LM822 WiFi Module with IC Antenna

Host Controller Interface (HCI) via USB Interface

USER MANUAL

Revision	Date	Changes Description
v1.0	19/07/2017	First revision of this user manual.

Contents

1. Introduction
1.1. Features

- WiFi 802.11 b/g/n
- Operates in 2.4 GHz Frequency bands
- Onboard Chip Antenna
- Plug and Play (Linux, macOS X, Windows XP – 10 and Windows Compact Embedded 6/7 compatible)
- Up to 150Mbps Data Transfer Rate
- 802.11e-compatible bursting and I standards
- BPSK, QPSK, 16 QAM and 64 QAM modulation schemes
- WEP, TKIP, and AES, WPA and WPA2 encryption schemes
- Fully-featured software utility for easy configuration and management

1.2. Optional Features

- DC power input 3.3V or 5V
- WPS or PDN control function on half-hole pin 6
- Support LED function when choose WPS option

1.3. System Requirements

Host Operating System	OS Version Number (LM Tested)
Linux	- Ubuntu 15.10 (Kernel 4.2.0-16-generic) - Ubuntu 14.04.03 (Kernel 3.13.0-77-generic)
MAC OSX	- OSX 10.11 (El Capitan) - OSX 10.6 (Snow Leopard)
Windows	- Win 10 (32-bit & 64-Bit) - Win 8/8.1 (32-bit & 64-Bit) - Win 7 (64-bit) - Win XP (32-bit)

2. Windows Driver / Utility Installation

The installation of the driver and utility on the host computer will automatically activate, the autorun installation program after you click the exe application. All module drivers for the relevant host operating can be found on our website.

Click here for downloadable drivers.

Step 1 :
Download the compatible driver for your host operating system. Choose the Setup Language and click **Next** button.
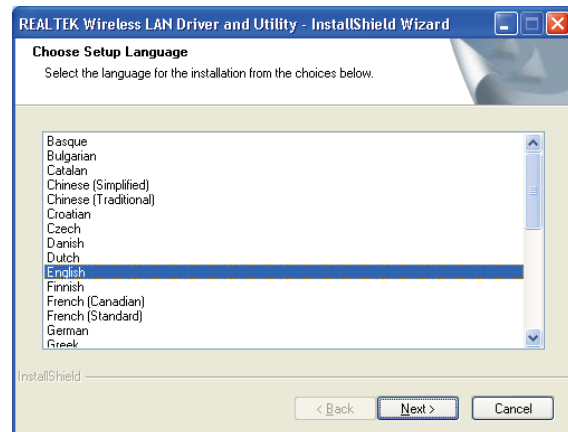
Step 2 :
Installation descriptions shown.
Click **Next** to continue.

Click **Install** to begin the installation.

Installing & configuring Realtek utility.
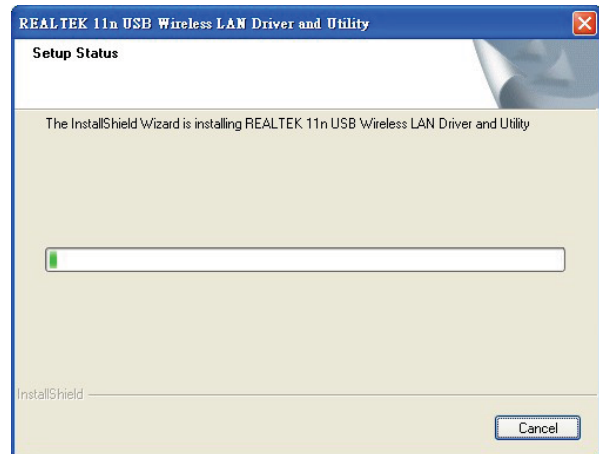
Installing Drivers.
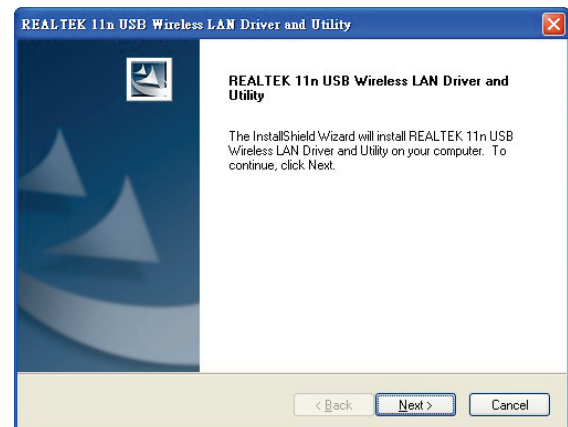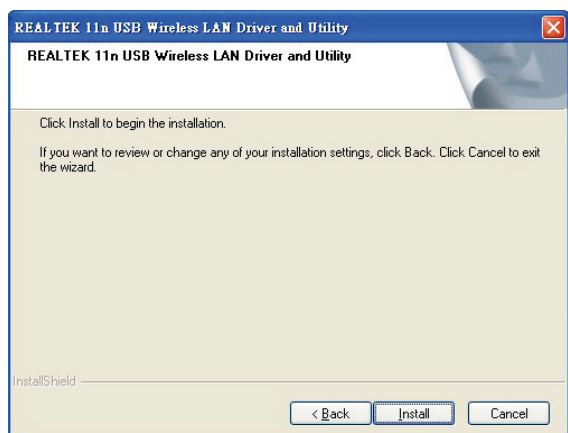

Step 3 :
Click **Finish** to complete installation.
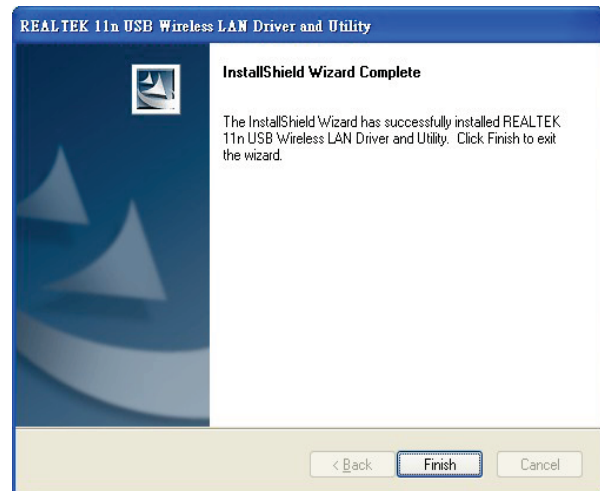
3. MAC OS Driver / Utility Installation
3.1. Installation Process

Please follow the steps below for setting up the LM822 on MAC host computer:

Step 1 :
Download the correct driver for the MAC OS version from LM822 product page.

Click here for downloadable drivers.

Step 2 :
Save the installable file on the MAC
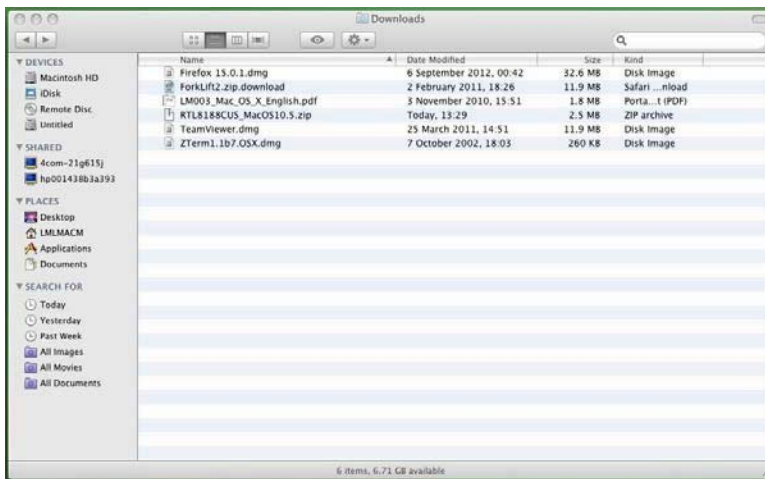
Step 3 :
Please ensure there are no other Realtek USB module drivers already installed on your MAC. Any existing drivers may conflict with the new driver and the USB module may not be detected. If an existing driver is found then uninstall it from your MAC.

Step 4 :
Please ensure the Ethernet interface such as Airport or physical LAN connection is enabled.

Step 5 :
Make sure the LM822 is unplugged from the USB port. Unzip the driver file and start the installation.

Step 6 :
Wait for the installation to finish before restarting the machine
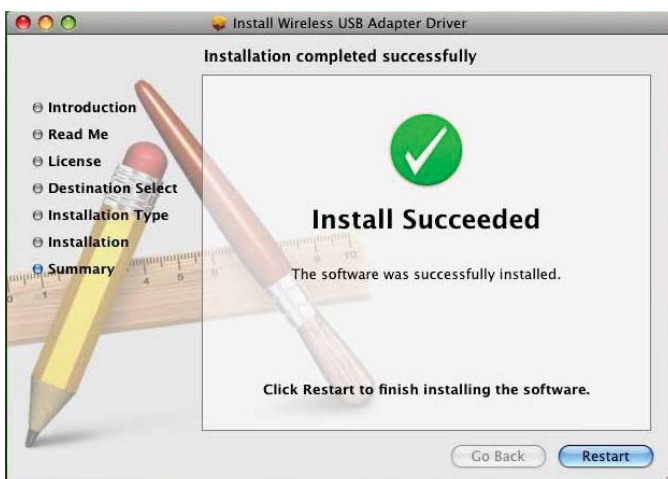
Step 7 :
Once the MAC has restarted, connect the LM822 module to the USB port. The
Wireless Network Utility will launch automatically and a message will appear to
enable WLAN card.
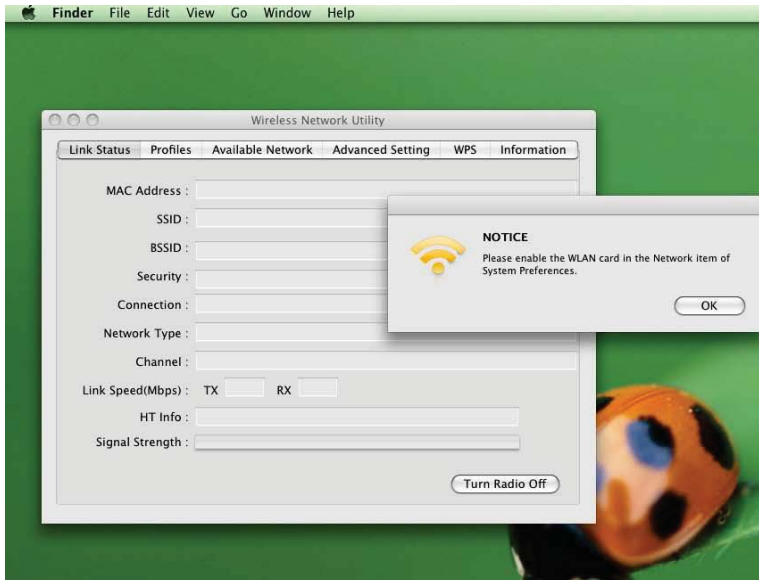
Step 8 :
Open the **Network Preferences** and a pop up message will appear stating a new
network interface has been detected. A new network interface e.g. **en2 or en3**
will appear in the list of the network interfaces.

Step 9 :
Click **OK** to the pop up message. Select the new Ethernet interface created (en2, en3 or similar) then press **Apply**. This enables the selected Ethernet interface and the **Wireless Network Utility** detects the LM822. The MAC address of the LM822 and link status is updated on the **Wireless Network Utility** window.
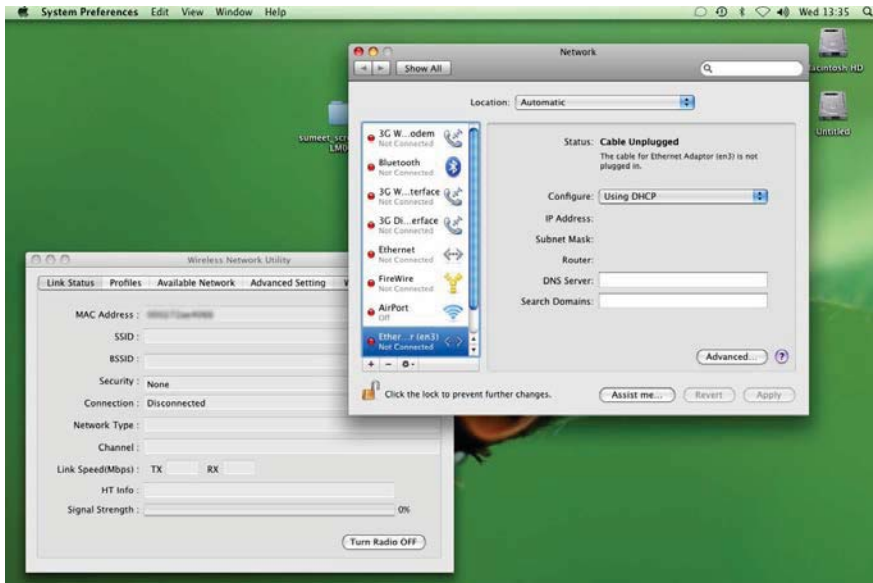
Step 10 :
Check the **Available Network** section on the **Wireless Network Utility** and connect to the wireless network.

Step 11 :
Once the network has connected, press **Add to Profile** to save the network and it will connect automatically.
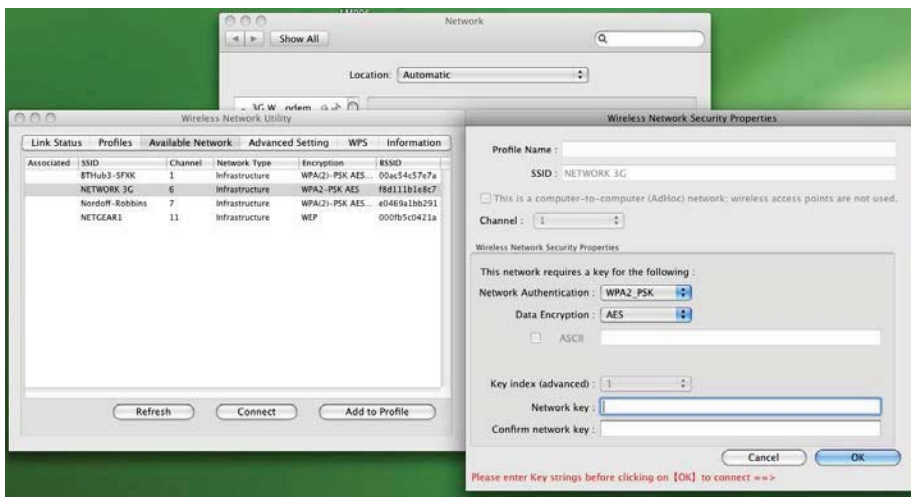
Step 12 :
Once the network is connected, the LM822 network interface should appear as connected in the **Network Preferences** and on the **Link Status** window, the signal strength, connection status and statistics should be shown
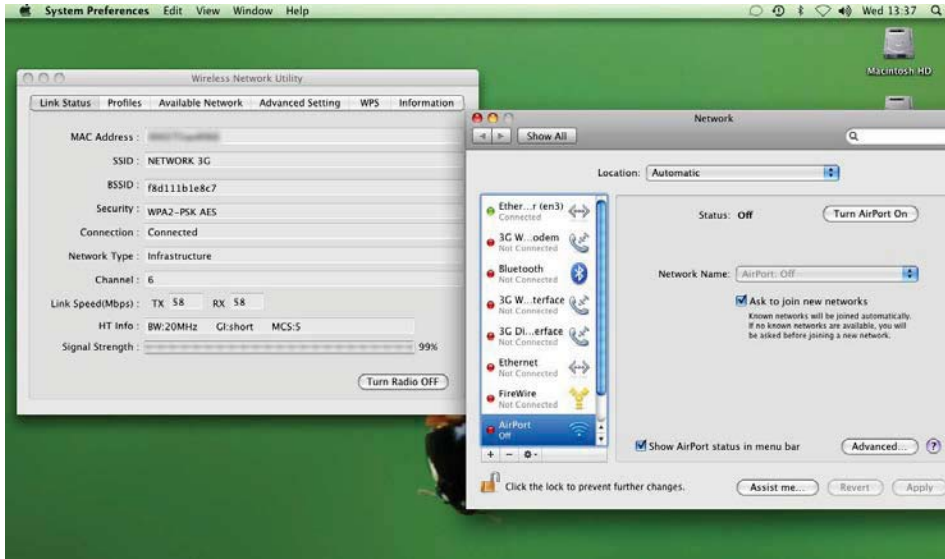
3.2. Uninstalling the MAC OSX Driver

Please follow the below steps to uninstall the LM822 driver on a MAC host computer.

Step 1 :
Run the uninstall.command script in the same folder the driver is extracted.
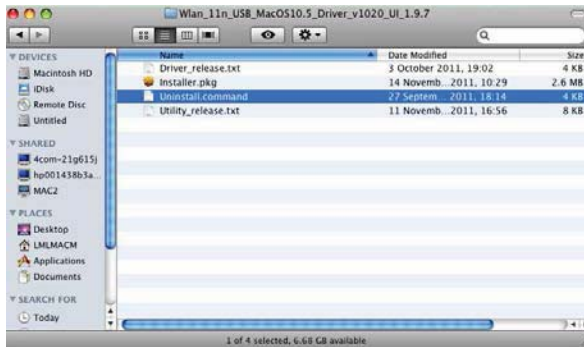
Step 2 :
You would need the root password to uninstall the driver. Enter the password when prompted in the terminal
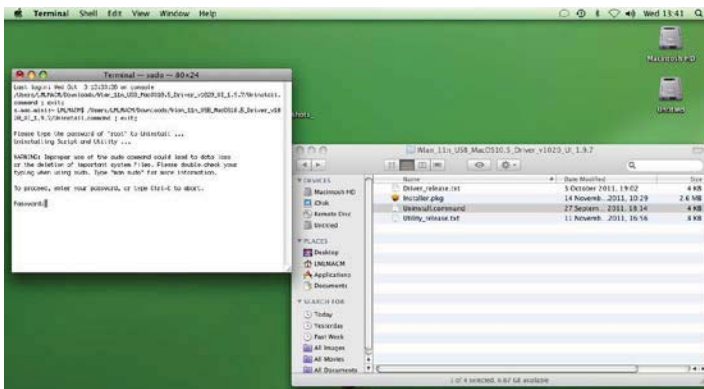
Step 3 :
Once the password is provided the script will uninstall the driver.

Note :
Please DONOT delete the network interface (en2, en3 or similar) created in the network preference because MAC does not recreate this interface when the driver installation is executed the next time. It may become difficult to get the LM822 working if the network interface is deleted.

4. Wireless LAN Basics

Wireless LAN network defined by IEEE 802.11b/g/n standard committee can be configured in the following modes:
- Ad Hoc (Point-to-point) wireless LAN.
- Infrastructure wireless LAN.
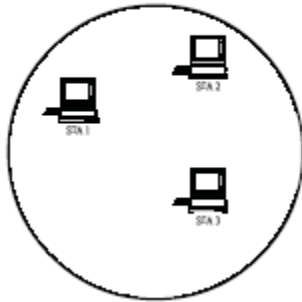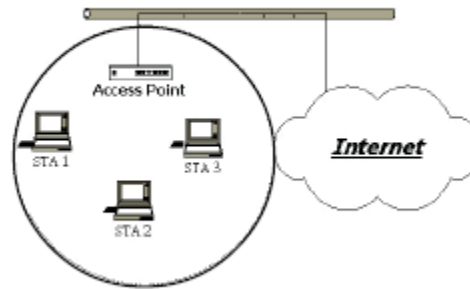
Ad Hoc Wireless Network   **Infrastructure** Wireless Network

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 cannot connect to the **Internet**.

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

Depending on your application requirements, you can easily set up your PC's network to be an "**Ad Hoc**" or "**Infrastructure**" wireless network. Generally speaking, if your network includes an **Access Point**, we recommend setting your network as an "**Infrastructure**" network to allow connectivity to the **Interne**

5. IP Address

To use this WiFi module with a computing device, the host device must be equipped with a USB interface. All drivers and supporting software for the module must be installed and configured first.

Ask your system administrator for the following information, which might be needed during the driver installation:
- Wireless Client Name
- Wireless SSID
- The host's unique client and workgroup name

For your network account you will need the following:
- Username
- Password
- IP address
- Gateway address
- Subnet mask (if you're not using a DHCP client)

Any computer on a network is identified by a unique IP address. There are two methods to assign an IP address to a computer on a TCP/IP network:
- Static IP addressing
- Dynamic IP addressing (DHCP Client)

In networks 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 onto the network. You may manually change the IP address in the **Network Properties dialog box.** Networks using static IP addresses is easy to set up and do not require additional network management software.

In networks with dynamic IP addressing, a DHCP server in the network dynamically assigns IP addresses to all clients every time they log onto the network. Networks using dynamic IP addresses require setting up and running a DHCP Server.

6. Wireless Network Configuration

The LM822 uses its own management software. All functions controlled by users are provided by this application. When you connect the module via USB to your laptop or desktop, an icon should appear in the Windows System Tray automatically.

6.1. Utility Icon

Client mode utility running but no module plugged in

Client mode utility running and module connected to scan available networks.

Client mode utility running and module cannot scan any access points

AP mode utility running.

6.2. Client Mode (Default Setting)

Wireless Device Control:

Show Tray Icon – Show or hide icon in system tray.
Radio Off – Stop wireless signal.
Disable Adapter – Stop wireless device

6.3. General Settings

Once device is setup, 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 also displayed.
The status bar displays the quality and strength of the link between the node and its Access Point. Link Quality is a measurement of the receiving and transmitting performances over the radio.
Network Address displays current MAC Address, IP Address, Subnet Mask address and Gateway address.
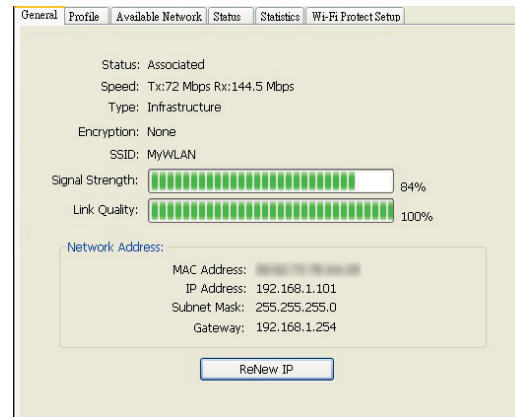
Click **Renew IP** button to refresh the IP address leased from the connected wireless AP.

6.4. Profiling Settings

In profile tab, you can
Add, **Remove**, **Edit**, **Duplicate** and **Set Default** to manipulate profile content manually. Strongly recommend using profile after you check **Available Networks**
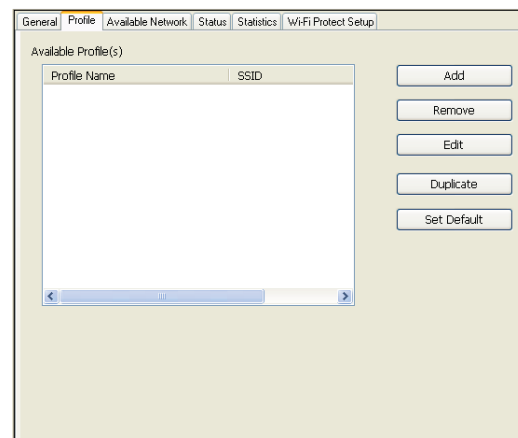
6.5.   Available Network Settings

Click **Available Network** tab and it will show all available networks that the radio reaches. Select the SSID & BSSID you want to connect with.

Click **Refresh** button to rescan available networks.
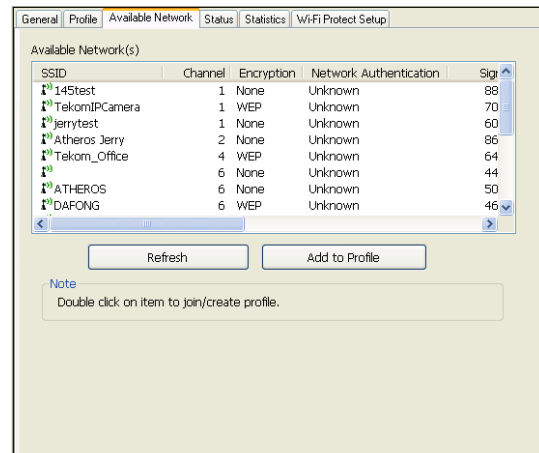
Select one of SSIDs, and click **Add to Profile** to create profile that can be configured with more wireless parameters. In this tab you can edit your profile name and configure wireless security such as WEP, WPA, WPA2, 802.1x ...etc. After finishing setup, click **OK** button to save configuration

6.6.   Status

Status tab shows all wireless networking and device driver versions in details.

Manufacturer	= REALTEK
NDIS Driver Version	= 5.1066.327.2009
Short Radio Header	= No
Encryption	= Disabled
Authenticate	= Open System
Channel Set	= ETSI
MAC Address	=
Data Rate (AUTO)	= Tx:72 Mbps Rx:144.5 Mbps
Channel (Frequency)	= 11 (2462 MHz)
Status	= Associated
SSID	= MyWLAN
Network Type	= Infrastructure
Power Save Mode	= None
Associated AP MAC	=
Up Time (hh:mm:ss)	= 0:03:55

6.7.   Statistics

Statistics tab shows real-time TX/RX relative counters to check or evaluate the wireless performance.

Click **Reset** button to reset the 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

Reset

6.8.   Wi-Fi Protected Setup

For an easy and secure setup solution for WiFi network, you can select PIN Code or Push Button methods to connect to an AP.

Pin method:

Step 1:

Push the PIN button.

Step 2:

Select a specific AP

Then enter the PIN code into your AP.

Step 3:

Select AP that you want to configure.
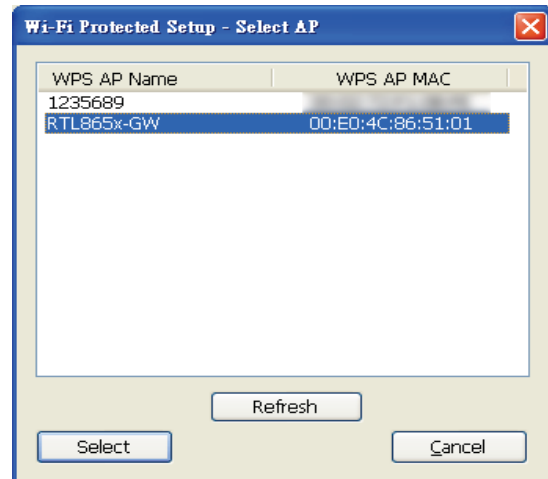
Step 4:

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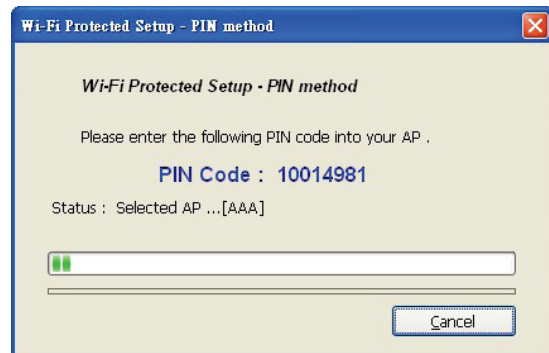
PBC method:

Step 1:

Push the PBC button.
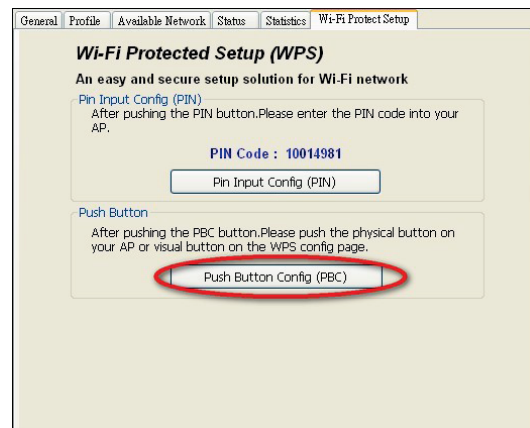
Step 2:

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

Soft AP:

Step 1:

Click **Access Point** to change AP mode
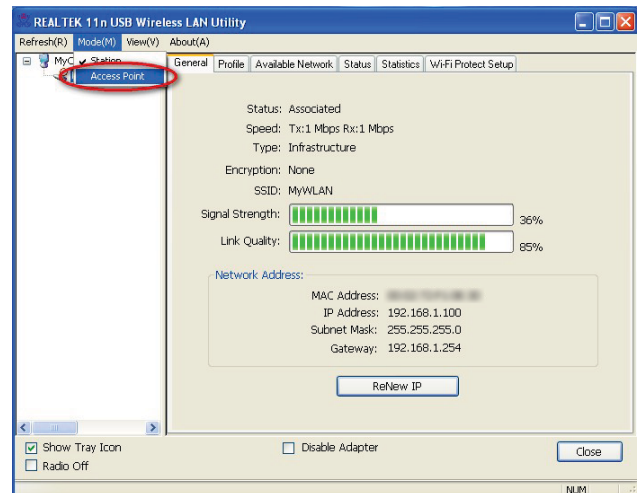
Step 2 :

Click **Config** to set AP.
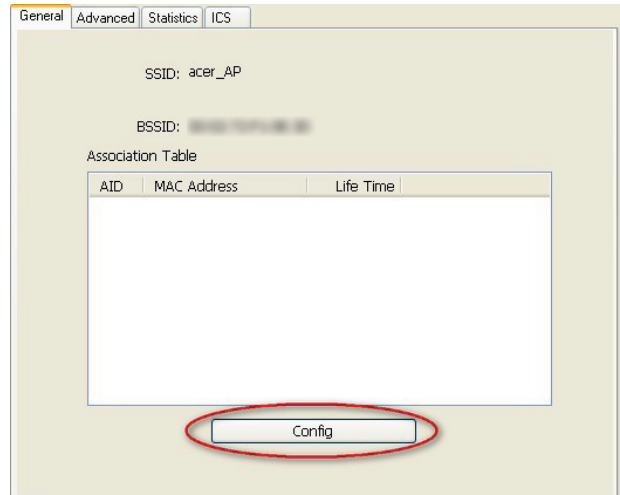
Step 3:

Setting SSID and Security
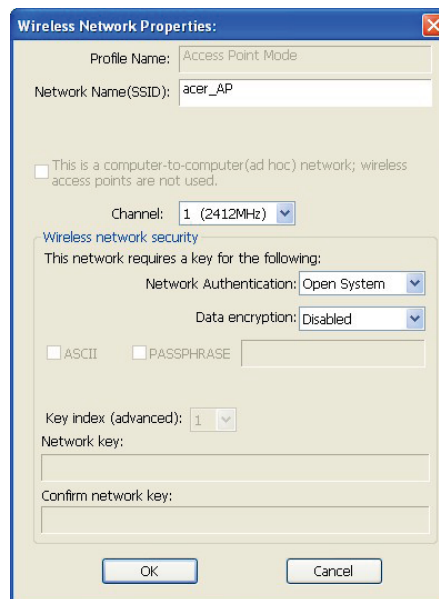
Step 4:

Select the Ethernet controller and click
Apply (to bridge your Soft AP).
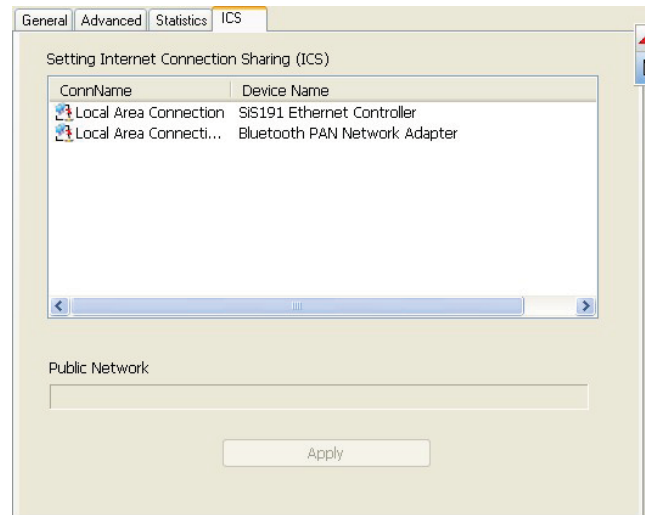
7. Glossary

IEEE 802.11 Standard

The IEEE 802.11 Wireless LAN standards subcommittee, which is formulates 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 module, 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 a 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 module 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 is 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 a 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.

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 3DE

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 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.

FCC Warning

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: 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 or more 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.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party 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 mobile or fixed condition, this module is to be installed only in mobile or fixed applications.

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: Additional testing and certification may be necessary when multiple modules are used.

Note 4: The module may be operated only with the antenna with which it is authorized. Any antenna that is of the same type and of equal or less directional gain as an antenna that is authorized with the intentional radiator may be marketed with, and used with, that intentional radiator.

Note 5: 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 6: FCC ID label on the final system must be labeled with "Contains FCC ID: VVXLM822" or "Contains transmitter module FCC ID: VVXLM822".