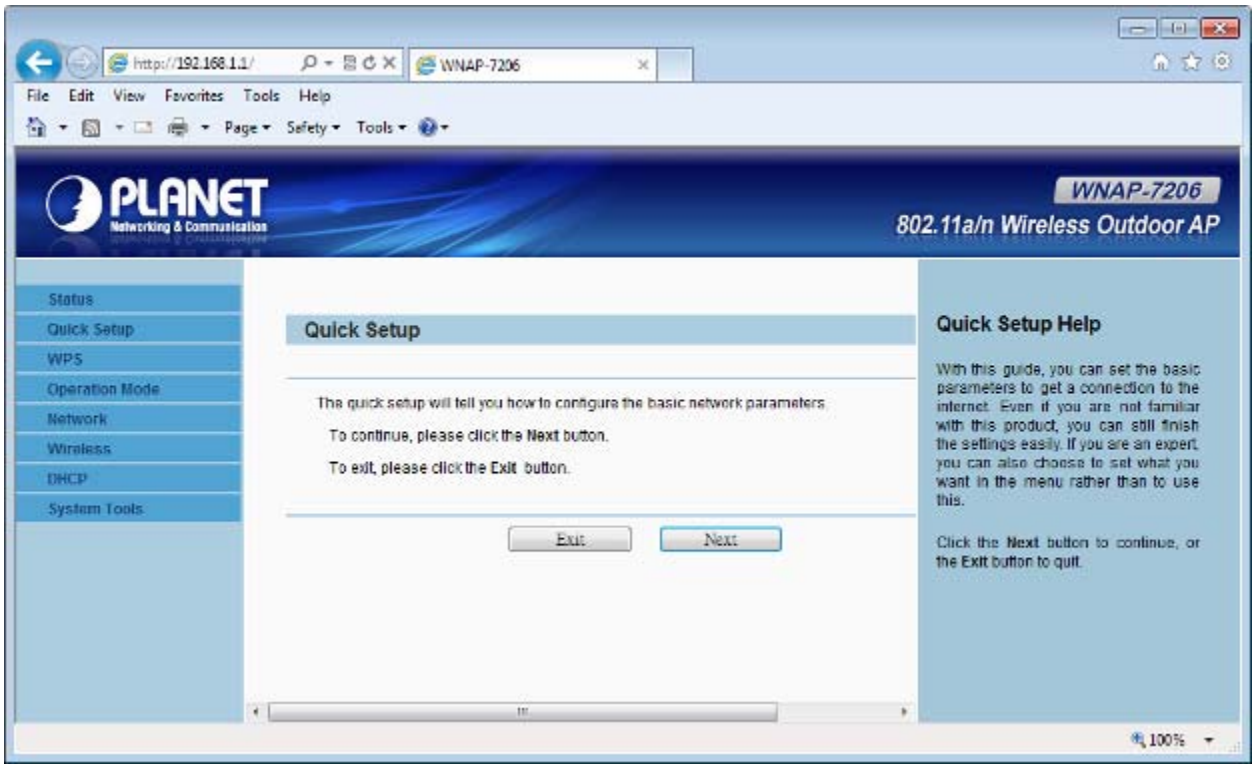


Figure 4-9 WNAP-7206 Web UI Screenshot

Step 3. Click **Next** to choose an Operation Mode. The default is "**Standard AP**" Mode. Please refer to the instructions in the next chapter for configuring the other Operation Modes.

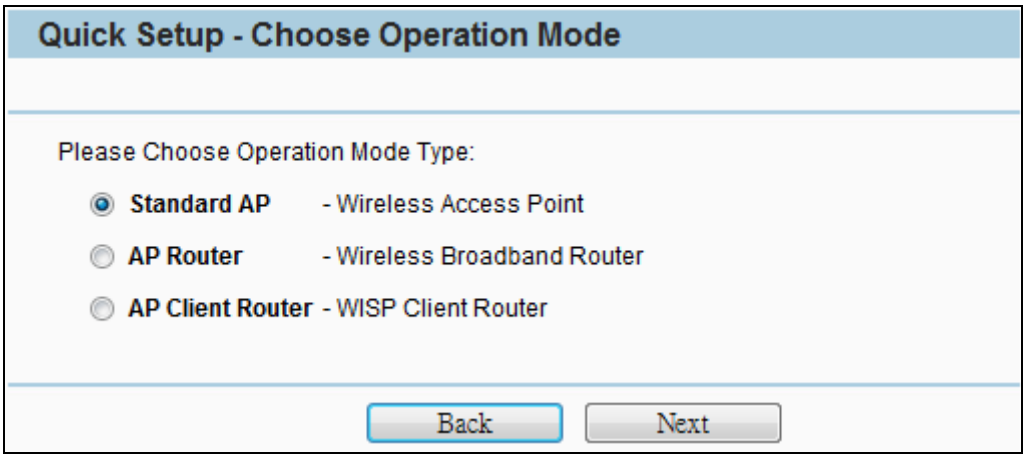


Figure 4-10 Choose Operation Mode

Step 4. Please enter the SSID, configure your Encryption Settings, Pre-Shared Key and etc. Then click **Next** button to make the configuration take effect immediately.

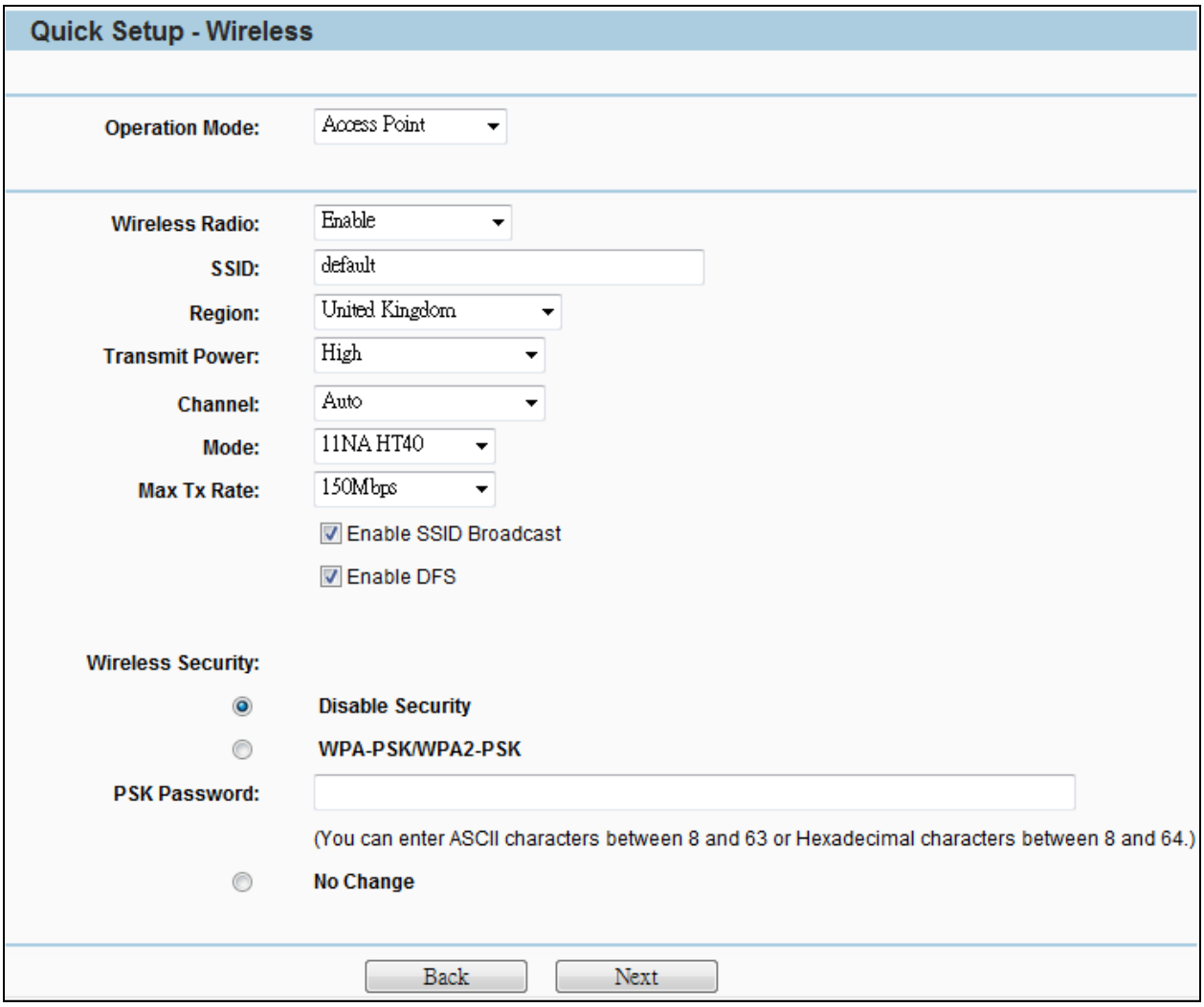


Figure 4-11 Configure Wireless Settings

Step 5. Click **Finish** button to complete the configuration, or click **Back** to re-configure the setting.

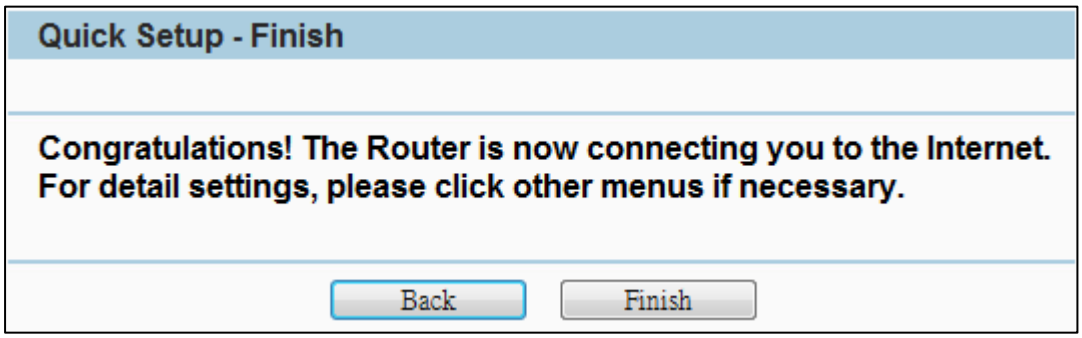
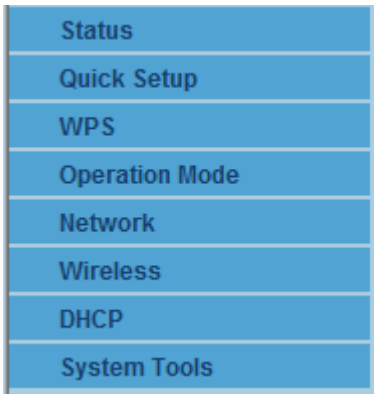


Figure 4-12 Finish Settings

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and features allowing you to manage the AP with ease.



5.1 Status

In this page, you can view information about the current running status of WNAP-7206, including WAN interface, LAN interface, Wireless interface, and firmware version information.

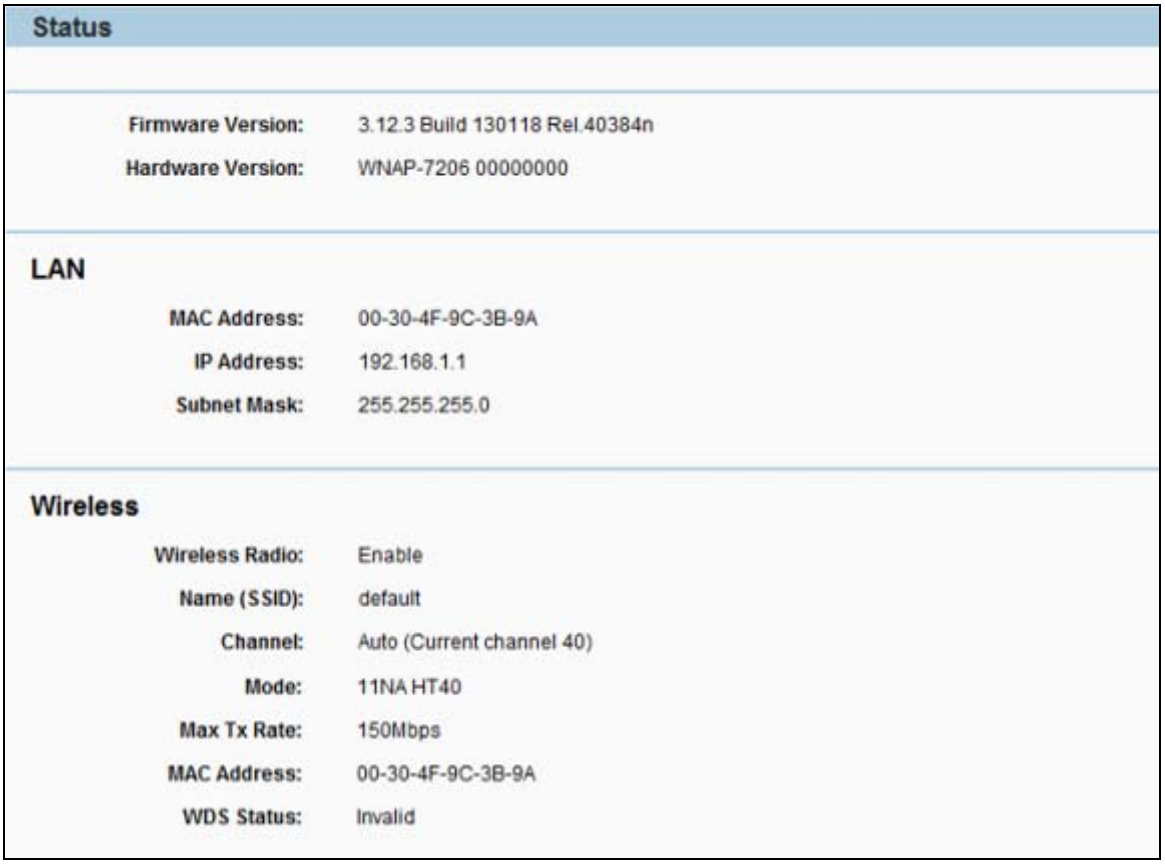


Figure 5-1-1 Status

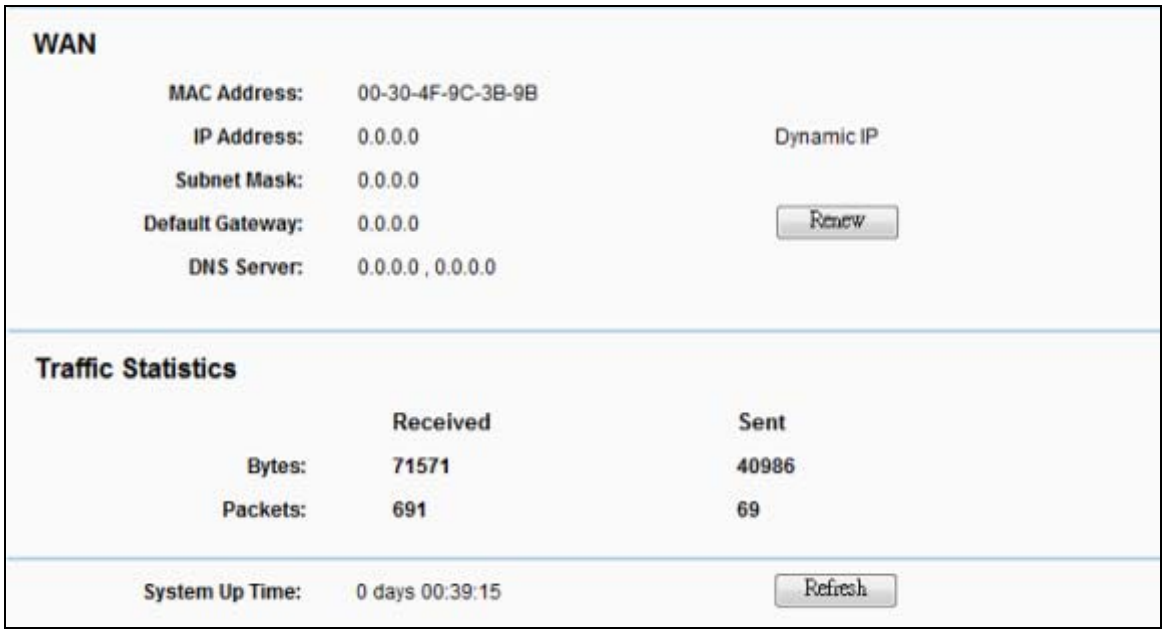


Figure 5-1-2 Status

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

Object	Description
• **Firmware Version**	The current firmware version of the AP.
• **Hardware Version**	The current hardware version of the AP.
LAN	
• **MAC Address**	The physical address of the system, as seen from the LAN.
• **IP Address**	The IP address of the wired LAN.
• **Subnet Mask**	The subnet mask associated with IP address.
Wireless	
• **Wireless Radio**	Indicates whether the wireless radio feature of the Device is enabled or disabled.
• **Wireless AP Mode**	The current wireless AP mode which the AP works on. This field is only available in AP Router Mode.
• **Name (SSID)**	The SSID of the Device.
• **Channel**	The current wireless channel in use.
• **Mode**	The current wireless mode which the AP works on.
• **Max Tx Rate**	The maximum Transmitting Rate.
• **MAC Address**	The physical address of the AP, as seen from the WLAN.
• **Client Status**	The status of client. This field is only available in AP Client Mode. ■ Init: Connection is down; ■ Scan: Try to find the AP;

	■ Auth: Try to authenticate; ■ ASSOC: Try to associate; ■ Run: Associated successfully.
• **WDS Status**	The status of WDS. This field is only available in AP Router Mode.
WAN	
• **MAC Address**	The physical address of the WAN port, as seen from the Internet.
• **IP Address**	The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to Internet.
• **Subnet Mask**	The subnet mask associated with the WAN IP Address.
• **Default Gateway**	The Gateway currently used by the Device is shown here. When you use Dynamic IP as the connection Internet type, the **Renew** button will be displayed here. Click the **Renew** button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, **Release** button will be displayed here. Click the **Release** button to release the IP address the Device has obtained from the ISP.
• **DNS Server**	The DNS (Domain Name System) Server IP addresses currently used by the Device. Multiple DNS IP settings are common. Usually, the first available DNS Server is used.
• **Online Time**	The time that you are online. When you use PPPoE as WAN connection type, the online time is displayed here. Click the Connect or Disconnect button to connect to or disconnect from Internet.
Traffic Statistics	
• **Sent (Bytes)**	Traffic that counted in bytes has been sent out from the current interface.
• **Sent (Packets)**	Traffic that counted in packets has been sent out from the current interface.
• **Received (Bytes)**	Traffic that counted in bytes has been received from the current interface.
• **Received (Packets)**	Traffic that counted in packets has been received from the current interface.
• **System Up Time**	The length of the time since the Device was last powered on or reset. Click the **Refresh** button to get the latest status and settings of the Device.

5.2 Quick Setup

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

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

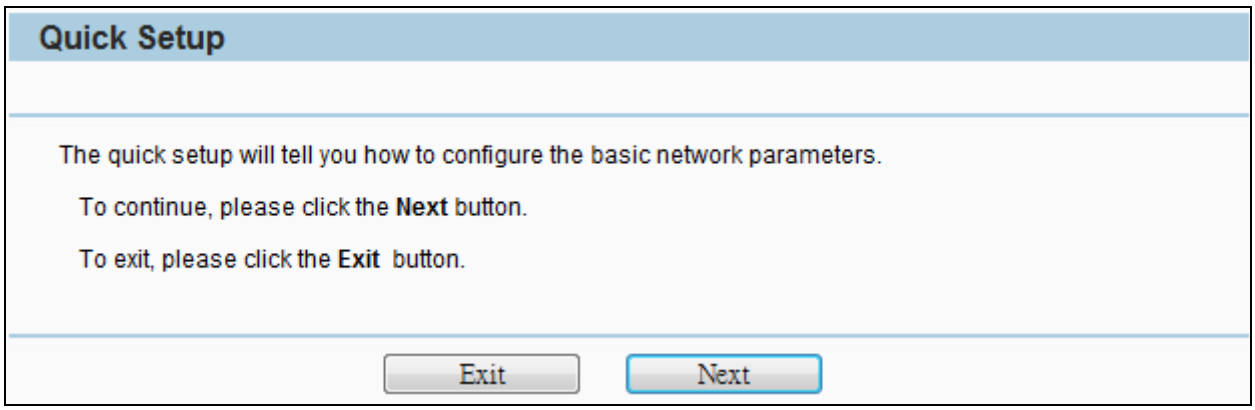


Figure 5-2-1 Quick Setup

5.3 WPS

WPS (Wi-Fi Protected Setup) makes it easy for users who know little of wireless security to establish a secure wireless home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings.

Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.

Note

The WPS function is only available when the Operation Mode is set to Access Point and Multi-SSID.

The hardware WPS button is not supported in WNAP-7206.

Select menu WPS, you will see the next screen as shown in **Figure 5-3-1**.

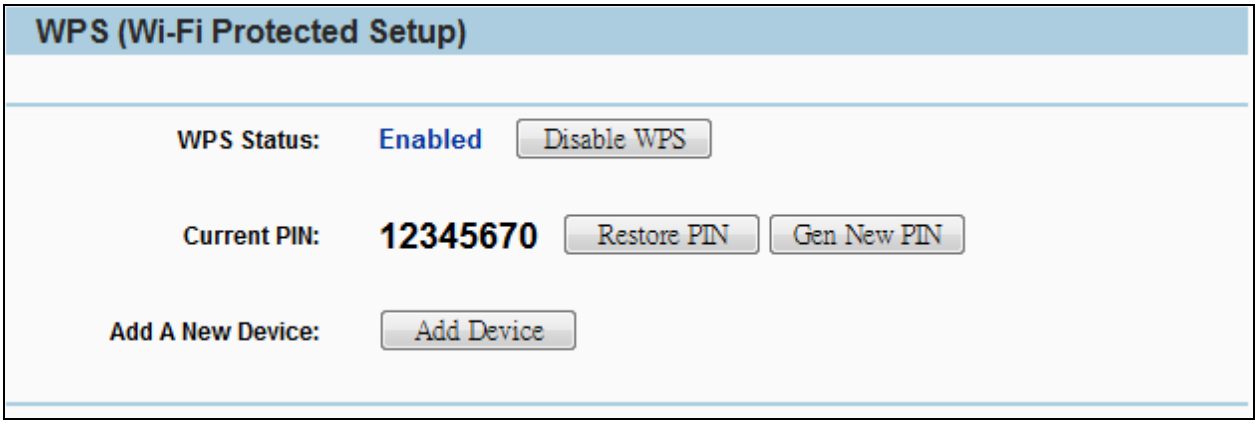


Figure 5-3-1 WPS

The page includes the following fields:

Object	Description
• **WPS Status**	Enable or disable the WPS function here.
• **Current PIN**	The current value of the Device's PIN displayed here. The default PIN of the Device can be found in the label or User Guide. ■ Restore PIN - Restore the PIN of the Device to its default. ■ Gen New PIN - Click this button, and then you can get a new random value for the Device's PIN. You can ensure the network security by generating a new PIN.
• **Add A New Device**	You can add the new device to the existing network manually by clicking Add Device button.

The WPS function cannot be configured if the Wireless Function of the Device is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

To add a new device:

1. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing the configuration button on the device.
2. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering the Device's PIN.

For the configuration of the new device, here takes the Planet Wireless Adapter "**WDL-U700**" for example. The WNAP-7206 is configured to "**Standard AP**" Mode.

5.3.1 Push Button Config (PBC)

This is the easiest way to establish secure connection by WPS, but if there're more than one WPS-supported access point using Push-Button config, please use **PIN / numeric code** instead.

a. To use the PBC method, select "**Press the button of the new device in two minutes**" in the AP.

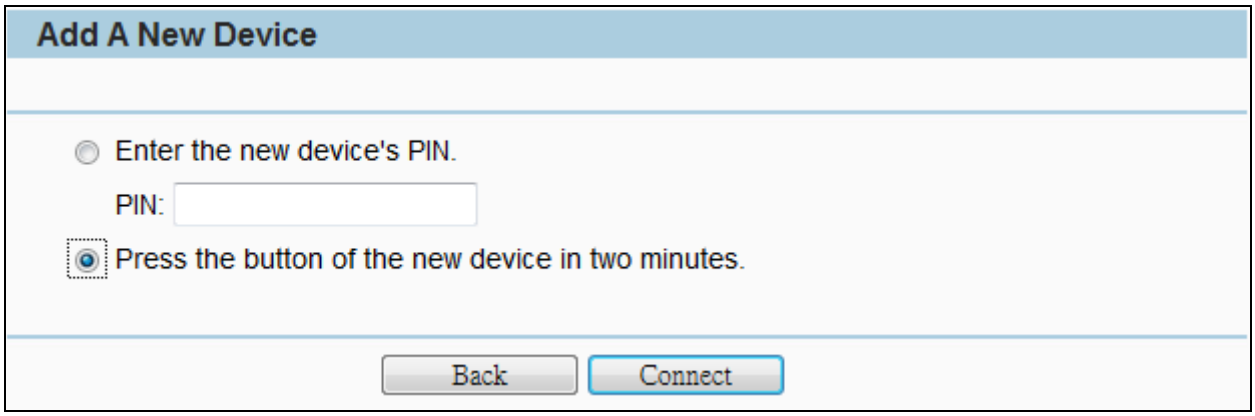


Figure 5-3-1-1 PBC

b. Click **Connect** to start the process.

c. At the same time (within 120 seconds) in the wireless adapter, select "**Push-Button**" in the **Add WPS Profile**. Then, click the right arrow to go next step.

Figure 5-3-1-2 Client - WPS

d. Click "**Start PBC**" to start the WPS process.

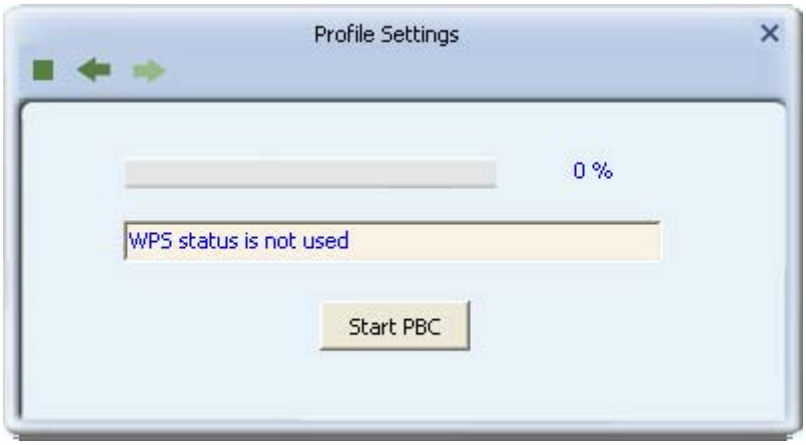


Figure 5-3-1-3 Client – Start PBC

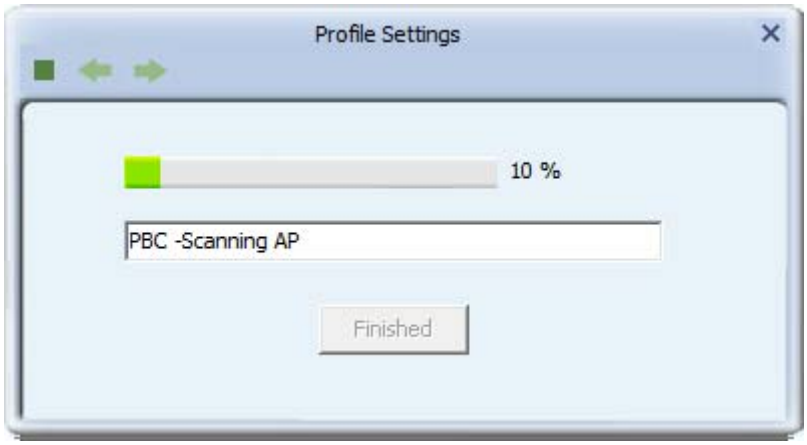


Figure 5-3-1-4

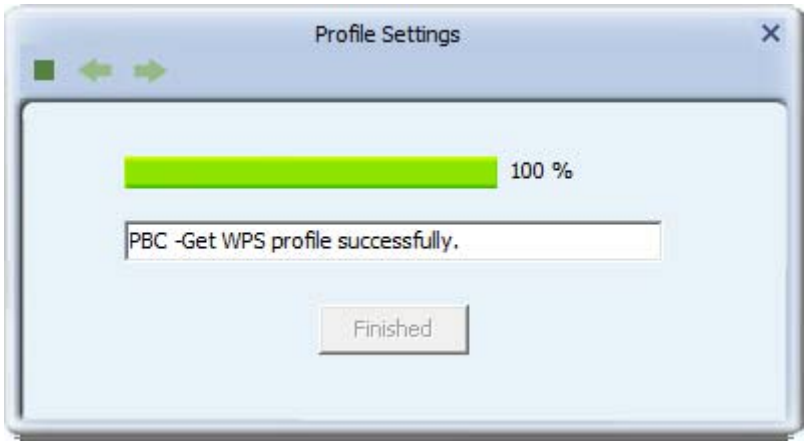


Figure 5-3-1-5

e. Once connected, your WPS profile appears in the Profile List screen of Wireless Adapter, and the "**Connect Successfully!**" message appears in the WNAP-7206.

Figure 5-3-1-6 Client – Profile List

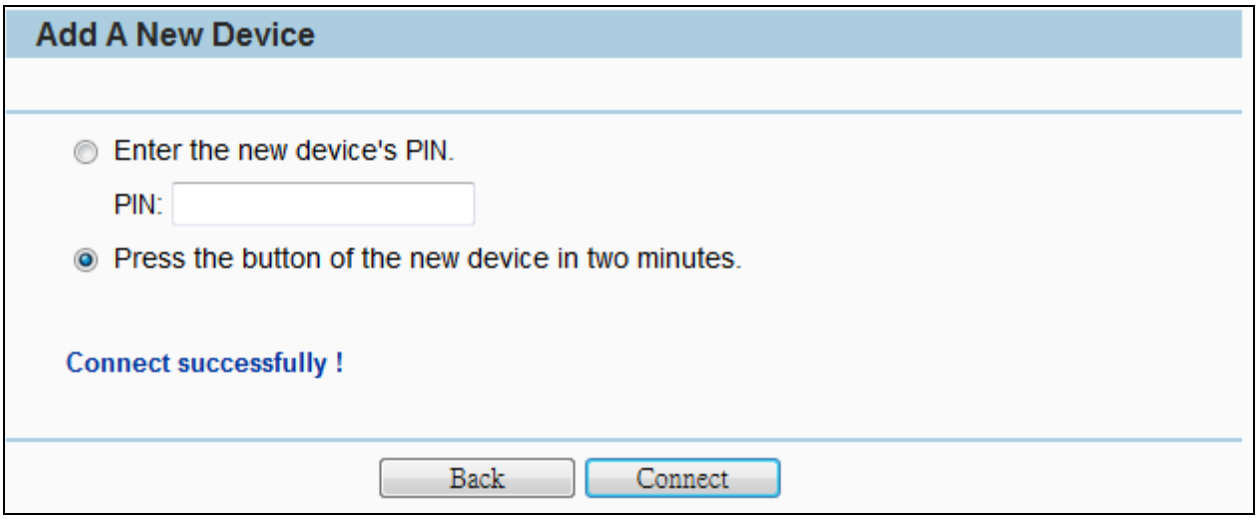


Figure 5-3-1-6 AP – PBC Connect Successfully

5.3.2 PIN Input Config (PIN)

If the device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN in the following two methods.

Method One: Enter the PIN into my AP

a. To use the PIN method, select "**PIN**" and, in the "**WPS AP List**" field, select the name of the network to which you connecting. Click the right arrow to save your settings.

Figure 5-3-2-1 Client – PIN

b. Record the PIN code of the Wireless Adapter.

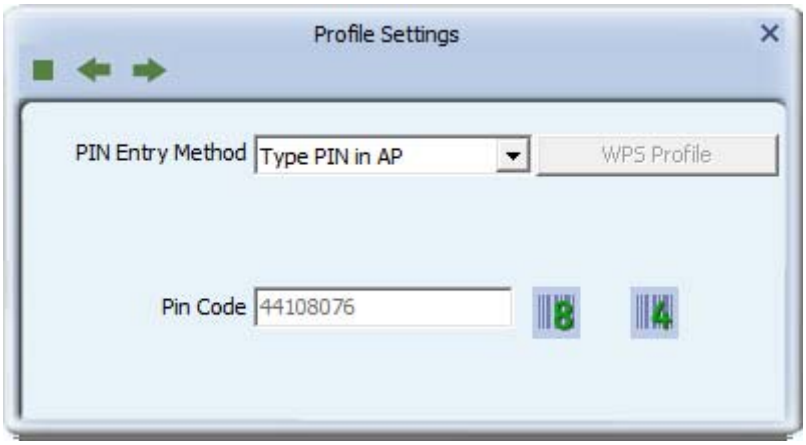


Figure 5-3-2-2 Client – Type PIN in AP

c. In the AP, enter the PIN Code of the Wireless Adapter. Click **Connect** to start the process.

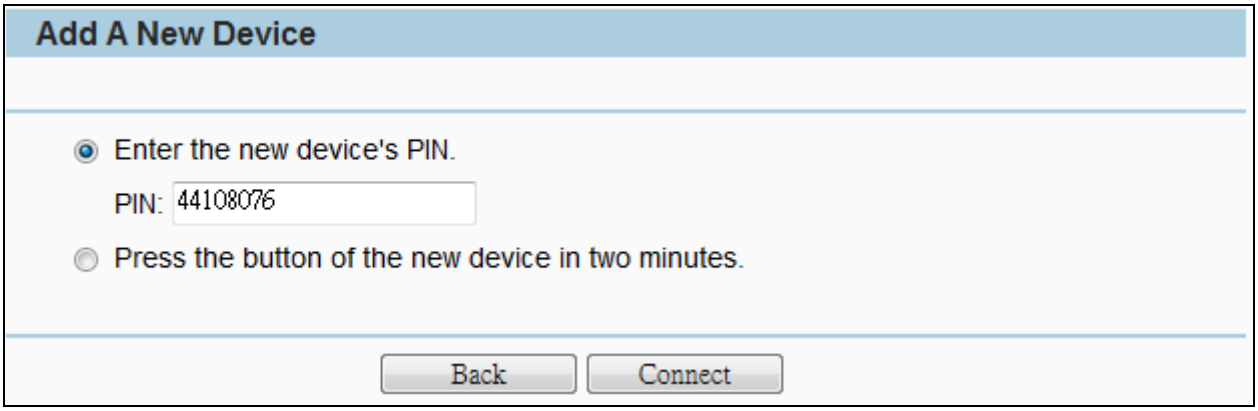


Figure 5-3-2-3 AP – Enter the new device's PIN

d. Click **Start PIN** in Wireless Adapter.

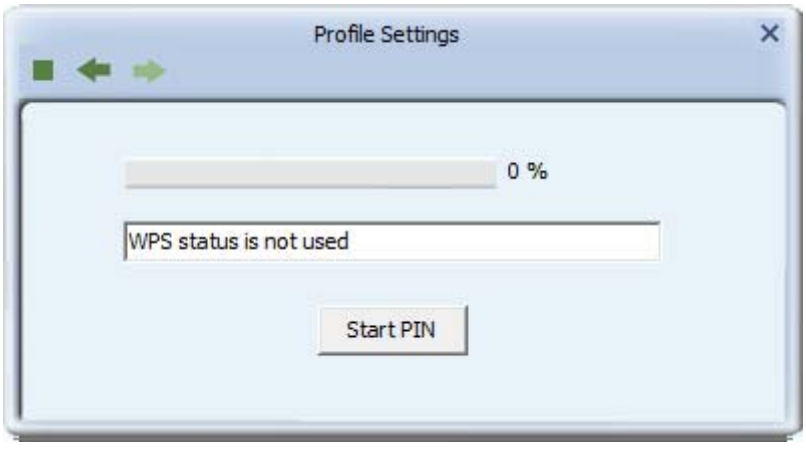


Figure 5-3-2-4 Client – Start PIN

e. Once connected, your WPS profile appears in the Profile List screen of Wireless Adapter, and the "**Connect Successfully!**" message appears in the WNAP-7206.

Figure 5-3-2-5 Client – Profile List

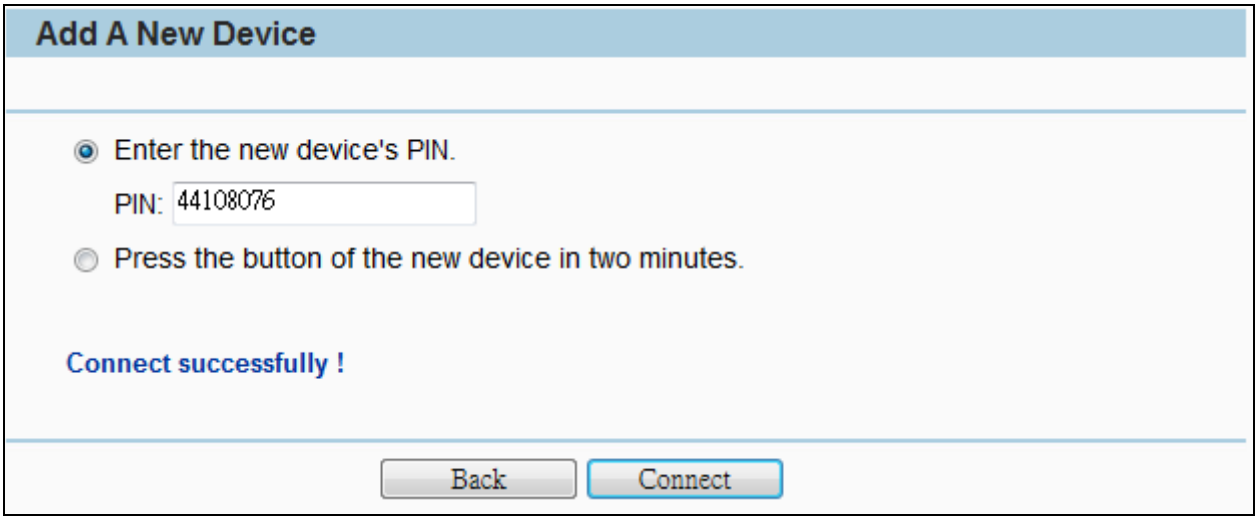


Figure 5-3-2-5 AP – PIN Connect Successfully

Method Two: Enter the PIN from my AP

a. Get the Current PIN code of the AP in **Figure 5-3-1** (Each AP has its unique PIN code. Here takes the default PIN code 12345670 of this AP for example).

b. In the Client, select "**PIN**" and, in the "**WPS AP List**" field, select the name of the network to which you connecting. Click the right arrow to save your settings.

Figure 5-3-2-6 Client – PIN

c. In the PIN Entry Method, select "**Type PIN below**", and enter the PIN Code of AP in the **PIN Code** field.

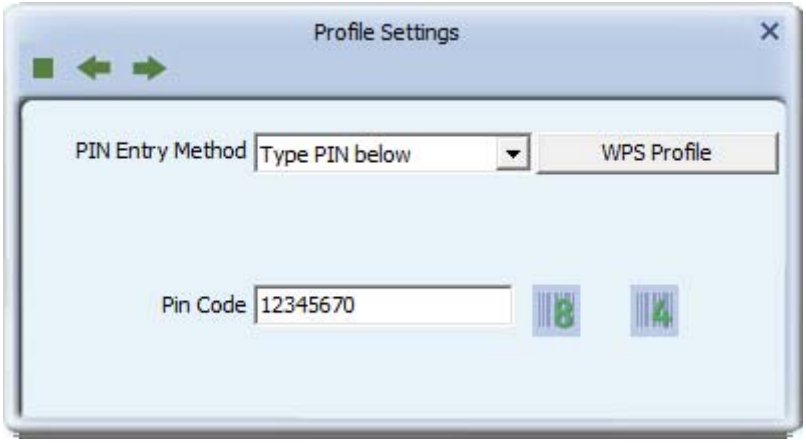


Figure 5-3-2-7 Client – Enter PIN Code

f. Go to next step, click **Start PIN**.

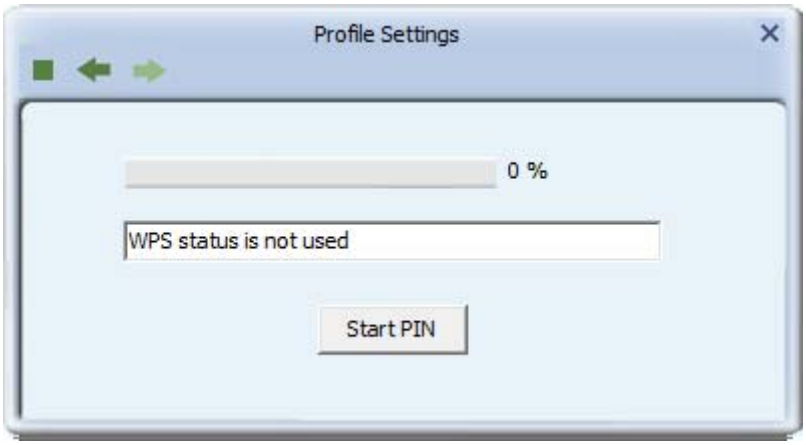


Figure 5-3-2-8 Client – Start PIN

d. In the AP, click **Connect**.

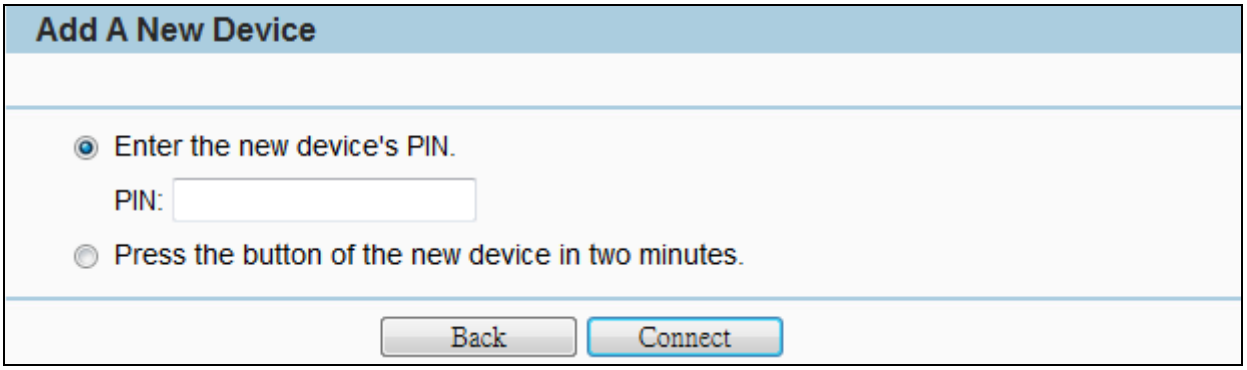


Figure 5-3-2-9 AP – PIN

e. Once connected, your WPS profile appears in the Profile List screen of Wireless Adapter, and the "**Connect Successfully!**" message appears in the WNAP-7206.

Figure 5-3-2-10 Client – Profile List

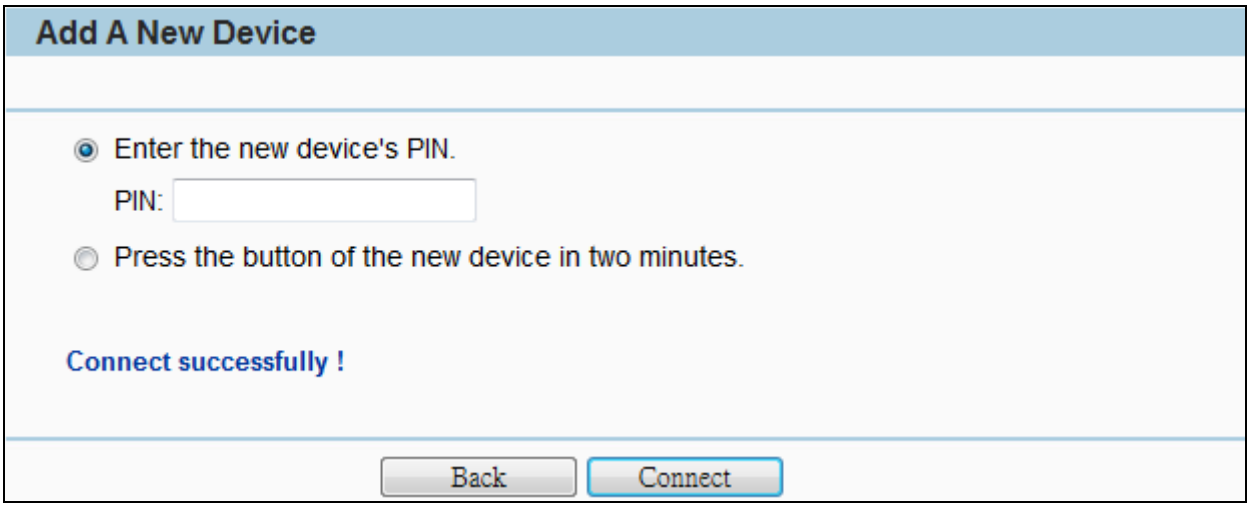


Figure 5-3-2-11 AP – PIN Connect Successfully

5.4 Operation Mode

There are 3 operation modes (Standard AP, AP Router, AP Client Router) can be configured to meet various applications.

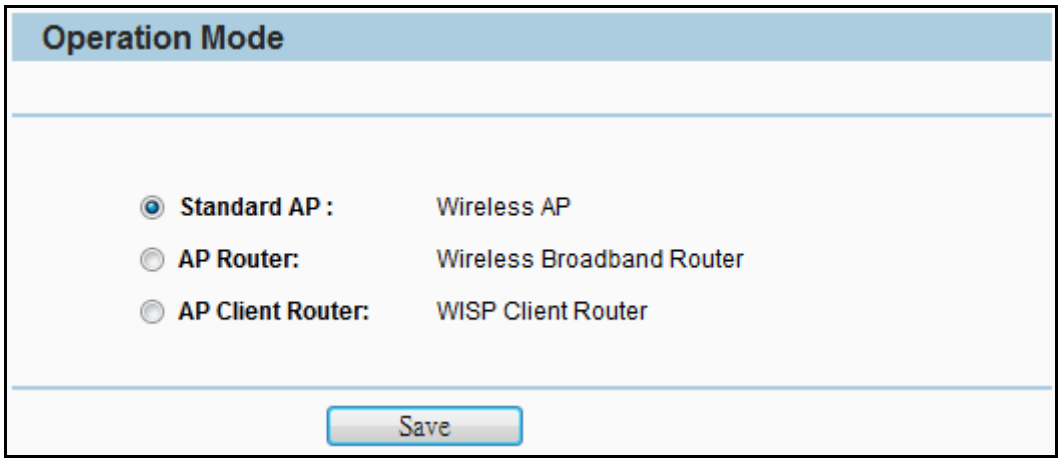


Figure 5-4-1 Operation Mode

The page includes the following fields:

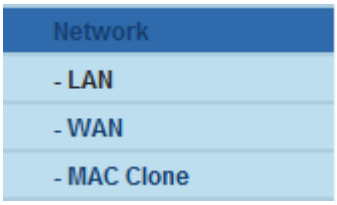
Object	Description
• **Standard AP**	In this mode, the device enables multi-users to access, and provides six wireless modes: **Access Point, Multi-SSID, Client, Repeater, Universal Repeater, and Bridge with AP**.
• **AP Router**	In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.
• **AP Client Router**	In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.

Be sure to click the **Save** button to save your settings on this page.

The Device will reboot automatically after you click the Save button.

5.5 Network

The **Network** option allows you to customize your local network manually by changing the default settings of the AP.



5.5.1 LAN

Selecting **Network > LAN** will enable you to configure the IP parameters of LAN on the following page.

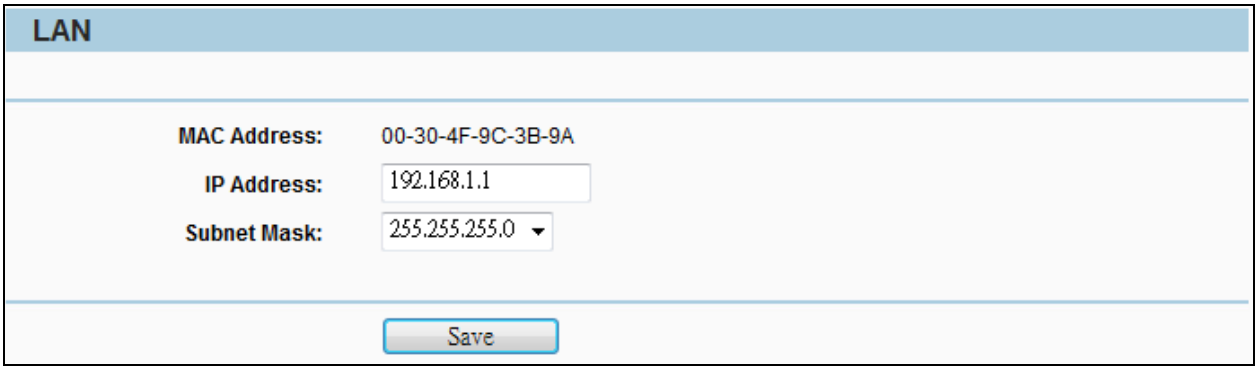


Figure 5-5-1 LAN

The page includes the following fields:

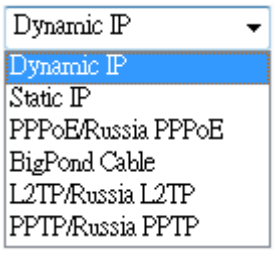
Object	Description
• **MAC Address**	Display the LAN port MAC address of the Wireless AP.
• **IP Address**	The Wireless AP's LAN IP. The default is **192.168.1.1**. You can change it according to your need.
• **Subnet Mask**	Enter the subnet mask of the LAN IP.

5.5.2 WAN

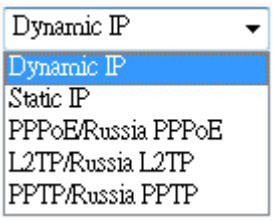
Choose menu "**Network > WAN**", and then you can configure the IP parameters of the WAN on the screen below.

WAN Connection Types:

a. AP Router Mode



b. AP Client Router Mode



5.5.2.1. Dynamic IP

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

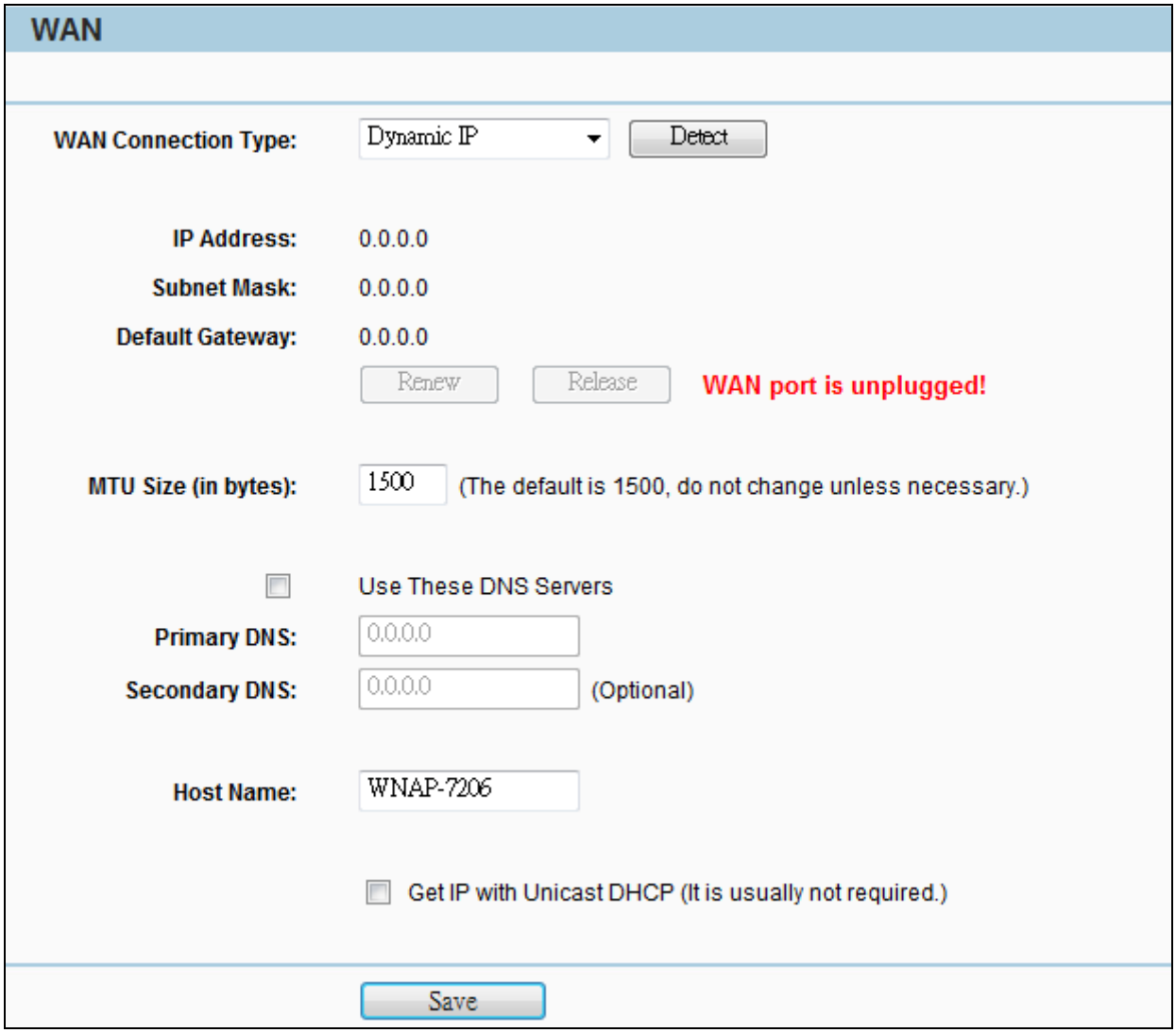


Figure 5-5-2 WAN - DHCP

The page includes the following fields:

Object	Description
• **WAN Connection Type**	Select **Dynamic IP** from the list.
• **IP Address**	The IP address assigned by your ISP dynamically.
• **Subnet Mask**	The subnet mask assigned by your ISP dynamically.
• **Default Gateway**	The default gateway assigned dynamically by your ISP.
• **Renew**	Click the **Renew** button to renew the IP parameters from your ISP.
• **Release**	Click the **Release** button to release the IP parameters. If you get **Address not found** error when you access a Web

	site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.
• **MTU Size (in bytes)**	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
• **Use These DNS Servers**	If your ISP gives you one or two DNS IP addresses, select **Use These DNS Servers** and enter the **Primary DNS** and **Secondary DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.
• **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.
• **Host Name**	This option specifies the Host Name of the AP Router.
• **Get IP with Unicast DHCP**	A few ISPs' DHCP servers do not support the broadcast applications. If you can't get the IP Address normally, you can choose Unicast. It is usually not required in generally condition.

5.5.2.2. Static IP

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

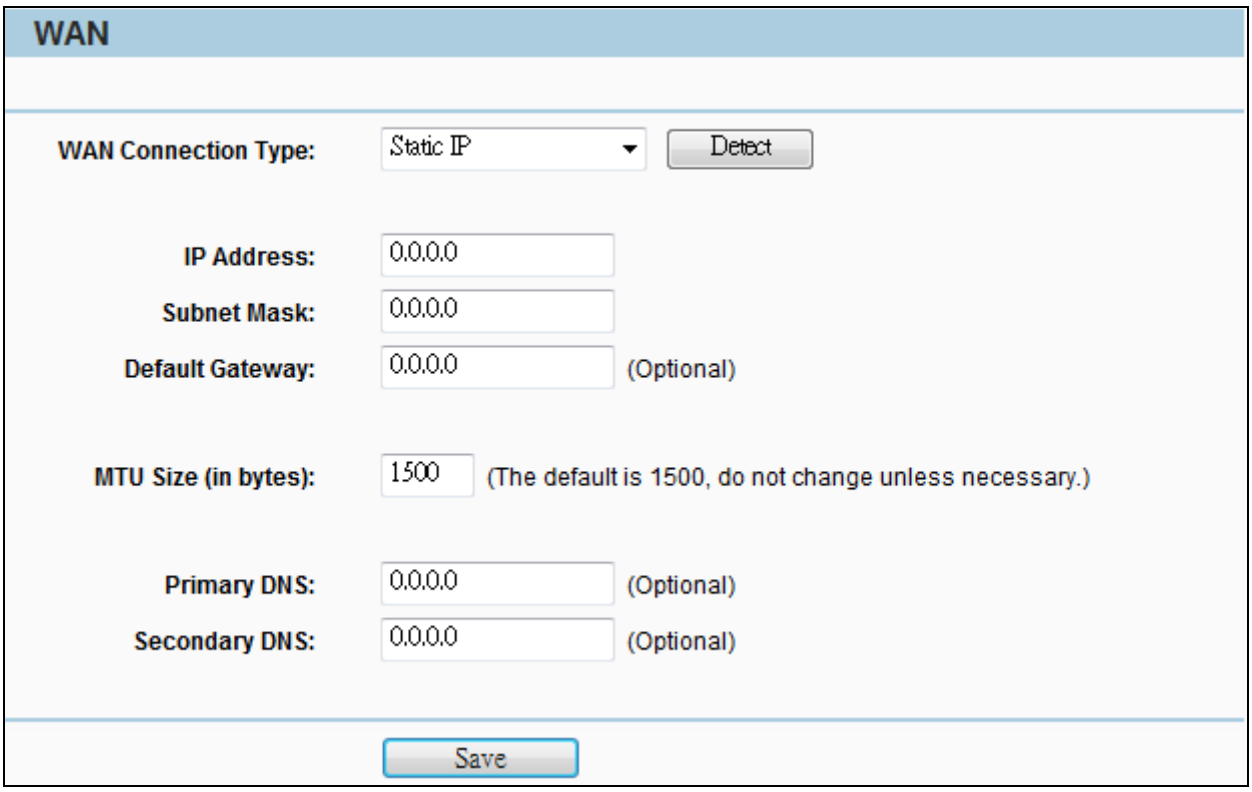


Figure 5-5-3 WAN – Static IP

The page includes the following fields:

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.
• **MTU Size (in bytes)**	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
• **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.

5.5.2.3. PPPoE/Russia PPPoE

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

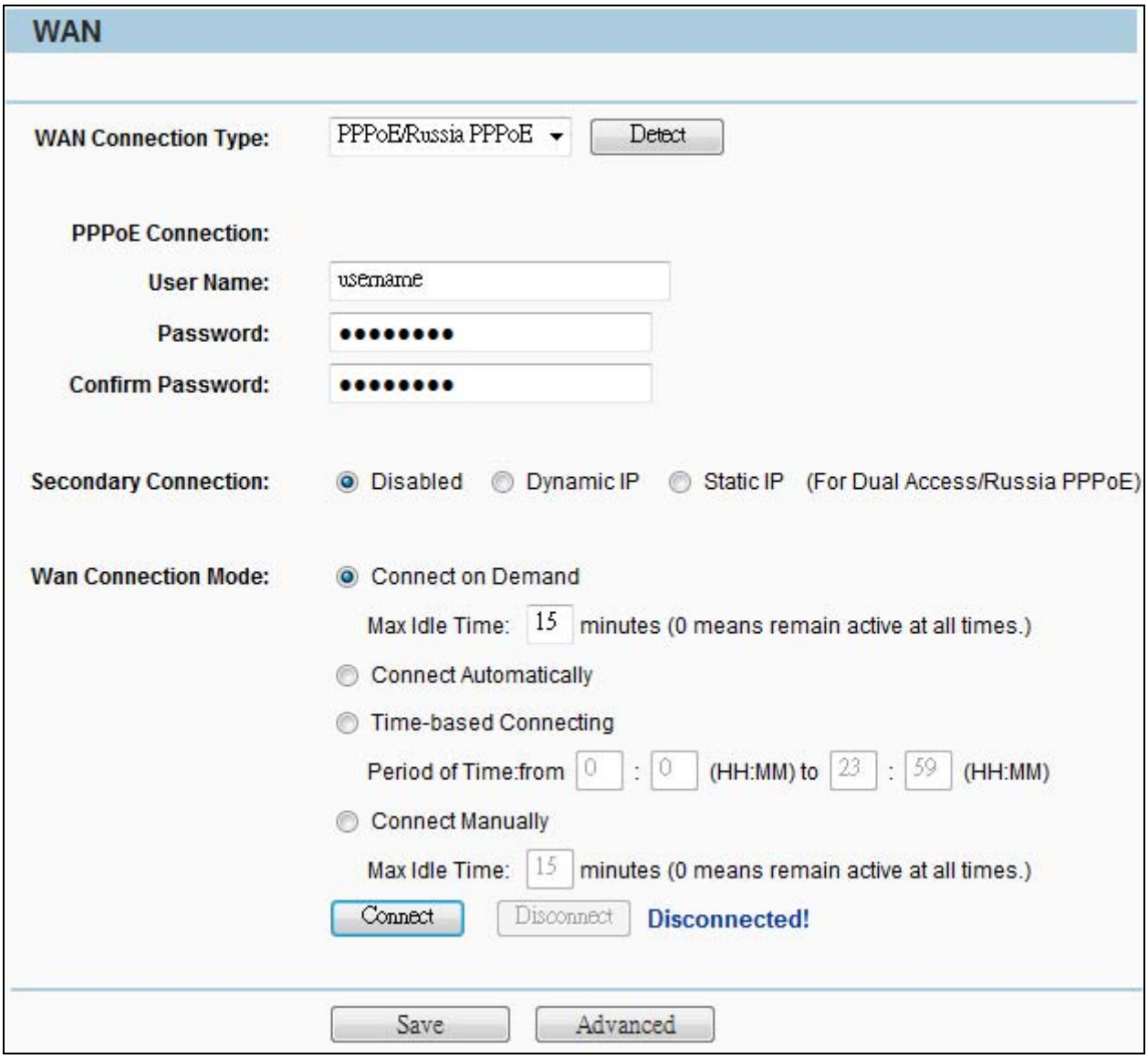


Figure 5-5-4 WAN – PPPoE

The page includes the following fields:

Object	Description
• **WAN Connections**	Select **PPPoE/Russia PPPoE** from the list.
PPPoE Connection	
• **User Name**	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
• **Password**	
• **Confirm Password**	Enter the same password entered above for the confirmation.
Secondary Connection	

• **Disabled**	The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
• **Dynamic IP**	Use dynamic IP address to connect to the local area network provided by ISP.
• **Static IP (For Dual Access/Russia PPPoE)**	Use static IP address to connect to the local area network provided by ISP.
Wan Connection Mode	
• **Connect on Demand**	You can configure the Device to disconnect your Internet connection after a specified period of the Internet connectivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Device to automatically re-establish your connection when you attempt to access the Internet again. If you wish to activate Connect on Demand, put a check mark in the circle. If you want your Internet connection to remain active all the time, enter 0 in the Max Idle Time field. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time (0~99 mins) because some applications visit the Internet continually in the background.
• **Connect Automatically**	Connect automatically after the Device is disconnected. To use this option, click the radio button.
• **Time-based Connecting**	You can configure the Device to make it connect or disconnect based on time. Enter the start time in HH-MM for connecting and end time in HH-MM for disconnecting in the Period of Time fields.
• **Connect Manually**	You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Device will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active all the times, enter 0 in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.
• **Connect**	Click the **Connect** button to connect immediately.
• **Disconnect**	Click the **Disconnect** button to disconnect immediately.
• **Save**	Click the **Save** button to save your settings.

• **Advanced**	Click the **Advanced** button to set up the advanced options.

If you want to do some advanced configurations, please click the **Advanced** button, and then the page shown in **Figure 5-5-5** will appear.

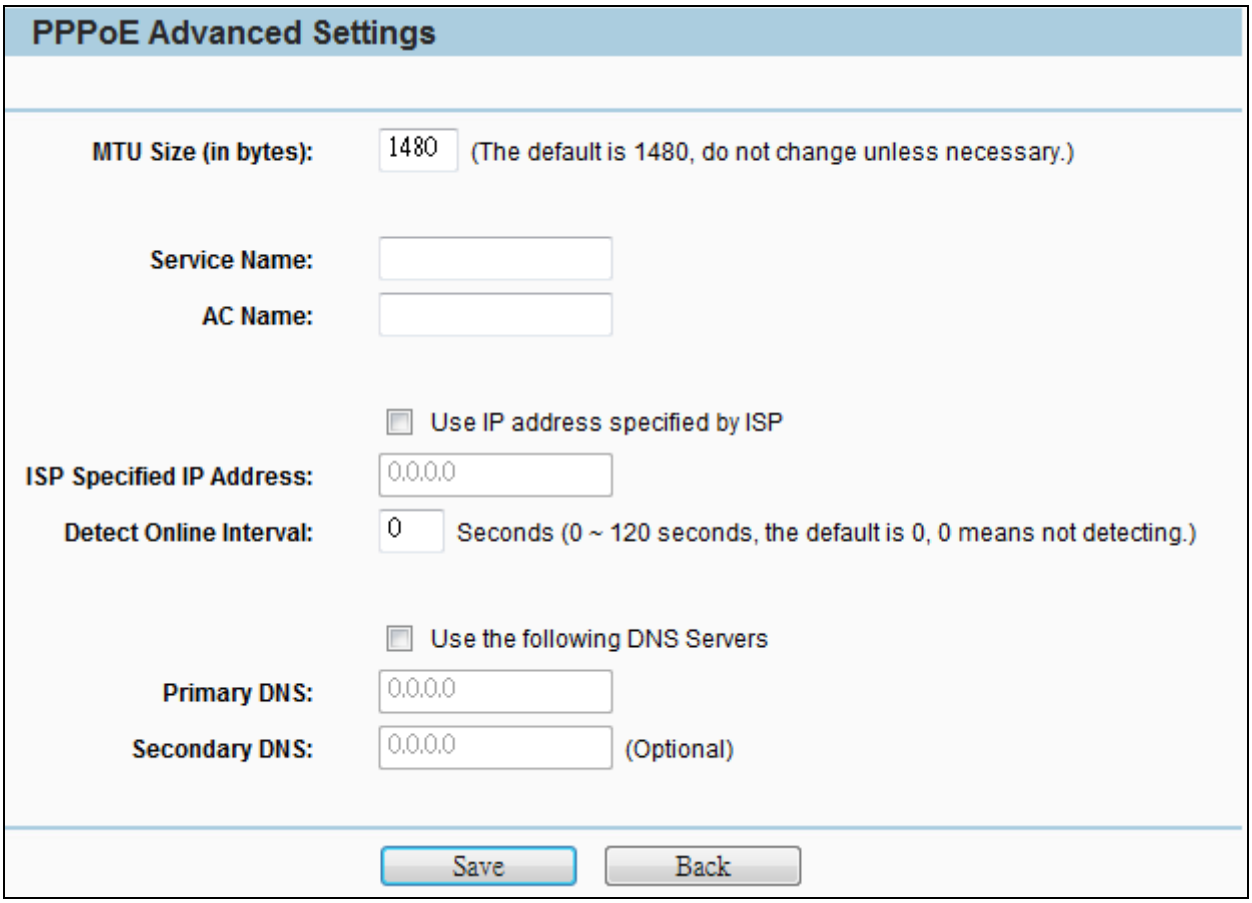


Figure 5-5-5 PPPoE - Advanced

The page includes the following fields:

Object	Description
• **MTU Size**	The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
• **Service Name/AC Name**	They should not be done unless you are sure it is necessary for your ISP.
• **ISP Specified IP Address**	If you know that your ISP does not automatically transmit IP address to the Device during login, click "Use the IP Address specified by ISP" checkbutton and enter the IP address in dotted-decimal notation, which is provided by your ISP.
• **Detect Online Interval**	The default value is 0. You can input the value between 0 and

	120. The Device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.
• **Use the following DNS Servers**	If your ISP specifies a DNS server IP address for you, click the checkbox, and fill the Primary DNS and Secondary DNS blanks below. The Secondary DNS is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
• **Primary DNS**	(Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
• **Secondary DNS**	(Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.
• **Save**	Click the **Save** button to save your settings.
• **Back**	Click the **Back** button when finished.

The new advanced PPPoE parameters will not take effect until you dial-up again.

5.5.2.4. L2TP/Russia L2TP

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

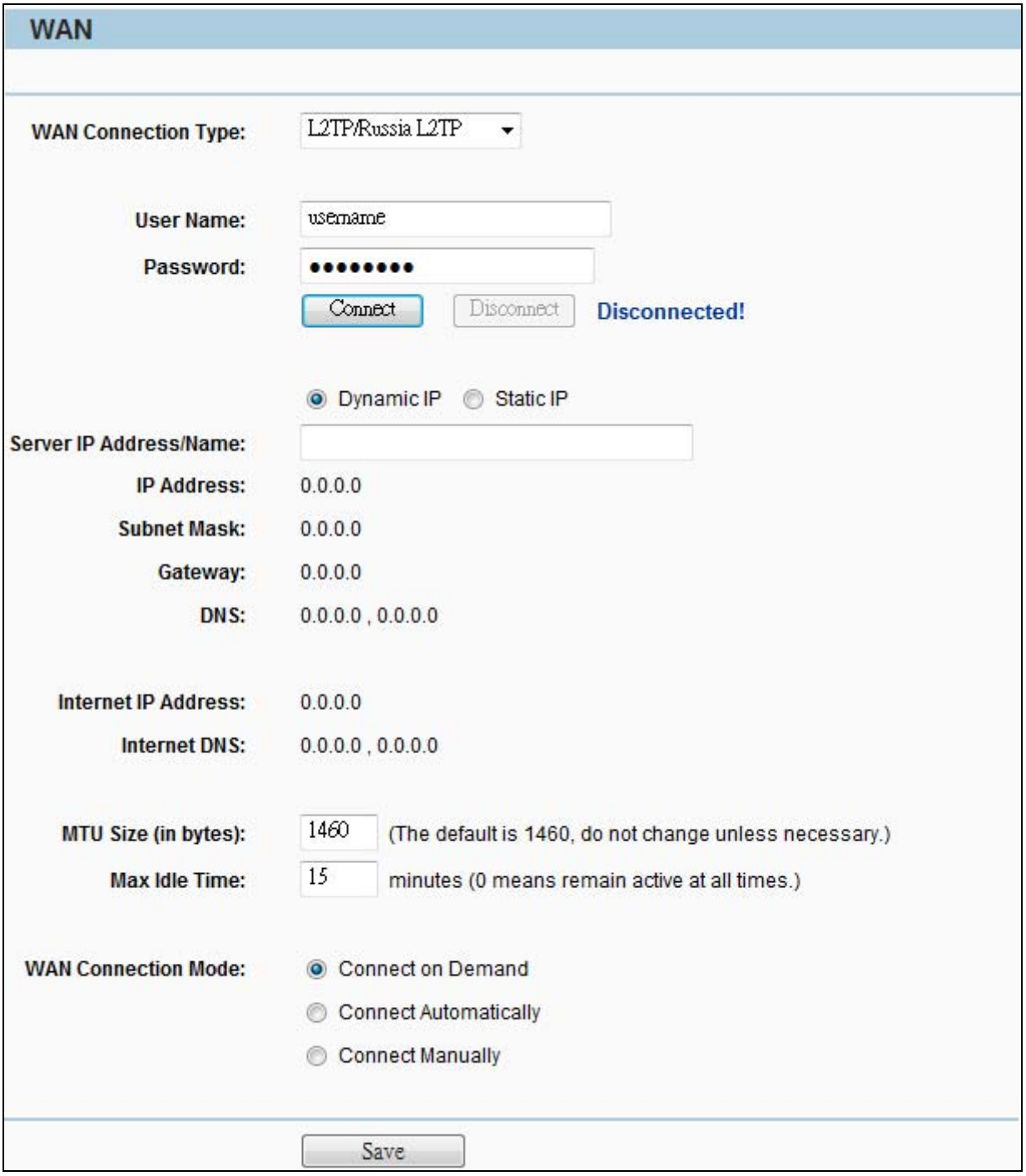


Figure 5-5-6 L2TP

The page includes the following fields:

Object	Description
• **WAN Connections**	Select **L2TP/Russia L2TP** from the list.
• **User Name**	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
• **Password**	
• **Dynamic IP/ Static IP**	Choose either one as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.

• **Server IP Address/Name**	Enter the Server IP address or domain name provided by your ISP.
• **IP Address**	Enter the IP address used for dial-up. (Only can be configured when Static IP is selected)
• **Subnet Mask**	Enter the subnet Mask provided by your ISP. (Only can be configured when Static IP is selected)
• **Gateway**	Enter gateway provided by your ISP. (Only can be configured when Static IP is selected)
• **DNS**	Enter DNS Server provided by your ISP. (Only can be configured when Static IP is selected)
• **Internet IP Address**	The Internet IP address assigned by L2TP server.
• **Internet DNS**	The Internet DNS server address assigned by L2TP server.
• **MTU Size (in bytes)**	The default MTU (Maximum Transmission Unit) value is 1460 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
• **Max Idle Time**	You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If you want your Internet connection to remain active at all time, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
• **Connect on Demand**	If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, check the radio button.
• **Connect Automatically**	Connect automatically after the Device is disconnected. To use this option, check the radio button.
• **Connect Manually**	You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all time, enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.
• **Save**	Click the **Save** button to save your settings.

Note

Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, because some applications are visiting the Internet continually in the background.

5.5.2.5. PPTP/Russia PPTP

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

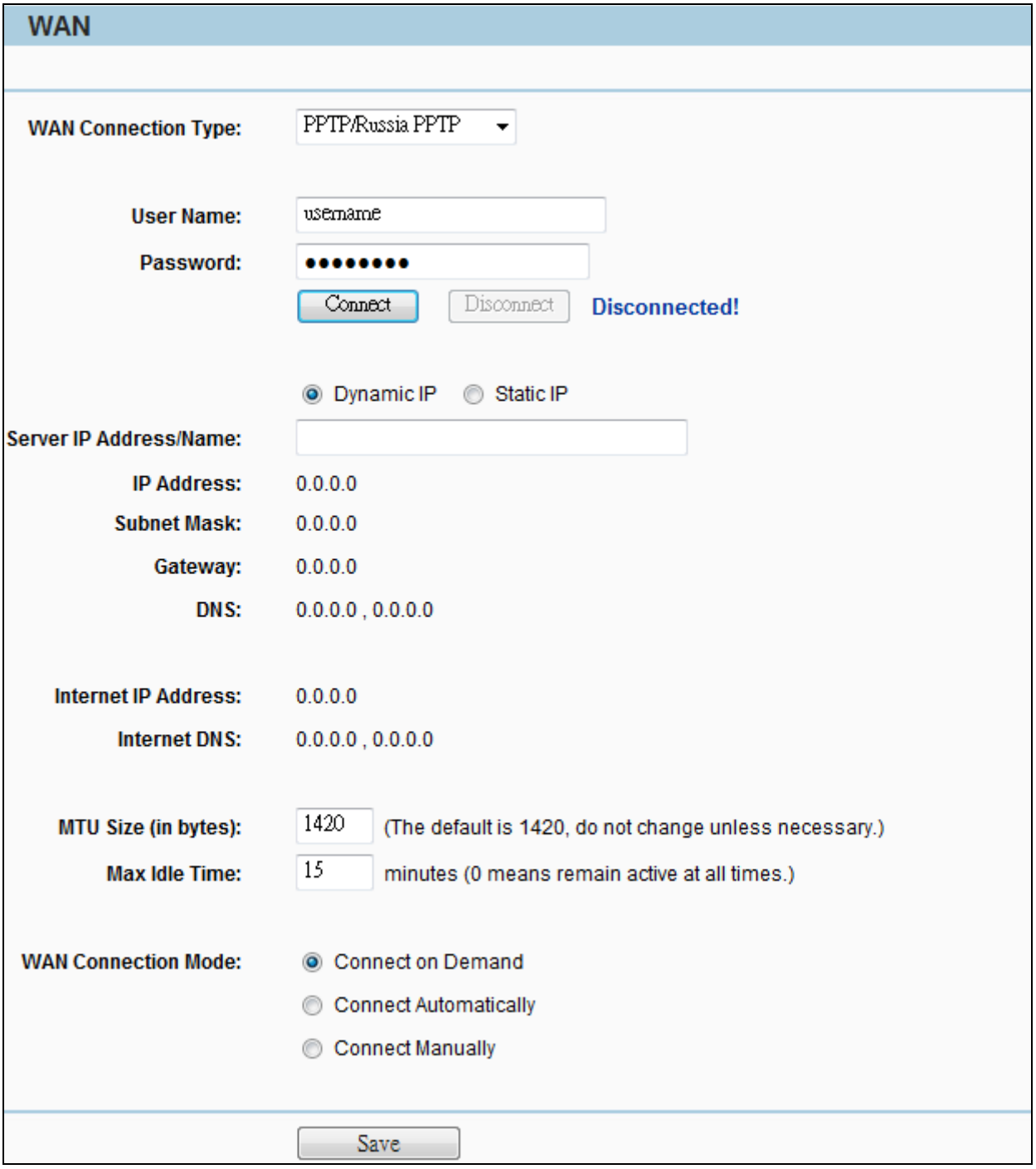


Figure 5-5-7 PPTP

The page includes the following fields:

Object	Description
• **WAN Connections**	Select **PPTP/Russia PPTP** from the list.
• **User Name**	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
• **Password**	
• **Dynamic IP/ Static IP**	Choose either one as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
• **Server IP Address/Name**	Enter the Server IP address or domain name provided by your ISP.
• **IP Address**	Enter the IP address used for dial-up. (Only can be configured when Static IP is selected)
• **Subnet Mask**	Enter the subnet Mask provided by your ISP. (Only can be configured when Static IP is selected)
• **Gateway**	Enter gateway provided by your ISP. (Only can be configured when Static IP is selected)
• **DNS**	Enter DNS Server provided by your ISP. (Only can be configured when Static IP is selected)
• **Internet IP Address**	The Internet IP address assigned by PPTP server.
• **Internet DNS**	The Internet DNS server address assigned by PPTP server.
• **MTU Size (in bytes)**	The default MTU (Maximum Transmission Unit) value is 1420 Bytes. For some ISPs you need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
• **Max Idle Time**	You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If you want your Internet connection to remain active at all time, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
• **Connect on Demand**	If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, check the radio button.
• **Connect Automatically**	Connect automatically after the Device is disconnected. To use this option, check the radio button.
• **Connect Manually**	You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want

	your Internet connection to remain active at all time, enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.
• **Save**	Click the **Save** button to save your settings.

Note

Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, because some applications are visiting the Internet continually in the background.

5.5.2.6. BigPond Cable

If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option. And then you should enter the following parameters.

This type of WAN Connection is only available in **AP Router** mode, but not in **AP Client Router** Mode.

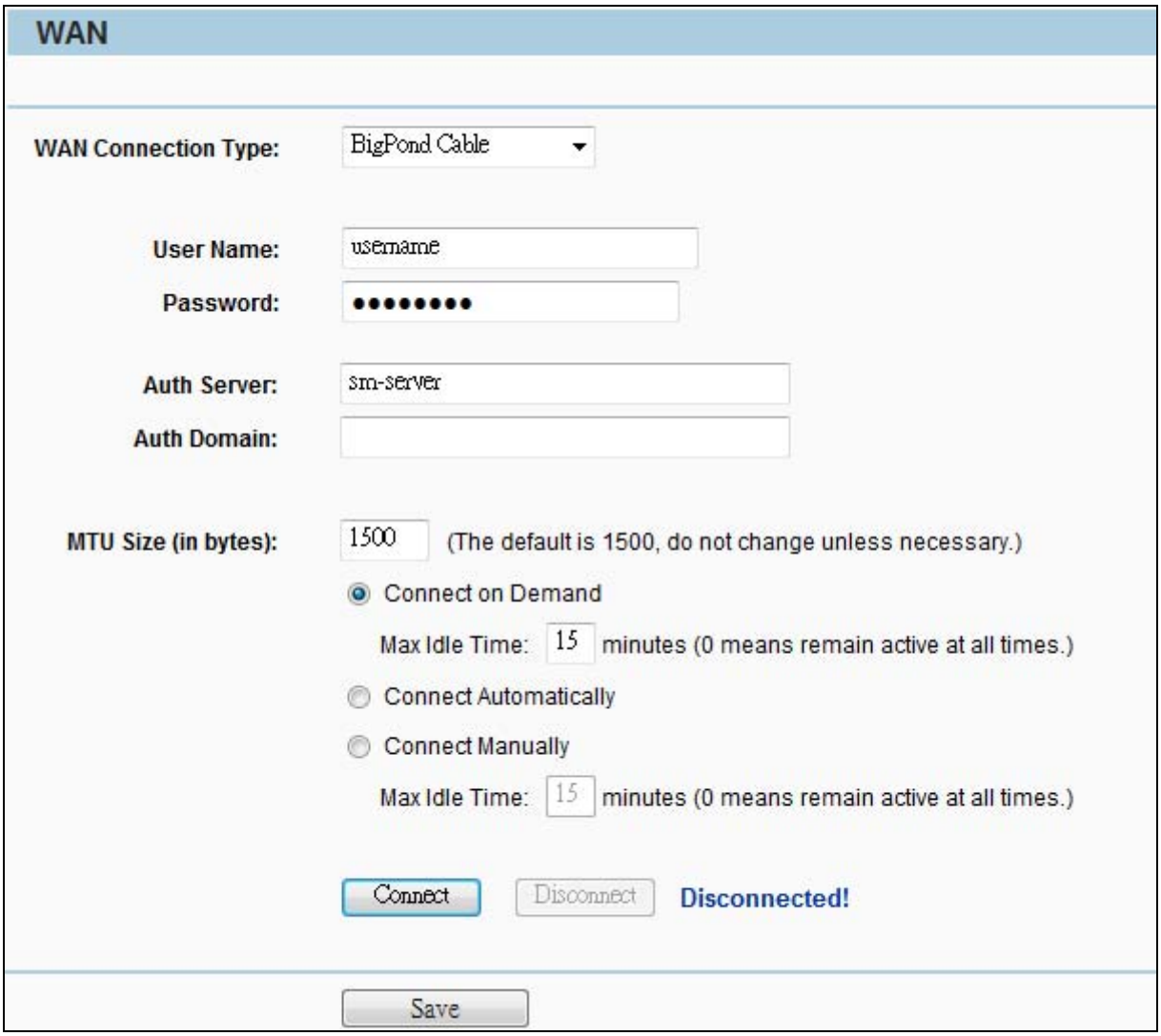


Figure 5-5-8 BigPond Cable

The page includes the following fields:

Object	Description
• **WAN Connections**	Select **BigPond Cable** from the list.
• **User Name**	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
• **Password**	
• **Auth Server**	Enter the authenticating server IP address or host name.
• **Auth Domain**	Type in the domain suffix server name based on your location. NSW / ACT - **nsw.bigpond.net.au** VIC / TAS / WA / SA / NT - **vic.bigpond.net.au** QLD - **qld.bigpond.net.au**
• **MTU Size (in bytes)**	The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
• **Connect on Demand**	In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
• **Connect Automatically**	Connect automatically after the Device is disconnected. To use this option, check the radio button.
• **Connect Manually**	You can click the Connect/Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.
• **Connect**	Click the **Connect** button to connect immediately.
• **Disconnect**	Click the **Disconnect** button to disconnect immediately.
• **Save**	Click the **Save** button to save your settings.

Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, because some applications are visiting the Internet continually in the background.

5.5.3 MAC Clone

Choose menu "**Network > MAC Clone**", and then you can configure the **WAN MAC Address** on the screen below, as shown in **Figure 5-5-8**.

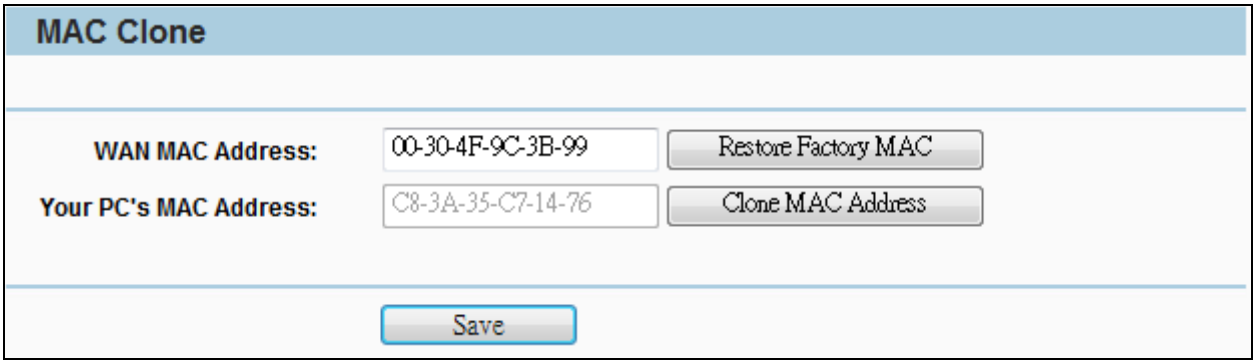


Figure 5-5-8 MAC Clone

The page includes the following fields:

Object	Description
• **WAN MAC Address**	This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address of your adapter, please enter the correct MAC address into this field. Usually, you do not need to change anything here. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
• **Your PC's MAC Address**	This field displays the MAC address of the PC that is managing the Device. If the MAC address of your adapter is registered, you can click the **Clone MAC Address** button, and then it will be filled into the WAN MAC Address field.
• **Restore Factory MAC**	Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.
• **Save**	Click the **Save** button to save your settings.

Note

1. Only the PC(s) in your LAN can use the MAC Address Clone feature.
2. If you change WAN MAC Address when the WAN connection type is PPPoE, it will not take effect until the connection is re-established.

5.6 Wireless

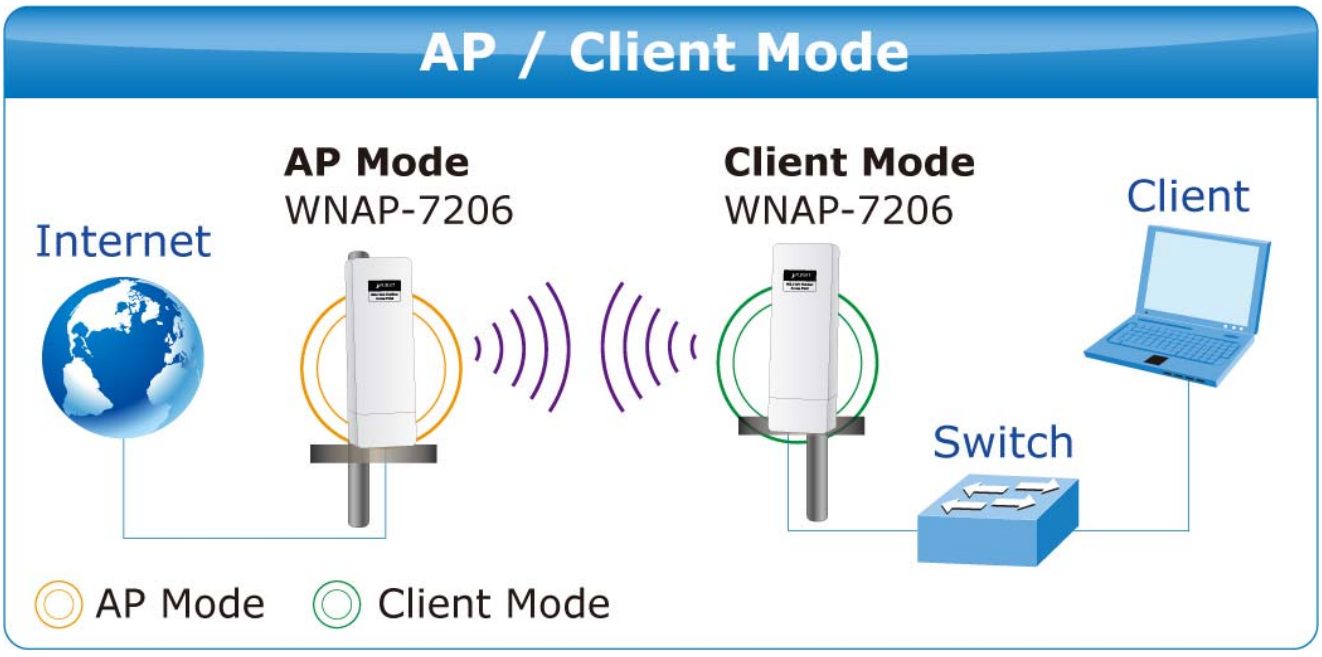
You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

5.6.1 Wireless Settings

Choose menu "**Wireless > Wireless Settings**", and then you can configure the basic settings for the wireless network on the Wireless Settings page

The Wireless Settings page in **Standard AP** mode allows you to configure the wireless mode for your device. Six operation modes are supported here, including **Access Point, Multi-SSID, Client, Repeater, Universal Repeater and Bridge with AP.**

5.6.1.1. Access Point Mode



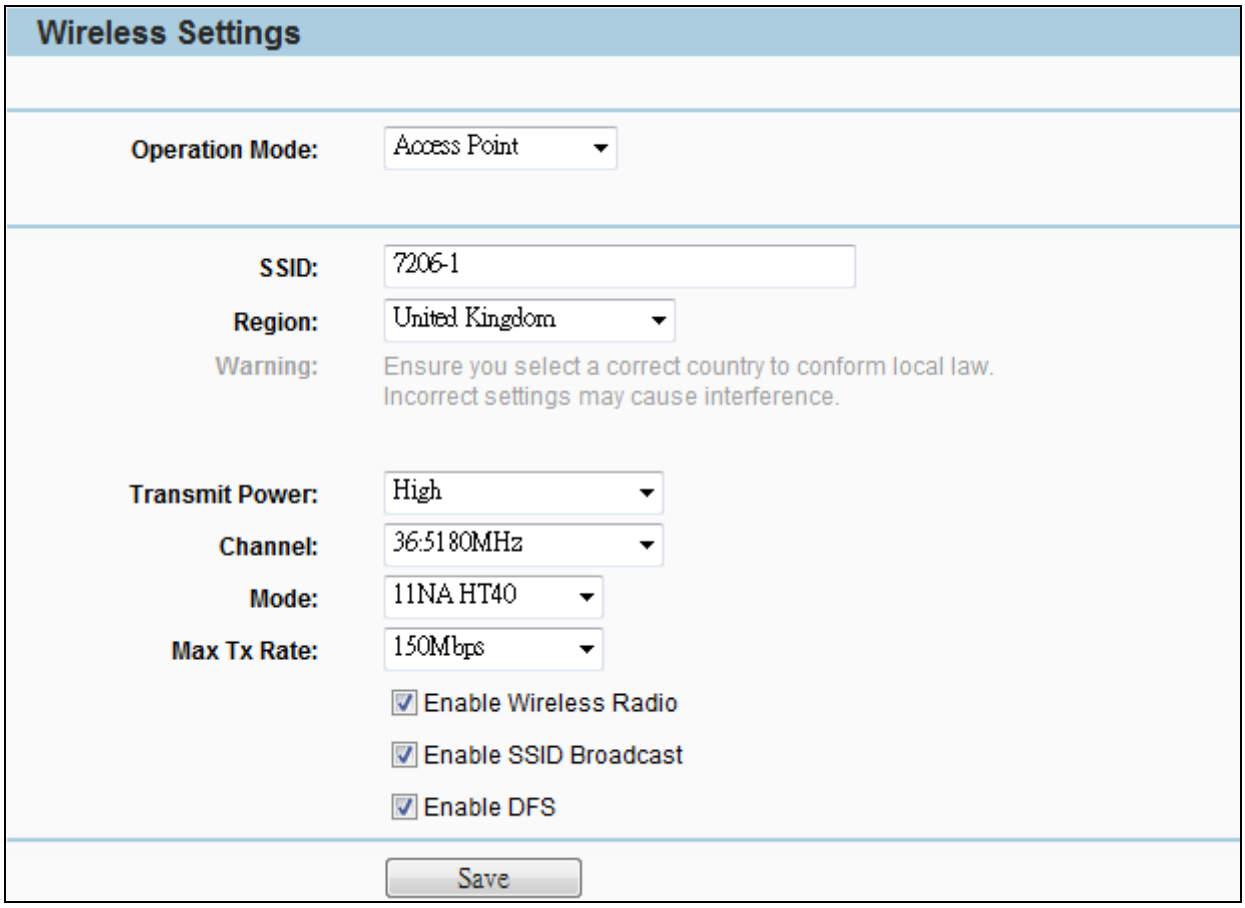


Figure 5-6-1-1 AP Mode

Note

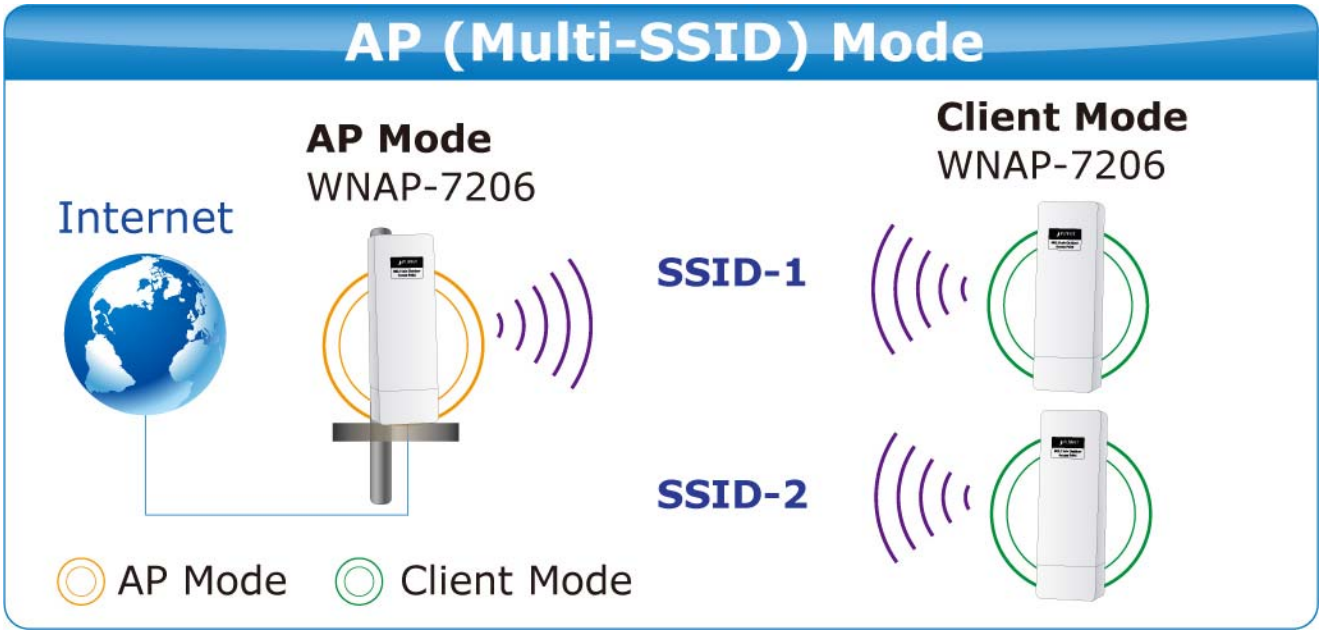
First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

Object	Description
• **SSID**	Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **default**. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Channel**	This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
• **Mode**	This field determines the wireless mode which the Device works on.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable SSID Broadcast**	If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.2. Multi-SSID Mode



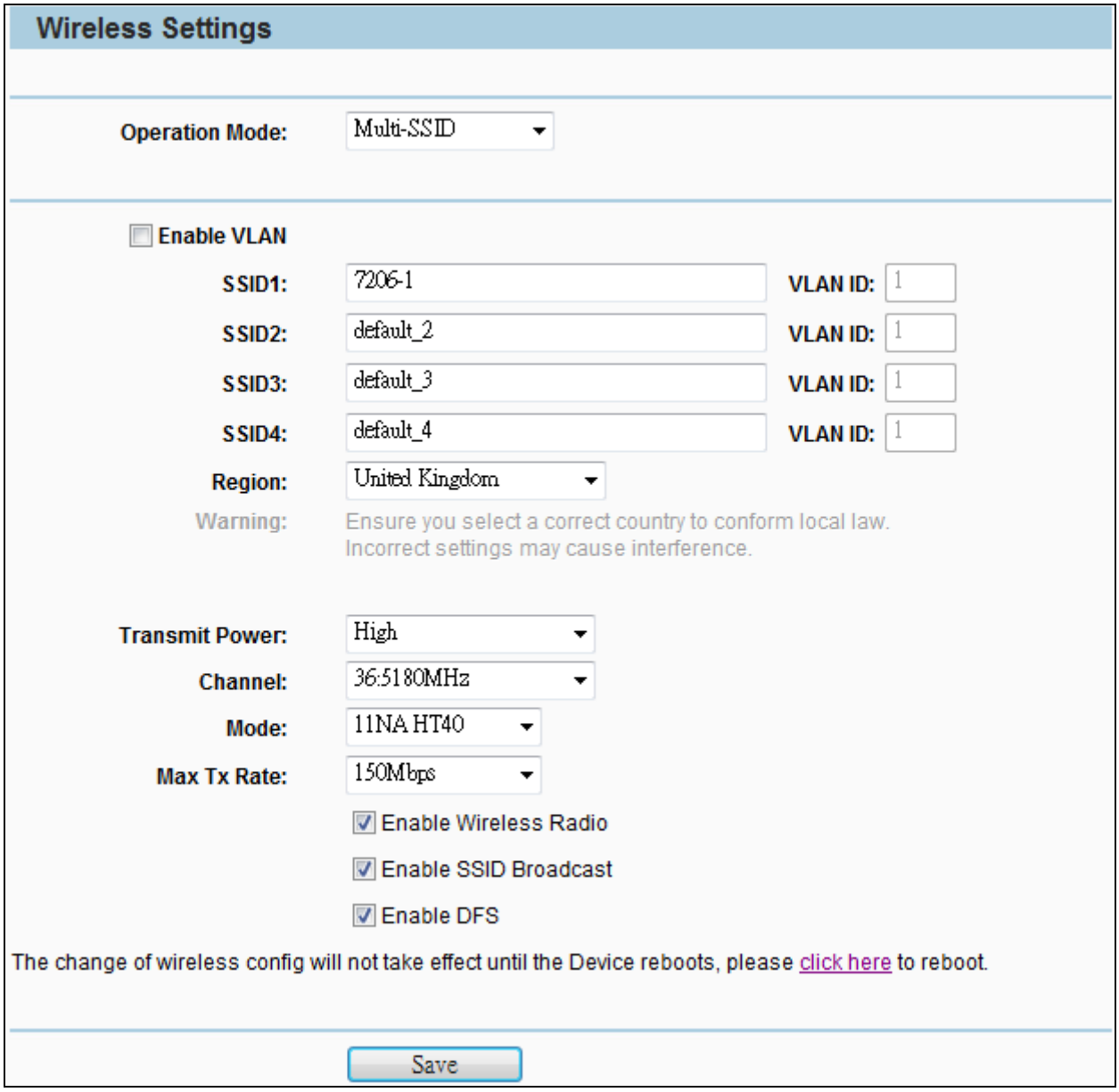


Figure 5-6-1-2 Multi-SSID Mode

Note

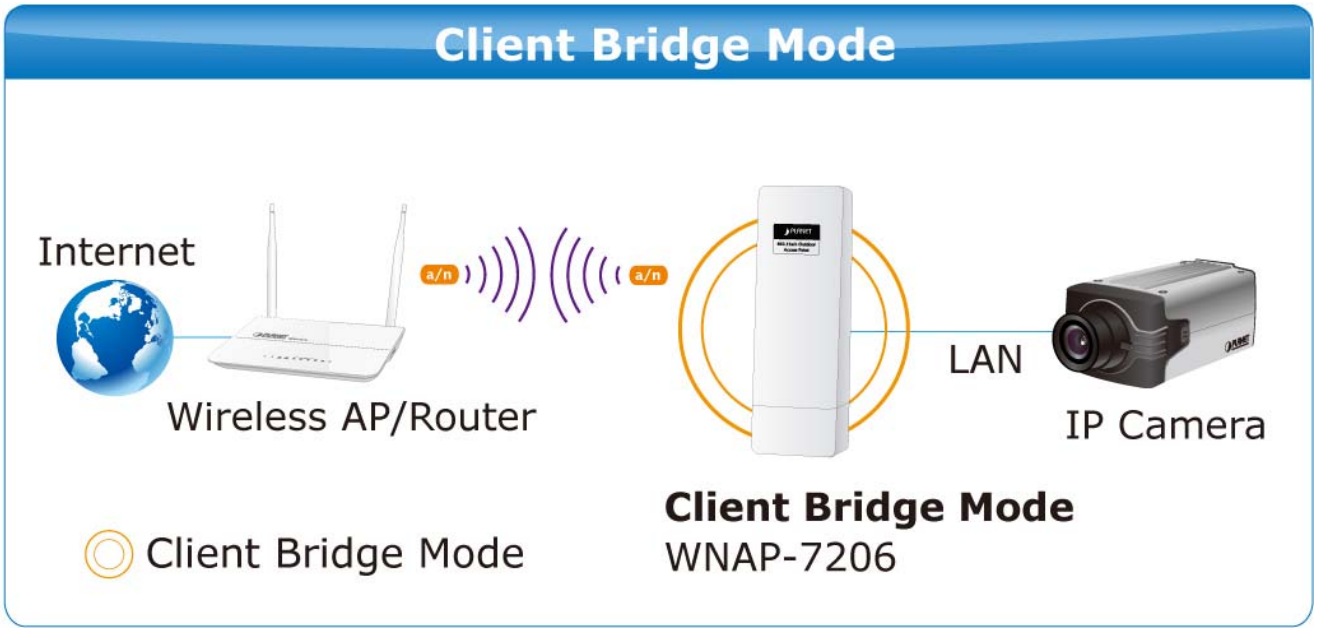
First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

Object	Description
• **Enable VLAN**	Check this box to enable the VLAN function. The AP supports up to 4 VLANs. All wireless PCs in the VLANs are able to access this AP. The AP can also work with an IEEE 802.1Q Tag VLAN supporting Switch. If this Switch enables the Tag VLAN function, besides all wireless PCs, only the PCs in the VLAN same with SSID1 are able to access the AP. If a PC is

	directly connected to the LAN port of the AP, please make sure that its adapter supports Tag function, or this PC will not be able to access the AP.
• **SSID**	Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. In Multi-SSID operation mode, enter SSID for each BSS in the field "SSID1" ~ "SSID4".
• **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.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Channel**	This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
• **Mode**	This field determines the wireless mode which the Device works on.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable SSID Broadcast**	If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.3. Client Mode (Client Bridge)



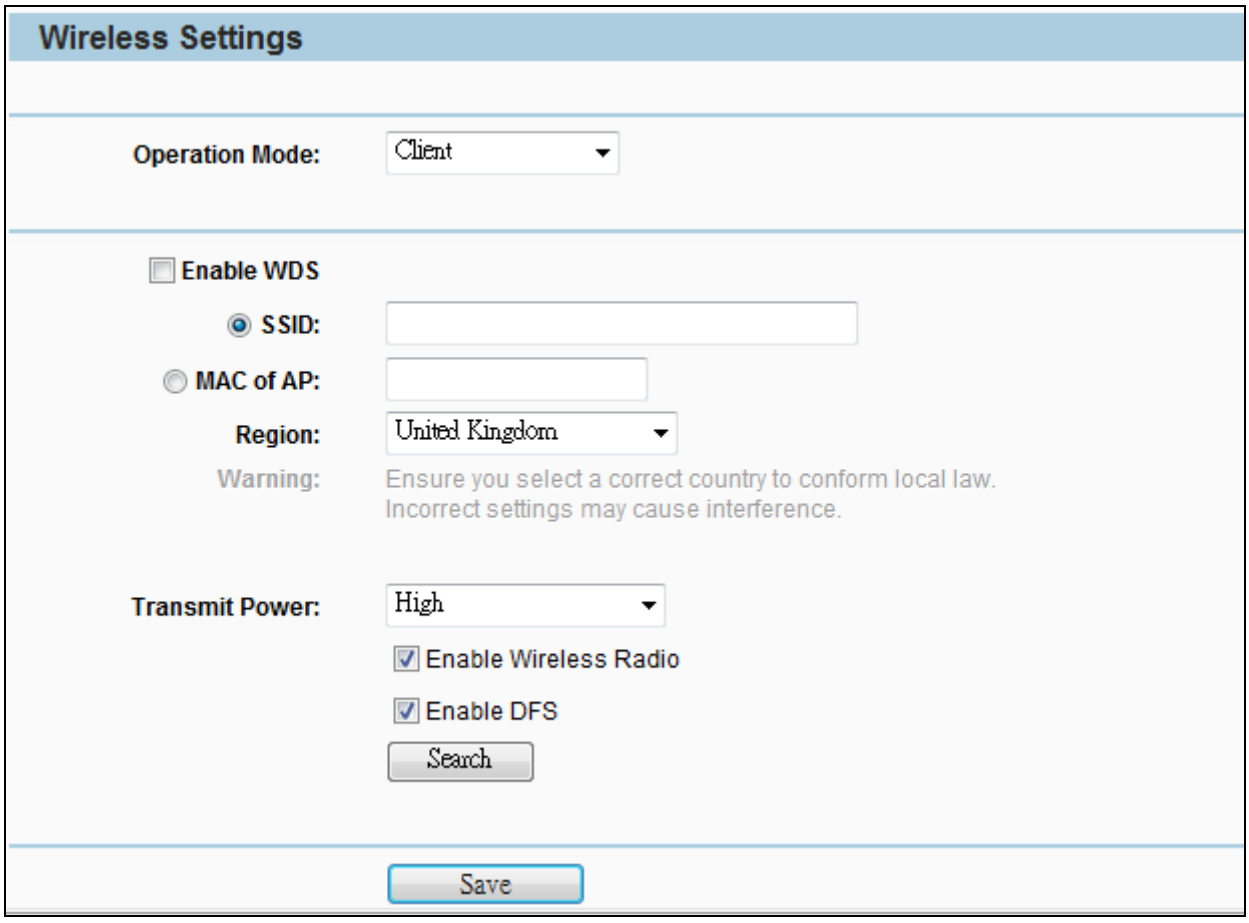


Figure 5-6-1-3 Client Mode

Note

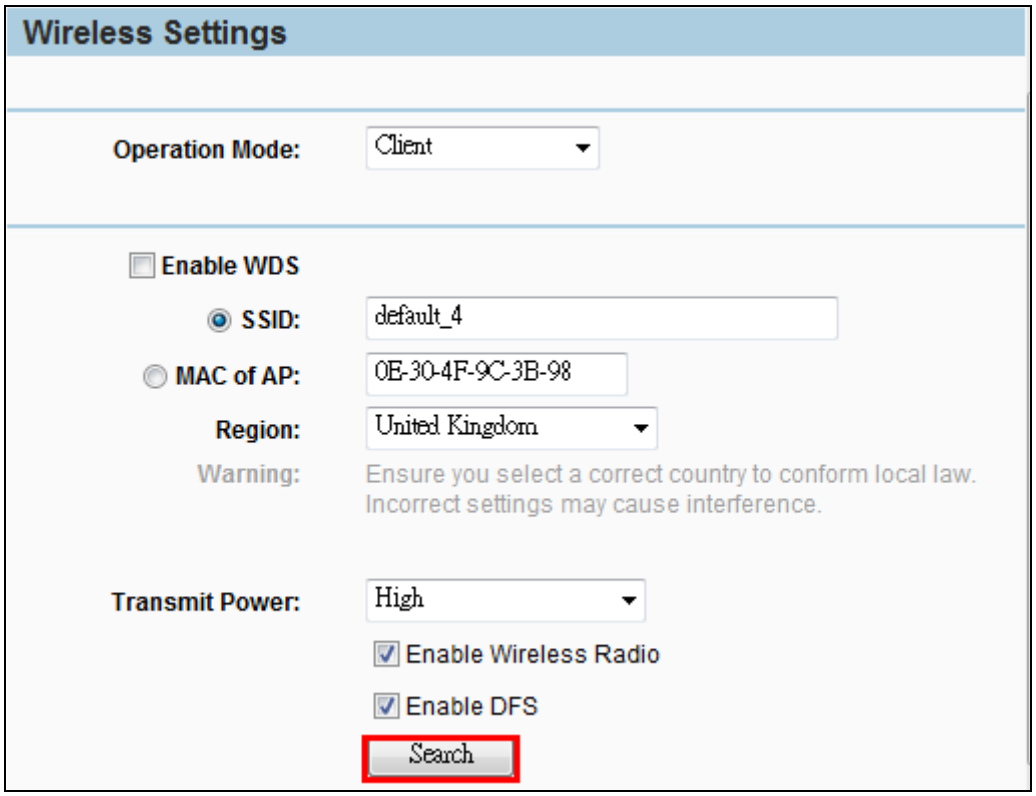
First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

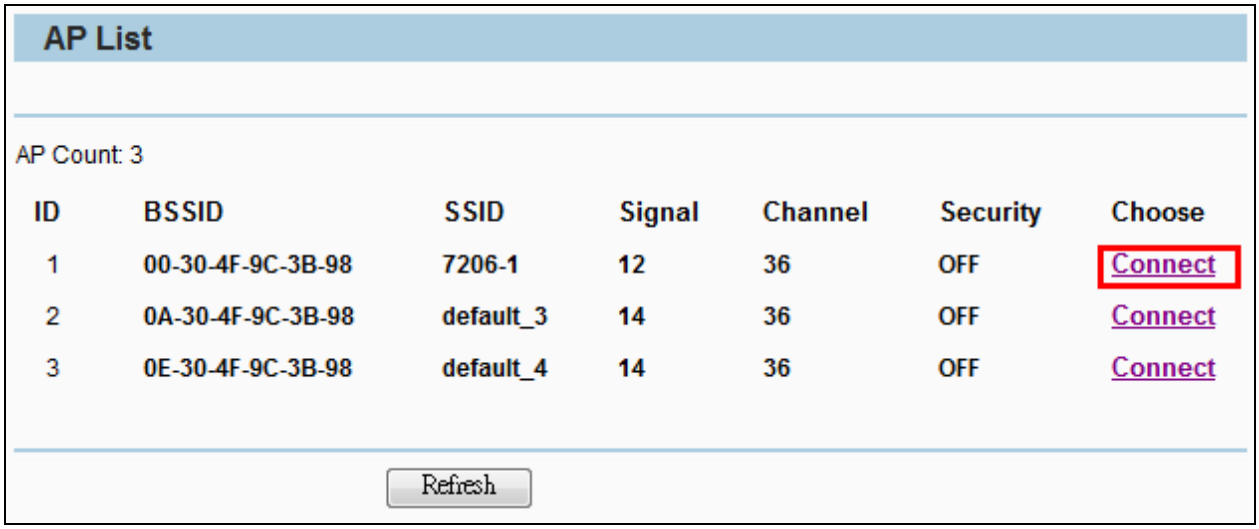
Object	Description
• **Enable WDS**	The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please enable this option.
• **SSID**	The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select a SSID to join. If you know the SSID of the desired AP, you can also input it to the field "SSID" manually.
• **MAC of AP**	The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Search**	Click this button; you can search the AP which runs in the current channel.
• **Save**	Click the **Save** button to save your settings on this page.

To establish connection with remote AP, please follow the instructions as below:

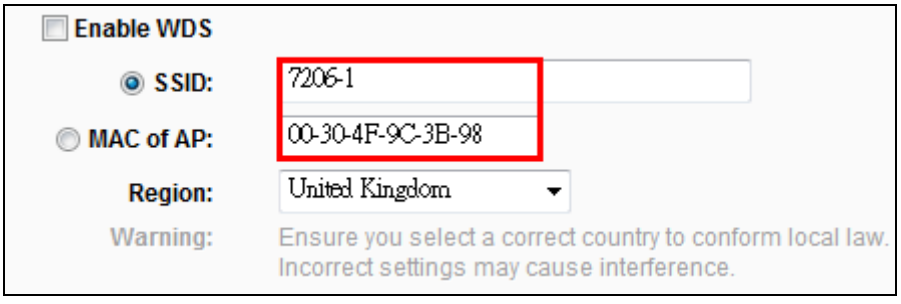
1. Click **Search** button.



2. In the AP List, select the AP you want to access, and click **Connect**.



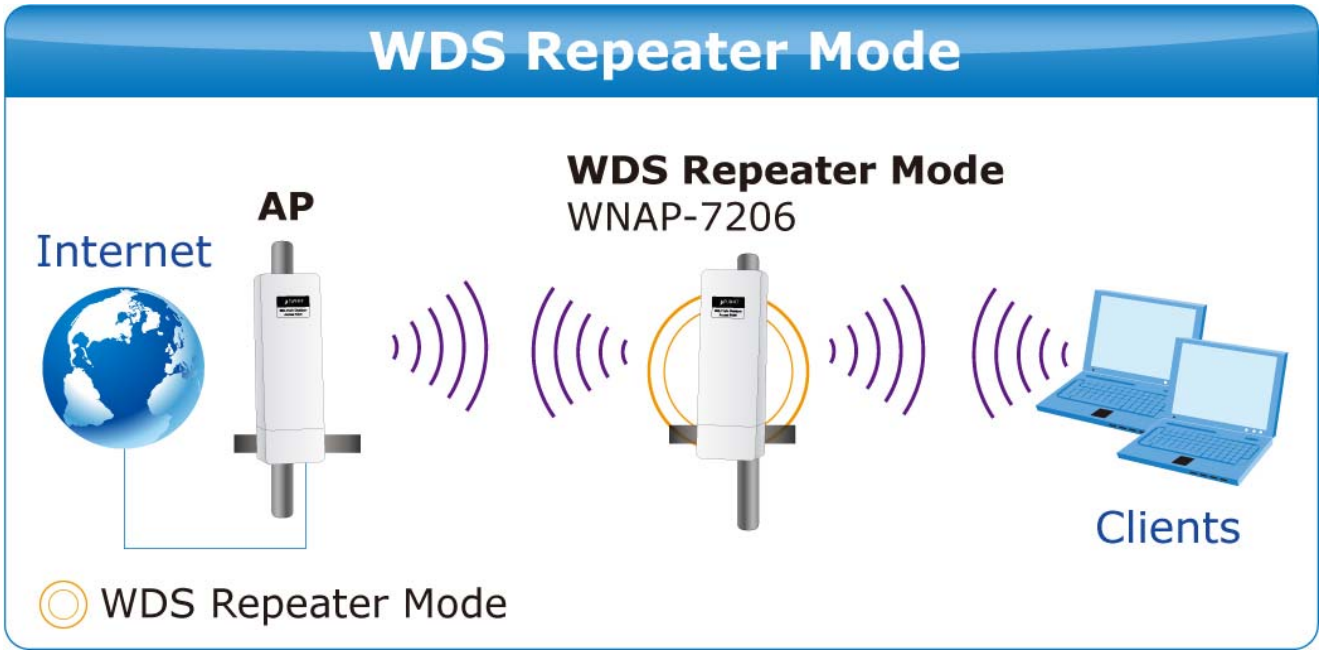
3. The target network's SSID will be automatically filled into the SSID field. Click **Save** to apply the setting.



The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device:

- Near the center of the area in which your wireless stations will operate;
- In an elevated location such as a high shelf;
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones;
- With the Antenna in the upright position;
- Away from large metal surfaces.

5.6.1.4. Repeater Mode



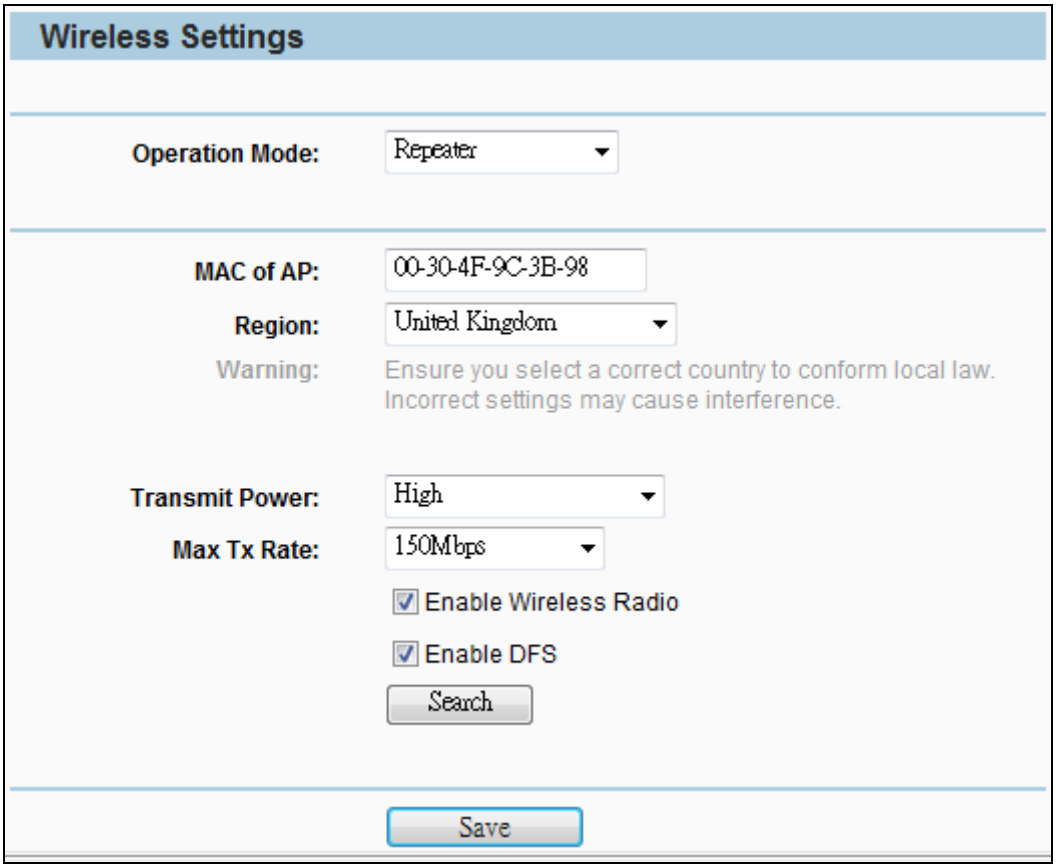


Figure 5-6-1-4 Repeater Mode

Note

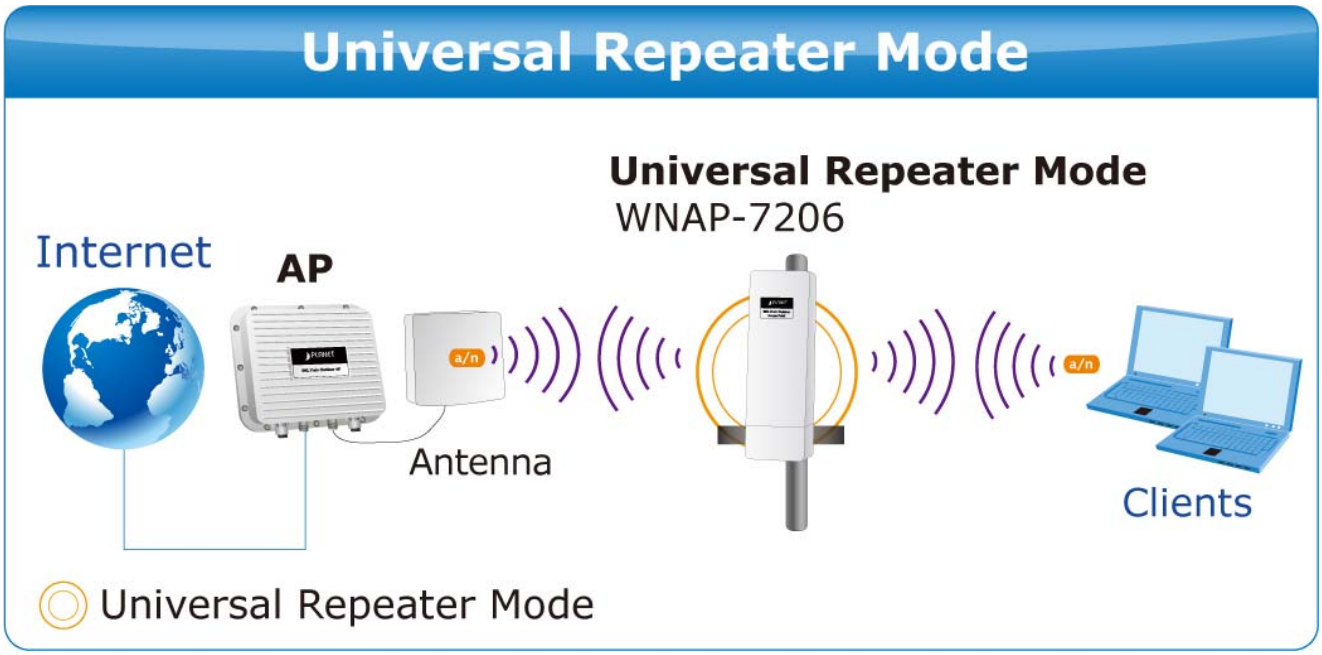
First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

Object	Description
• **MAC of AP**	The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able

	to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Search**	Click this button; you can search the AP which runs in the current channel.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.5. Universal Repeater Mode



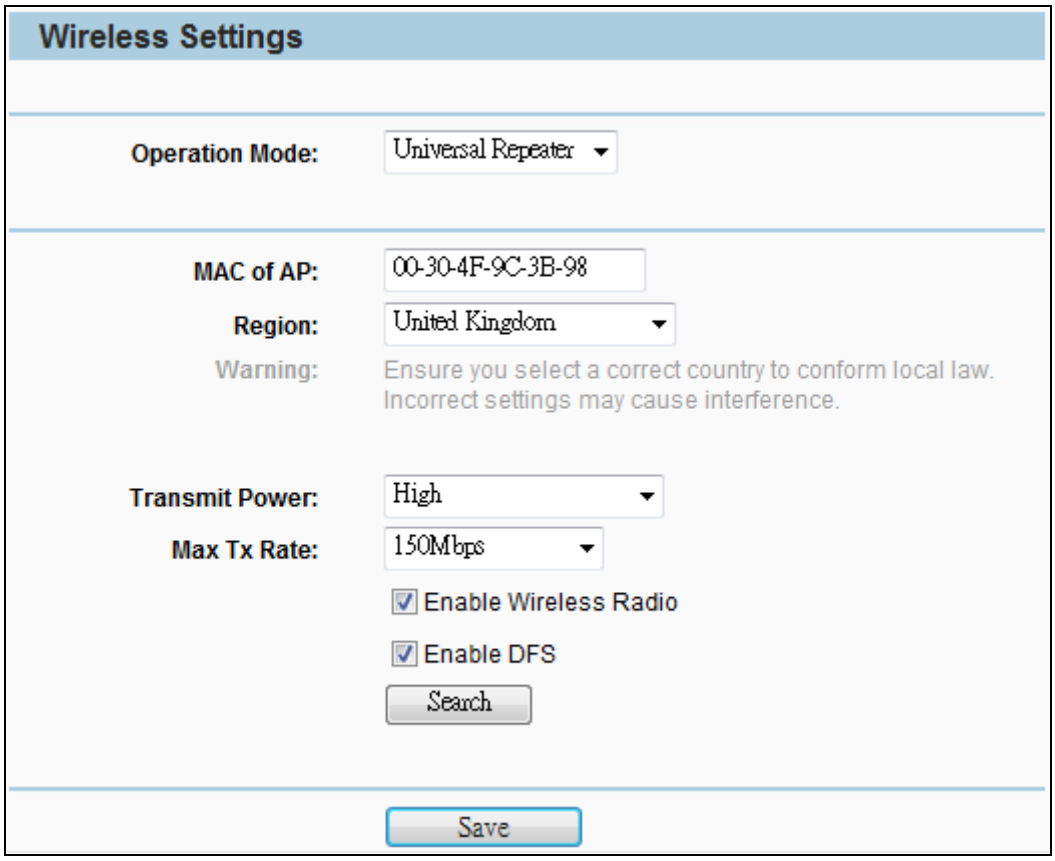


Figure 5-6-1-5 Universal Repeater Mode

Note

First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

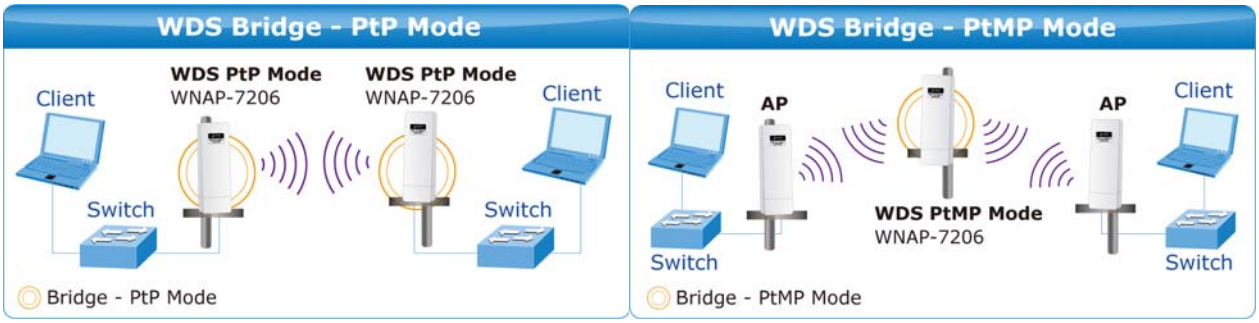
The page includes the following fields:

Object	Description
• **MAC of AP**	The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to

	access the Device.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Search**	Click this button; you can search the AP which runs in the current channel.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.6. Bridge with AP Mode (PtP & PtMP)

In this mode, you can establish **Point to Point** (PtP) connection or **Point to Multi-Point** (**PtMP**) connection.



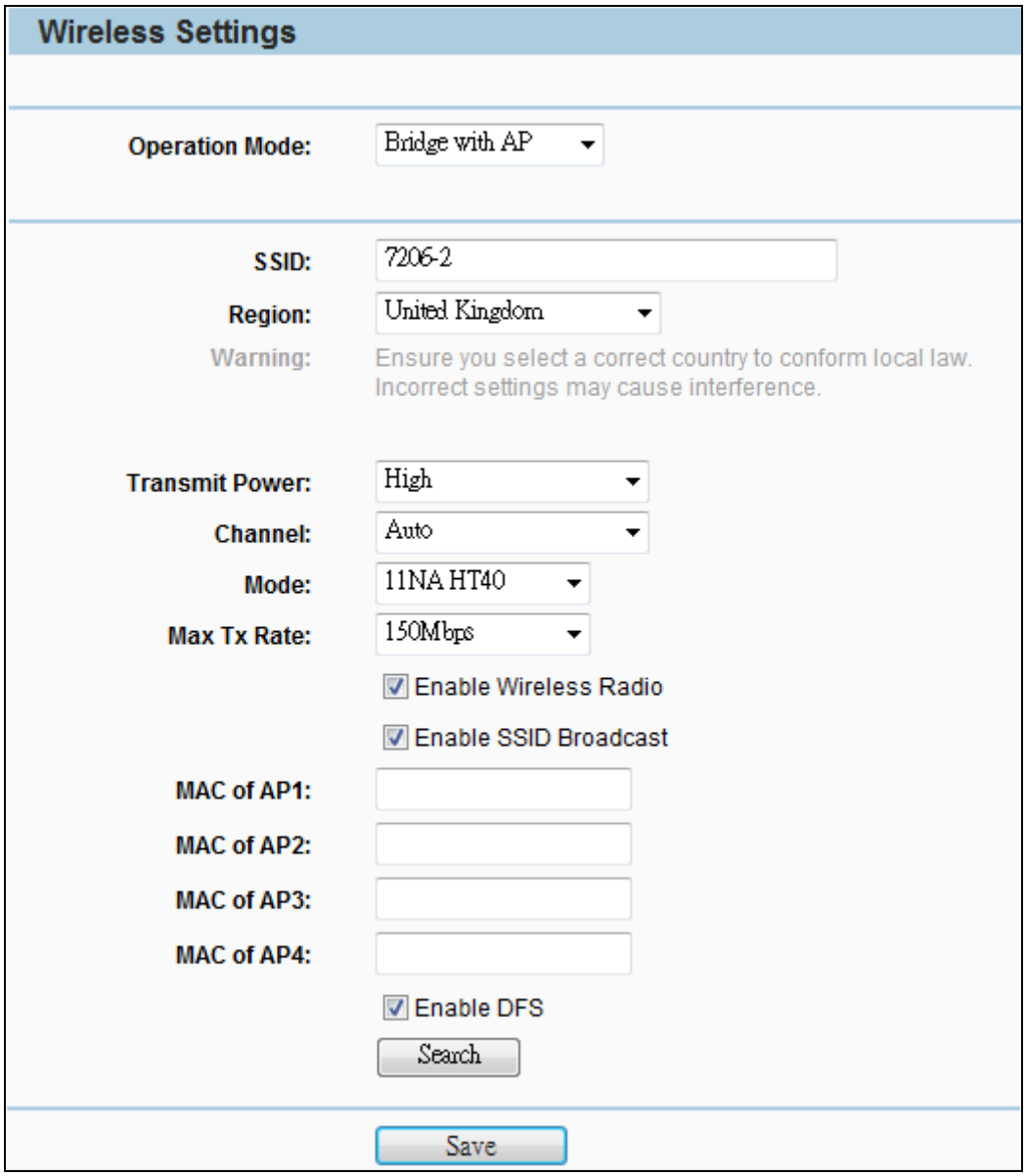


Figure 5-6-1-6 Bridge with AP Mode

Note

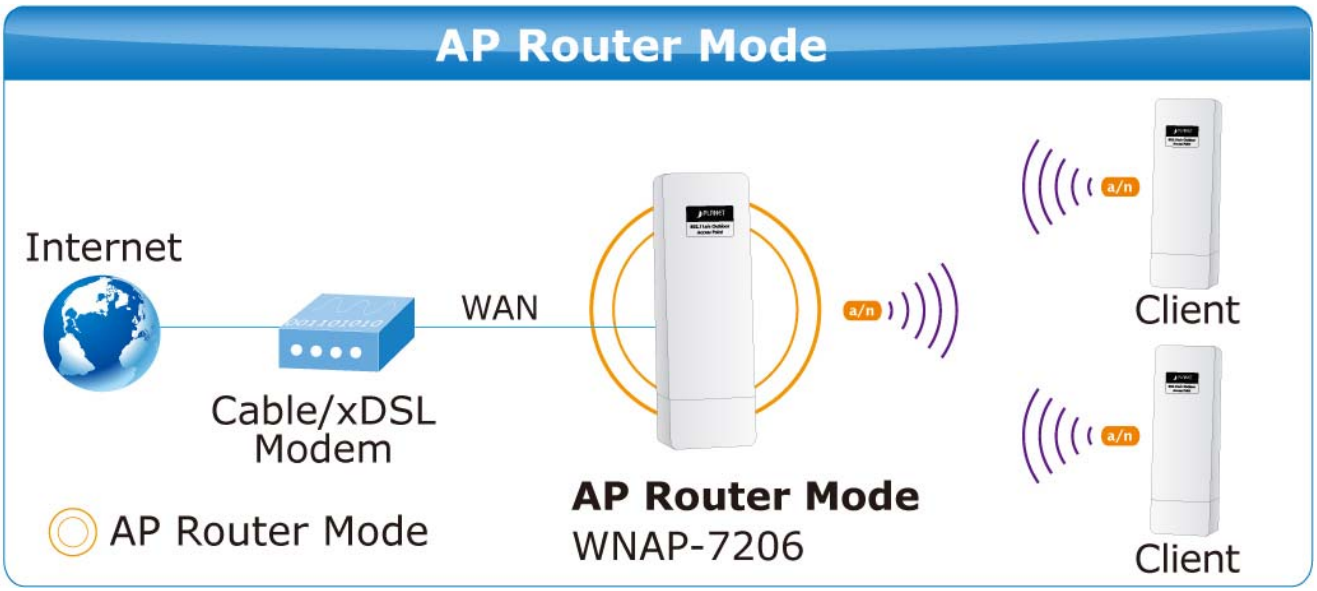
First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

Object	Description
• **SSID**	Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. In Multi-SSID operation mode, enter SSID for each BSS in the field "SSID1" ~ "SSID4".
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may

	be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Channel**	This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
• **Mode**	This field determines the wireless mode which the Device works on.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable SSID Broadcast**	If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **MAC of AP1~4**	Enter the MAC address of AP that you want to access. If you select the radio button before **MAC of AP**, the AP client will connect to AP according to MAC address.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Search**	Click this button; you can search the AP which runs in the current channel.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.7. AP Router Mode



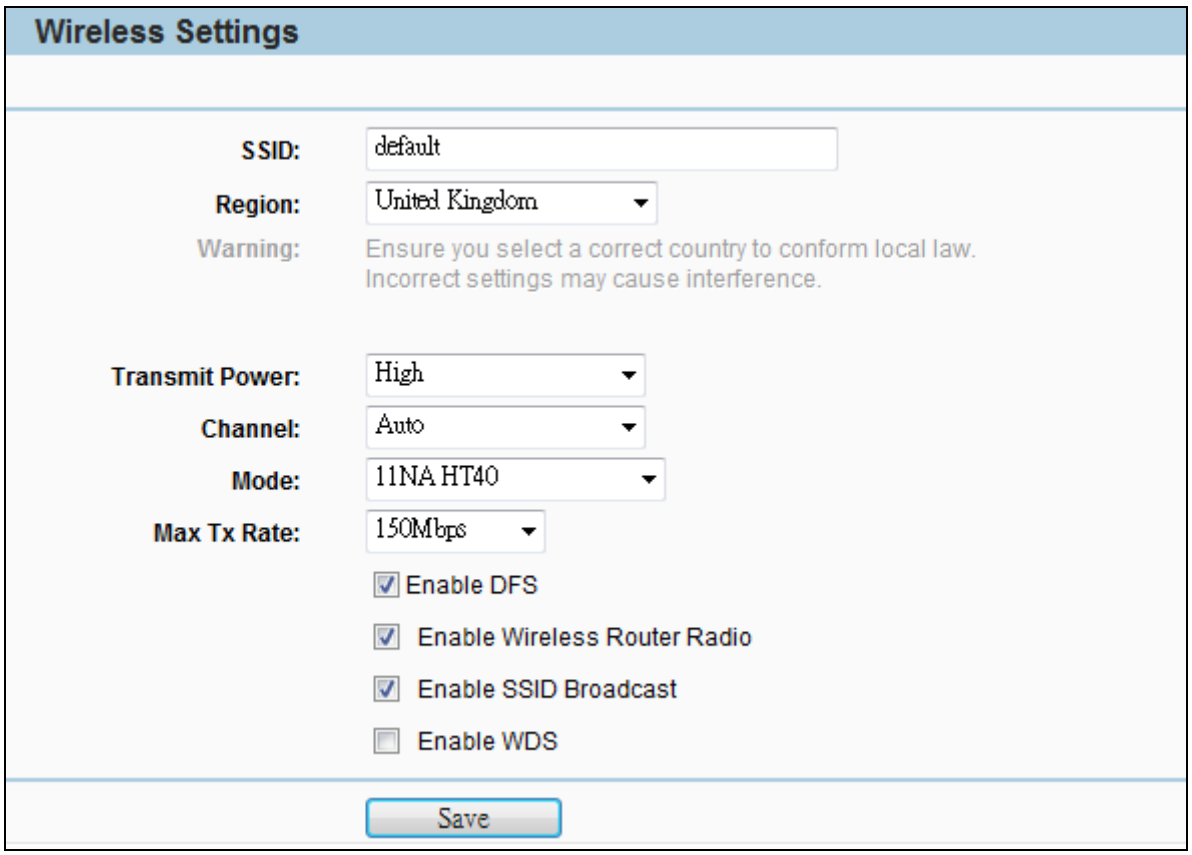


Figure 5-6-1-7 AP Router Mode

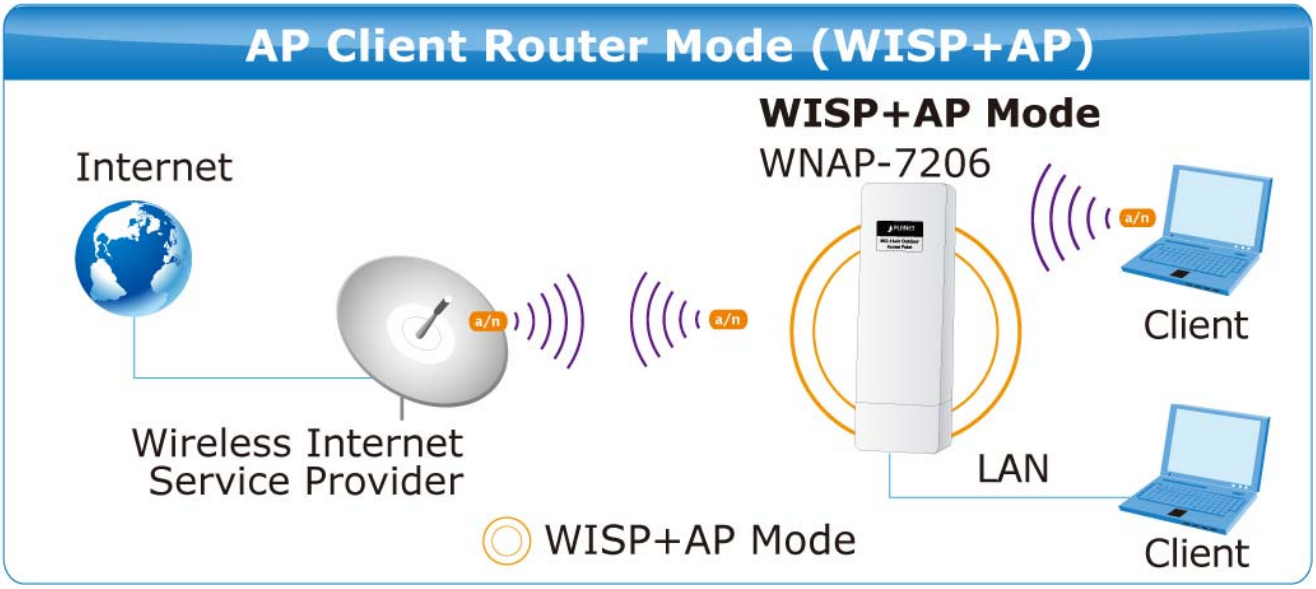
Note

First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

The page includes the following fields:

Object	Description
• **SSID**	Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **default**. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Channel**	This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
• **Mode**	This field determines the wireless mode which the Device works on.
• **Max Tx Rate**	You can limit the maximum tx rate of the Device through this field. You can select one of the options listed as the below items.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Enable Wireless Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable SSID Broadcast**	If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **Enable WDS**	If you select the **Enable WDS** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **Save**	Click the **Save** button to save your settings on this page.

5.6.1.8. AP Client Router Mode (WISP+AP)



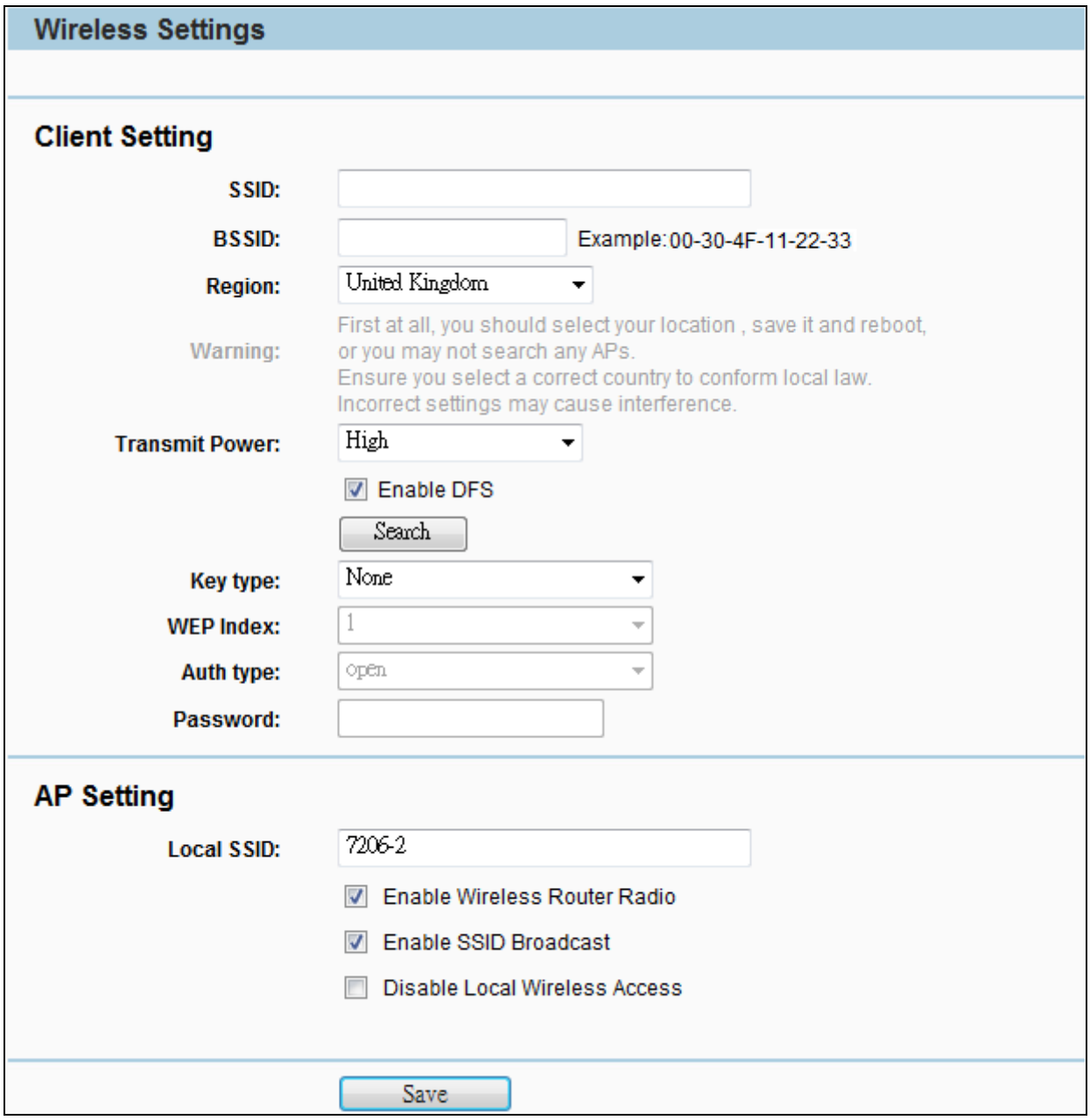


Figure 5-6-1-8 AP Client Router Mode

Note

First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

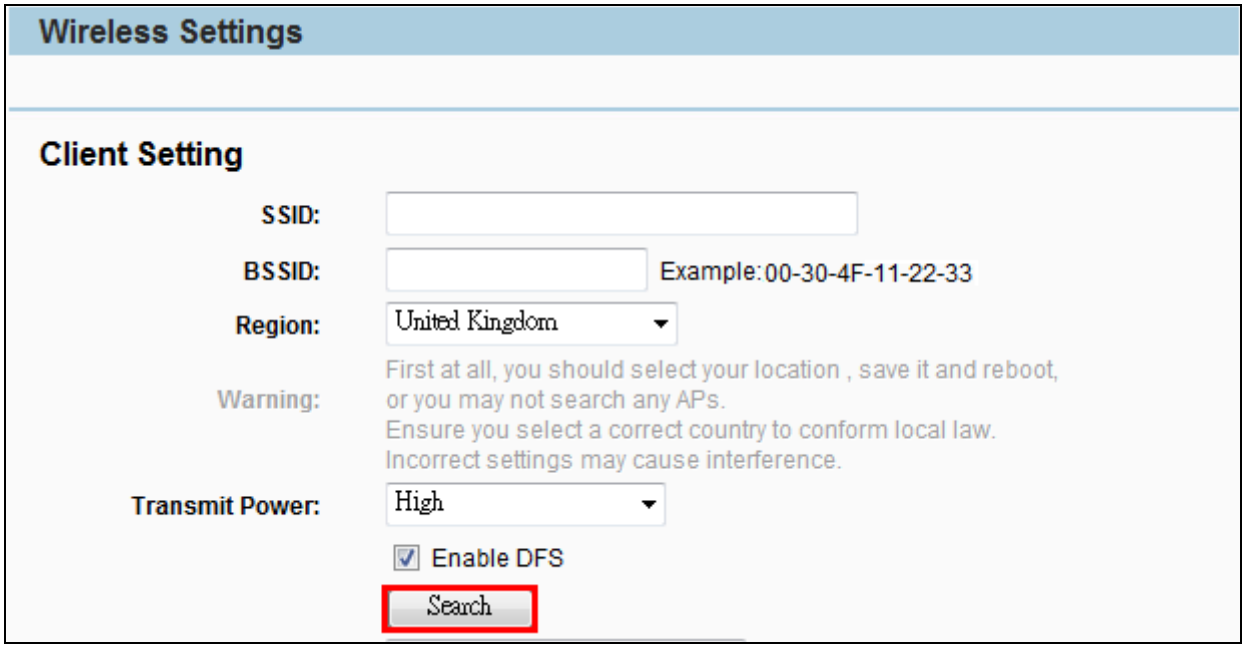
The page includes the following fields:

Object	Description
• **SSID**	The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select a SSID to join. If you know the SSID of the desired AP, you can also input it to the field "SSID" manually.

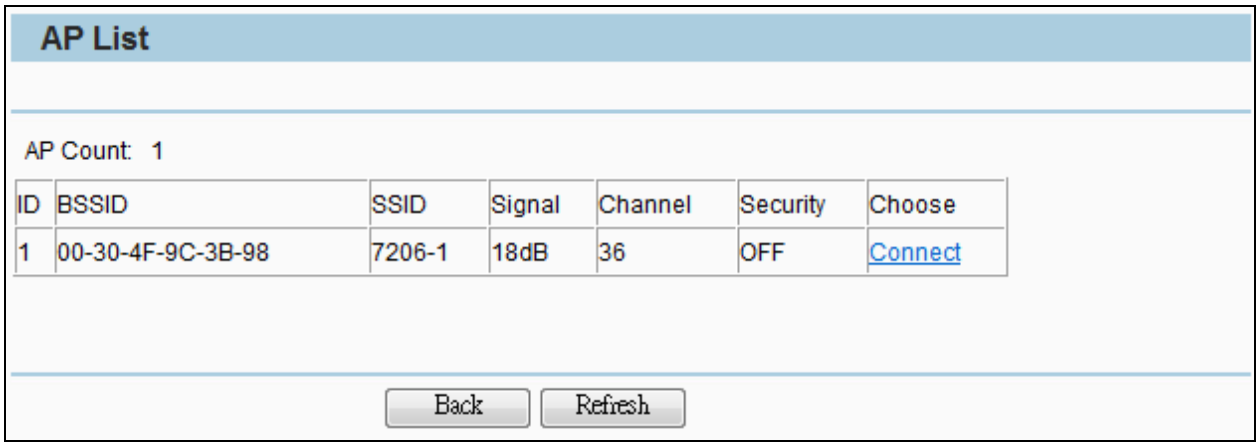
• **BSSID**	The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
• **Region**	Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
• **Transmit Power**	You can limit the Transmit Power of the Device through this field. You can select one of the options listed as the below items.
• **Enable DFS**	Check **Enable DFS** to enable DFS function.
• **Search**	Click this button; you can search the AP which runs in the current channel.
• **Key type**	This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
• **WEP Index**	This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
• **Auth Type**	This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
• **Password**	If the AP your Device is going to connect needs password, you need to fill the password in this blank.
• **Local SSID**	Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
• **Enable Wireless Router Radio**	The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
• **Enable SSID Broadcast**	If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
• **Disable Local Wireless Access**	If you select the **Disable Local Wireless Access** checkbox, the wireless Device will disable local wireless access; other stations will not be able to access the Device by wireless.
• **Save**	Click the **Save** button to save your settings on this page.

To establish connection with remote AP, please follow the instructions as below:

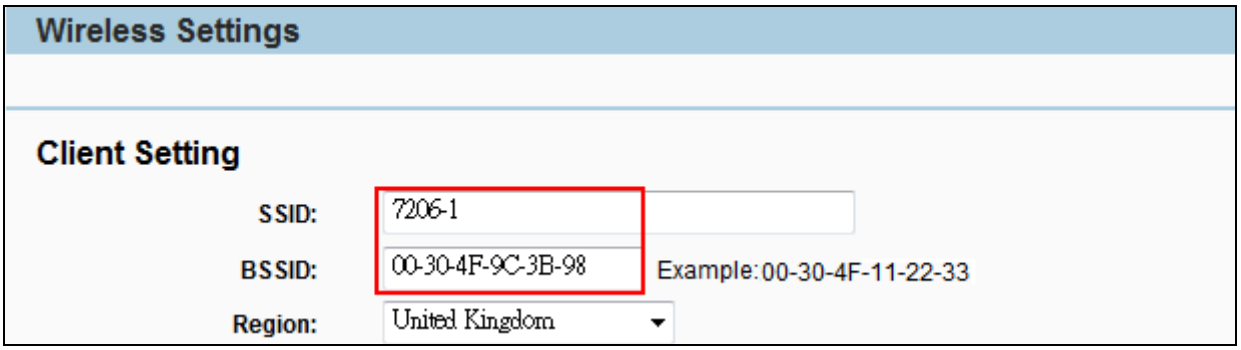
1. Click **Search** button.



2. In the AP List, select the AP you want to access, and click **Connect**.



3. The target network's SSID will be automatically filled into the SSID field. Click **Save** to apply the setting.



Note

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device:

- Near the center of the area in which your wireless stations will operate;
- In an elevated location such as a high shelf;

- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones;
- With the Antenna in the upright position;
- Away from large metal surfaces.

5.6.2 Wireless Security

Choose menu "**Wireless > Wireless Security**", and then you can configure the security settings of your wireless network.

There are three wireless security modes supported by the Device: **WEP** (Wired Equivalent Privacy), **WPA/WPA2** (Wi-Fi Protected Access/ Wi-Fi Protected Access 2), and **WPA-PSK/WPA2-PSK** (Pre-Shared Key). The security options are different for different operation mode.

Only in Standard AP mode, the current operation mode is shown at the top. Besides, if Multi-SSID, a sub mode of Standard AP, is selected, you can choose one of the 4 SSIDs from the pull-down list.

5.6.2.1. Operation Mode – Access Point

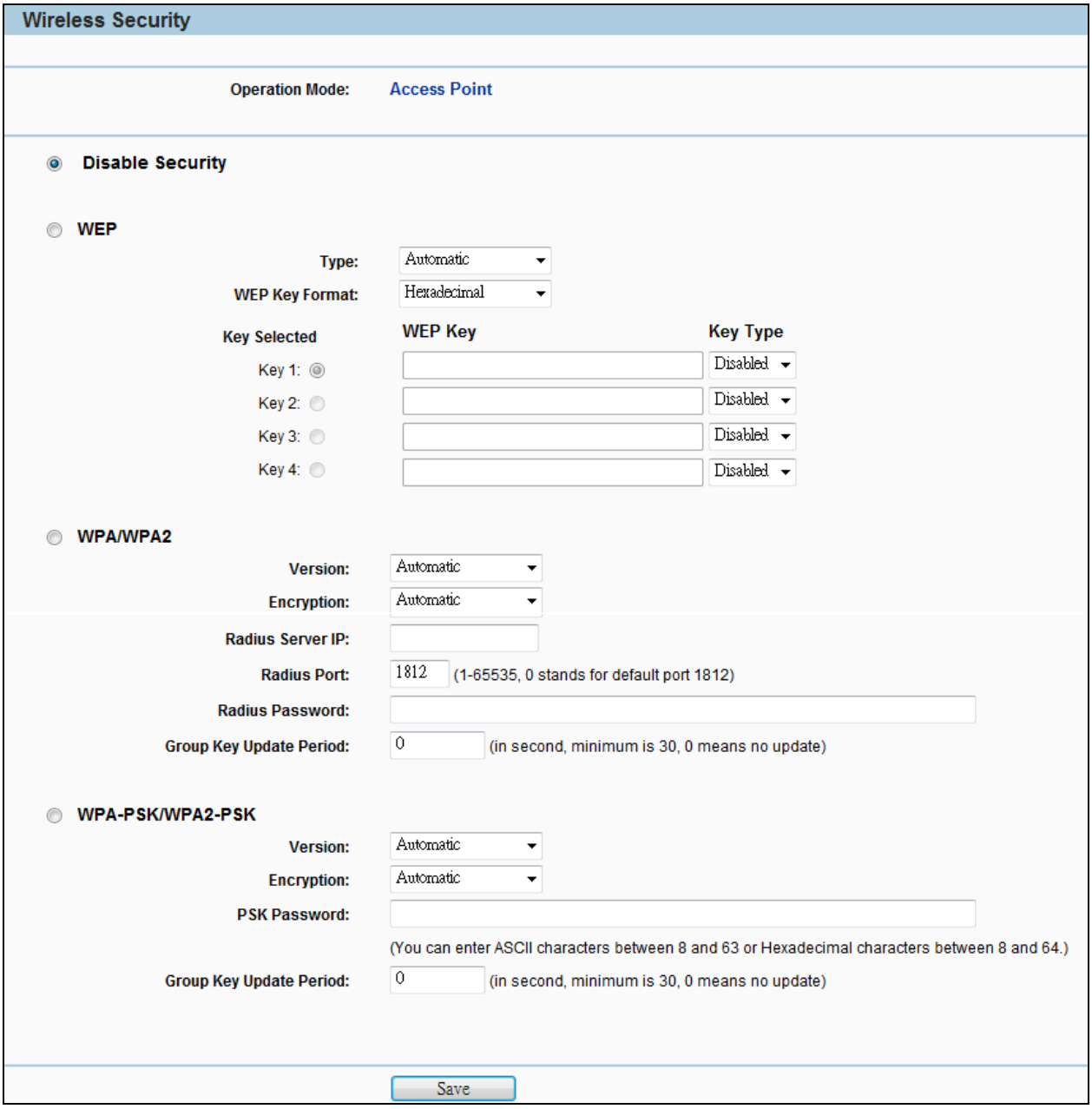


Figure 5-6-2-1 Wireless Security - AP

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WEP**	Select 802.11 WEP security.
• **WPA/WPA2**	Select WPA based on Radius Server.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• **Type**	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• **WEP Key Format**	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• **WEP Key settings**	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• **Key Type**	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA/WPA2

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic** - Select WPA or WPA2 automatically based on the wireless station's capability and request.

	■ **WPA** - Wi-Fi Protected Access. ■ **WPA2** - WPA version 2.
• **Encryption**	You can select either **Automatic**, or **TKIP** or **AES**.
• **Radius Server IP**	Enter the IP address of the Radius Server.
• **Radius Port**	Enter the port that radius service uses.
• **Radius Password**	Enter the password for the Radius Server.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.
• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.2. Operation Mode – Multi-SSID

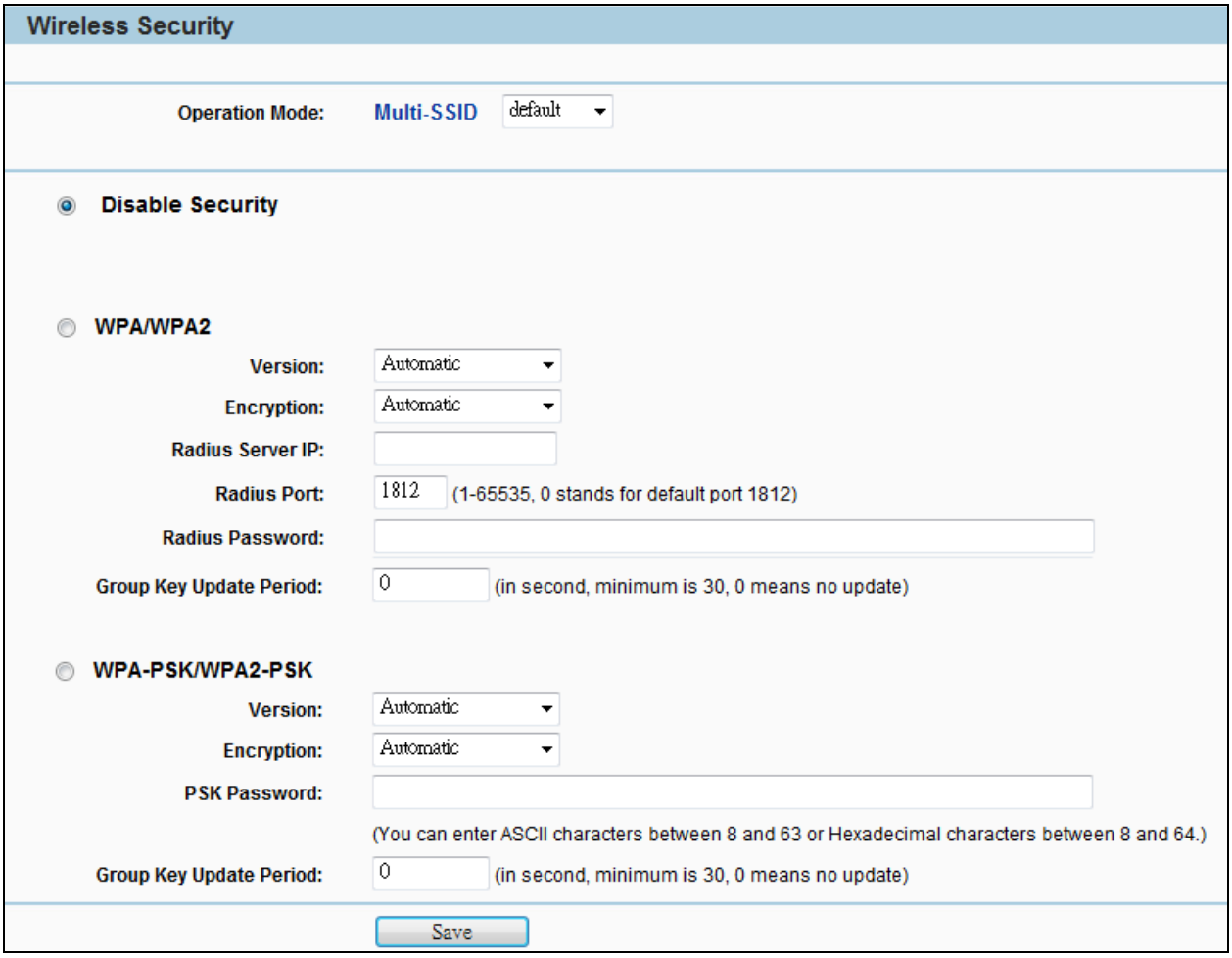


Figure 5-6-2-2 Wireless Security – Multi-SSID

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WPA/WPA2**	Select WPA based on Radius Server.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WPA/WPA2

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic** - Select WPA or WPA2 automatically based on the wireless station's capability and request.

	■ **WPA** - Wi-Fi Protected Access. ■ **WPA2** - WPA version 2.
• **Encryption**	You can select either **Automatic**, or **TKIP** or **AES**.
• **Radius Server IP**	Enter the IP address of the Radius Server.
• **Radius Port**	Enter the port that radius service uses.
• **Radius Password**	Enter the password for the Radius Server.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

This security option will become unavailable, if the Enable VLAN in **Wireless Settings** under Multi-SSID mode.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.
• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.3. Operation Mode – Client

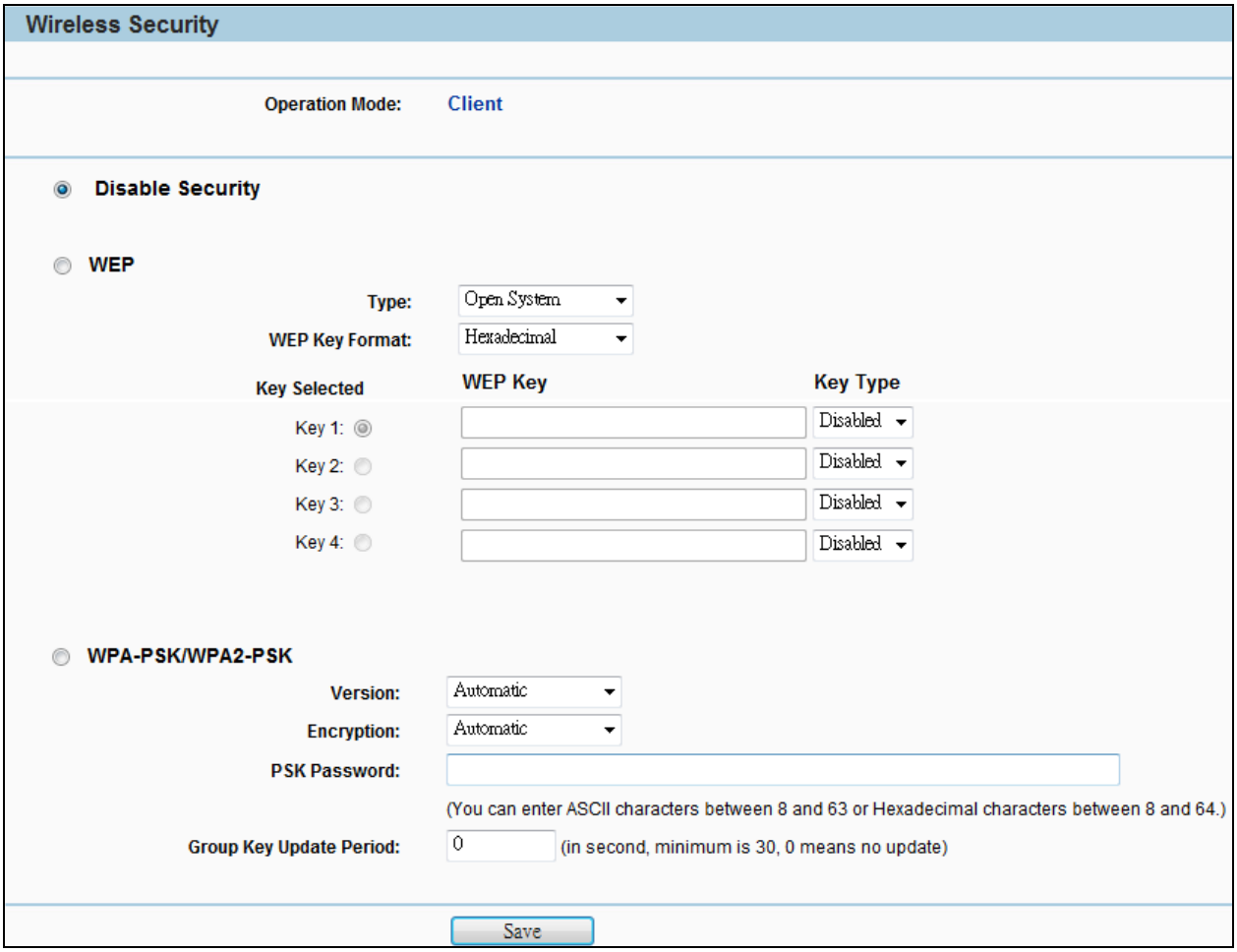


Figure 5-6-2-3 Wireless Security - Client

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WEP**	Select 802.11 WEP security.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• **Type**	You can select one of following types:

	■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• **WEP Key Format**	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• **WEP Key settings**	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• **Key Type**	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.

• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.4. Operation Mode – Repeater

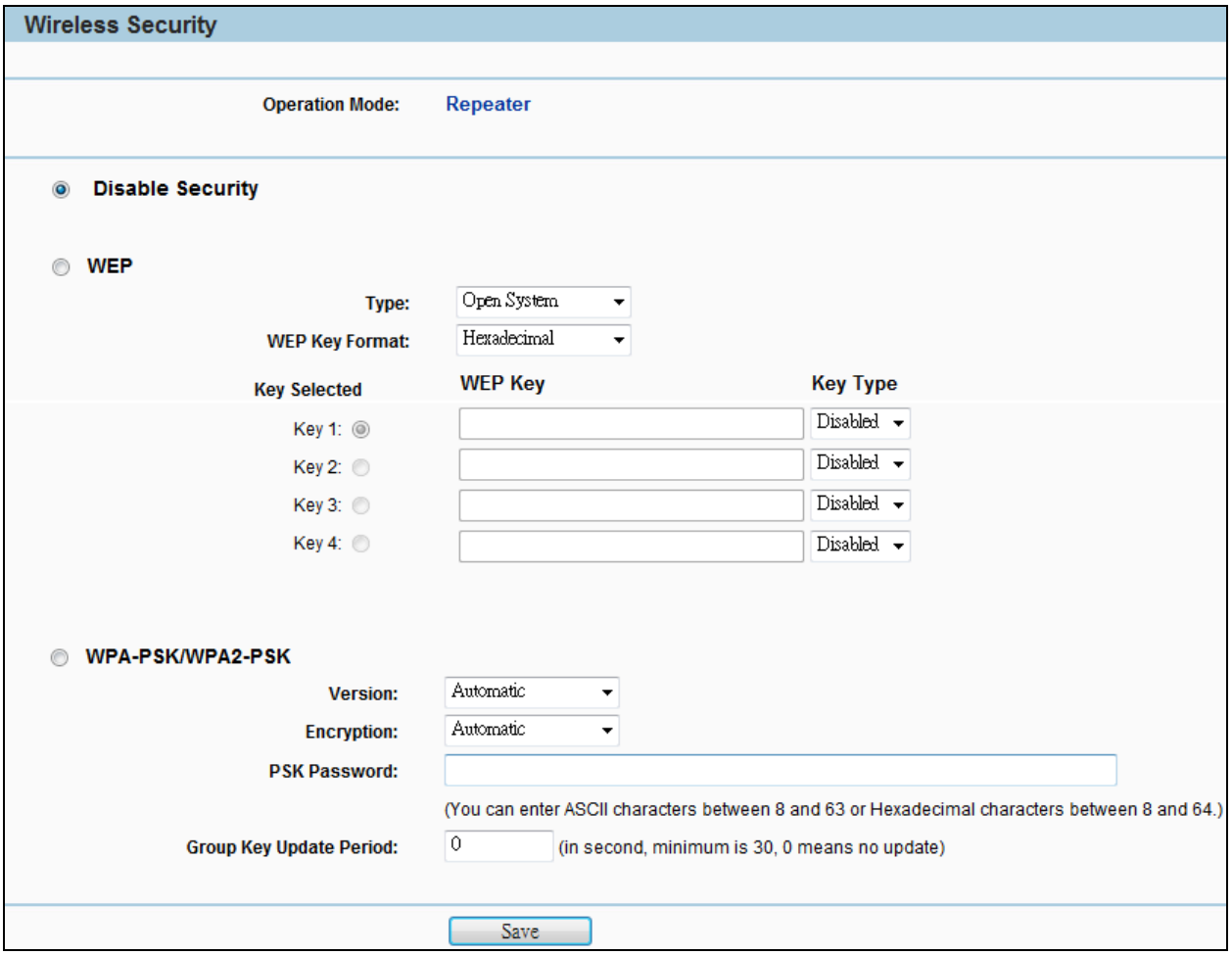


Figure 5-6-2-4 Wireless Security - Repeater

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WEP**	Select 802.11 WEP security.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• **Type**	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• **WEP Key Format**	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• **WEP Key settings**	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• **Key Type**	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• Version	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• Encryption	You can select either Automatic, or TKIP or AES.
• PSK Password	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• Group Key Update Period	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.5. Operation Mode – Universal Repeater

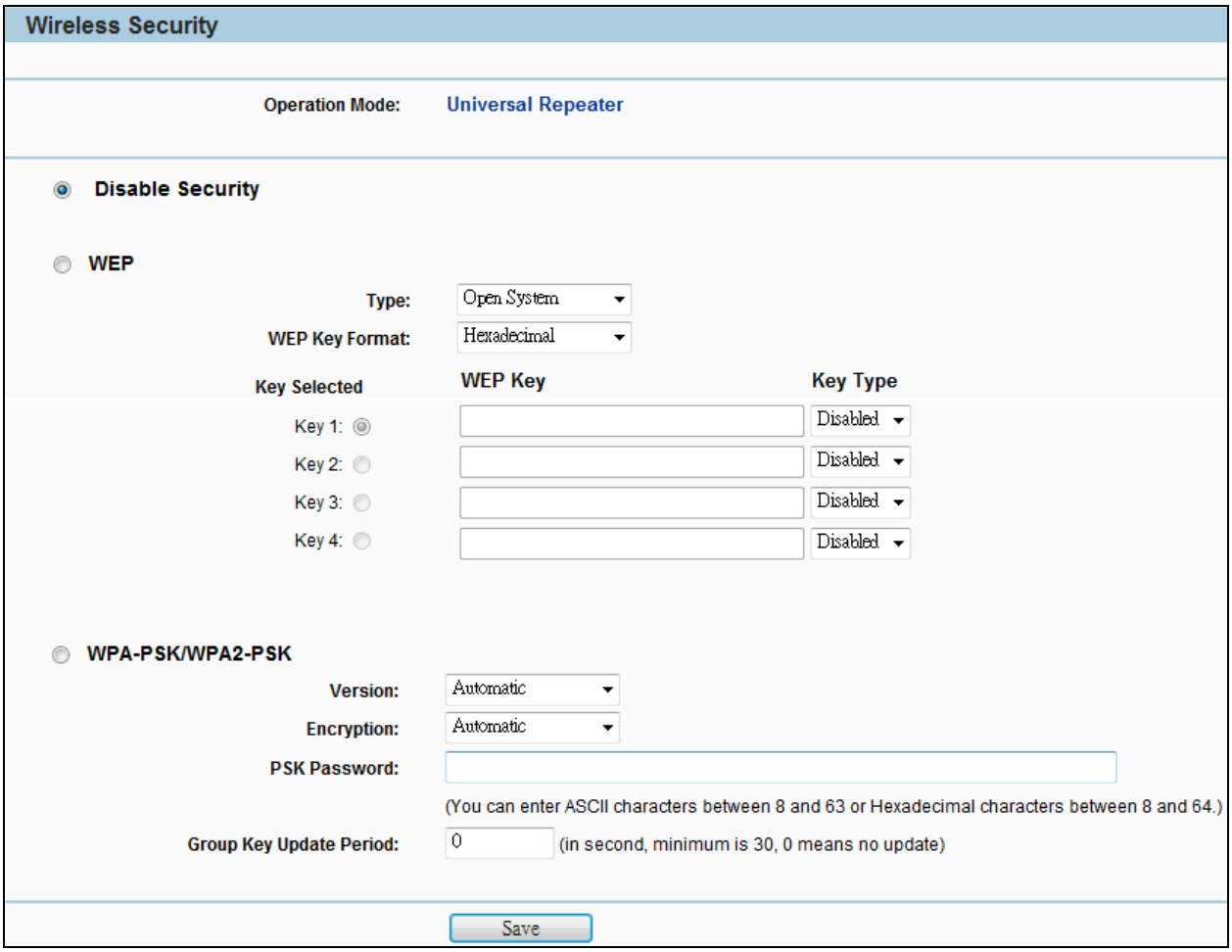


Figure 5-6-2-5 Wireless Security – Universal Repeater

Object	Description
• Disable Security	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• WEP	Select 802.11 WEP security.
• WPA/WPA2	Select WPA based on Radius Server.
• WPA-PSK/WPA2-PSK	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• Type	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• WEP Key Format	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• WEP Key settings	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• Key Type	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.
• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.6. Operation Mode – Bridge with AP

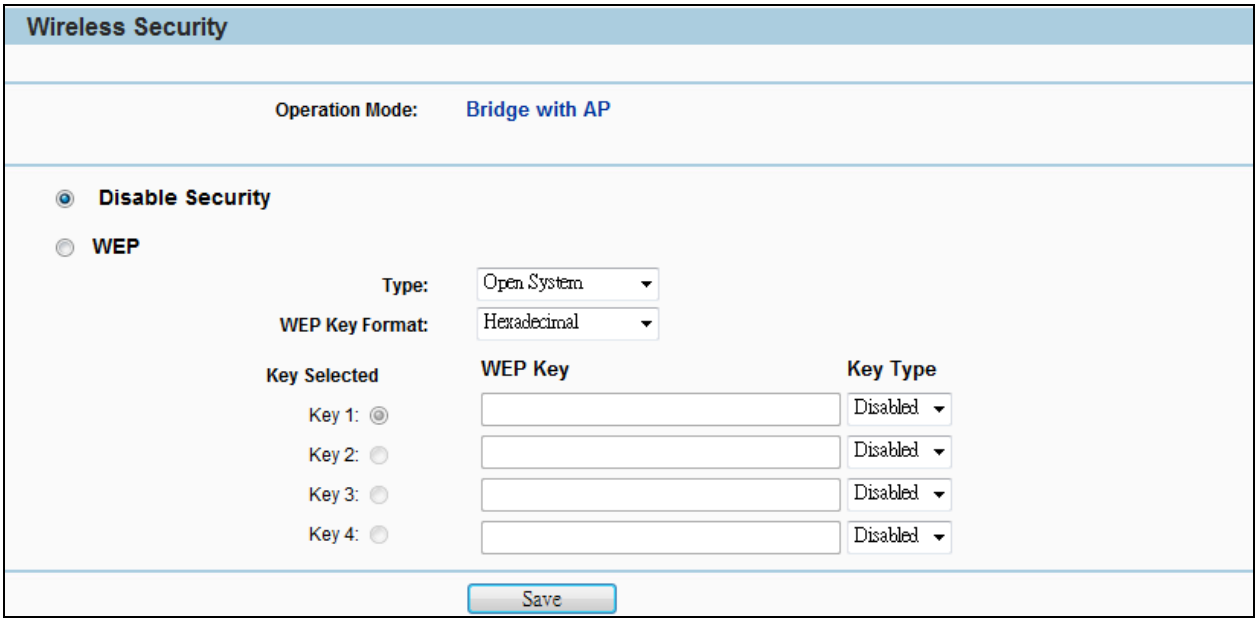


Figure 5-6-2-6 Wireless Security – Bridge with AP

Object	Description
• Disable Security	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• WEP	Select 802.11 WEP security.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• Type	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• WEP Key Format	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• WEP Key settings	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• Key Type	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

5.6.2.7. Operation Mode – AP Router

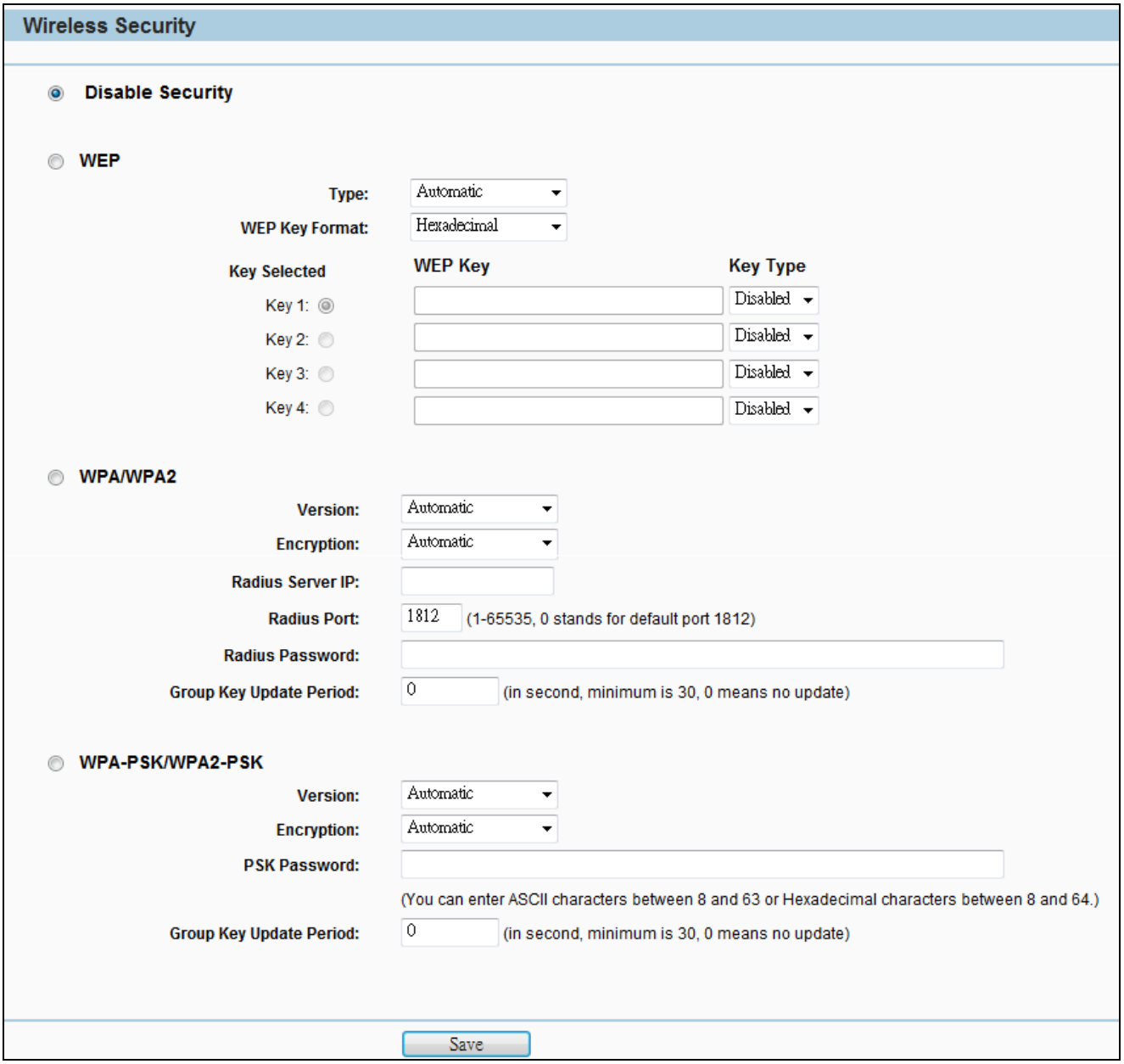


Figure 5-6-2-7 Wireless Security – AP Router

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WEP**	Select 802.11 WEP security.
• **WPA/WPA2**	Select WPA based on Radius Server.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• **Type**	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• **WEP Key Format**	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• **WEP Key settings**	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• **Key Type**	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA/WPA2

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic** - Select WPA or WPA2 automatically based on the wireless station's capability and request. ■ **WPA** - Wi-Fi Protected Access.

	■ **WPA2** - WPA version 2.
• **Encryption**	You can select either **Automatic**, or **TKIP** or **AES**.
• **Radius Server IP**	Enter the IP address of the Radius Server.
• **Radius Port**	Enter the port that radius service uses.
• **Radius Password**	Enter the password for the Radius Server.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.
• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.2.8. Operation Mode – AP Client Router

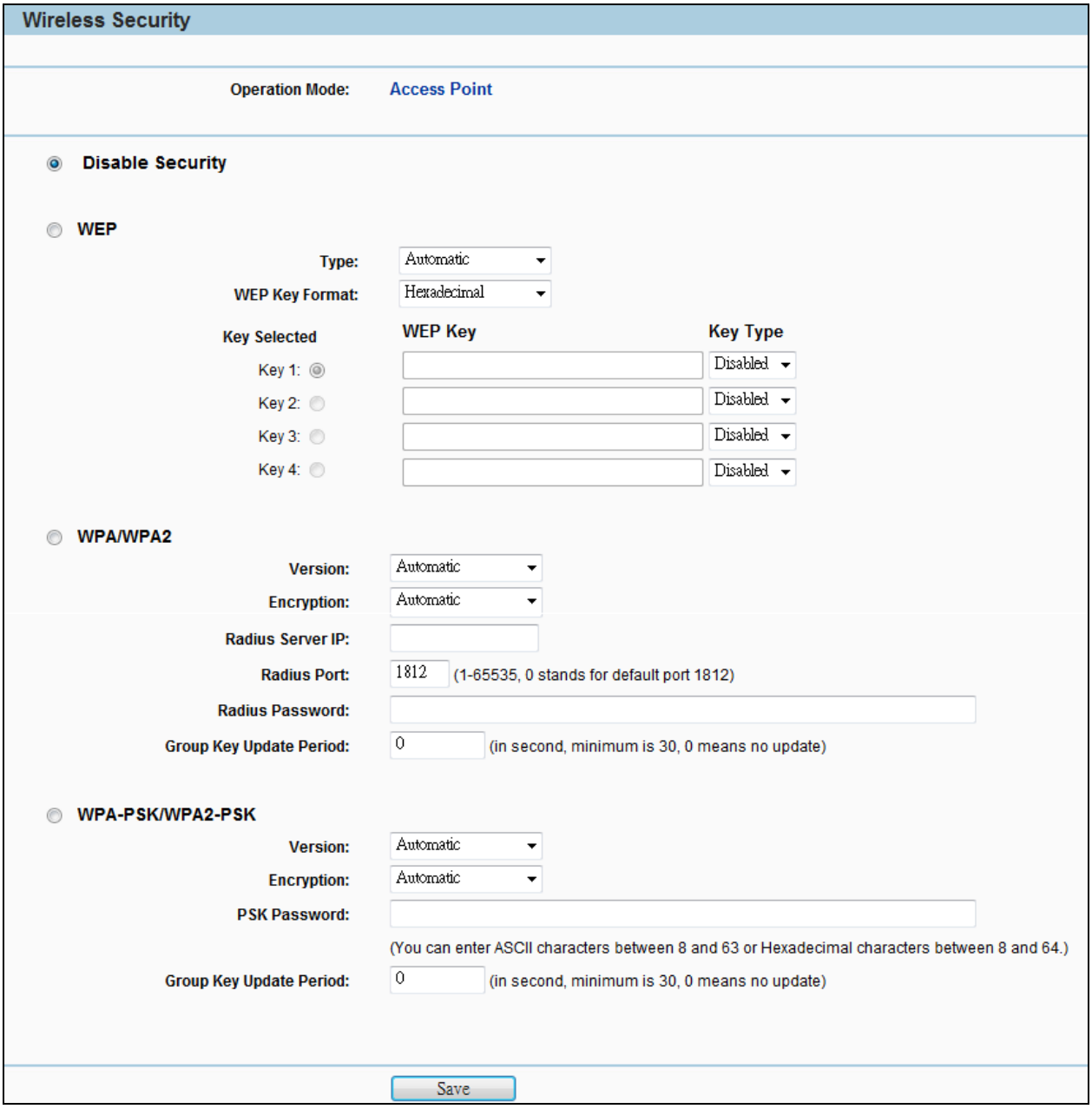


Figure 5-6-2-8 Wireless Security – AP Client Router

Object	Description
• **Disable Security**	The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.
• **WEP**	Select 802.11 WEP security.
• **WPA/WPA2**	Select WPA based on Radius Server.
• **WPA-PSK/WPA2-PSK**	Select WPA based on pre-shared passphrase.

Each security option has its own settings as described follows:

■ WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

Object	Description
• **Type**	You can select one of following types: ■ **Automatic -** Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request. ■ **Shared Key -** Select 802.11 Shared Key authentication. ■ **Open System -** Select 802.11 Open System authentication.
• **WEP Key Format**	You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
• **WEP Key settings**	Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
• **Key Type**	You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid. **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

■ WPA/WPA2

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic** - Select WPA or WPA2 automatically based on the wireless station's capability and request.

	■ **WPA** - Wi-Fi Protected Access. ■ **WPA2** - WPA version 2.
• **Encryption**	You can select either **Automatic**, or **TKIP** or **AES**.
• **Radius Server IP**	Enter the IP address of the Radius Server.
• **Radius Port**	Enter the port that radius service uses.
• **Radius Password**	Enter the password for the Radius Server.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

■ WPA-PSK/WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Object	Description
• **Version**	You can select one of following versions: ■ **Automatic -** Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. ■ **WPA-PSK -** Pre-shared key of WPA. ■ **WPA2-PSK -** Pre-shared key of WPA2.
• **Encryption**	You can select either Automatic, or TKIP or AES.
• **PSK Password**	You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
• **Group Key Update Period**	Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

5.6.3 Wireless MAC Filtering

Choose menu "**Wireless > MAC Filtering**", and then you can control the wireless access by configuring the Wireless MAC Filtering function, as shown in **Figure 5-6-3-1**.

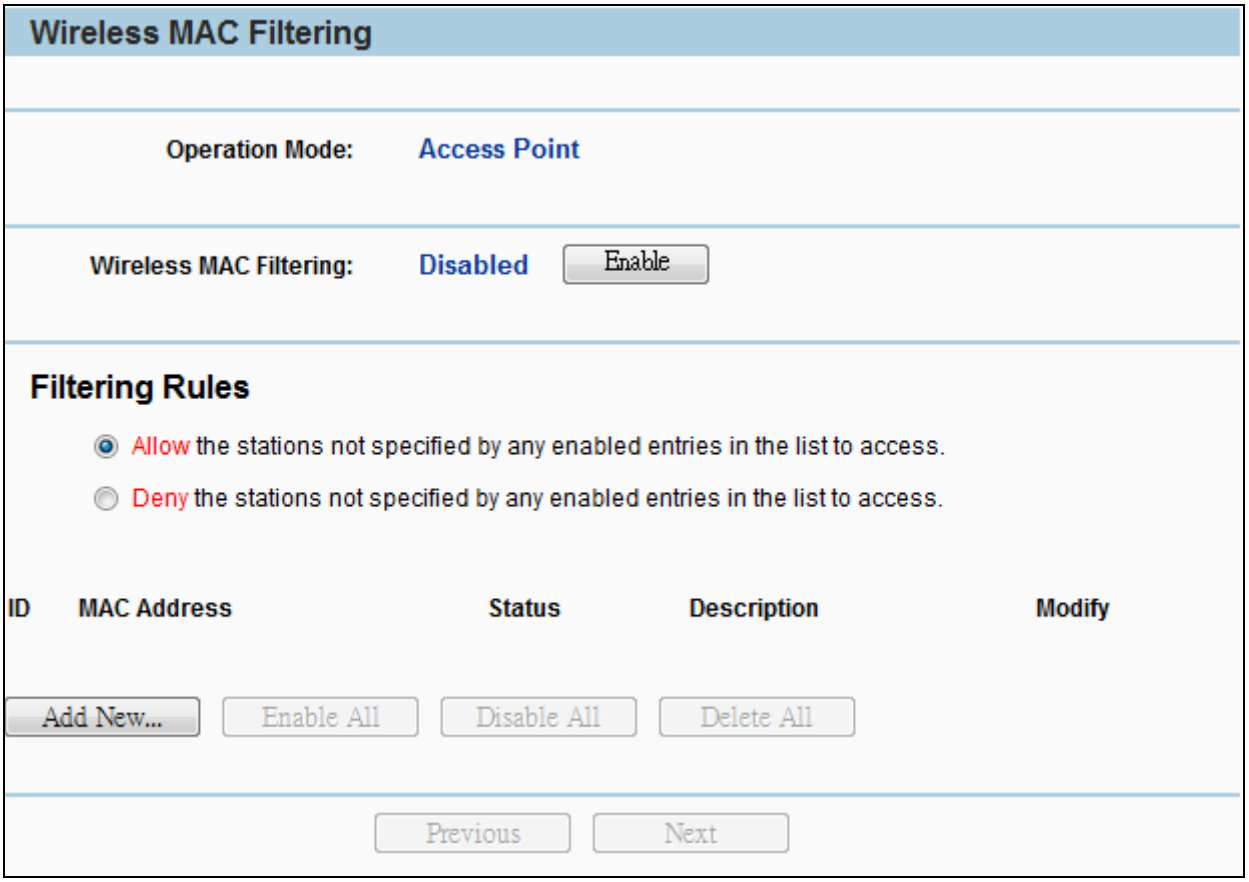


Figure 5-6-3-1 Wireless Advanced

The page includes the following fields:

Object	Description
• **Operation Mode**	Display the current operation mode.
• **Wireless MAC Filtering**	**Enable:** Click **Enable** to enable the MAC Filtering. **Disable:** Click **Disable** to disable the MAC Filtering. The MAC Filtering was not available in Client Mode.
• **Filtering Rules**	There are two policies can be used for filtering rule. Select a policy by clicking the radio button in front of the following items. ■ **Allow the stations not specified by any enabled entries in the list to access.** ■ **Deny the station not specified by any enabled entries in the list to access.**
• **MAC Address**	The wireless station's MAC address that you want to filter.
• **Status**	The status of this entry either Enabled or Disabled.
• **Description**	A simple description of the wireless station.

5.6.4 Wireless Advanced

Choose menu "**Wireless > Wireless Advanced**", and then you can configure the advanced settings of your

wireless network.

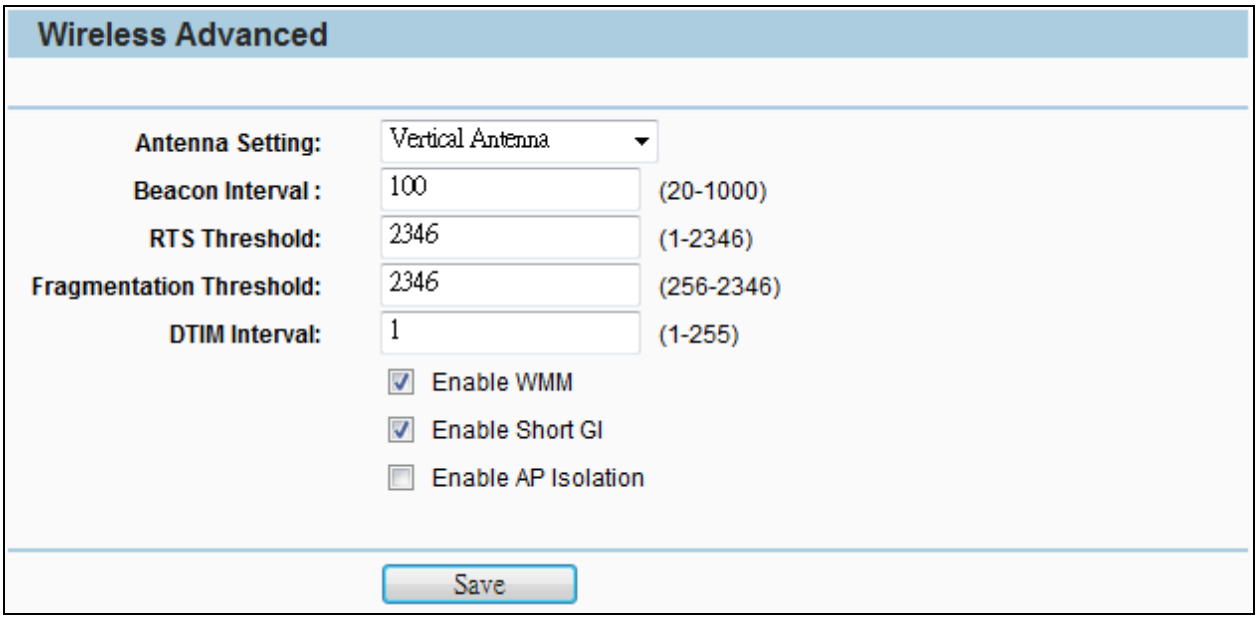


Figure 5-6-4-1 Wireless Advanced

The page includes the following fields:

Object	Description
• **Antenna Setting**	The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna, or External Antenna.
• **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.
• **RTS Threshold**	Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
• **Fragmentation Threshold**	This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
• **DTIM Interval**	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.
• **Enable WMM**	WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly

	recommended enabled.
• **Enable Short GI**	This function is recommended for it will increase the data capacity by reducing the guard interval time.
• **Enable AP Isolation**	Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.
• **Save**	Click the **Save** button to save the setting.

5.6.5 Antenna Alignment

Choose menu "**Wireless > Antenna Alignment**", and then you can know how remote the Device's signal strength changes while changing the antenna's direction.

1. This function is not available in AP Router mode, but in both Standard AP mode and AP Client Router mode.
2. It only works after you have established connection to remote AP in client mode.

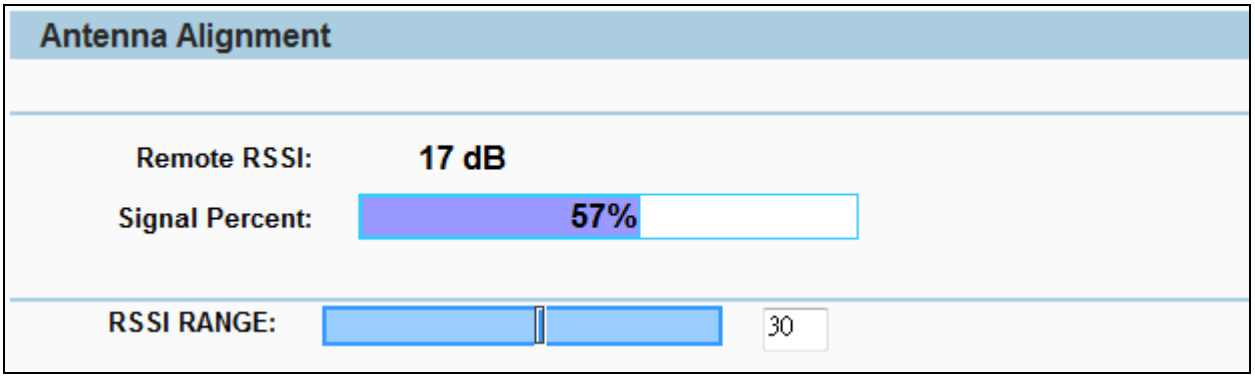


Figure 5-6-5-1 Antenna Alignment

The page includes the following fields:

Object	Description
• **Remote RSSI**	Remote AP's signal strength value.
• **Signal Percent**	The ratio of RSSI to RSSI RANGE in percentage.
• **RSSI RANGE**	You can drag the Slider to set or input the RSSI RANGE value.

5.6.6 Distance Setting

Choose menu "**Wireless > Distance Settings**", and then you can adjust the wireless range in outdoor conditions.

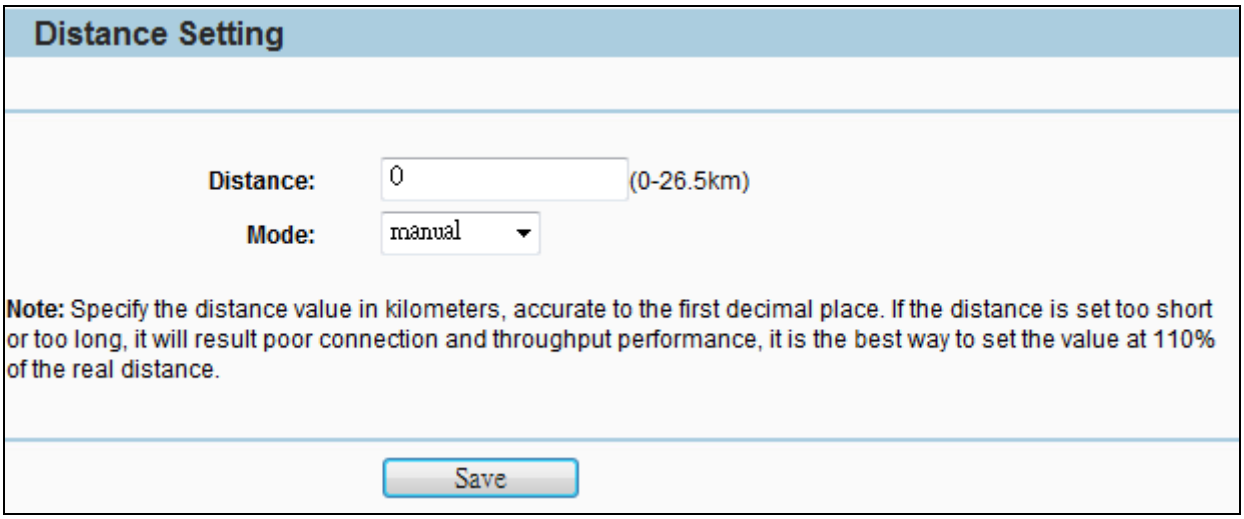


Figure 5-6-6-1 Distance Setting

This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link, and then the software will optimize the frame ACK timeout value automatically.
One hundred-meter is the smallest unit of this setting.

The page includes the following fields:

Object	Description
• **Distance**	Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result poor connection and throughput performance, it is the best way to set the value at 110% of the real distance. One hundred-meter is the smallest unit of this setting.
• **Mode**	0: Select it for outdoor application. Enter the actual distance in the range of 0~26.5km. Indoor: Select it for indoor application, the distance will be disabled when choose this mode..

5.6.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in **Figure 5-6-7-1**.

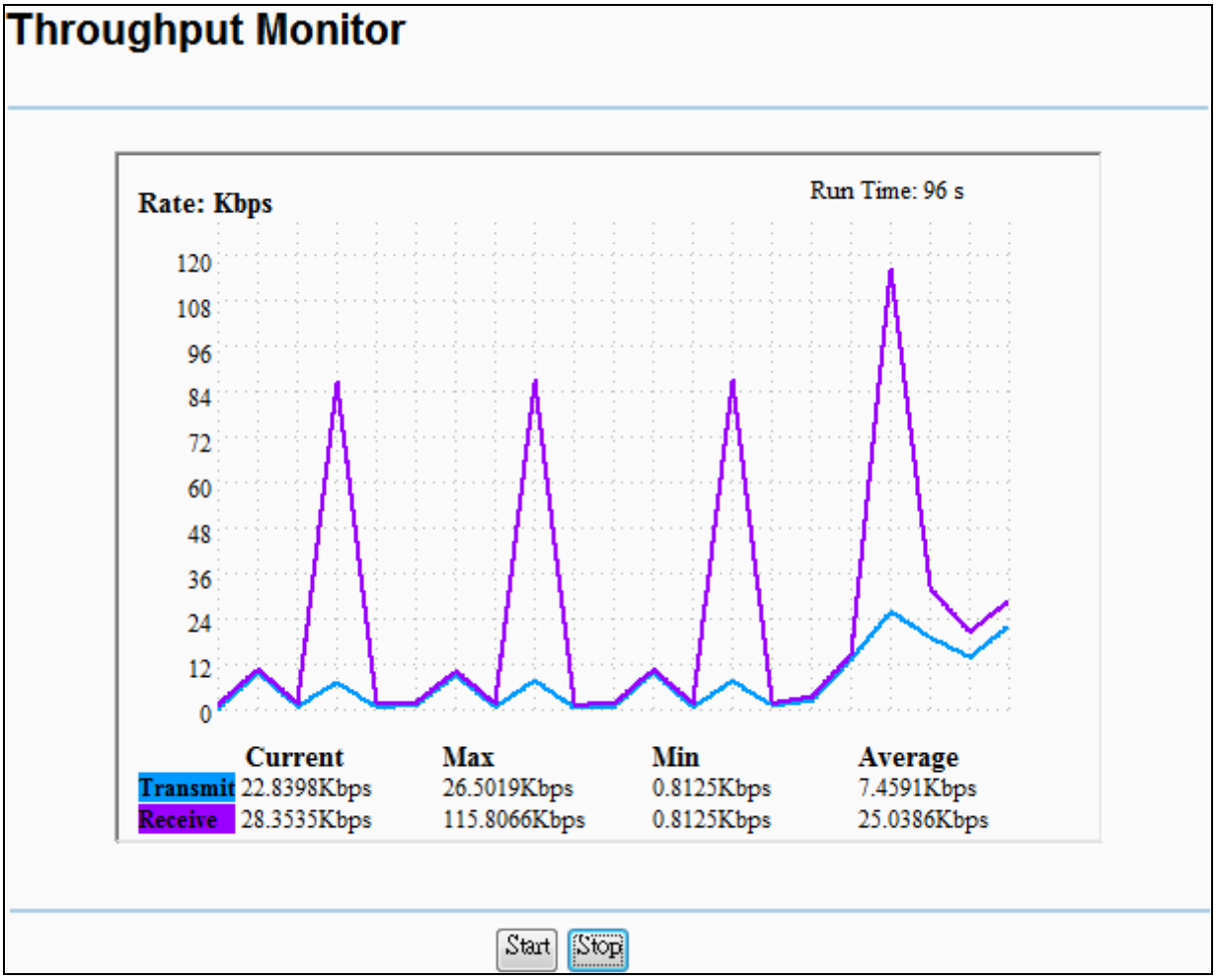


Figure 5-6-7-1 Throughput Monitor

The page includes the following fields:

Object	Description
• **Rate**	The Throughput unit.
• **Run Time**	How long this function is running.
• **Transmit**	The Wireless transmit rate information.
• **Receive**	The Wireless receive rate information.
• **Start**	Click the **Start** button to start wireless throughput monitor.
• **Stop**	Click the **Stop** button to stop wireless throughput monitor.

5.6.8 Wireless Statistics

Choose menu "**Wireless > Wireless Statistics**", and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

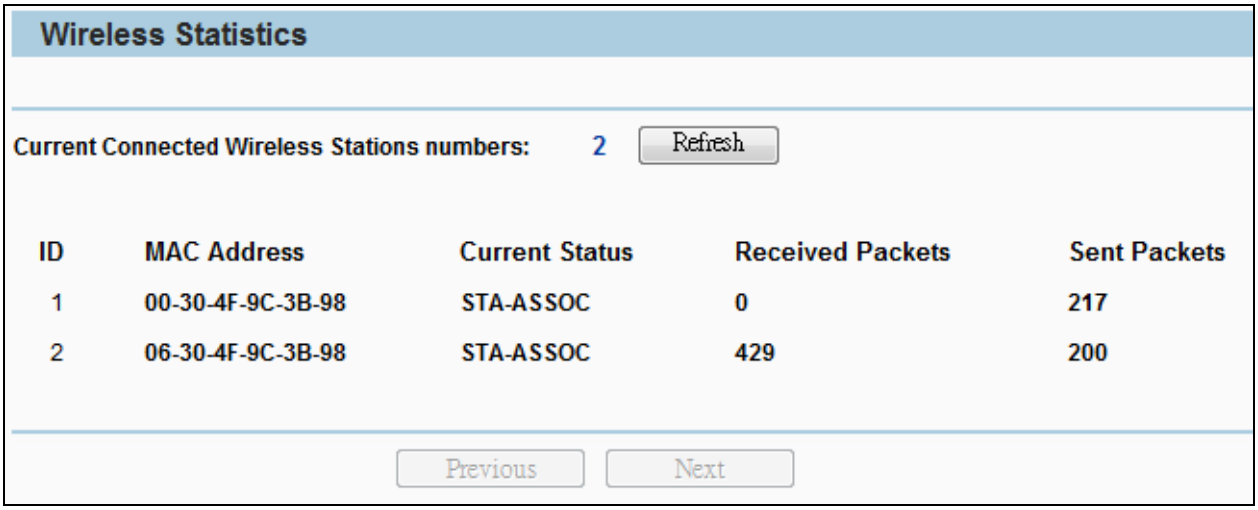


Figure 5-6-8-1 Wireless Statistics

The page includes the following fields:

Object	Description
• **MAC Address**	The connected wireless station's MAC address.
• **Current Status**	the connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
• **Received Packets**	packets received by the station.
• **Sent Packets**	packets sent by the station.

To update this page and to show the current connected wireless stations, click on the **Refresh** button.

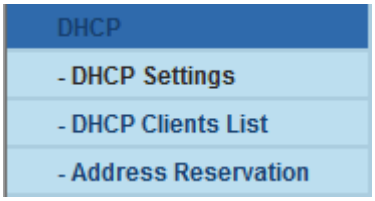
If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

This page will be refreshed automatically every 5 seconds.

5.7 DHCP

The DHCP (Dynamic Host Configuration Protocol) Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

There are three submenus under the DHCP menu: **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



5.7.1 DHCP Settings

Selecting **DHCP > DHCP Settings** will enable you to set up the AP as a DHCP server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server is Disable by default, and can be configured on the page (shown as **Figure 5-7-1**):

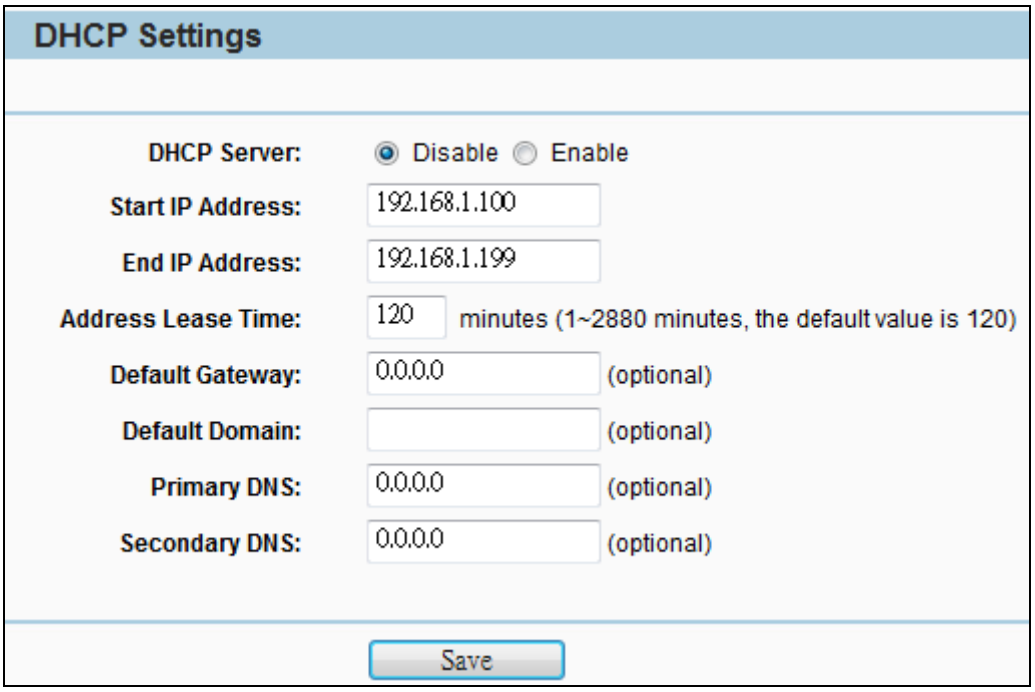


Figure 5-7-1 DHCP Settings

The page includes the following fields:

Object	Description
• **DHCP Server**	**Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
• **Start IP Address**	This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
• **End IP Address**	This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
• **Address Lease Time**	It is the length of time a network user will be allowed to keep

	connecting to the device with the current DHCP Address. Enter the amount of time (in minutes), and then the DHCP address will be "leased". The time range is 1~2880 minutes. The default value is 120 minutes.
• **Default Gateway**	(Optional) Input the IP Address of the gateway.
• **Default Domain**	(Optional) Input the domain name of your network.
• **Primary DNS**	(Optional) Input the DNS IP address provided by your ISP or consult your ISP.
• **Secondary DNS**	(Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Note

To use the DHCP server function of the device, you should configure all computers in the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the device reboots.

5.7.2 DHCP Clients List

Choose menu "**DHCP > DHCP Clients List**", and then you can view the information about the clients attached to the Device in the screen as shown in **Figure 5-7-2**.

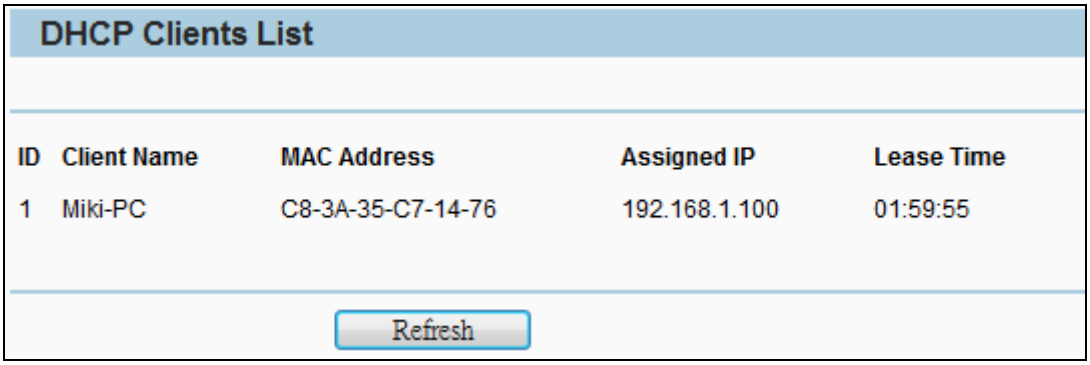


Figure 5-7-2 DHCP Client List

The page includes the following fields:

Object	Description
• **Client Name**	The name of the DHCP client.
• **MAC Address**	The MAC address of the DHCP client.
• **Assigned IP**	The IP address that the device has allocated to the DHCP client.
• **Lease Time**	The time of the DHCP client leased.

To update this page and to show the current connected devices, click on the **Refresh** button.

5.7.3 Address Reservation

Choose menu "**DHCP > Address Reservation**", and then you can view or add a reserved address for clients via the next screen (shown in **Figure 5-7-3**).

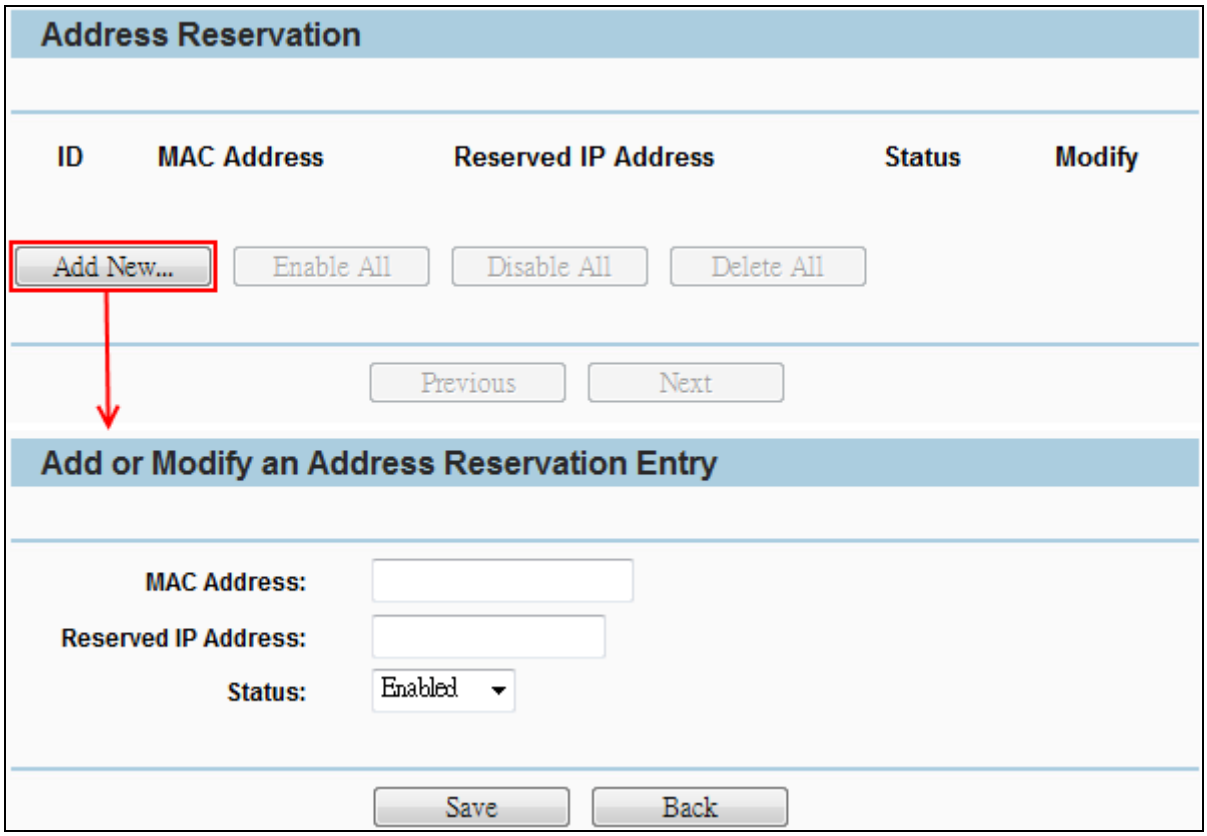


Figure 5-7-3 Address Reservation

The page includes the following fields:

Object	Description
• **MAC Address**	The MAC Address of the PC that you want to reserve an IP address for.
• **Reserved IP Address**	The IP address that the device reserved.
• **Status**	It shows whether the entry is enabled or not.
• **Modify**	To modify or delete an existing entry.
• **Add New…**	Click the **Add New...** button to add a new Address Reservation entry.
• **Enable All**	Click the **Enable All** button to enable all the entries in the table.
• **Disable All**	Click the **Disable All** button to disable all the entries in the table.

• **Delete All**	Click the **Delete All** button to delete all the entries in the table.
• **Next**	Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

■ How to Reserve IP Addresses

1. Click the **Add New...** button to add a new Address Reservation entry.
2. Enter the MAC Address (the format for the MAC Address is XX-XX-XX-XX-XX-XX.) and the IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button.

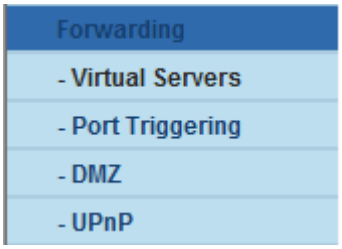
■ How to Modify a Reserved IP Address

1. Select the reserved address entry as you desired, **modify** it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

The changes will not take effect until the device reboots.

5.8 Forwarding

There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.



5.8.1 Virtual Servers

Choose menu "**Forwarding > Virtual Servers**", and then you can view and add virtual servers in the screen as shown in **Figure 5-8-1-1**.

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that is used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

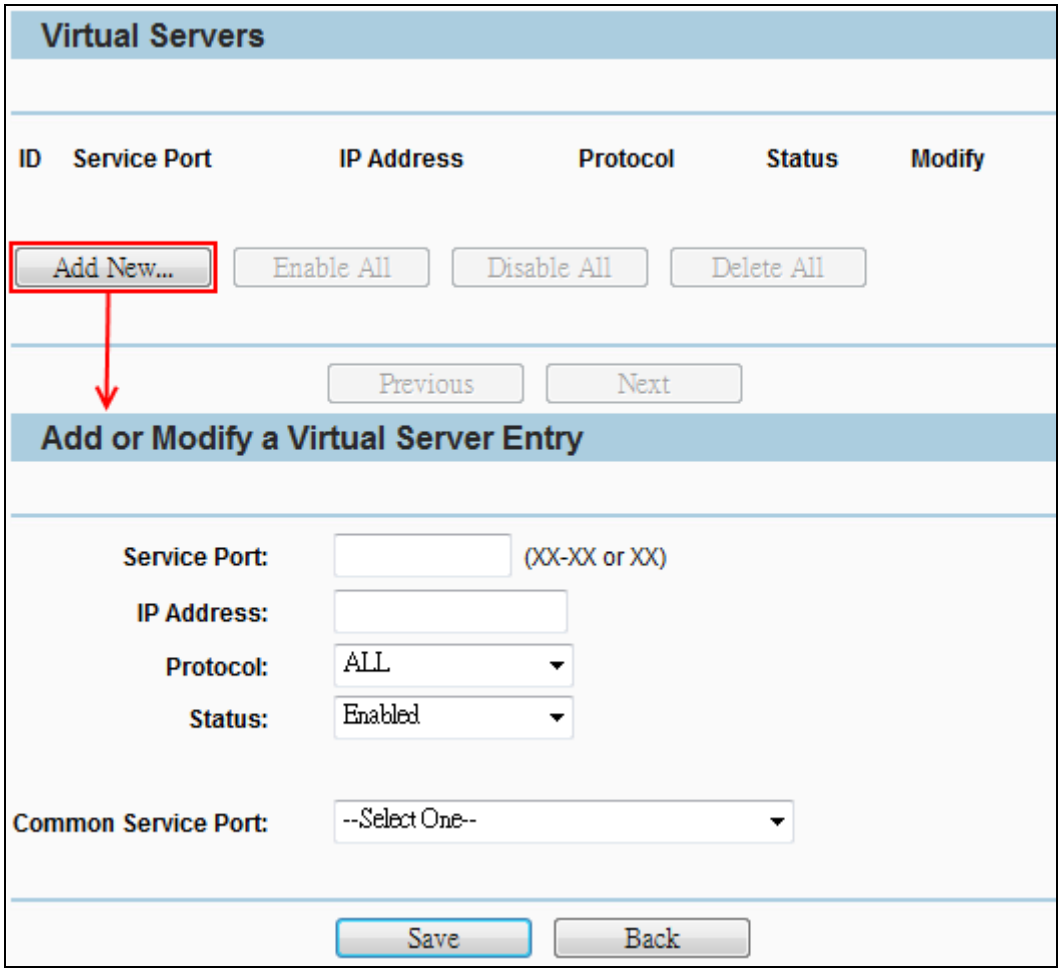


Figure 5-8-1-1 Virtual Servers

To setup a virtual server entry, **you can follow these steps:**

1. Click the **Add New...** button.
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** box.
3. Enter the IP address of the computer running the service application in the **IP Address** box.
4. Select the protocol used for this application in the **Protocol** box: **TCP**, **UDP**, or **All**.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

The page includes the following fields:

Object	Description
• **Service Port**	The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
• **IP Address**	The IP address of the PC running the service application.
• **Protocol**	The protocol used for this application, either TCP, UDP, or All (all

	protocols are supported by the Device.).
• **Status**	The status of this entry. "Enabled" means the virtual server entry is enabled.
• **Common Service Port**	Some common services already exist in the pull-down list.
• **Modify**	To modify or delete an existing entry.

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

   Click the **Enable/Disabled** All button to make all entries enabled/disabled.

   Click the **Delete All** button to delete all entries.

   Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

5.8.2 Port Triggering

Choose menu "**Forwarding > Port Triggering**", and then you can view and add port triggering in the screen as shown in **Figure 5-8-2-1**.

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Once configured, operation is as follows:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

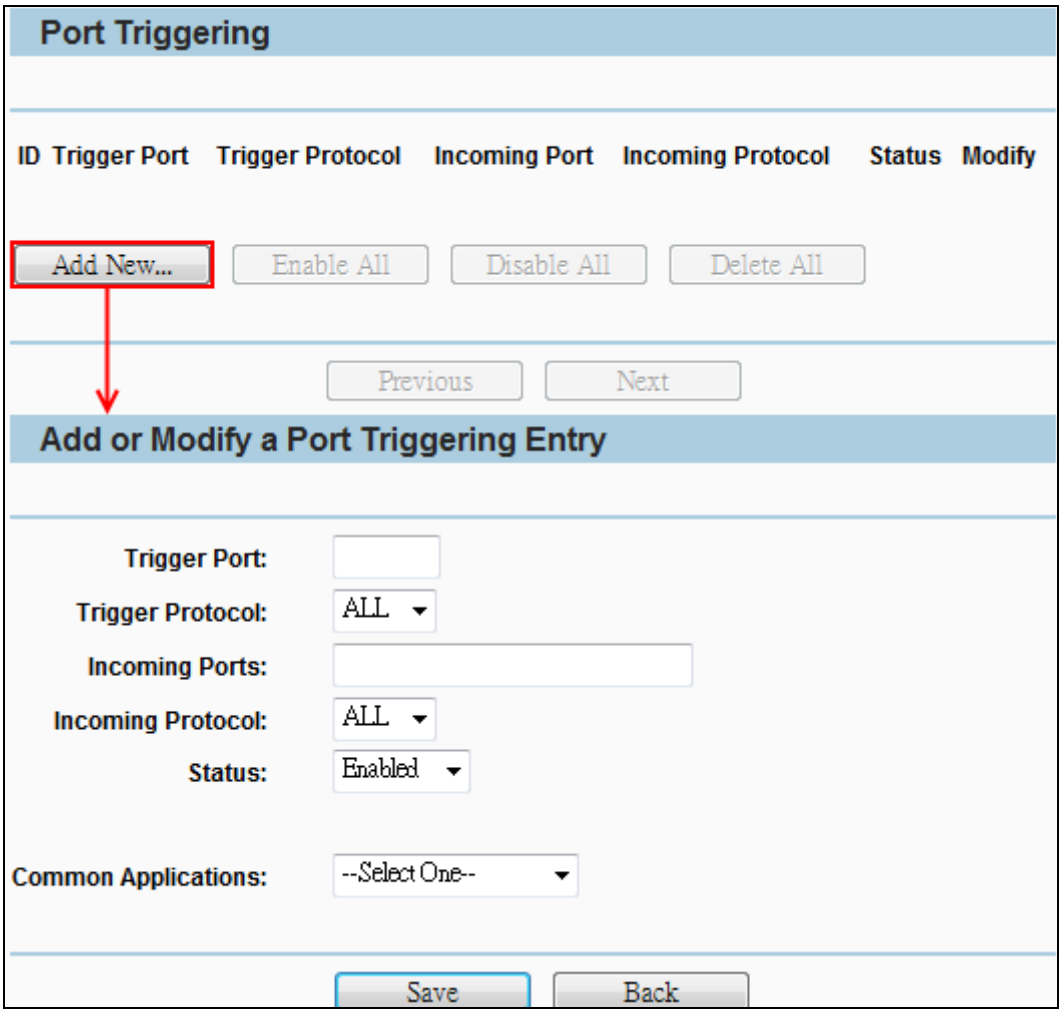


Figure 5-8-2-1 Port Triggering

To add a new rule on the Port Triggering screen:

1. Click the **Add New...** button.
2. Enter a port number used by the application to send an outgoing request in the Trigger Port box.
3. Select the protocol used for the **Trigger Port** from the pull-down list of Trigger Protocol, either TCP, UDP, or All.
4. Enter the range of port numbers used by the remote system when it responds to the PC's request in the Incoming Ports box.
5. Select the protocol used for **Incoming Ports** range from the pull-down list, either TCP, UDP, or All.
6. Select the **Enabled** option in the **Status** pull-down list.
7. Click the **Save** button to save the new rule.

The page includes the following fields:

Object	Description
• **Trigger Port**	The port for outgoing traffic. An outgoing connection using this port will Trigger this rule.
• **Trigger Protocol**	The protocol used for Trigger Ports, either **TCP, UDP**, or **All** (all protocols are supported by the Device.).

• **Incoming Port**	The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",". For example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
• **Incoming Protocol**	The protocol used for Incoming Port, either TCP, UDP, or ALL (all protocols are supported by the Device.).
• **Status**	The status of this entry. Enabled means the Port Triggering entry is enabled.
• **Modify**	To modify or delete an existing entry.
• **Common Applications**	Some popular applications already listed in the from the pull-down list of Incoming Protocol.

There are many popular applications in the Common Application list. You can select an application and then the boxes of Trigger Port and Incoming Ports will be automatically filled in. This has the same effect as adding a new rule.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.
   Click the **Enable All** button to enable all entries.
   Click the **Disable All** button to disable all entries.
   Click the **Delete All** button to delete all entries.
   Click the **Next** button to go to the next page and Click the **Previous** button to return to the previous page.

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Incoming Ports** ranges cannot overlap each other.

5.8.3 DMZ

Choose menu "**Forwarding > DMZ**", and then you can view and configure DMZ host in the screen as shown in **Figure 5-8-3-1**.

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video-conferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

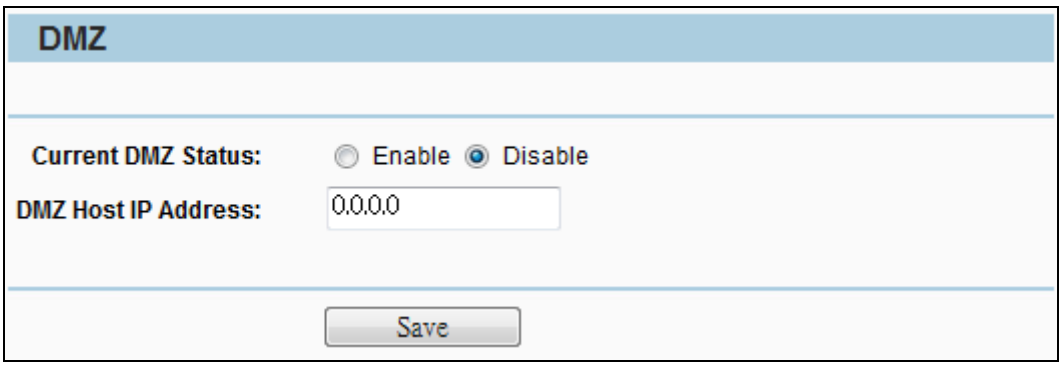


Figure 5-8-3-1 DMZ

Object	Description
• **Current DMZ Status**	Click the **Enable** button to enable DMZ.
• **DMZ Host IP Address**	Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
• **Save**	Click **Save** button to save the settings.

To assign a computer or server to be a DMZ server:

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

5.8.4 UPnP

Choose menu "**Forwarding > UPnP**", and then you can view the information about UPnP (Universal Plug and Play) in the screen as shown in **Figure 5-8-4-1**.

The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

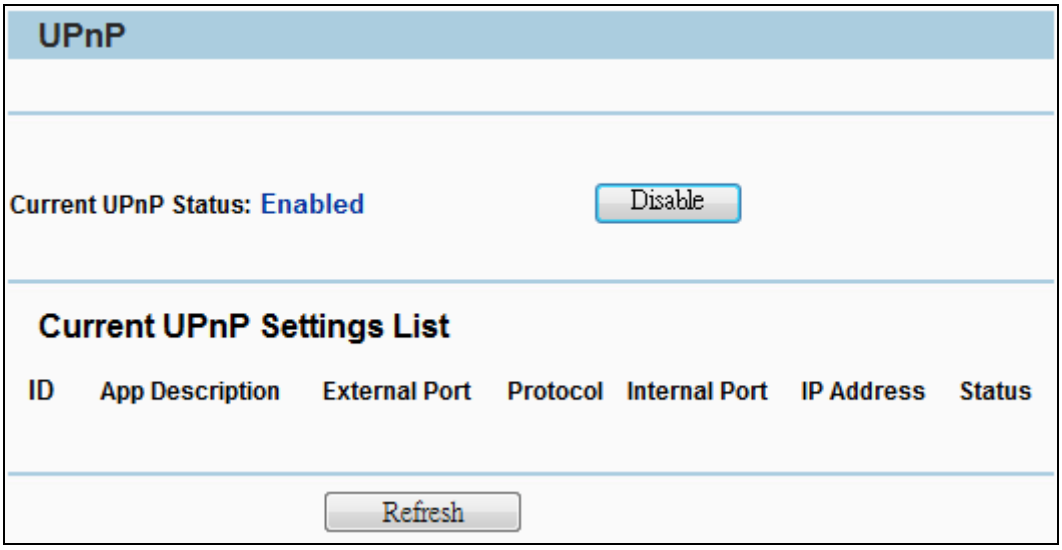


Figure 5-8-4-1 UPnP

Object	Description
• **Enable UPnP**	UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
• **Current UPnP Settings List**	Displays the current UPnP information.
• **App Description**	Description about the application which initiates the UPnP request.
• **External Port**	Port that the Device opened for the application.
• **Protocol**	Type of protocol that is opened.
• **Internal Port**	Port that the Device opened for local host.
• **IP Address**	IP address of the local host which initiates the UPnP request.
• **Status**	Either Enabled or Disabled. **Enabled** means that port is still active; otherwise, the port is inactive.
• **Enable**	Click the **Enable** button to enable UPnP.
• **Disable**	Click the **Disable** button to disable UPnP.
• **Refresh**	Click the **Refresh** button to update the Current UPnP Settings List.

In the computer connected with WNAP-7206, go to "**Network**" to check the WNAP-7206 is displayed in the list. Double-click it to logon the Web UI of WNAP-7206.

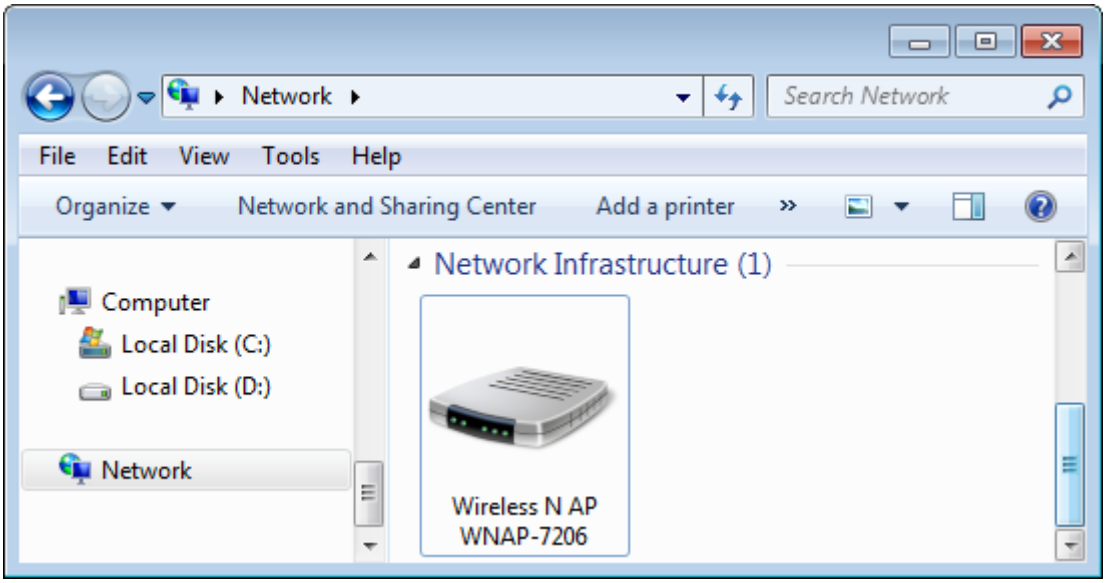


Figure 5-8-4-2 UPnP – Network Device

5.9 Security

There are four submenus under the Security menu: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

5.9.1 Basic Security

Choose menu "**Security > Basic Security**" and then you can configure the basic security in the screen as shown in **Figure 5-9-1-1**.

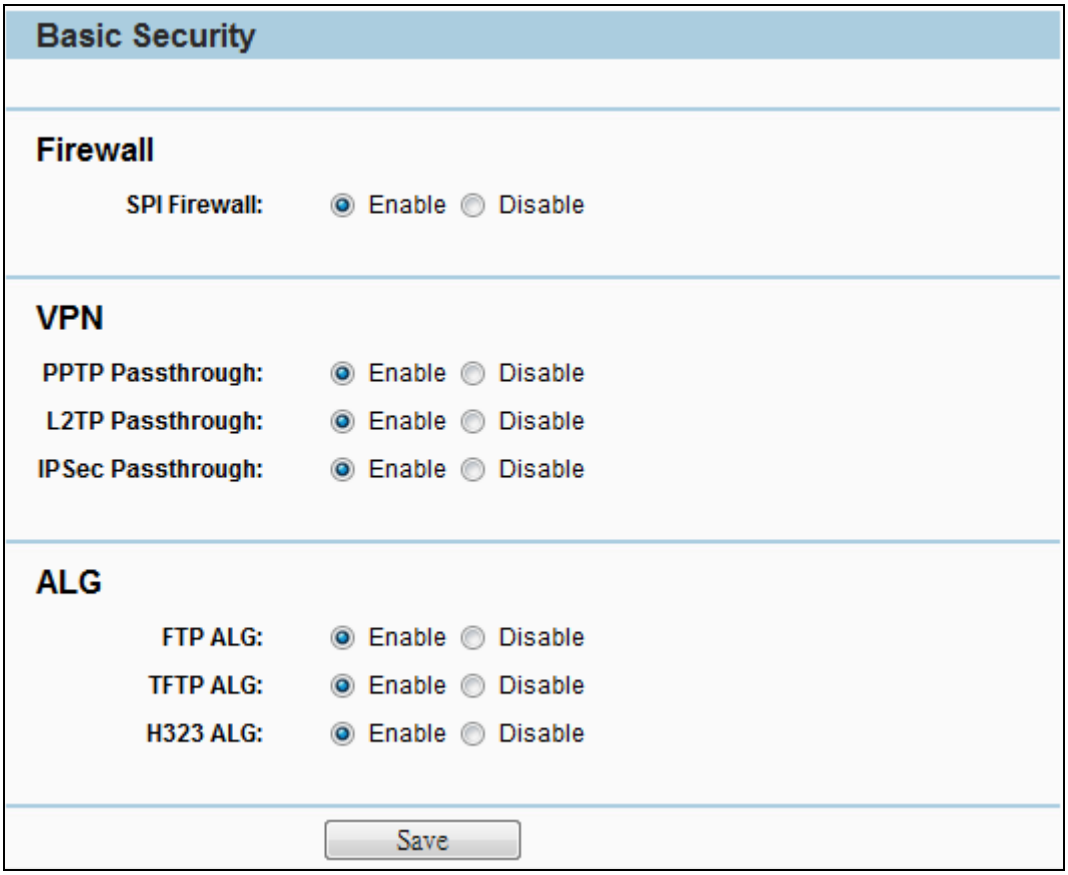


Figure 5-9-1-1 Basic Security Settings

You can configure the Basic Security Settings on this page.

Object	Description
• **Firewall**	Here you can enable or disable the Router's firewall.
• **VPN**	VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.

• **ALG**	It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

The page includes the following fields:

Object	Description
Firewall	
• **SPI Firewall**	Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
VPN	
• **PPTP Passthrough**	PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable.
• **L2TP Passthrough**	Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable.
• **IPSec Passthrough**	Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.
ALG	
• **FTP ALG**	To allow FTP clients and servers to transfer data across NAT, click Enable.
• **TFTP ALG**	To allow TFTP clients and servers to transfer data across NAT, click Enable.
• **H323 ALG**	To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.
• **Save**	Click the **Save** button to save the settings.

5.9.2 Advanced Security

Choose menu "**Security > Advanced Security**", and then you can protect the Device from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood in the screen as shown in **Figure 5-9-2-1**.

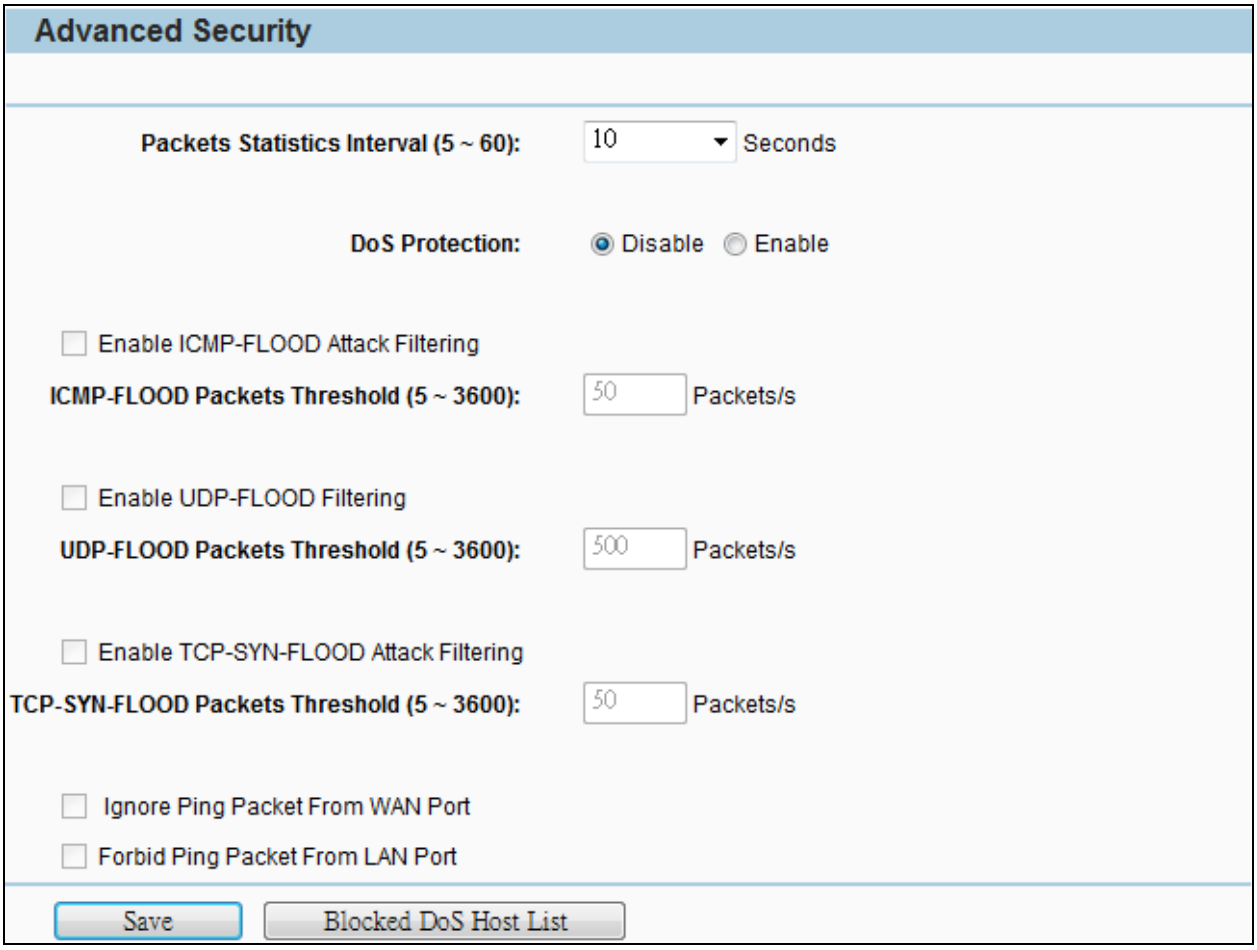


Figure 5-9-2-1 Advanced Security Settings

The page includes the following fields:

Object	Description
• **Packets Statistics interval (5~60)**	The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood.
• **DoS Protection**	Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
• **Enable ICMP-FLOOD Attack Filtering**	Enable or Disable the ICMP-FLOOD Attack Filtering.
• **ICMP-FLOOD Packets Threshold (5~3600)**	The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.

• **Enable UDP-FLOOD Filtering**	Enable or Disable the UDP-FLOOD Filtering.
• **UDP-FLOOD Packets Threshold (5~3600)**	The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.
• **Enable TCP-SYN-FLOOD Attack Filtering**	Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
• **TCP-SYN-FLOOD Packets Threshold (5~3600)**	The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.
• **Ignore Ping Packet From WAN Port**	Enable or Disable Ignore Ping Packet From WAN Port. The default setting is Disabled. If enabled, the ping packet from Internet cannot access the Device.
• **Forbid Ping Packet From LAN Port**	Enable or Disable Forbid Ping Packet From LAN Port. The default setting is Disabled. If enabled, the ping packet from LAN cannot access the Device and defend against some viruses.
• **Save**	Click the **Save** button to save the settings.
• **Blocked DoS Host List**	Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

FLOOD Filtering will take effect only when the **Traffic Statistics** in **System Tools** is enabled.

5.9.3 Local Management

Choose menu "**Security > Local Management**", and then you can configure the management rule in the screen as shown in **Figure 5-9-3-1**. The management feature allows you to deny computers in LAN from accessing the Device.

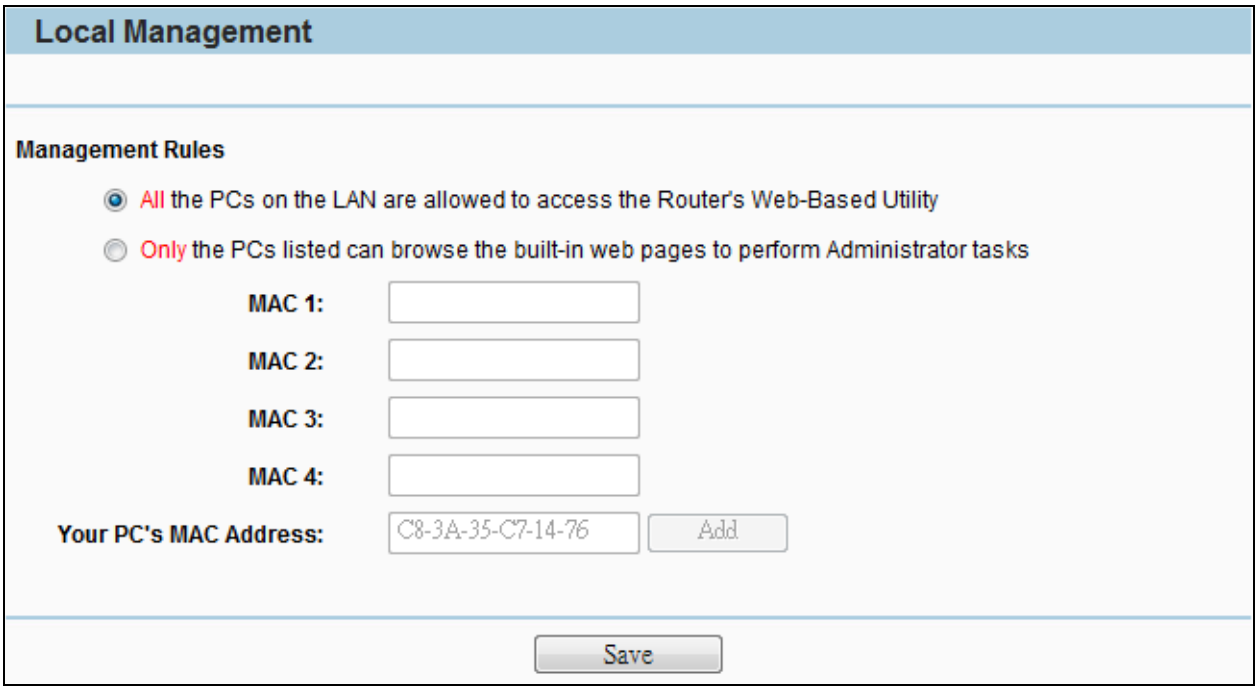


Figure 5-9-3-1 Local Management Settings

By default, the radio button **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** is selected. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally, from inside the network, click the radio button **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the Control List above.
Click the **Save** button to save your settings.

Note

If your PC is blocked and you want to access the Router again, use a pin to press and hold the **Reset Button** on the back panel about 5 seconds to reset the Router's factory defaults in the Router's Web-Based Utility.

5.9.4 Remote Management

Choose menu "**Security > Remote Management**", and then you can configure the Remote Management function in the screen as shown in **Figure 5-9-4-1**. This feature allows you to manage your Device from a remote location via the Internet.

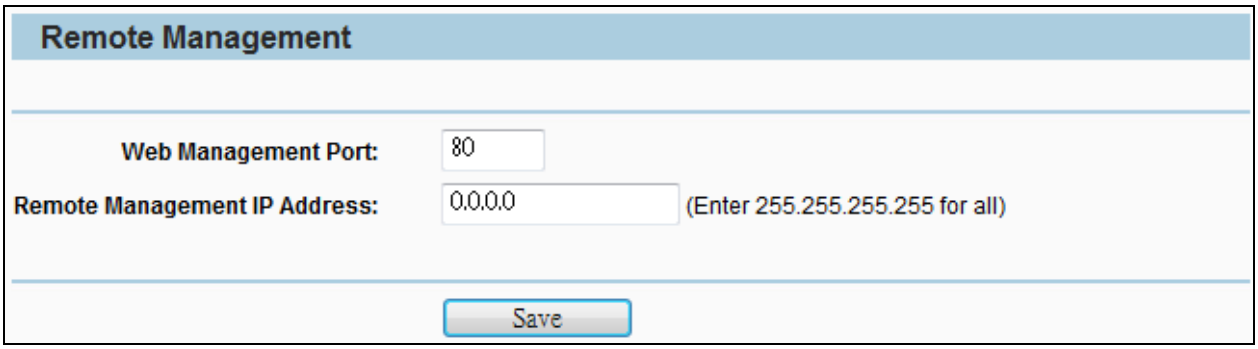


Figure 5-9-4-1 Remote Management Settings

The page includes the following fields:

Object	Description
• **Web Management Port**	Web browser access normally uses the standard HTTP service port 80. This Device's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65535 but do not use the number of any common service port.
• **Remote Management IP Address**	This is the current address you will use when accessing your Device from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function you should change 0.0.0.0 to a valid IP address. If set to be 255.255.255.255, then all the hosts can access the Device from Internet.
• **Save**	Click the **Save** button to save the settings.

To access the Device, you should enter your Device's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box.

..

For example, if your Device's WAN address is 210.66.155.72 and you use port number 8080, enter http://210.66.155.72:8080 in your browser. If you use the default port 80, you just need to enter http://210.66.155.72 in your browser. You will be asked for the Device's password.

After successfully entering the password, you will be able to access the Device's web-based utility.

5.10 Parental Control

Choose menu "**Parental Control**", and then you can configure the parental control in the screen as shown in **Figure 5-10-1**. The Parental Control function can be used to control the Internet activities of the children, their access to certain websites, as well as the time of surfing.

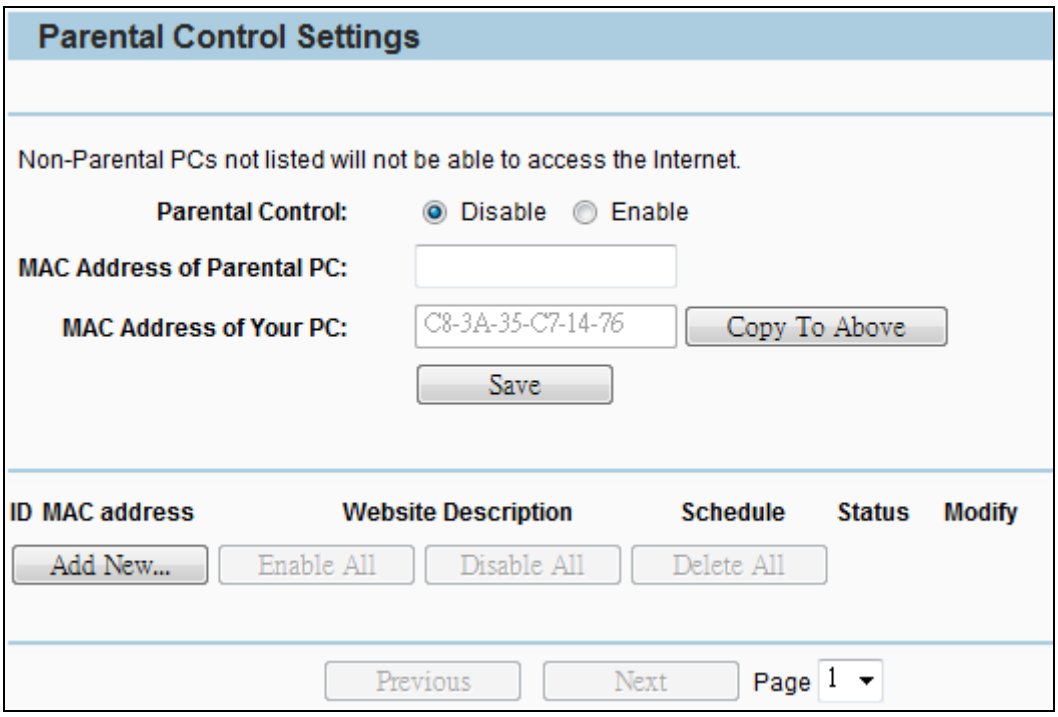


Figure 5-10-1 Parental Control Settings

The page includes the following fields:

Object	Description
• **Parental Control**	Check Enable if you want this function to take effect, otherwise check Disable.
• **MAC Address of Parental PC**	In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above button** below.
• **MAC Address of Your PC**	This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
• **Website Description**	Description of the allowed website for the PC controlled.
• **Schedule**	The time period allowed for the PC controlled to access the Internet. For detailed information, please go to **Access Control > Schedule**.
• **Modify**	Here you can edit or delete an existing entry.
• **Copy to Above**	Copy the **MAC Address of Your PC** to the field **MAC Address of Parental PC**.
• **Save**	Click **Save** to save above settings.

• **Add New...**	Click the **Add New...** button to add a new Parental Control entry
• **Enable All**	Click the **Enable All** button to enable all the rules in the list.
• **Disable All**	Click the **Disable All** button to disable all the rules in the list.
• **Delete All**	Click the **Delete All** button to delete all the entries in the table.
• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
• **MAC Address of Childen's PC**	Enter the MAC address of the PC you want to control, or you can make use of the All MAC Address In Current LAN item below. If you leave it blank, then the rule will be applied to all of the PCs except the parental PC.
• **ALL MAC Address In Current LAN**	You can see the MAC addresses of all PCs in current LAN by clicking on the drop-down button. Choose one of them, then this MAC address will be filled to the MAC Address of Child PC field.
• **Website description**	In this field, create a description for the website(s). Note that this description should be **unique**.
• **Allowed Website Name**	In this field, you can enter 8 domain names allowed for the child to access, either the full name or the keywords (for example google). Any domain name with keywords in it (www.google.com, news.google.com) will be allowed.
• **Effective Time**	In this field, choose the effective time for the rule or you can make use of **Access Control > Schedule** to create the schedule as you like. The default value is Anytime.
• **Status**	In this field, there are two options, Enabled or Disabled. Enabled means that this rule will take effect while Disabled means that this rule won't take effect.
• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.

5.11 Access Control

There are four submenus under the Access Control menu: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

The Device, providing convenient and strong **Internet access control** function, can control the Internet activities of hosts in the LAN. Moreover, you can flexibly combine the **Host List**, **Target List** and **Schedule** to restrict the Internet surfing of these hosts.

5.11.1 Rule

Choose menu "**Access Control > Rule**", and then you can view and set Access Control rules in the screen as shown in **Figure 5-11-1-1**.

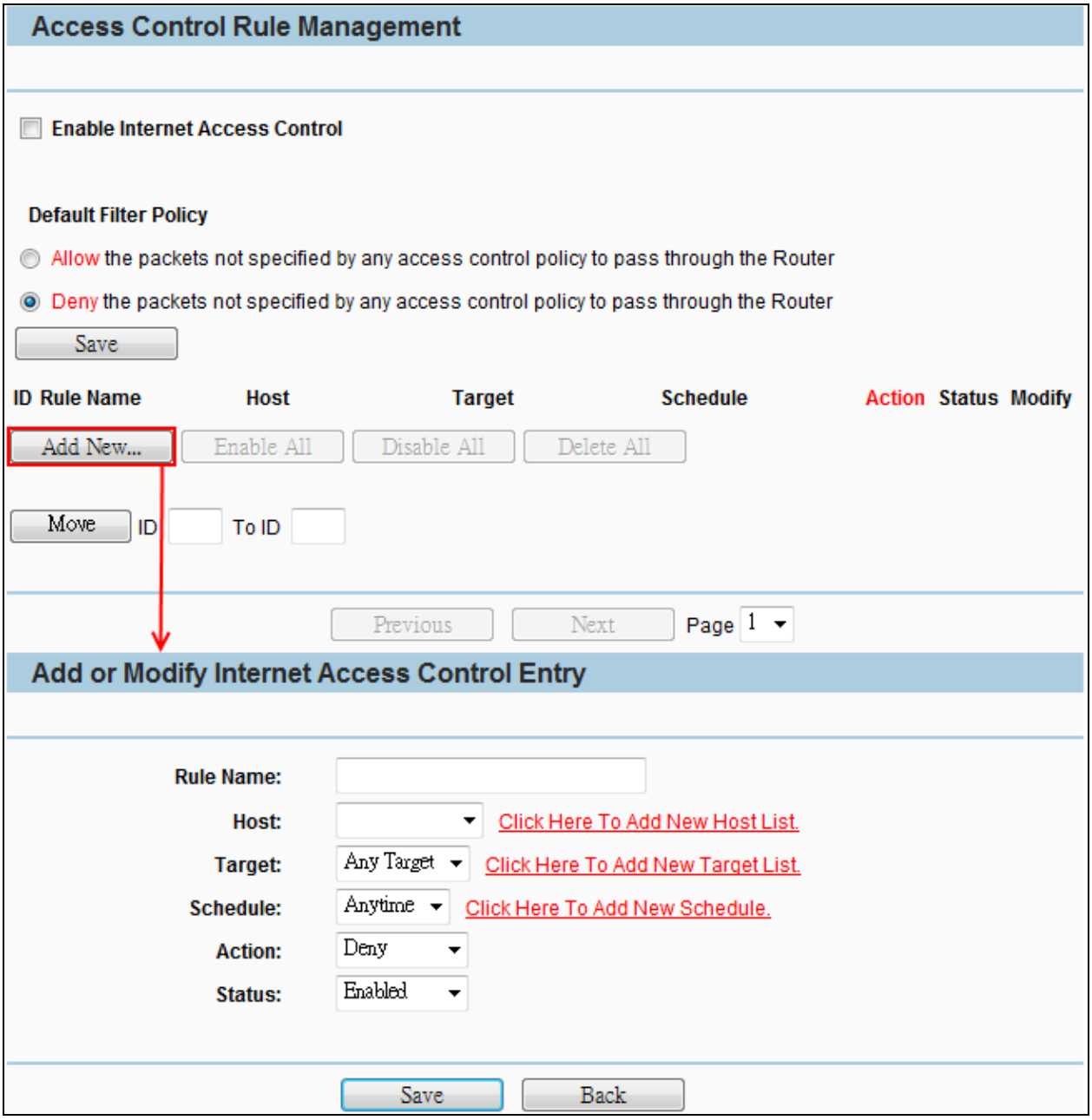


Figure 5-11-1-1 Rule Setting

The page includes the following fields:

Object	Description
• **Enable Internet Access Control**	Select the check box to enable the Internet Access Control function, and then the **Default Filter Policy** can take effect.
• **Rule Name**	Here displays the name of the rule and this name is unique.
• **Host**	Here displays the host selected in the corresponding rule.
• **Target**	Here displays the target selected in the corresponding rule.
• **Schedule**	Here displays the schedule selected in the corresponding rule.
• **Action**	Here displays the action the Device takes to deal with the packets. It could be **Allow** or **Deny**. **Allow** means that the Device permits the packets to go through the Device. **Deny** means that the Device rejects the packets to go through the Device.
• **Status**	This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
• **Modify**	Here you can edit or delete an existing rule.
• **Add New...**	Click the **Add New...** button to add a new host entry.
• **Enable All**	Click the **Enable All** button to enable all the rules in the list.
• **Disable All**	Click the **Disable All** button to disable all the rules in the list.
• **Delete All**	Click the **Delete All** button to delete all the entries in the table.
• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
• **Rule Name**	In this field, create a name for the rule. Note that this name should be **unique**.
• **Host**	In this field, select a host from the drop-down list for the rule.
• **Target**	In this filed, select a target from the drop-down list for the rule. The default value is Any Target.
• **Schedule**	In this field, select a schedule from the drop-down list for the rule. The default value is Anytime.
• **Action**	In this field, there are two options, **Allow** or **Deny**. **Allow** means the Router permits the packets to go through the Router. **Deny** means the Router rejects the packets to go through the Router.
• **Status**	In this field, there are two options, **Enable** or **Disable**. Select Enable so that the rule will take effect. Select Disable so that the rule won't take effect.
• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.

5.11.2 Host

Choose menu "**Access Control > Host**", and then you can view and set a Host list in the screen as shown in Figure 5-11-2-1. The host list is necessary for the Access Control Rule.

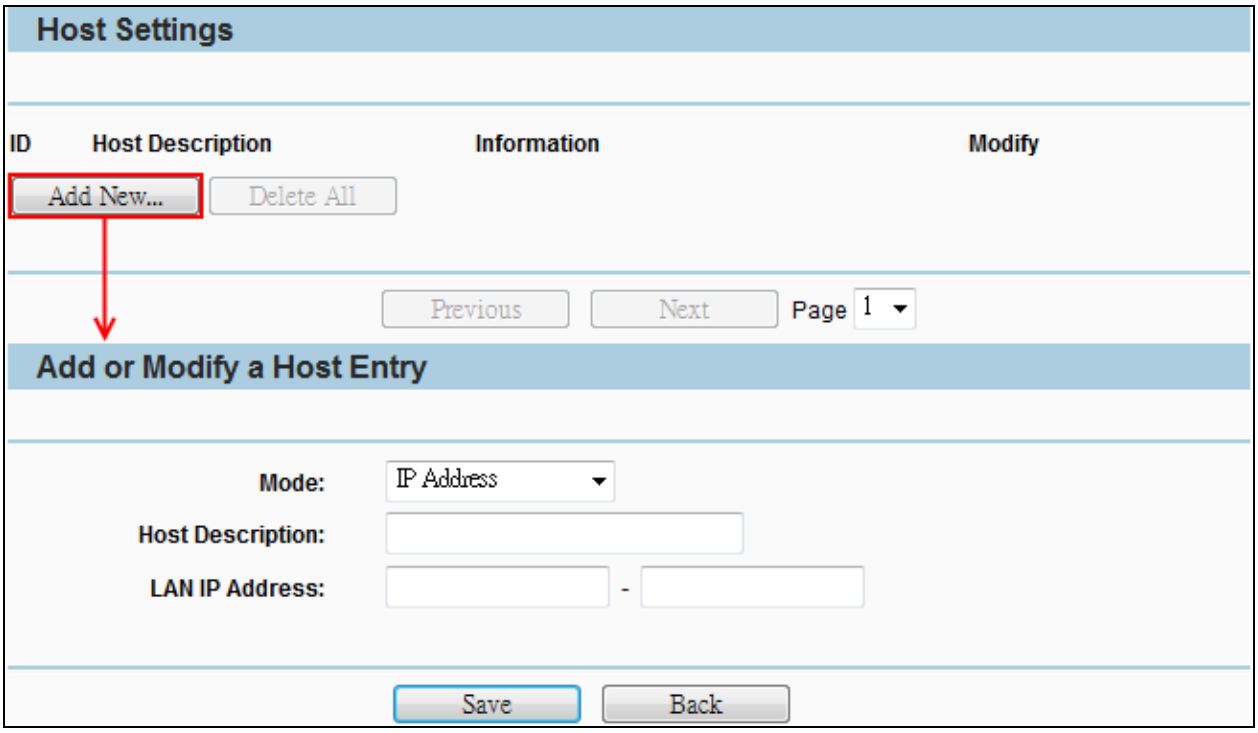


Figure 5-11-2-1 Host Setting

The page includes the following fields:

Object	Description
• **Host Description**	Here displays the description of the host and this description is **unique**.
• **Information**	Here displays the information about the host. It can be IP or MAC.
• **Modify**	To modify or delete an existing entry.
• **Add New...**	Click the **Add New...** button to add a new host entry.
• **Delete All**	Click the **Delete All** button to delete all entries.
• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
• **Mode**	Here are two options, IP Address and Domain Name. You can choose either of them from the drop-down list.
• **LAN IP Address**	If the IP Address Mode is selected, you can see the following item: **IP Address** - Enter the IP address (or address range) of the host in dotted-decimal format, for example 192.168.1.23.
• **MAC Address**	If the MAC Address Mode is selected, you can see the following item: **MAC Address** - Enter the MAC address of the host in XX-XX-XX-XX-XX-XX format, for example 00-11-22-33-44-AA.

• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.

5.11.3 Target

Choose menu "**Access Control > Target**", and then you can view and set a Target list in the screen as shown in **Figure 5-11-3-1**. The target list is necessary for the Access Control Rule.

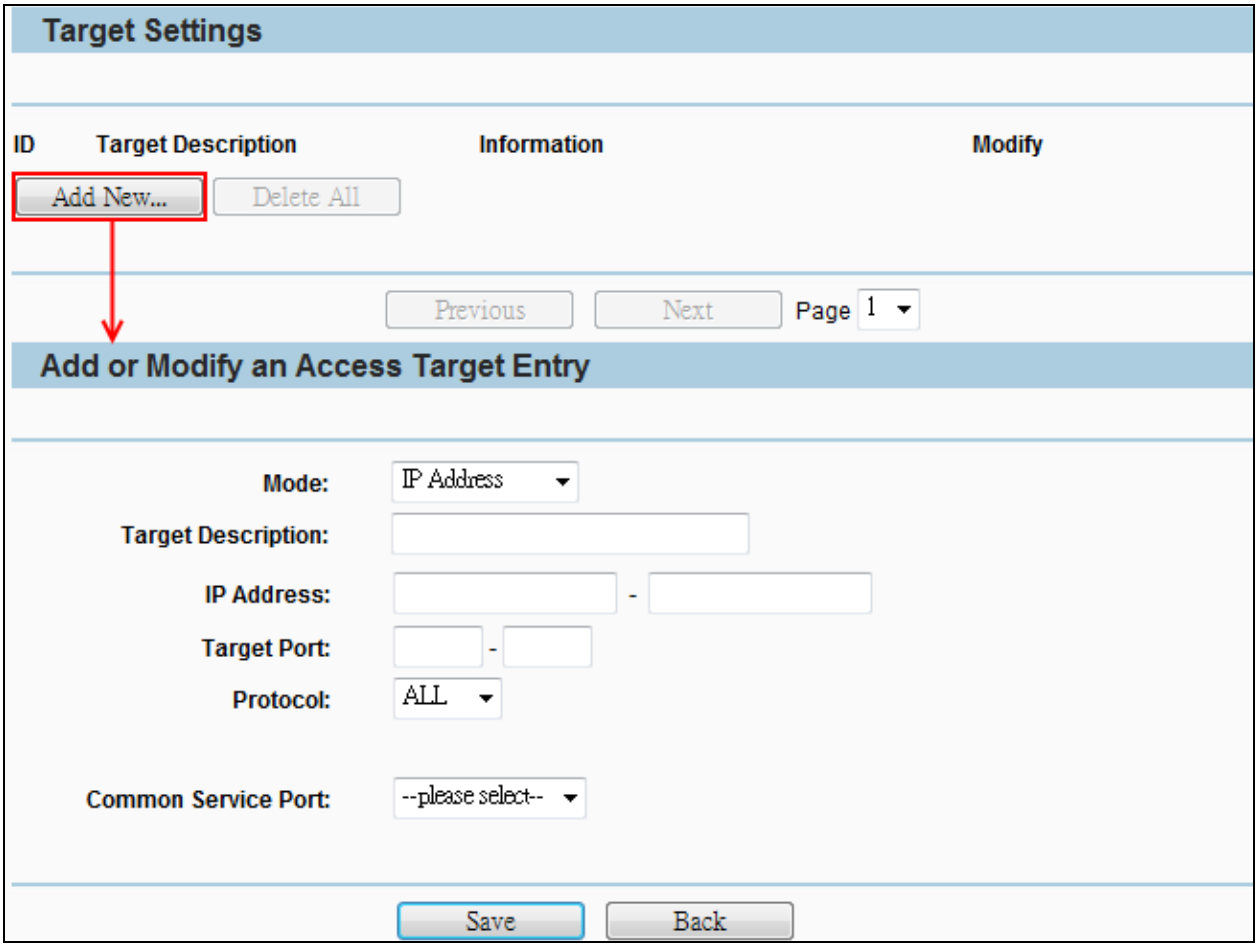


Figure 5-11-3-1 Target Setting

The page includes the following fields:

Object	Description
• **Target Description**	Here displays the description about the target and this description is **unique**.
• **Information**	The target can be IP address, port, or domain name.
• **Modify**	To modify or delete an existing entry.
• **Add New...**	Click the **Add New...** button to add a new target entry.
• **Delete All**	Click the **Delete All** button to delete all entries.

• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
• **Mode**	Here are two options, IP Address and Domain Name. You can choose either of them from the drop-down list.
• **IP Address**	Enter the IP address (or address range) of the target (targets) in dotted-decimal format, for example 192.168.1.23.
• **Target Port**	Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
• **Protocol**	Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
• **Common Service Port**	Here lists some common service ports. Select one from the drop-down list, and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.
• **Domain Name**	If the Domain Name is selected, you will see the following items **Domain Name** - Here you can enter 4 domain names, either the full name or the keywords (for example google). Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed.
• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.

5.11.4 Schedule

Choose menu “**Access Control > Schedule**” screen as shown in **Figure 5-11-4-1**. The Schedule list is necessary for the Access Control Rule.

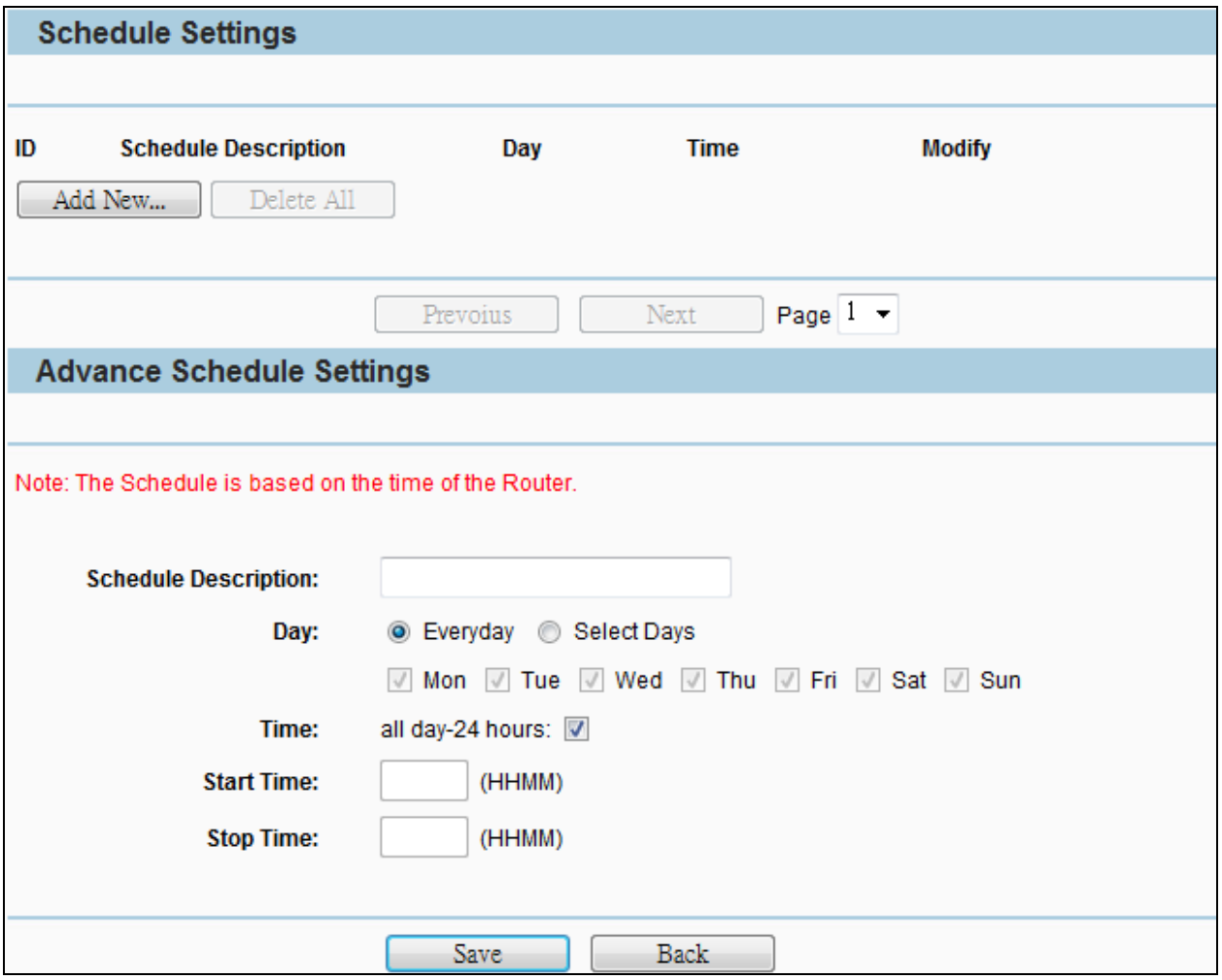


Figure 5-11-4-1 Schedule Setting

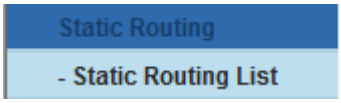
The page includes the following fields:

Object	Description
• **Schedule Description**	In this field, create a description for the schedule. Note that this description should be **unique**, for example Schedule_1.
• **Day**	Here displays the day(s) in a week.
• **Time**	Here displays the time period in a day.
• **Modify**	Here you can edit or delete an existing schedule.
• **Add New...**	Click the **Add New...** button to add a new target entry.
• **Delete All**	Click the **Delete All** button to delete all entries.
• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
• **Start Time**	Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
• **Stop Time**	Enter the stop time in HHMM format (HHMM are 4 numbers). For

	example 2000 is 20:00.
• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.

5.12 Static Routing

There is only one submenu under the Static Routing menu: **Static Routing List**. Click it, and you will be able to configure the corresponding function.



Choose menu "**Static Routing > Static Routing List**", and then you can configure the static route in the next screen (shown in **Figure 5-12-1**).

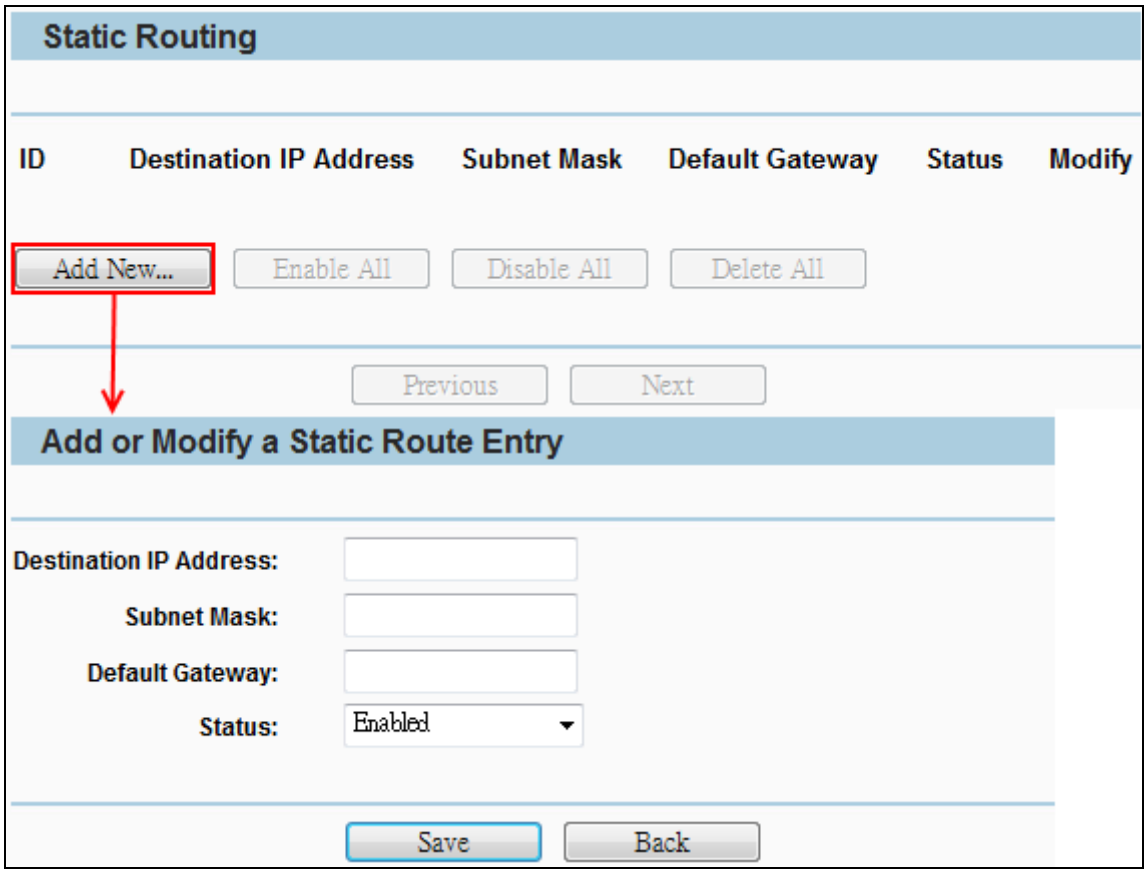


Figure 5-12-1 State Routing

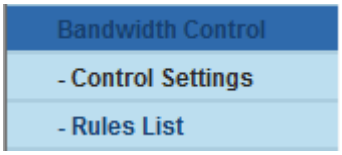
The page includes the following fields:

Object	Description
• **Add New…**	Click the **Add New...** button to add a static routing entry.

• **Destination IP Address**	The address of the network or host that you want to assign to a static route
• **Subnet Mask**	Determines which portion of an IP address is the network portion, and which portion is the host portion.
• **Default Gateway**	The IP address of the default gateway device that allows for the contact between the Device and the network or host
• **Status**	• **Enable -** Select the **Enabled** in the **Status** pull-down list to enable the entry. • **Disable -** Select the **Disabled** in the **Status** pull-down list to disable the entry.
• **Save**	Click the **Save** button to save the changes.
• **Back**	Click the **Back** button to back to the previous page.
• **Enable All**	Click the **Enable All** button to enable all entries.
• **Disable All**	Click the **Disable All** button to disable all entries.
• **Delete All**	Click the **Delete All** button to delete all entries.

5.13 Bandwidth Control

There are two submenus under the Bandwidth Control menu: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



5.13.1 Control Settings

Choose menu "**Bandwidth Control > Control Settings**", and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in **Figure 5-13-1-1**). Their values should be configured less than 1000000Kbps.

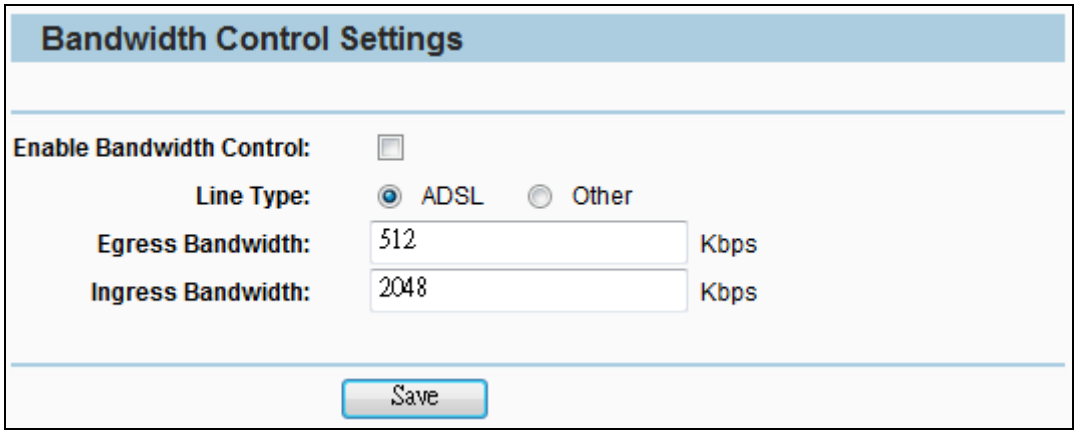


Figure 5-13-1-1 Bandwidth Control Settings

The page includes the following fields:

Object	Description
• **Enable Bandwidth Control**	If enabled, the Bandwidth Control rules will take effect.
• **Line Type**	Select your Line Type provided by your ISP.
• **Egress Bandwidth**	The upload speed through the WAN port.
• **Ingress Bandwidth**	The download speed through the WAN port.

5.13.2 Rules List

Choose menu "**Bandwidth Control > Rules List**", and then you can view and configure the Bandwidth Control rules in the screen below.

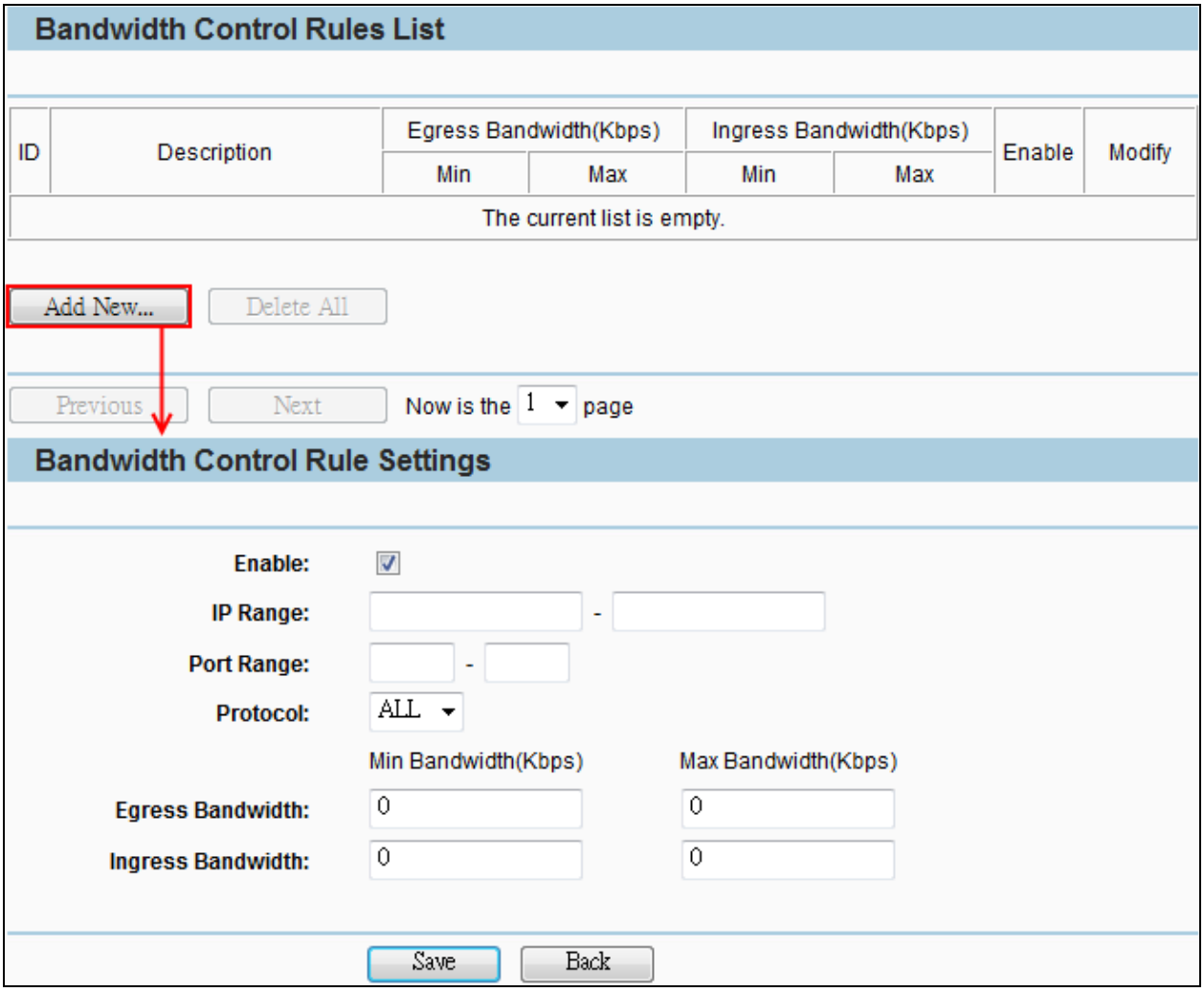


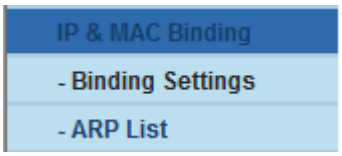
Figure 5-13-2-1 Rules List

The page includes the following fields:

Object	Description
• **ID**	The sequence of entry.
• **Description**	The information of description includes address range, the port range and protocol of transport layer.
• **Egress Bandwidth**	The max upload speed which through the WAN port. The default number is 0.
• **Ingress Bandwidth**	The max download speed which through the WAN port. The default number is 0.
• **Enable**	Rule status, which shows whether the rule takes effect.
• **Modify**	Choose to modify or delete an existing entry.

5.14 IP & MAC Binding

There are two submenus under the IP &MAC Binding menu: **Binding Settings** and **ARP List**. Click either of them, and you will be able to view or configure the corresponding function. The detailed explanations for each submenu are provided below.



5.14.1 Binding Settings

Choose menu "**IP & MAC Binding > Binding Settings**", and then you can view and configure the IP&MAC Binding in the screen below.

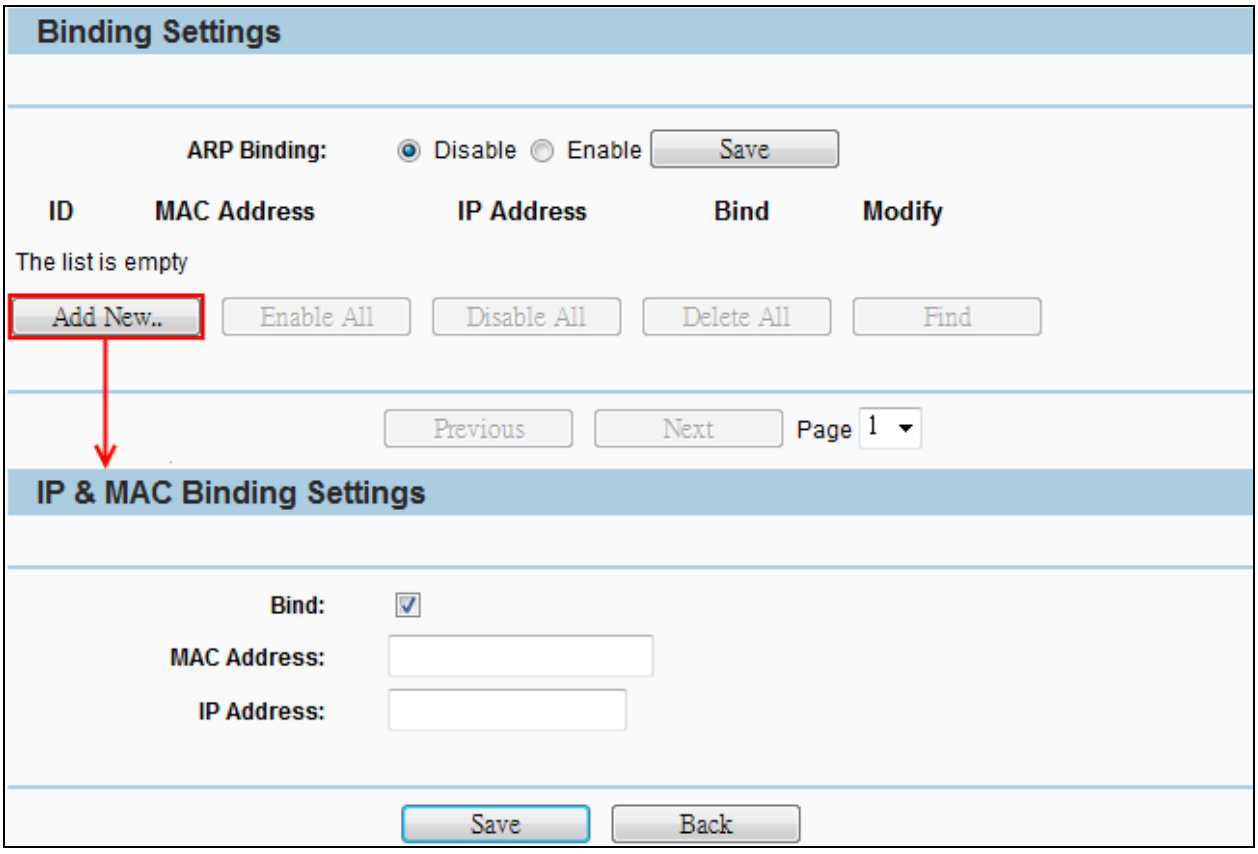


Figure 5-14-1-1 Binding Settings

The page includes the following fields:

Object	Description
• **MAC Address**	The MAC address of the controlled computer in the LAN.
• **IP Address**	The assigned IP address of the controlled computer in the LAN.
• **Bind**	Check this option to enable ARP binding for a specific device.
• **Modify**	To modify or delete an existing entry.

• **Add New…**	Click the **Add New…** button to add a new entry to the table.
• **Enable All**	Click the **Enable All** button to enable all entries.
• **Disable All**	Click the **Disable All** button to disable all entries.
• **Delete All**	Click the **Delete All** button to delete all entries.
• **Find**	Click **Find** button to find existed entry you want.

5.14.2 ARP List

Choose menu "**IP&MAC Binding > ARP List**", and then you can view and configure the ARP List in the screen below shown in **Figure 5-14-2-1**.

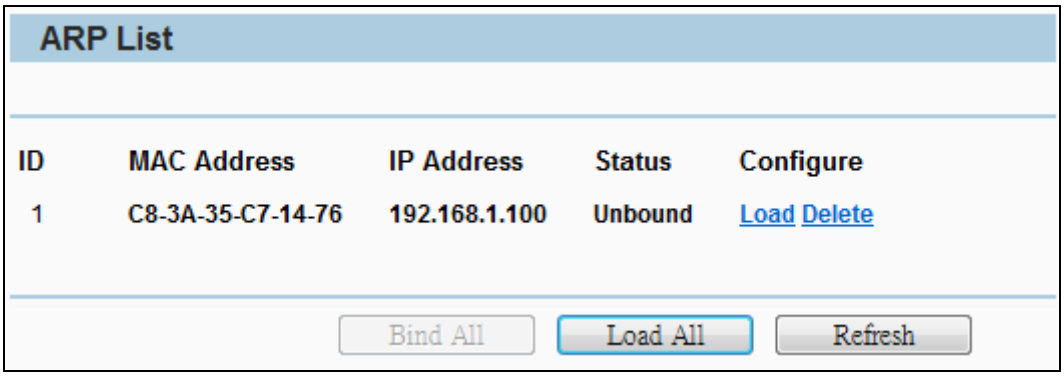


Figure 5-14-2-1 ARP List

The page includes the following fields:

Object	Description
• **MAC Address**	The MAC address of a controlled computer in the LAN.
• **IP Address**	The assigned IP address of a controlled computer in the LAN.
• **Status**	Indicates whether or not the MAC and IP addresses are bound.
• **Configure**	These buttons are for loading or deleting an item. ■ **Load** - Load the item to the IP & MAC Binding list. ■ **Delete** - Delete the item from the list.
• **Bind All**	Bind all current items. This option is only available when ARP Binding is enabled and saved in the Binding Setting page.
• **Load All**	Load all items into the IP & MAC Binding list.

Note

An item cannot be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items have no interference with the IP & MAC Binding list.

5.15 Dynamic DNS

The Device offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Device. Before using this feature, you can sign up the PLANET DDNS free service www.planetddns.com. Then you will be able to use PLANET DDNS service.

Figure 5-15-1

The page includes the following fields:

Object	Description
• **Service Provider**	Select your Dynamic DNS Provider from the list.
• **User Name**	Enter the name of your DDNS account.
• **Password**	Password: Enter the password of the DDNS account.
• **Domain Name**	Enter the host name or domain name provided by your DDNS service provider.
• **Enable DDNS**	Check Enable DDNS to enable DDNS service.
• **Connection Status**	The status of the DDNS service connection is displayed here.
• **Login**	Click the **Login** button to login the DDNS service.
• **Logout**	Click **Logout** to logout the DDNS service.

Note

If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

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) for how to register a free account.

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

Step 1. Select "**Planet (www.planetddns.com)**" from the service provider's list.
If you didn't have Planet DDNS account, click the hyperlink Go to register… to register a new account.

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

User Name: Enter your DDNS account

Password: Enter your DDNS account's password

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

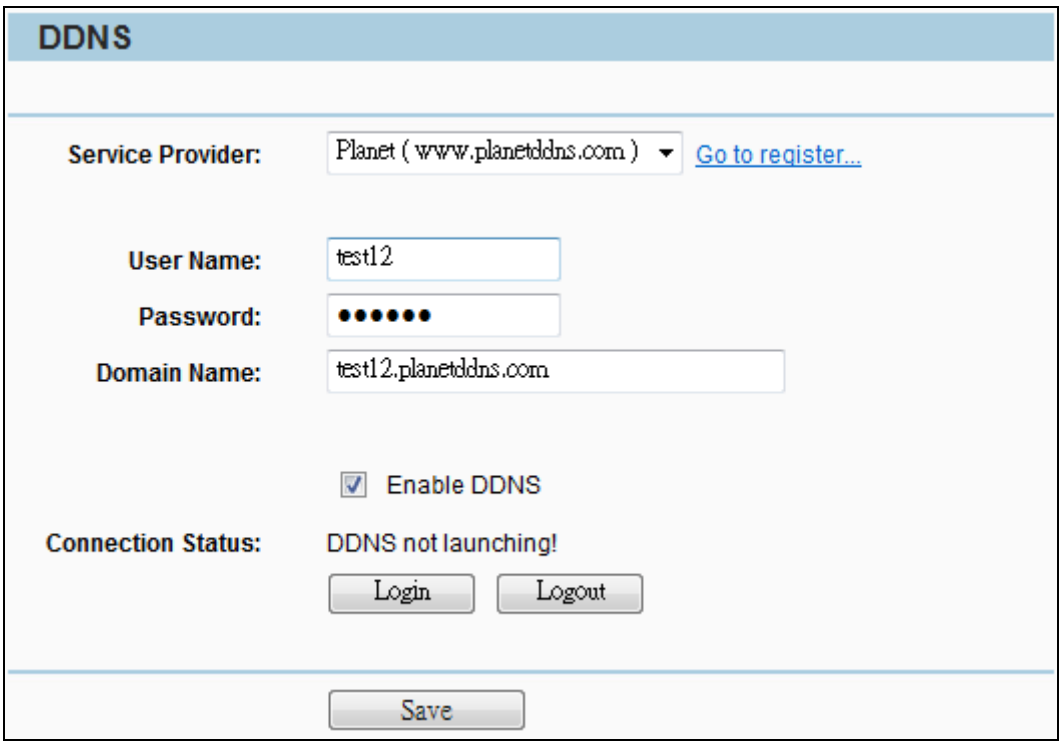


Figure 5-15-2

Step 3. Go to "**Security-> Remote Management**" to configure the IP Address of remote access from WAN port.

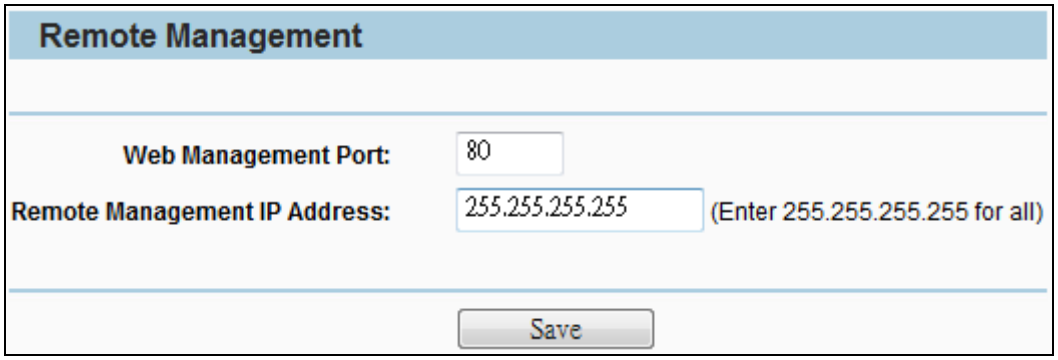


Figure 5-15-3

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

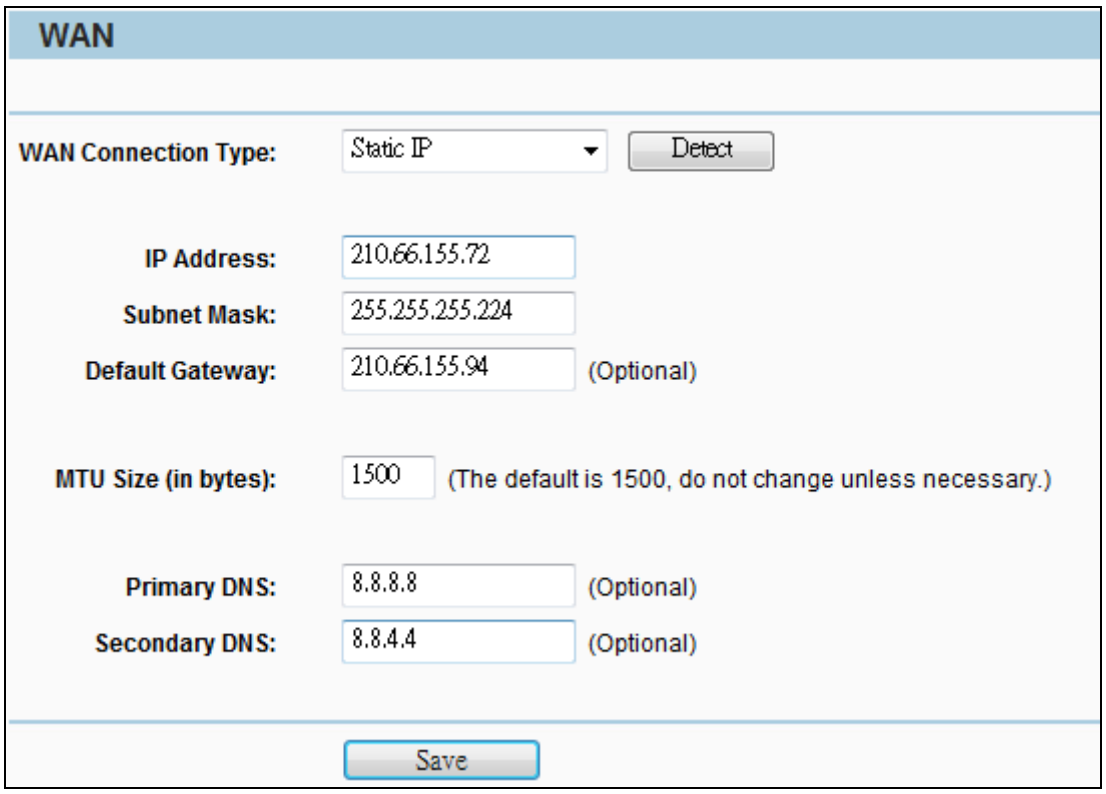


Figure 5-15-4

Step 5. Save 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 shown as below. Then, you should be able to login the WNAP-7350 remotely.

Please remember to enter the remote management port number that you have configured in Step 3 except port 80.

Figure 5-15-5

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 work properly.

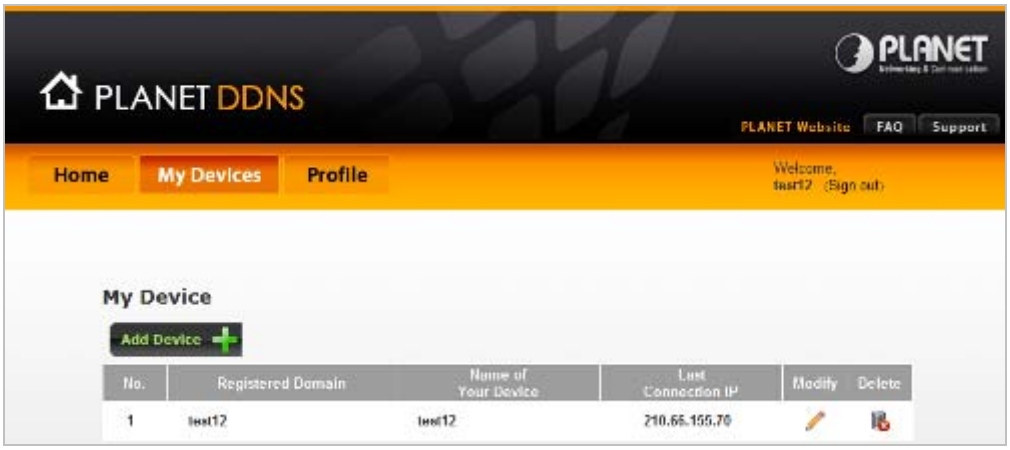
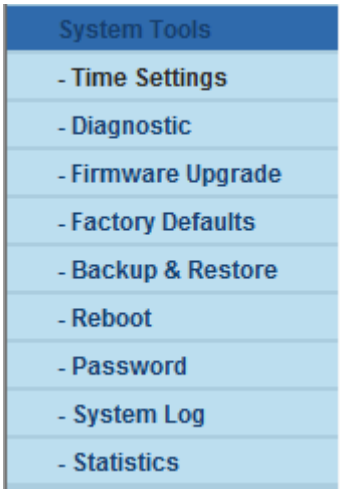


Figure 5-15-6

5.16 System Tools

There are nine submenus under the **System Tools** main menu (as shown in Figure 5-78): **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults, Backup & Restore, Reboot, Password, System Log** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



5.16.1 Time Settings

Choose menu "**System Tools > Time Settings**" and then you can configure the time on the following screen.

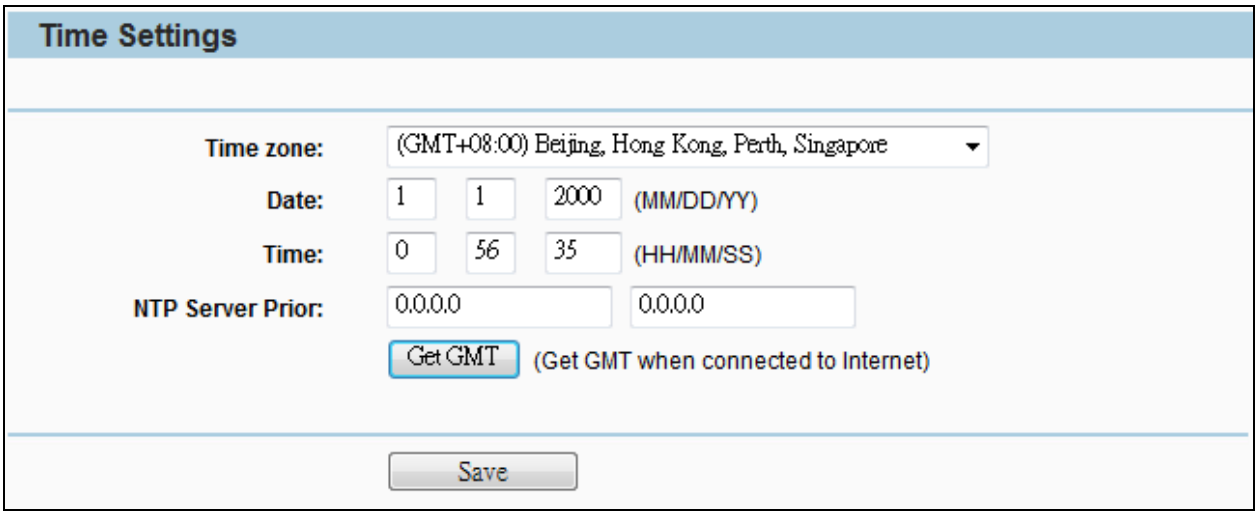


Figure 5-16-1-1 Time Settings

The page includes the following fields:

Object	Description
• **Time Zone**	Select your current time zone.
• **Date**	To set time manually: Enter the **Date** in Month/Day/Year format. Enter the **Time** in Hour/Minute/Second format.
• **Time**	
• **NTP Server Prior**	For automatic time synchronization: Enter the address of the **NTP Server Prior**. Click the **Get GMT** button to get GMT from the Internet.
• **Get GMT**	
• **Save**	Click the **Save** button to save the settings.

Note

1. This setting will be used for some time-based functions such as firewall functions. These time-dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Device.
2. The time will be lost if the Device is turned off.
3. The Device will automatically obtain GMT from the Internet if it is configured accordingly.

5.16.2 Diagnostic

Choose menu "**System Tools > Diagnostic**" and then you can transact **Ping** or **Traceroute** function to check connectivity of your network in the following screen.

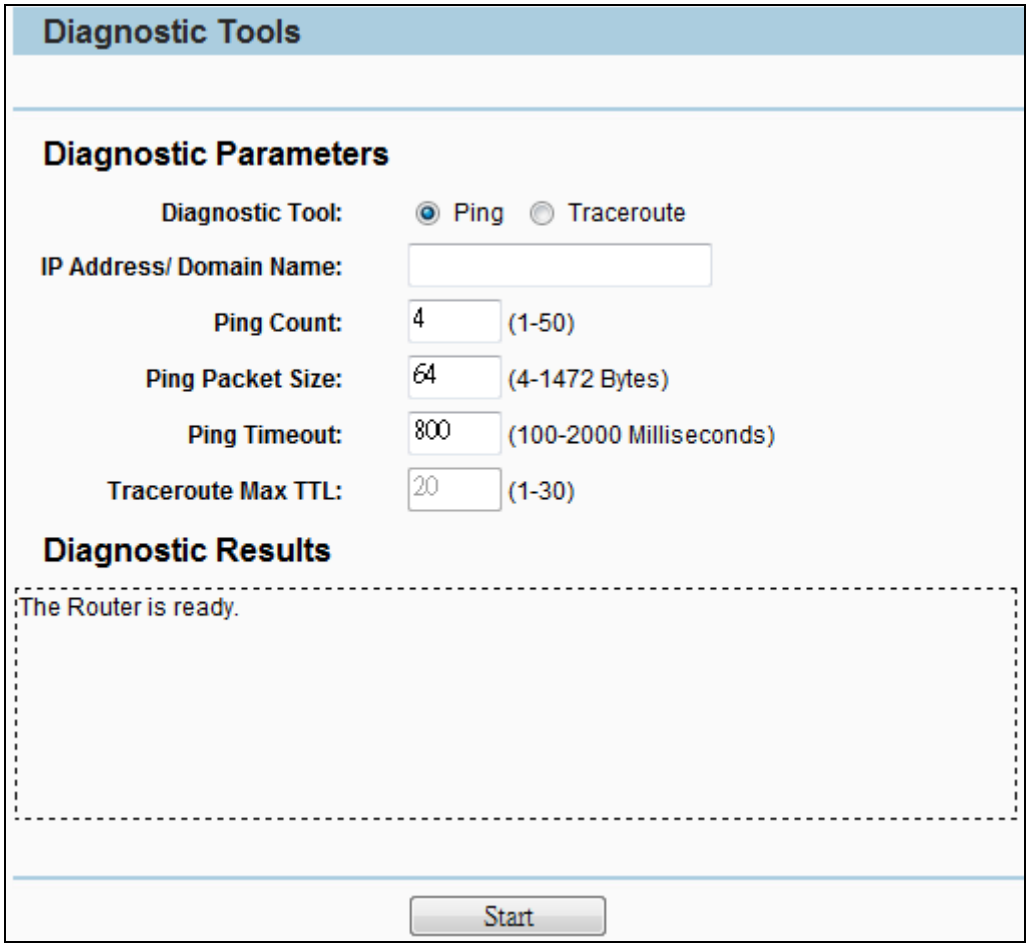


Figure 5-16-2-1 Diagnostic

The page includes the following fields:

Object	Description
• **Ping**	This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
• **Traceroute**	This diagnostic tool tests the performance of a connection.
• **IP Address/ Domain Name**	Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
• **Ping Count**	Specifies the number of Echo Request messages sent. The default is 4.
• **Ping Packet Size**	Specifies the number of data bytes to be sent. The default is 64.
• **Ping Timeout**	Time to wait for a response, in milliseconds. The default is 800.
• **Traceroute Max TTL**	Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.
• **Start**	Click the **Start** button to start the diagnostic procedure.

5.16.3 Ping Watch Dog

Selecting "**System Tools > Ping Watch Dog**" allows you to continuously monitor the particular connection between the device and a remote host. It makes this device continuously ping a user defined IP address (it can be the Internet gateway for example.). If it is unable to ping under the user defined constraints, this device will automatically reboot.

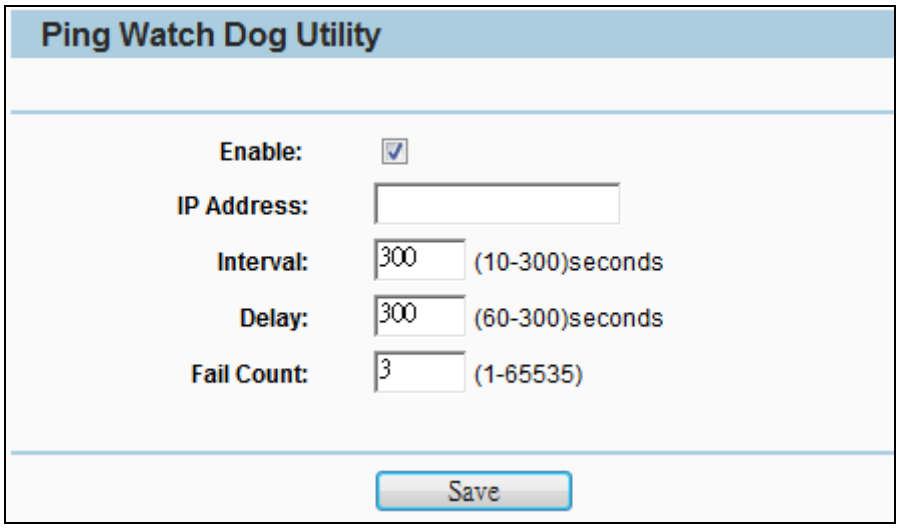


Figure 5-16-3-1 Ping Watch Dog

Note

This function is only available in **Standard AP** Mode.

The page includes the following fields:

Object	Description
• **Enable**	Turn on/off Ping Watch Dog.
• **IP Address**	The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
• **Interval**	Time interval between two ping packets which are sent out continuously.
• **Delay**	Time delay before first ping packet is sent out when the device is restarted.
• **Fail Count**	Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.
• **Save**	Click the **Save** button to save the settings.

5.16.4 Speed Test

Selecting "**System Tools > Speed Test**" helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It should be used for the preliminary throughput estimation between two network devices.

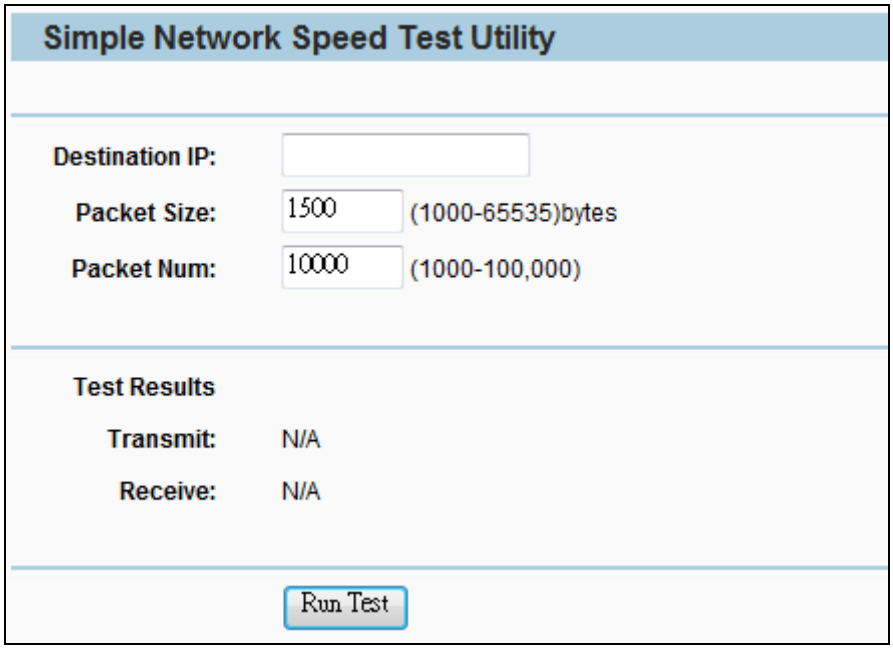


Figure 5-16-4-1 Speed Test

Note

This function is only available in **Standard AP** Mode.

The page includes the following fields:

Object	Description
• **Destination IP**	The Remote device's IP address.
• **Packet Size**	Specifies the size of packet sent. The default is 1500, and the range is 1000~65535.
• **Packet Num**	Specifies the number of packet sent. The default is 10000, and the range is 1000~100,000.
• **Transmit**	Estimate the outgoing throughput (Tx).
• **Receive**	Estimate the ingoing throughput (Rx).
• **Run Test**	Click the **Run Test** button to start the speed test procedure.

5.16.5 Firmware Upgrade

Choose menu "**System Tools > Firmware Upgrade**", and then you can update the latest version of firmware for the Device on the following screen.

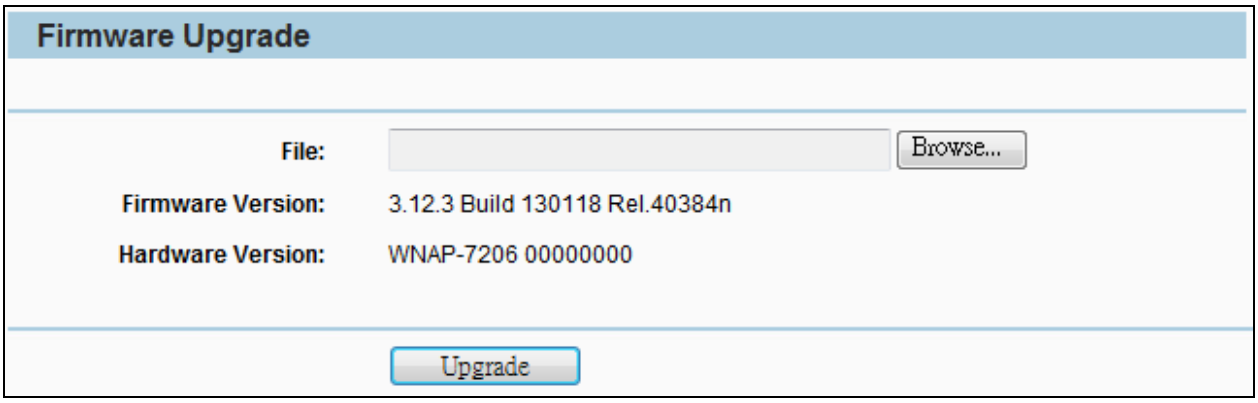


Figure 5-16-5-1 Firmware Upgrade

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

Object	Description
• **Firmware Version**	Display the current Software Version info.
• **Hardware Version**	Display the current Hardware Version info.
• **File**	Click the "**Browse…**" button to select the new firmware in this field.
• **Upgrade**	Click the "**Upgrade**" button to upgrade the new firmware.

IMPORTANT SAFETY PRECAUTIONS:

The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

5.16.6 Factory Defaults

Choose menu "**System Tools > Factory Defaults**" and you can restore the configurations of the Device to factory defaults on the following screen.

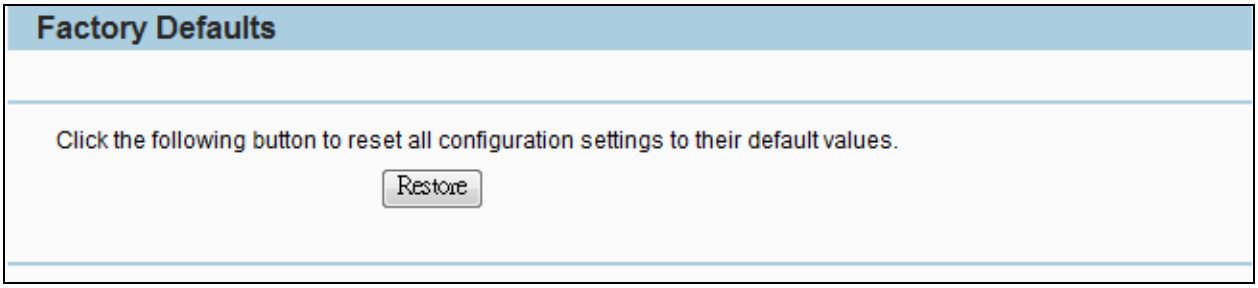


Figure 5-16-6-1 Factory Defaults

Click the **Restore** button to reset all configuration settings to their default values.

- Default User Name - admin.
- Default Password - admin.
- Default IP Address - 192.168.1.1.
- Default Subnet Mask - 255.255.255.0.
- Default SSID – default

All changed settings will be lost when defaults are restored.

5.16.7 Backup & Restore

Choose menu "**System Tools > Backup & Restore**", and then you can save the current configuration of the Device as a backup file and restore the configuration via a backup file as shown in **Figure 5-16-7-1**.

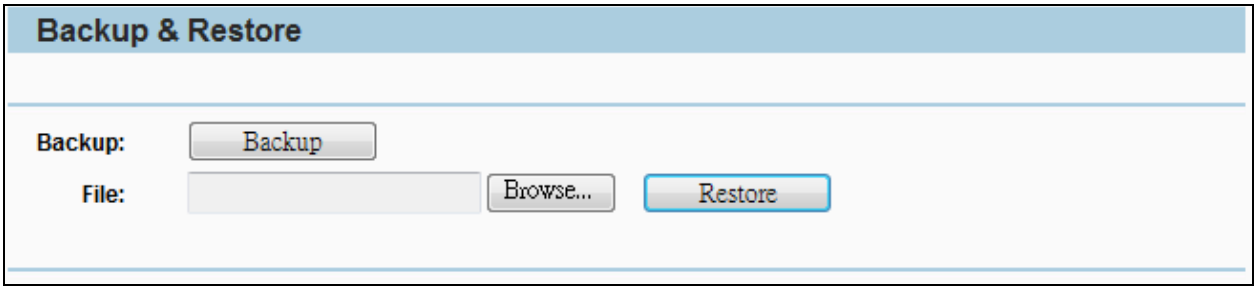


Figure 5-16-7-1 Backup & Restore

Click the **Backup** button to backup the configuration of the Wireless AP, and click **Restore** to restore the configuration.

Object	Description

• **Backup**	Click the **Backup** button to backup the configuration.
• **Browse…**	Click the **Browse…** button to select the configuration file in this field for restoring settings.
• **Restore**	Click the **Restore** button to restore the configuration.

5.16.8 Reboot

Choose menu "**System Tools > Reboot**", and then you can click the **Reboot** button to reboot the Device via the next screen.

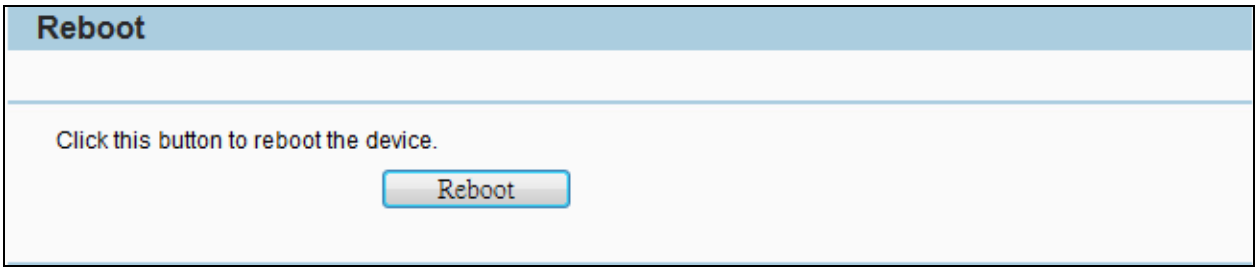


Figure 5-16-8-1 Reboot

Click the Reboot button to reboot the Device.

The settings of the Device will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Device (system will reboot automatically.).
- Restore the Device's settings to the factory defaults (system will reboot automatically.).
- Update the configuration with the file (system will reboot automatically.).

5.16.9 Password

Choose menu "**System Tools > Password**", and then you can change the factory default user name and password of the Device in the next screen as shown in **Figure 5-16-9-1**.

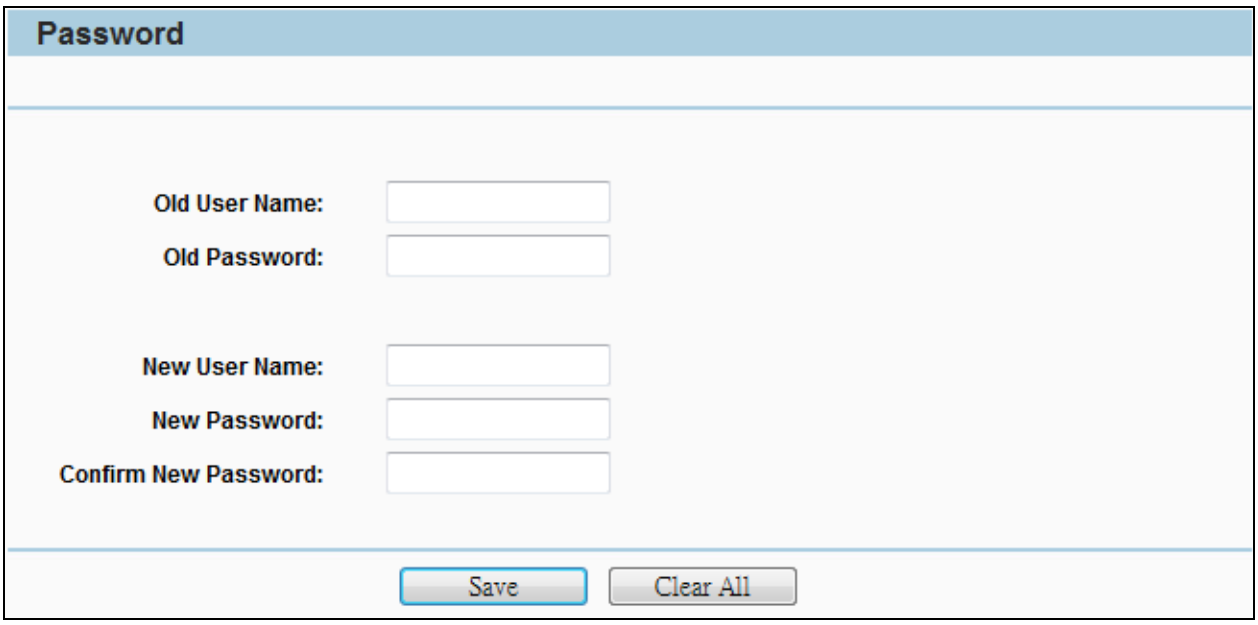


Figure 5-16-9-1 Password

Note

1. The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.
2. It is strongly recommended that you change the factory default user name and password of the AP. All users who try to access the AP's web-based utility will be prompted for the AP's user name and password.

The page includes the following fields:

Object	Description
• **Old User Name**	Enter the old user name that you prefer for modification.
• **Old Password**	Enter the old password that you prefer for modification.
• **New User Name**	Enter the new user name that you prefer for login.
• **New Password**	Enter the new password that you prefer for login.
• **Confirm New Password**	Re-enter the new password to confirm.
• **Save**	Click the **Save** button when finished.
• **Clear All**	Click the **Clear All** button to clear all.

5.16.10 System Log

Choose menu "**System Tools > System Log**", and then you can view the logs of the Device.

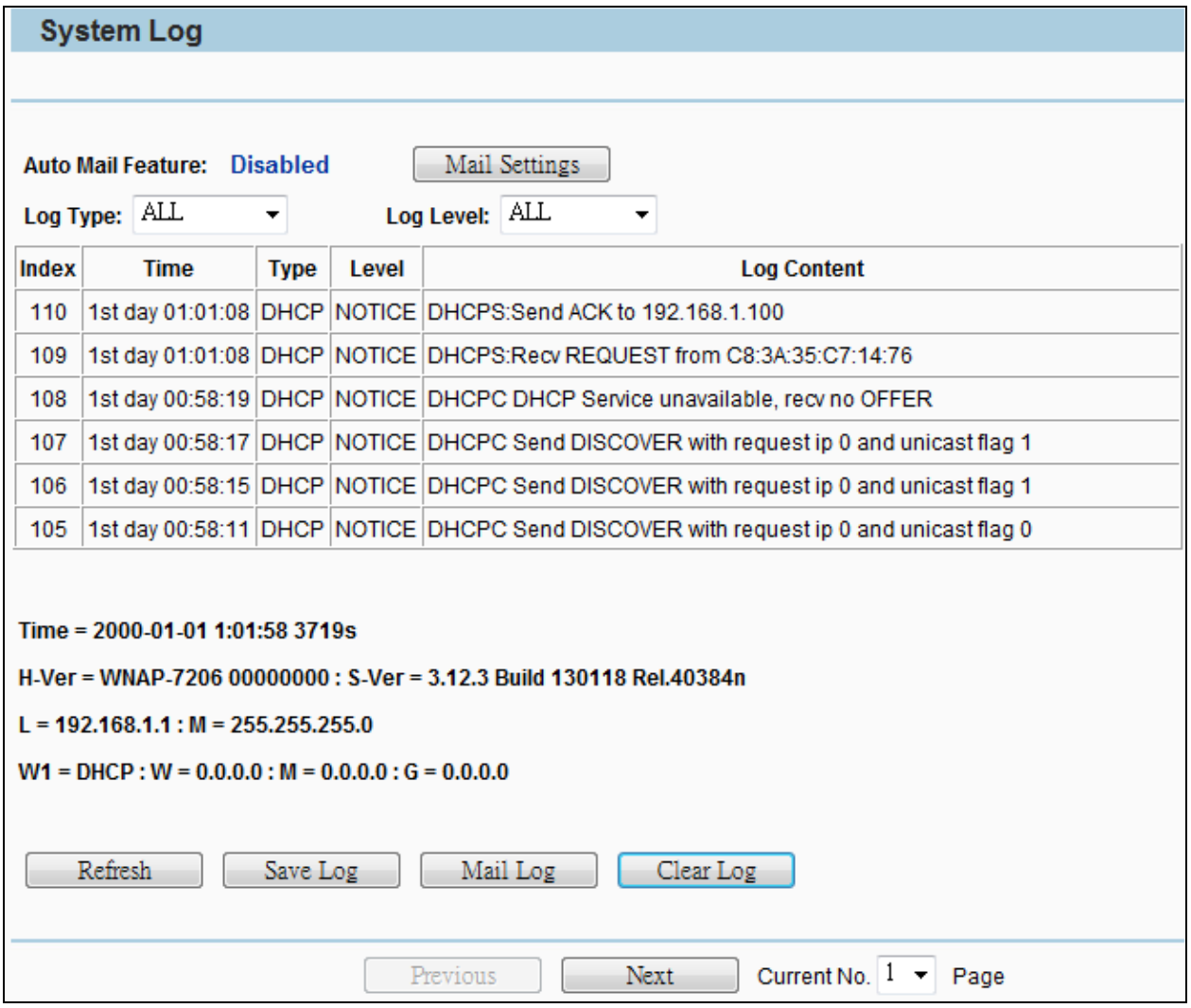


Figure 5-16-10-1 System Log

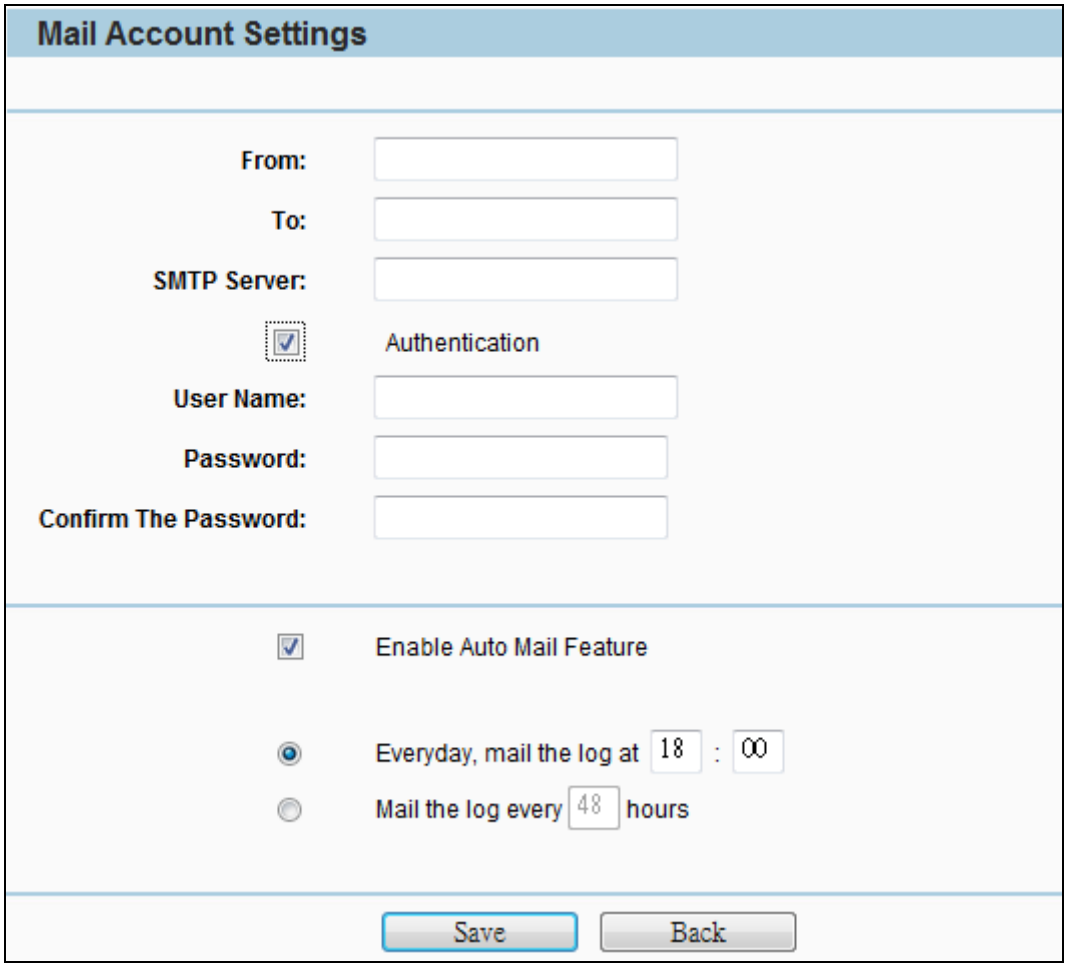


Figure 5-16-10-2 Mail Account Settings

The page includes the following fields:

Object	Description
• **Log Type**	By selecting the log type, only logs of this type will be shown.
• **Log Level**	By selecting the log level, only logs of this level will be shown.
• **Refresh**	Refresh the page to show the latest log list.
• **Save Log**	Click to save all the logs in a txt file.
• **Mail Log**	Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
• **Clear Log**	All the logs will be deleted from the Device permanently, not just from the page.
• **Next**	Click the **Next** button to go to the next page.
• **Previous**	Click the **Previous** button return to the previous page.
Mail Account Settings	

• **Mail Settings**	Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.
• **From**	Your mail box address.
• **To**	Recipient's address.
• **SMTP Server**	Your SMTP server.
• **Authentication**	Most SMTP Server requires Authentication.
• **User Name**	Your mail account name.
• **Password**	Your mail account password.
• **Confirm The Password**	Re-type your mail account password for confirmation.
• **Enable Auto Mail Feature**	**Auto Mail Feature** will help you monitor how your Device is running.
• **Everyday, mail the log at XX:XX**	Everyday, at specified time, the Device will automatically send the log to specified mailbox.
• **Mail the log every XX hours**	Every few hours, such as 2 hours, the Device will automatically send the log to specified mailbox.
• **Save**	Click **Save** to save the settings.
• **Back**	Click **Back** to back to the previous page.

5.16.11 Statistics

Choose menu "**System Tools > Statistics**", and then you can view the statistics of the Device, including total traffic and current traffic of the last Packets Statistic Interval.

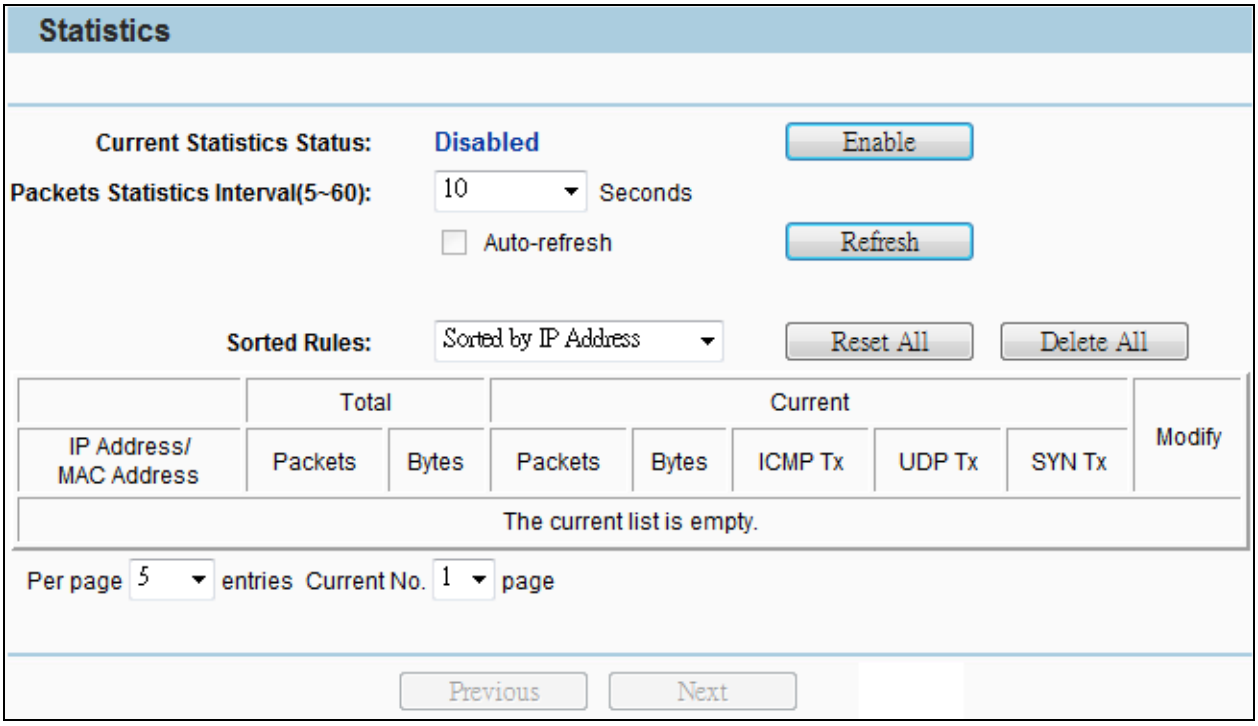


Figure 5-16-11-1 Statistics

The Statistics page shows the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

The page includes the following fields:

Object	Description
• **Current Statistics Status**	Enabled or Disabled. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be disabled.
• **Packets Statistics Interval**	The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
• **Sorted Rules**	Choose how displayed statistics are sorted.
• **Auto-refresh**	Check the **Auto-refresh** checkbox to refresh automatically.
• **Refresh**	Click the **Refresh** button to refresh the page.
• **Reset All**	Click the **Reset All** button to reset the values of all entries to zero.
• **Delete All**	Click the **Delete All** button to delete all entries in the table.

Appendix A: FAQ

A.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

(1) Open the Command program in the Microsoft Windows.
(2) Type in "ipconfig /all", then press the Enter button.
(3) Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

A.2 What is Wireless LAN?

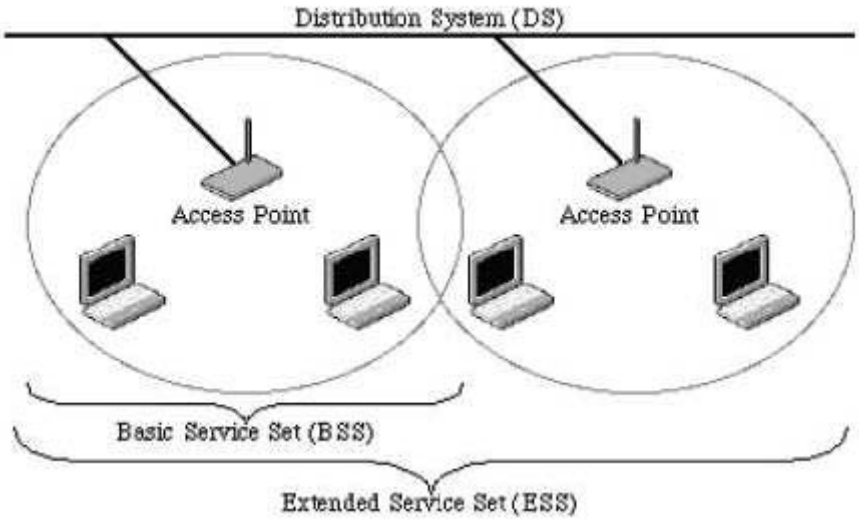
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

A.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/-13 MHz, 2450 +/-50 MHz and 5800 +/-75 MHz.

A.4 How does wireless networking work?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single sub-network. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).

Example 2: wireless Ad Hoc Mode

A.5 What is BSSID?

A six-byte address is that distinguish a particular a particular access point from others. Also know as just SSID. Serve as a network ID or name.

A.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

A.7 What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture… etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- Minimizing the number of walls and ceilings.
- Position the WLAN antenna for best reception.
- Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors…etc.
- Add additional WLAN Access Points if necessary.

A.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

A.9 What is WEP?

An option of IEEE 802.11 function is that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

A.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may

want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

A.11 What is RTS (Request to Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/ CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

A.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 include management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

A.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

A.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to

run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

A.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

A.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

A.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

A.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

A.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

A.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

A.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless WDS or repeater service.

A.22 What is Universal Plug and Play (UPnP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

A.23 What is Maximum Transmission Unit (MTU) Size?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer's MRU.

A.24 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address. Since that all the clients will communicate outside world through the WLAN Broadband Router, so have the cloned MAC address set on the WLAN Broadband Router will solve the issue.

A.25 What is DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user owned the DNS server with dynamic WAN IP address.

A.26 What is NTP Client?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

A.27 What is VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

A.28 What is IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

A.29 What is WLAN Block Relay between Clients?

An Infrastructure Basic Service Set is a BSS with a component called an Access Point (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

A.30 What is WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

A.31 What is WLAN ACK TIMEOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

A.32 What is Modulation Coding Scheme (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of an AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

A.33 What is Frame Aggregation?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

A.34 What is Guard Intervals (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol. The 802.11n specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.

Appendix B: Configuring the PC in Windows 7

In this section, we'll introduce how to configure the TCP/IP correctly in Windows 7. First make sure your Network Adapter is working, refer to the adapter's manual if needed.

1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.

2) Click the **Network and Sharing Center** icon, and then click the **Change adapter settings** on the left side of the screen.

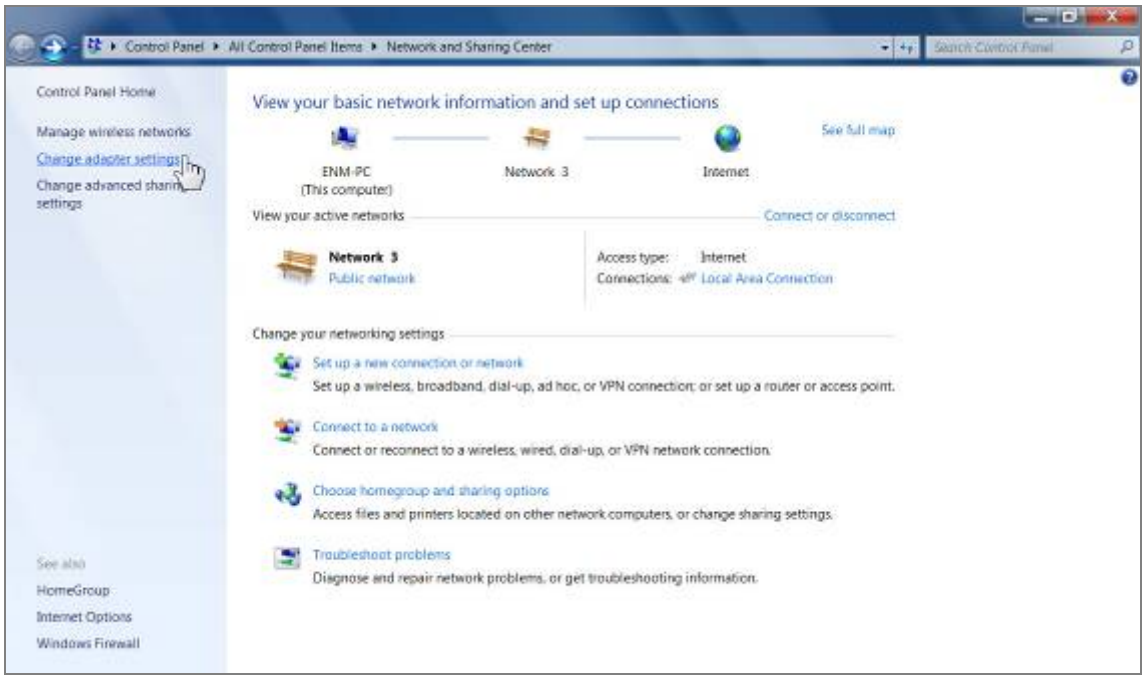


Figure B-1

3) Right click the icon of the network adapter shown in the figure below, and select Properties on the prompt window.

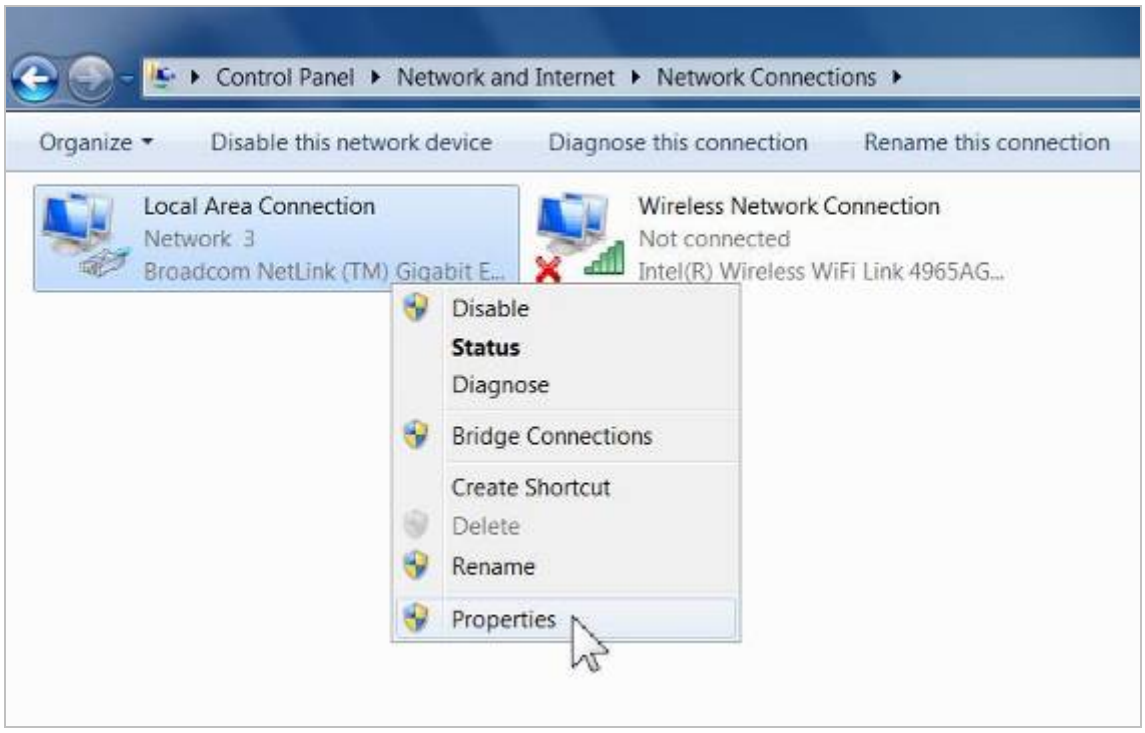


Figure B-2

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

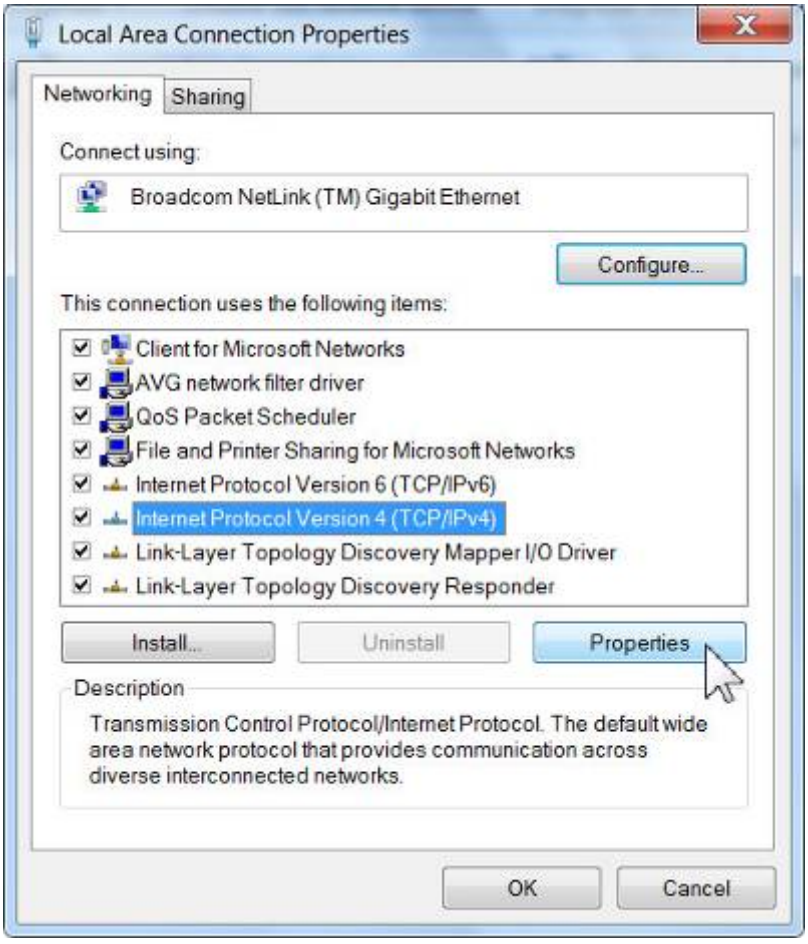


Figure B-3

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you can configure the **TCP/IP** protocol below:

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button.

2 If the AP's LAN IP address is 192.168.1.1, type in 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 type the DNS server IP address which has been provided by your ISP

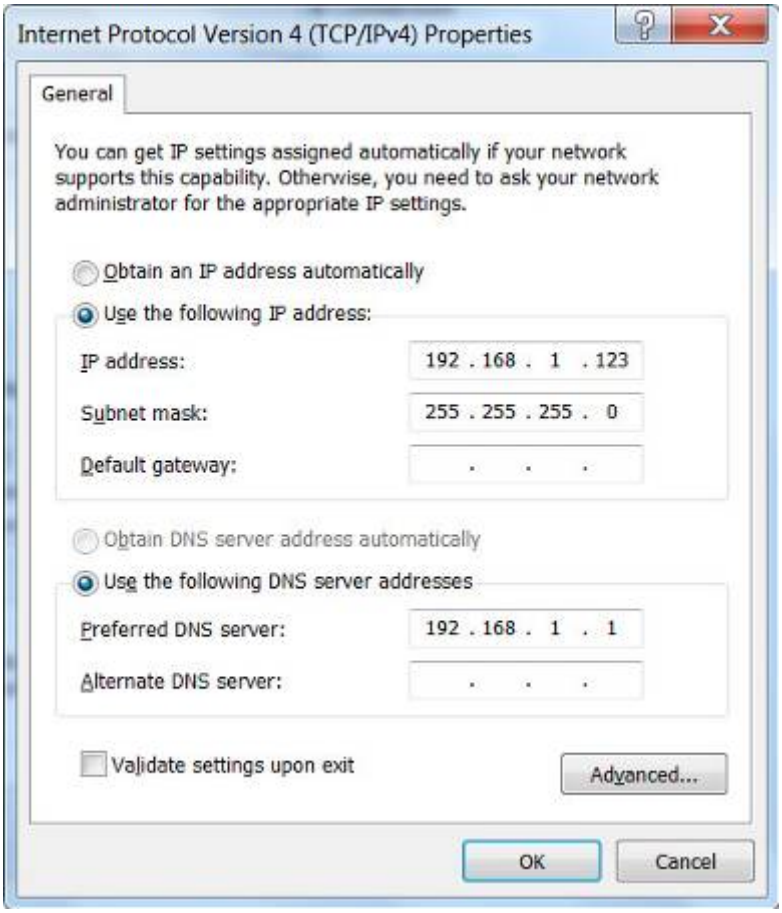


Figure B-4

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

Appendix C: Specifications

Product	**WNAP-7206** 150Mbps 802.11a/n Wireless Outdoor Access Point
Hardware	
Standard compliance	IEEE 802.11a/n IEEE 802.3 IEEE 802.3u IEEE 802.3x
Memory	32 Mbytes DDR SDRAM 4 Mbytes Flash
Button	Reset Button x 1
LED	Provides 4-Level signal LED indicator
PoE	Passive PoE (Up to 60 meters)
Interface	Wireless IEEE 802.11a/n LAN / WAN: 10/100Base-TX, Auto-MDI/MDIX x 1 Grounding Terminal x 1
Antenna	Internal (Default): 15dBi directional antenna (Dual-Polarization) ■ Horizontal: 60 degree ■ Vertical: 14 degree External (Option): RP-SMA Female type Connector ■ Switchable by Software ■ For External Antenna Mode, attach antenna before power on.
Data Rate	802.11a: 54, 48, 36, 24, 18, 12, 9 and 6Mbps 802.11n (20MHz): up to 72Mbps 802.11n (40MHz): up to 150Mbp
Media Access Control	CSMA/CA
Modulation	Transmission / Emission Type: OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM
Frequency Band	5.180-5.240GHz; 5.745-5.825GHz
Operating Channel	5.180GHz-CH36 5.200GHz-CH40 5.220GHz-CH44 5.240GHz-CH48 5.745GHz-CH149 5.765GHz-CH153 5.785GHz-CH157 5.805GHz-CH161 5.825GHz-CH165 *The actual channels will vary depends on the regulation in different regions

	and countries.	
RF Output Power	802.11a: 27 ± 1dBm 802.11n: 24 ± 1dBm	
Receiver Sensitivity	**802.11a:** 54M: -77dBm 48M: -79dBm 36M: -83dBm 24M: -86dBm 18M: -91dBm 12M: -92dBm 9M: -93dBm 6M: -94dBm	**802.11n:** 150M: -73dBm 121.5M: -76dBm 108M: -77dBm 81M: -81dBm 54M: -84dBm 40.5M: -88dBm 27M: -91dBm 13.5M: -93dBm
Output Power Control	High (default) Middle Low	
Power Requirements	Passive PoE 12V Pin 4,5 VDC+ Pin 7,8 VDC-	
Power Adapter	12V DC, 1A (switching)	
Environment & Certification		
Operation	Temperature: -30~70 Degree C, Humidity: 10~90% non-condensing	
Storage	Temperature: -40~70 Degree C, Humidity: 5~95% non-condensing	
Enclosure	Outdoor Weatherproof design 15KV ESD & 4000V Lightning Protection Grounding Terminal Integrated	
Regulatory	CE / FCC / RoHS	
Software		
LAN	Built-in DHCP server supporting static IP address distributing	
	Supports UPnP, Dynamic DNS	
	Supports Flow Statistics	
	IP & MAC Binding	
	IP / Protocol-based Bandwidth Control	
WAN	■ Static IP ■ Dynamic IP ■ PPPoE / Russia PPPoE ■ PPTP / Russia PPTP ■ L2TP / Russia L2TP ■ BigPond Cable	
VPN Passthrough	■ PPTP ■ L2TP ■ IPSec	
Operating Mode	■ Standard AP (Wireless AP) ■ AP Router (Wireless Broadband Router)	

	■ AP Client Router (WISP Client Router)
Firewall	NAT firewall with SPI (Stateful Packet Inspection)
	NAT with ALG (Application Layer Gateway)
	Built-in NAT server supporting Port Triggering, Virtual Server, and DMZ
	Built-in firewall with IP address / MAC / DNS filtering
	Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter, DoS protection
Wireless Mode	■ AP ■ Client ■ WDS PTP ■ WDS PTMP ■ WDS Repeater (AP+WDS) ■ Universal Repeater (AP+Client)
Channel Width	20MHz / 40MHz
Wireless Isolation	Enable to isolate each connected wireless clients
Wireless Security	64/128/152-bits WEP, WPA, WPA-PSK, WPA2, WPA2-PSK
	Wireless MAC address filtering
	Enable/Disable SSID Broadcast
Multiple SSID	Up to 3
Max. Wireless Client	25
Max. WDS AP	4
Max. Wired Client	60
WMM	Supports Wi-Fi Multimedia
NTP	Network Time Management
Management	Web-Based (HTTP) management interface
	Supports SNMP v1/v2 agent with MIB-II
	Remote management
	SNTP time synchronize
	Easy firmware upgrade
	Configuration Backup & Restore
	DHCP Client List
Diagnostic tool	System Log supports auto mail and save to local host
	Ping Watch Dog allows you to continuously monitor the particular connection between the device and a remote host.
	Throughput Monitor provides real-time wireless throughput information
	Speed Test helps to test the connection speed

Appendix D: Factory Default Settings

Item	Default Value
Common Default Settings	
Username	admin
Password	admin
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Wireless	
Operation Mode	Standard AP – Access Point
SSID	default
Wireless Security	Disable
Wireless MAC Address Filtering	Disable
DHCP	
DHCP Server	Disable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Address Lease Time	120 minutes (Range:1 ~ 2880 minutes)
Default Gateway (optional)	0.0.0.0
Primary DNS (optional)	0.0.0.0
Secondary DNS (optional)	0.0.0.0

EC Declaration of Conformity

For the following equipment:

*Type of Product : 5GHz 802.11a/n Wireless LAN Outdoor CPE AP/Router

*Model Number : WNAP-7206

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 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 301 489-1 V1.9.2	(2011-09)
EN 301 489-17 V2.1.1	(2009-05)
EN 301 893 V1.6.1	(2011-11)
EN 62311	(2008)
EN 60950-1	(2006 + A1:2010 + A11:2009 + A12:2011)

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 **Kent Kang**

Position / Title : **Product Manager**

Taiwan — *Place*

28th Feb., 2013 — *Date*

Legal Signature

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation,** declares that this **802.11a/n Wireless Outdoor AP/Router** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **802.11a/n Wireless Outdoor AP/Router** tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **802.11a/n Wireless Outdoor AP/Router** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **802.11a/n Wireless Outdoor AP/Router** megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **802.11a/n Wireless Outdoor AP/Router** overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **802.11a/n Wireless Outdoor AP/Router** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt **PLANET Technology Corporation,** dass sich dieses Gerät **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **802.11a/n Wireless Outdoor AP/Router** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC”.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **802.11a/n Wireless Outdoor AP/Router***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ* *ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*	**Português**	**PLANET Technology Corporation**, declara que este **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **802.11a/n Wireless Outdoor AP/Router** è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **802.11a/n Wireless Outdoor AP/Router** 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 **802.11a/n Wireless Outdoor AP/Router** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **802.11a/n Wireless Outdoor AP/Router** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.