

IEEE 802.11b/g/n

LM820 Wi-Fi SMT Module 802.11n 150Mbps

USER'S GUIDE

VERSION 1.0



© All rights reserved.

All trade names are registered trademarks of respective manufacturers listed.

This manual may not be copied in any media or form without the written consent of original maker.

TABLE OF CONTENTS

- Information To User I
- 1. Introduction 1
- 2. Wireless LAN Basics 3
- 3. IP ADDRESS 4
- 4. Install Driver/Utility 5
 - 4.1 Windows XP/Vista/Win7..... 5
- 5. Wireless Network Configuration 7
 - 5.1 Utility Icon 7
 - 5.2 Client Mode (Default Setting)..... 7
- 6. Technical Specifications 15
- 7. Troubleshooting 16
- 8. Glossary 17

INFORMATION TO USER

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

REGULATION INFORMATION

The WLAN 11n USB Client Adapter must be installed and used in strict accordance with the manufacturer's instructions. This device complies with the following radio frequency and safety standards.

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.

FCC RF Radiation Exposure Statement:

This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

Note 1: This module certified that complies with RF exposure requirement under portable or mobile or fixed condition, this module is to be installed only in portable or mobile or fixed applications.

A portable device is defined as a transmitting device designed to be used so that the radiating structure(s) of the device is/are within 20 centimeters of the body of the user

A mobile device is defined as a transmitting device designed to be used in other than fixed locations and to generally be used in such a way that a separation distance of at least 20 centimeters is normally maintained between the transmitter's radiating structure(s) and the body of the user or nearby persons. Transmitting devices designed to be used by consumers or workers that can be easily re-located, such as wireless devices associated with a personal computer, are considered to be mobile devices if they meet the 20 centimeter separation requirement.

A fixed device is defined as a device is physically secured at one location and is not able to be easily moved to another location.

Note 2: Any modifications made to the module will void the Grant of Certification, this module is limited to OEM installation only and must not be sold to end-users, end-user has no manual instructions to remove or install the device, only software or operating procedure shall be placed in the end-user operating manual of final products.

Note 3: The device must not transmit simultaneously with any other antenna or transmitter.

Note 4: To ensure compliance with all non-transmitter functions the host manufacturer is responsible for ensuring compliance with the module(s) installed and fully operational. For example, if a host was previously authorized as an unintentional radiator under the Declaration of Conformity procedure without a transmitter certified module and a module is added, the host manufacturer is responsible for ensuring that the after the module is installed and operational the host continues to be compliant with the Part 15B unintentional radiator requirements. Since this may depend on the details of how the module is integrated with the host, LM Technologies Ltd. shall provide guidance to the host manufacturer for compliance with the Part 15B requirements.

Note 5: FCC ID label on the final system must be labeled with “Contains FCC ID: VVX-LM820-0462” or “Contains transmitter module FCC ID: VVX-LM820-0462”.

The transmitter module must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the host product. LM Technologies Ltd. is responsible for the compliance of the module in all final hosts.

Europe- R&TTE Compliance Statement

Hereby, the company who declares that this equipment complies with the essential requirements and other relevant provisions of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

CE Declaration of Conformity

For the following equipment:

WLAN 11n USB Client Adapter

(Product Name) WLAN 11n USB Client Adapter



(Model Designation)

is herewith confirmed to comply with the requirements set out in the Council (European parliament) Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility of Radio and Telecom device (1999/5/EC). For the evaluation regarding this Directive, the following standards were applied:

EN 300 328 V1.7.1

EN 301 489-1 V1.8.1 ; EN 301 489-17 V2.1.1

EN 60950-1:2006+A11:2009

This equipment is marked with the **CE 1177**  symbol and can be used throughout the European community. Marking by the symbol  indicates that usage restrictions apply.

France - 2.4GHz for Metropolitan France:

In all Metropolitan départements, wireless LAN frequencies can be used under the following conditions, either for public or private use:

- Indoor use: maximum power (EIRP*) of 100 mW for the entire 2400-2483.5 MHz frequency band
- Outdoor use: maximum power (EIRP*) of 100 mW for the 2400-2454 MHz band and with maximum power (EIRP*) of 10 mW for the 2454-2483 MHz band

Caution: Exposure to Radio Frequency Radiation.

To comply with RF exposure compliance requirements, for mobile configurations, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

This device is intended for use as check in the following European Community countries:

- | | | | |
|------------------------------------|-----------------------------------|---|--------------------------------------|
| <input type="checkbox"/> Austria | <input type="checkbox"/> Belgium | <input type="checkbox"/> Czech Republic | <input type="checkbox"/> Cyprus |
| <input type="checkbox"/> Denmark | <input type="checkbox"/> Estonia | <input type="checkbox"/> France | <input type="checkbox"/> Finland |
| <input type="checkbox"/> Germany | <input type="checkbox"/> Greece | <input type="checkbox"/> Hungary | <input type="checkbox"/> Ireland |
| <input type="checkbox"/> Italy | <input type="checkbox"/> Iceland | <input type="checkbox"/> Luxemburg | <input type="checkbox"/> Latvia |
| <input type="checkbox"/> Lithuania | <input type="checkbox"/> Malta | <input type="checkbox"/> Norway | <input type="checkbox"/> Netherlands |
| <input type="checkbox"/> Portugal | <input type="checkbox"/> Poland | <input type="checkbox"/> Spain | <input type="checkbox"/> Sweden |
| <input type="checkbox"/> Slovakia | <input type="checkbox"/> Slovenia | <input type="checkbox"/> United Kingdom | |

The channel identifiers, channel center frequencies, and regulatory domains of each 22-MHz-wide channel are shown in following Table.

Channel Identifier	Frequency (MHZ)	Regulatory Domains					
		Japan	ETSI	North America	Israel	France Outdoor	Mexico
1	2412	●	●	●		●	
2	2417	●	●	●		●	
3	2422	●	●	●	●	●	
4	2427	●	●	●	●	●	
5	2432	●	●	●	●	●	
6	2437	●	●	●	●	●	
7	2442	●	●	●	●	●	
8	2447	●	●	●	●	●	
9	2452	●	●	●	●	●	
10	2457	●	●	●			●
11	2462	●	●	●			●
12	2467	●	●				
13	2472	●	●				
14	2484	●					



INTRODUCTION

Thank you for your purchase of the WLAN Adapter. Featuring wireless technology, this wireless networking solution has been designed for both large and small businesses, and it is scalable so that you can easily add more users and new network features depending on your business scale.

FEATURES

Support Microsoft XP(32bit/64bit) / Vista(32bit/64bit) / Win7(32bit/64bit).

Operating distance of up to 300 meters in free space.

150/120/90/60/54/48/36/30/24/22/18/12/11/6/5.5/2/1 Mbps selectable Data Rate.

64/128-bit WEP , WPA (Wi-Fi Protected Access), WPA2

2.400GHz ~ 2.4835GHz unlicensed ISM Frequency Band.

Modulation Method :

IEEE 802.11b : DSSS (Direct Sequence Spread Spectrum).

IEEE 802.11g / 802.11n : OFDM (Orthogonal Frequency Division Multiplexing). Easy operation and setting up.

SYSTEM REQUIREMENTS

Windows System : XP(32bit/64bit) / Vista(32bit/64bit) / Win7(32bit/64bit).

PCs must have a device driver installed. It allows you to communicate with WLAN 11n USB Client Adapter.

BEFORE YOU START

1. Confirm Box Contents

- ◆ WLAN 11n USB Client Adapter
- ◆ Quick Start Guide
- ◆ Driver CD

CONNECTING YOUR WLAN 11n USB Client Adapter TO PC

Quick Start Guide

Connect your WLAN 11n USB Client Adapter to your PC. Install driver.

GETTING TO KNOW WIRELESS LAN ADAPTER

LED

LED turns on when WLAN link to WLAN adaptor or AP.

LED is blinking when WLAN Adapter is active.

2

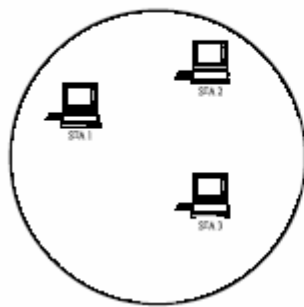
WIRELESS LAN BASICS

Wireless LAN network defined by IEEE 802.11b/g standard committee could be configured as :

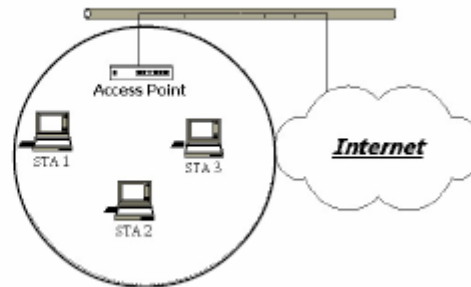
Ad Hoc wireless LAN.

Infrastructure wireless LAN.

Ad Hoc network is a group of PCs installed with wireless LAN cards, this group of PCs is called a BSS (Basic Service Set). PCs in this group can use their wireless LAN cards to communicate with each other, but can not connect to the **Internet**.



Ad Hoc Wireless Network



Infrastructure Wireless Network

The most obvious difference between **Infrastructure** wireless network and **Ad Hoc** wireless network is that the PCs in **Infrastructure** wireless network can access the resource in the Internet through **Access Point**.

Depending on your requirement, you can easily set up your PC's network to be a "**Ad Hoc**" or "**Infrastructure**" wireless network. Generally speaking, if in your network, there is an **Access Point** in it, we recommend you to set your network as an "**Infrastructure**", so it can connect to the **Internet**.

3

IP ADDRESS

To use the WLAN 11n USB Client Adapter with a computing device, the WLAN Adapter must be equipped with a proper Interface. All drivers and supporting software for the WLAN Adapter must be installed and configured first.

Ask your system administrator for the following information, which you may need to provide during driver installation :

Your Wireless Client

Name. Your Wireless
SSID.

Your computer's unique client name and workgroup name. For your network account, your user name and password.

Your IP address, gateway address, and subnet mask if you're not using a DHCP client.

Any computer on a network is identified by a unique network address. There are two methods to assign a network address to a computer on a TCP/IP network :

Static IP addressing.

Dynamic IP addressing (DHCP Client).

In network with static IP addressing, the network administrator manually assigns an IP address to each computer. Once a static IP address is assigned, a computer uses the same IP address every time it reboots and logs on to the network. You may manually change the IP address in the

Network Properties dialog box. Network using static IP address is easy to set up and do not require additional network management software.

In network with dynamic IP addressing, a DHCP server in the network dynamically assigns IP addresses to all clients every time they log on to the network. Network using dynamic IP address requires setting up and running a DHCP Server.

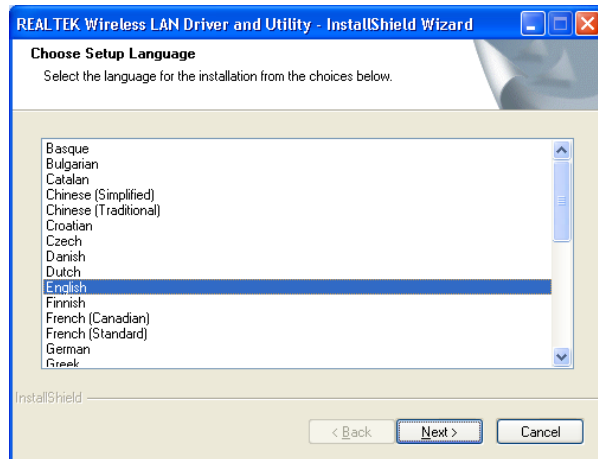
4

INSTALL DRIVER / UTILITY

The installation & driver CD will automatically activate the autorun installation program after you insert the disk into your CD drive.

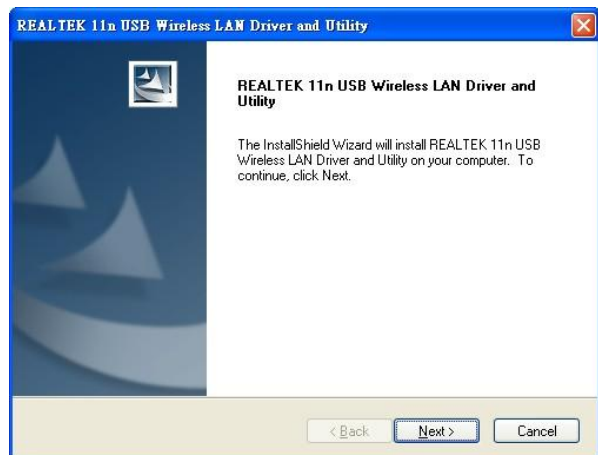
Step 1 :

Insert the installation CD into your CD-ROM. Choose the Setup Language and click **Next** button.

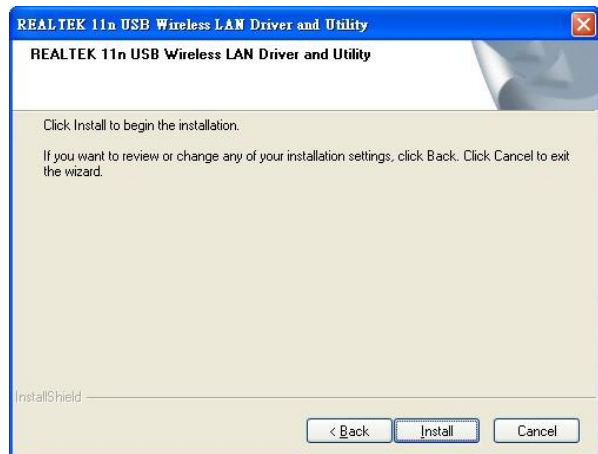


Step 2 :

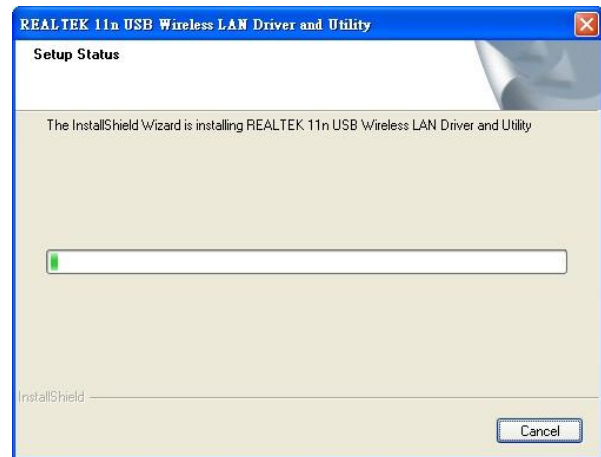
Installation descriptions shown. Click **Next** to continue.



Click **Install** to begin the installation



Installing & configuring WLAN utility

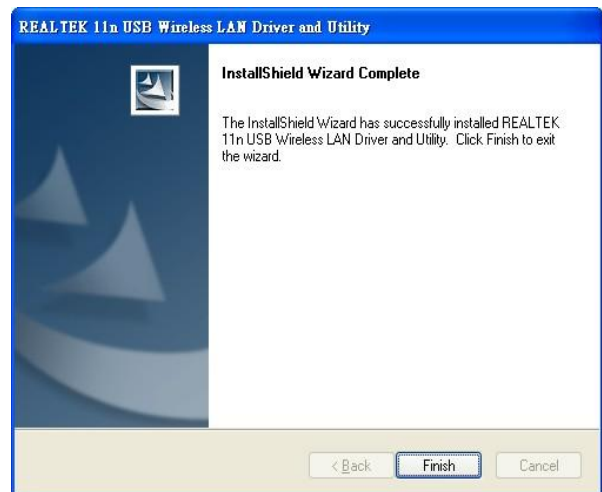


Installing Drivers.



Step 3 :

Click **Finish** to complete installation



5

WIRELESS NETWORK CONFIGURATION

WLAN 11n USB Client Adapter uses its own management software. All functions controlled by users are provided by this application. When you insert the WLAN Adapter into your laptop or desktop, a icon should appear in the Windows System Tray automatically.

5.1 Utility Icon

- Client mode utility running but no WLAN Adapter plugged



- Client mode utility running and WLAN Adapter scan available network.



- Client mode utility running and WLAN Adapter can not scan any AP



- AP mode utility running.



5.2 Client Mode (Default Setting)

Wireless Device Control :



- Show Tray Icon – Show icon or not show icon in systray.
- Radio Off – Stop wireless signal.
- Disable Adapter – Stop wireless device.
- Windows Zero Config – Stop Use Utility.

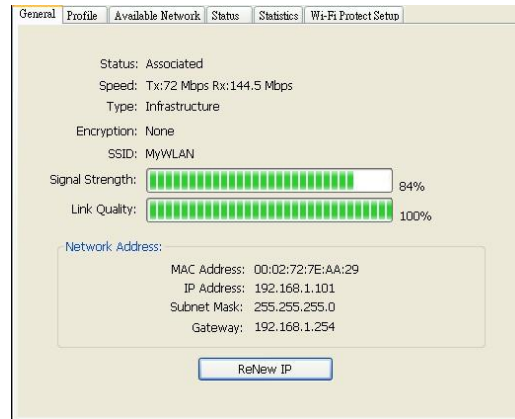
5.2.1 GENERAL SETTING

Once device is set, double click on that icon and the configuration window will pop up as shown. It shows the current connected network. The signal strength and link quality are displayed also. The bar graph displays the quality and strength of the link

between the node and its Access Point. Link Quality is a measurement of receiving and transmitting performances over the radio.

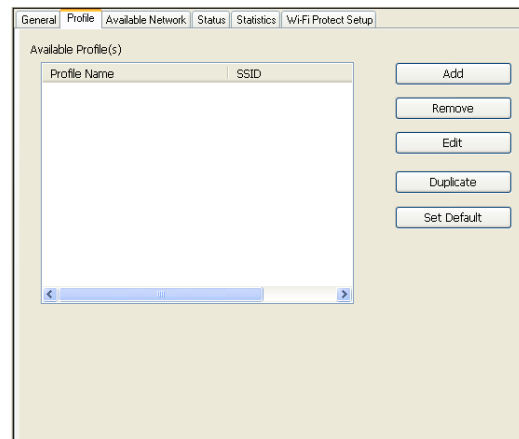
Network Address displays current MAC Address, IP Address, Subnet. and Gateway.

Click **Renew IP** button to refresh IP address leased from wireless AP.



5.2.2 PROFILE SETTING

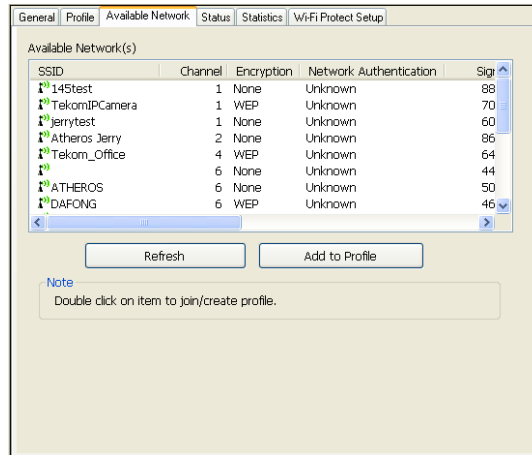
In profile tab, you can **Add, Remove, Edit, Duplicate** and **Set Default** to manipulate profile content manually. Strongly recommend to use profile after you do **Available Network**.



5.2.3 AVAILABLE NETWORK SETTING

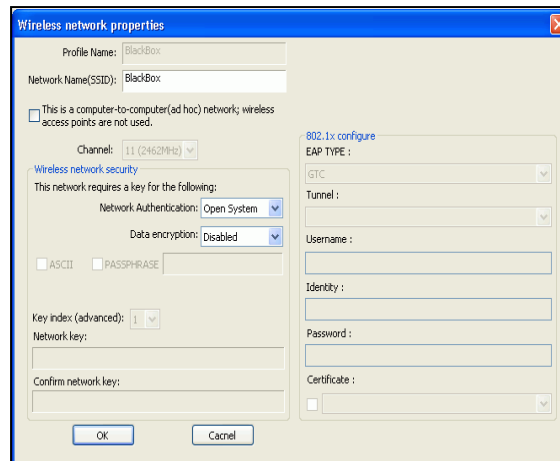
Click **Available Network** tab and it will show all available networks that radio can reach. Select proper SSID & BSSID you want to connect.

Click **Refresh** button to force and rescan available networks currently.



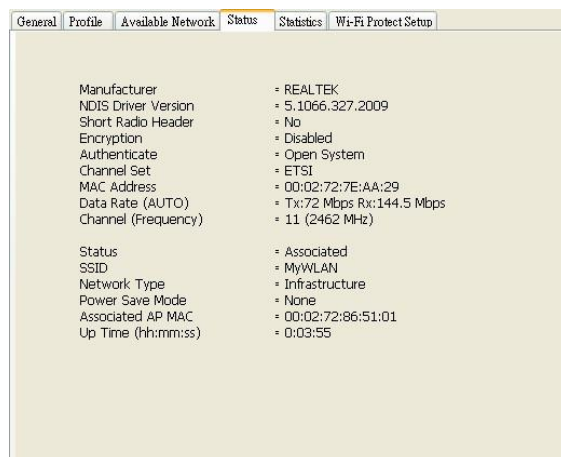
Select one of SSIDs, and click **Add to Profile** to create profile that can be configured more wireless parameters.

In this page, you can edit your profile name, configure wireless security like WEP, WPA, WPA2, 802.1x ...etc. After finishing setup, click **OK** button to save configuration



5.2.4 Status

Status page tab, shows all wireless, networking and device driver version in details.



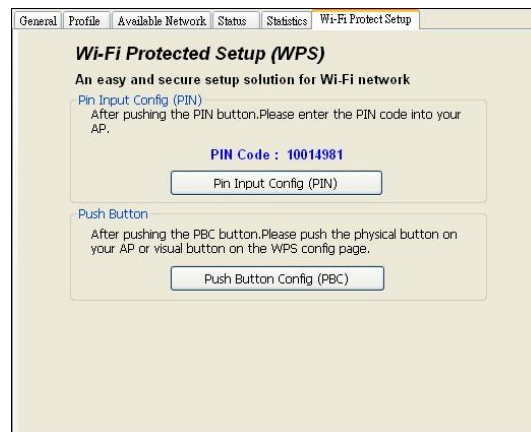
5.2.5 Statistics

Statistics page tab will show real-time TX/RX relative counters to check or evaluate the wireless performance. Click **Reset** button to set counter to zero.

Counter Name	Value
Tx OK	151
Tx Error	0
Rx OK	63
Rx Packet Count	63
Rx Retry	0
Rx ICV Error	0

5.2.6 Wi-Fi Protected Setup

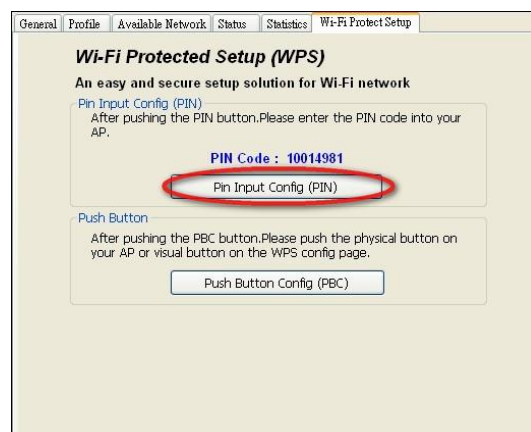
An easy and secure setup solution for Wi-Fi network. you can choose PIN Code or Push Button method to connect to an AP.



■ Pin method:

Step 1 :

Push the PIN button.



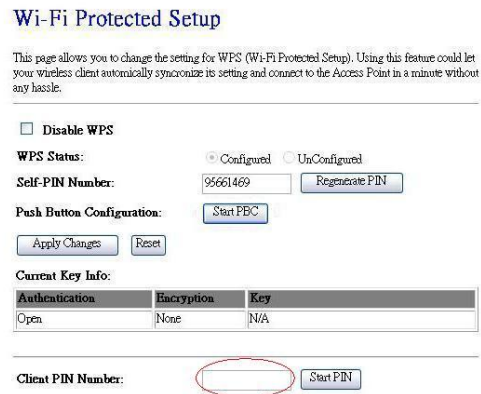
Step 2 :

Select a specific AP



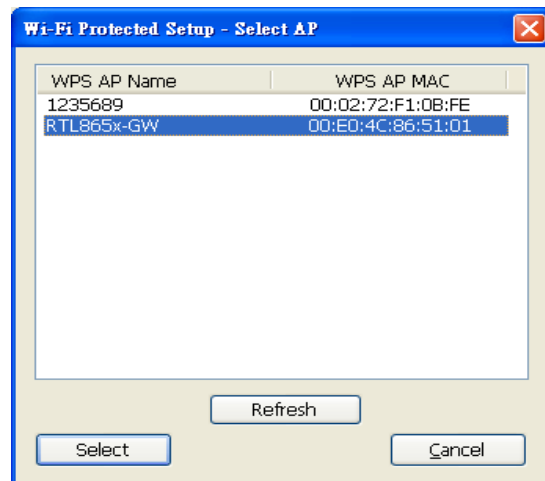
Step 3 :

Enter the PIN code into your AP.



Step 3 :

Select AP that you want to configure.



Step 4 :

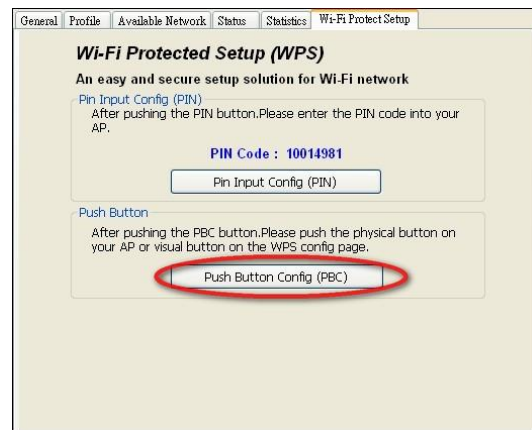
Wait for configuring your wireless AP to be the security setting.



■ PBC method:

Step 1 :

Push the PBC button.



Step 2 :

Push the physical button on your AP or visual button on the WPS config page.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let you wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number:

Push Button Configuration:

Current Key Info:

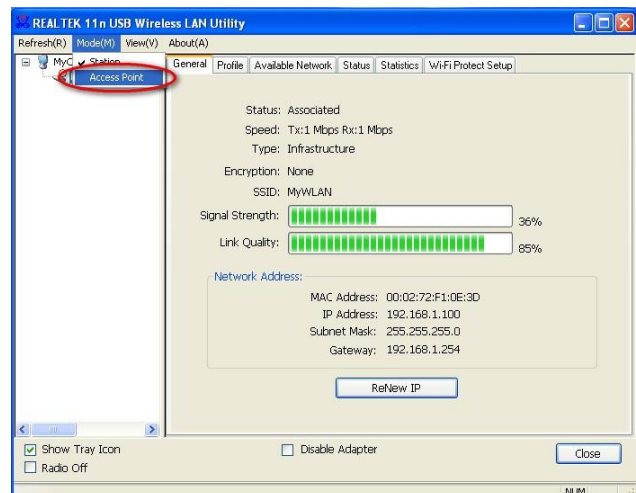
Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

■ Soft AP:

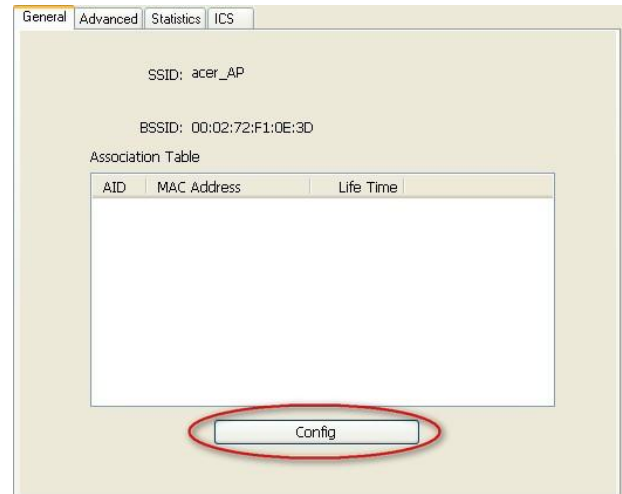
Step 1 :

Click Access Point to change AP mode



Step 2 :

Click **Config** to set AP.



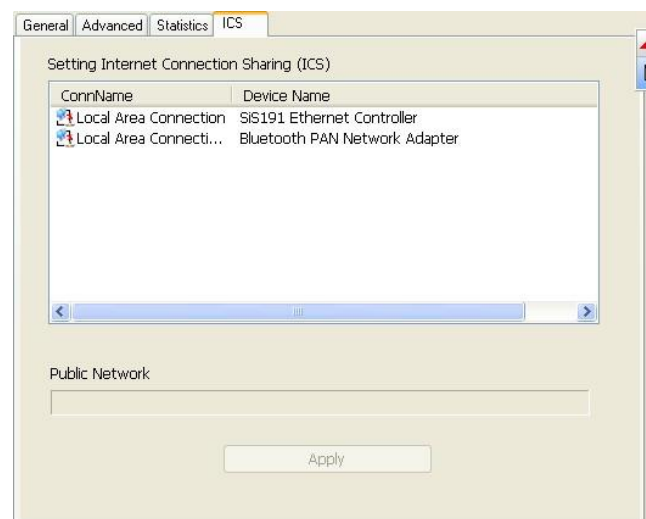
Step 3 :

Setting SSID and Security



Step 4 :

Choosing the Ethernet controller and click Apply to bridge your Soft AP.



6

TECHNICAL SPECIFICATIONS



WEP, TKIP, AES, WPA and WPA2



TROUBLESHOOTING

Symptom :

The LED is off.

Remedy :

Make sure the PC Card is inserted properly. Otherwise contact your vendor.

Symptom :

The LED is always on not blinking.

Remedy :

Make sure that you have installed the driver from attached CD. Otherwise contact your vendor.

Symptom :

The LED is blinking but the PC Card icon does not appear in your icon tray.

Remedy :

Make sure that you have installed the Utility from the attached CD.

Symptom :

The PC Card is linking, but can't share files with others.

Remedy :

Make sure the **file and printer sharing** function is enabled. You can enable the function by checking the icon of **My Computer -> Control Panel -> Network -> file and printer sharing -> I want to be able to give others to access to my files.**

Symptom :

Slow or poor performance under AP mode

Remedy :

Try to select another channel for the communicating group or move your device closer to the Access Point.



IEEE 802.11 Standard

The IEEE 802.11 Wireless LAN standards subcommittee, which is formulating a standard for the industry.

Access Point

An internetworking device that seamlessly connects wired and wireless networks together.

Ad Hoc

An Ad Hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. Ad Hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

BSSID

A specific Ad Hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

DHCP

Dynamic Host Configuration Protocol - a method in which IP addresses are assigned by server dynamically to clients on the network. DHCP is used for Dynamic IP Addressing and requires a dedicated DHCP server on the network.

Direct Sequence Spread Spectrum

This is the method the wireless cards use to transmit data over the frequency spectrum. The other method is frequency hopping. Direct sequence spreads the data over one frequency range (channel) while frequency hopping jumps from one narrow frequency band to another many times per second.

ESSID

An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while served as a continuous connection to the network wireless stations and Access Points within an ESS must be configured with the same ESSID and the same radio channel.

Ethernet

Ethernet is a 10/100Mbps network that runs over dedicated home/office wiring. Users must be wired to the network at all times to gain access.

Gateway

A gateway is a hardware and software device that connects two dissimilar

systems, such as a LAN and a mainframe. In Internet terminology, a gateway is another name for a router. Generally a gateway is used as a funnel for all traffic to the Internet.

IEEE

Institute of Electrical and Electronics Engineers
Infrastructure

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

ISM Band

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the so-called ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

Local Area Network (LAN)

A LAN is a group of computers, each equipped with the appropriate network adapter card connected by cable/air, that share applications, data, and peripherals. All connections are made via cable or wireless media, but a LAN does not use telephone services. It typically spans a single building or campus.

Network

A network is a system of computers that is connected. Data, files, and messages can be transmitted over this network. Networks may be local or wide area networks.

Protocol

A protocol is a standardized set of rules that specify how a conversation is to take place, including the format, timing, sequencing and/ or error checking.

SSID

A Network ID unique to a network. Only clients and Access Points that share the same SSID are able to communicate with each other. This string is case-sensitive.

Static IP Addressing

A method of assigning IP addresses to clients on the network. In networks with Static IP address, the network administrator manually assigns an IP address to each computer. Once a Static IP address is assigned, a computer

uses the same IP address every time it reboots and logs on to the network, unless it is manually changed.

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.

Transmission Control Protocol / Internet Protocol (TCP/IP)

TCP/IP is the protocol suite developed by the Advanced Research Projects Agency (ARPA). It is widely used in corporate Internet works, because of its superior design for WANs. TCP governs how packet is sequenced for transmission the network. The term "TCP/IP" is often used generically to refer to the entire suite of related protocols.

Transmit / Receive

The wireless throughput in Bytes per second averaged over two seconds.

Wi-Fi Alliance

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability. The organization is formerly known as WECA.

Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance put together WPA as a data encryption method for 802.11 wireless LANs. WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys.

Wide Area Network (WAN)

A WAN consists of multiple LANs that are tied together via telephone services and / or fiber optic cabling. WANs may span a city, a state, a country, or even the world.

Wired Equivalent Privacy (WEP)

Now widely recognized as flawed, WEP was a data encryption method used to protect the transmission between 802.11 wireless clients and APs. However, it used the same key among all communicating devices. WEP's problems are well-known, including an insufficient key length and no automated method for distributing the keys. WEP can be easily

cracked in a couple of hours with off-the-shelf tools.

Wireless LAN (WLAN)

A wireless LAN does not use cable to transmit signals, but rather uses radio or infrared to transmit packets through the air. Radio Frequency (RF) and infrared are the commonly used types of wireless transmission. Most wireless LANs use spread spectrum technology. It offers limited bandwidth, usually under 11Mbps, and users share the bandwidth with other devices in the spectrum; however, users can operate a spread spectrum device without licensing from the Federal Communications Commission (FCC).

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.

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.

Beacon Interval

In addition to data frames that carry information from higher layers, 802.11 includes 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).

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.

WPA2

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

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.

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.

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.