



LM811-0451

LM811 Wi-Fi & BT SMT Module

Dual Mode Class 1 - IEEE 802.11b/g/n

USER'S GUIDE

VERSION 1.3

**For Software & Downloads for this device, please visit
www.lm-technologies.com/downloads**

© 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 / 8 / 8.1 / 10.....	5
5. Wireless/Bluetooth 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

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	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	●				

1. Introduction

Thank you for your purchase of the LM811 WiFi Module. 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

Supports Microsoft Win7 / 8 / 8.1 / 10(32bit/64bit).
Operating distance of up to 150 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 set up.

SYSTEM REQUIREMENTS

Windows System : Win7 / 8 / 8.1 / 10(32bit/64bit).
System must have a device driver installed. It allows you to communicate with LM811 WiFi 11n USB Module.

BLUETOOTH

Bluetooth Version	v4.0
Frequency Range	2402-2480MHz
RF Output Power	5.77dBm (EIRP)

WIFI

Support Standards	802.11b, 802.11g, 802.11n-HT20/40
Frequency Range	2412-2472MHz for 802.11b/g/n (HT20) 2422-2462MHz for 802.11n (HT40)
RF Output Power	16.28dBm (EIRP)

BEFORE YOU START

Have the module and software ready

- ◆ LM811 WiFi 11n USB Module
- ◆ Software Downloadable from LM Technologies website.

<http://lm-technologies.com/product/wifi-and-bluetooth-usb-module-4-0-dual-mode-class-1-lm811/>

CONNECTING YOUR WLAN 11n USB Client Module

Connect your LM811 WLAN 11n USB Module. Install the driver.

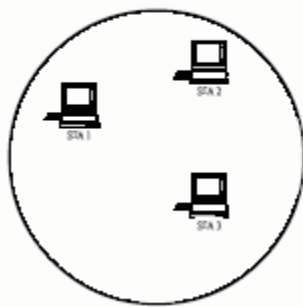
2. Wireless LAN Basics

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

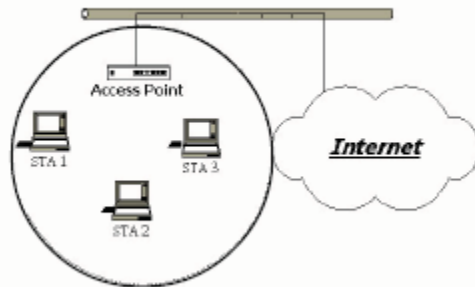
Ad Hoc wireless LAN.

Infrastructure wireless LAN.

Ad Hoc network is a group of wireless LAN cards, this group is called a BSS (Basic Service Set). 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 an **Infrastructure** wireless network and an **Ad Hoc** wireless network is the **Infrastructure** wireless network can access the resource in the Internet through an **Access Point**.

Depending on your requirement, you can easily set up your system network to be an “**Ad Hoc**” or “**Infrastructure**” wireless network.

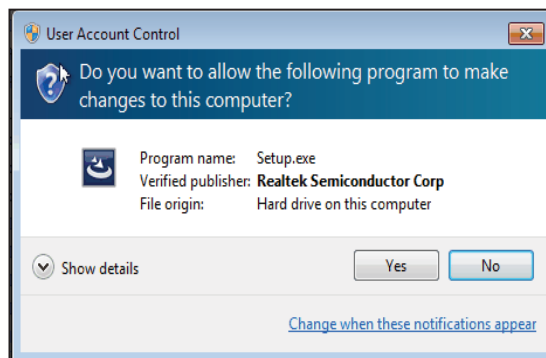
Generally speaking, if in your network, there is an **Access Point** in it, we recommend you to set your network as an “**Infrastructure**”, so it can connect to the **Internet**.

3. IP Address

After downloading the software, run it, you will be prompted as follows or similar.

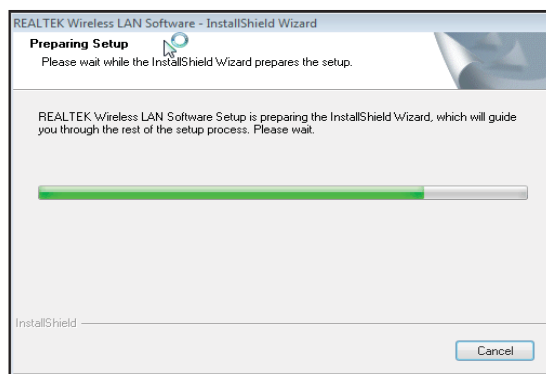
Step 1 :

Win UAC Dialog is shown. Click **Yes** to continue.



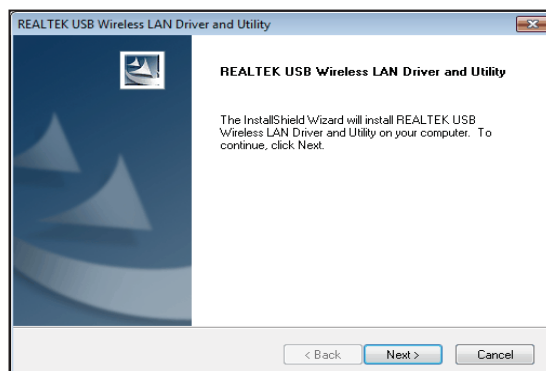
Step 2 :

Preparing Setup dialog is shown

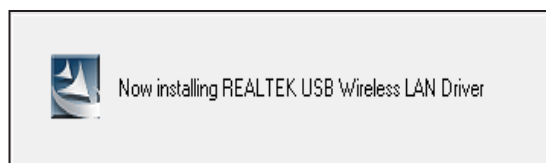


Step 3 :

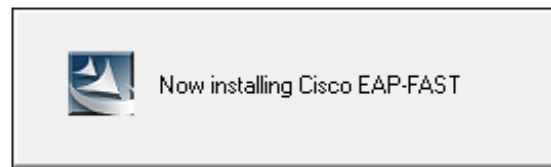
Wizard is ready to install the driver and utility. Click **Next** to begin the installation



Installing & configuring LM811 WiFi driver and utility

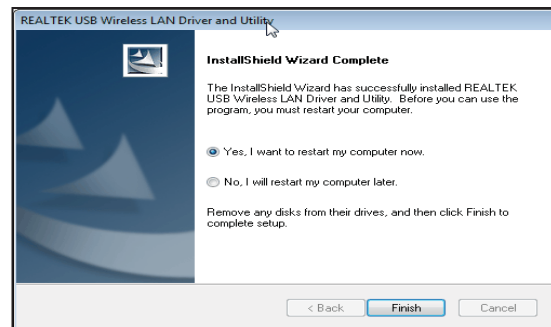


Installing Cisco 802.1x module



Step 4 :

Click **Finish** to complete the installation. The installation will take effect after windows restarts.



5. Wireless Network Configuration

The LM811 WiFi 11n USB Module uses its own management software. All functions controlled by users are provided by this application. When you insert the WLAN Module into your laptop or desktop, an icon should appear in the Windows System Tray, near the clock automatically.

5.1 Utility Icon

- Client mode utility running but no LM811 Module plugged in.



- Client mode utility running and LM811 scanning available networks.



- Client mode utility running and LM811 Module can not scan any AP



5.2 Client Mode (Default Setting)

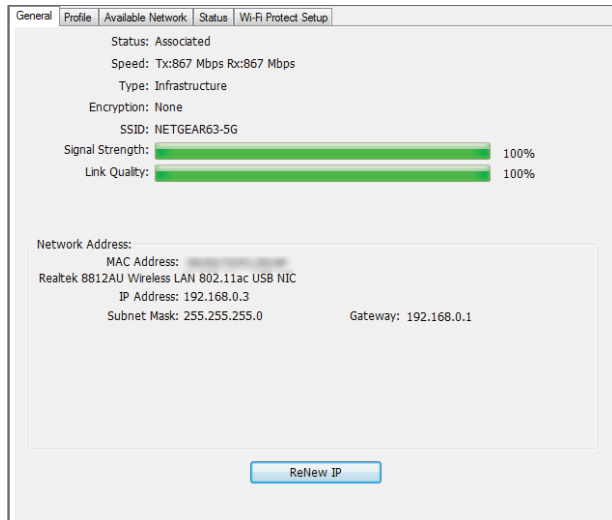
☒ Show Tray Icon	☐ Disable Adapter
☐ Radio Off	☐ Virtual WiFi allowed

Wireless Device Control :

- Show Tray Icon – Show icon or not show icon in system tray.
- Radio Off – To stop wireless signal.
- Disable Adapter – To stop wireless device.
- Virtual WiFi allowed – To enable Soft AP

5.2.1 GENERAL SETTING

Once the device is set, double click on the 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 bar graph displays the quality and strength of the link between the node and its Access Point.



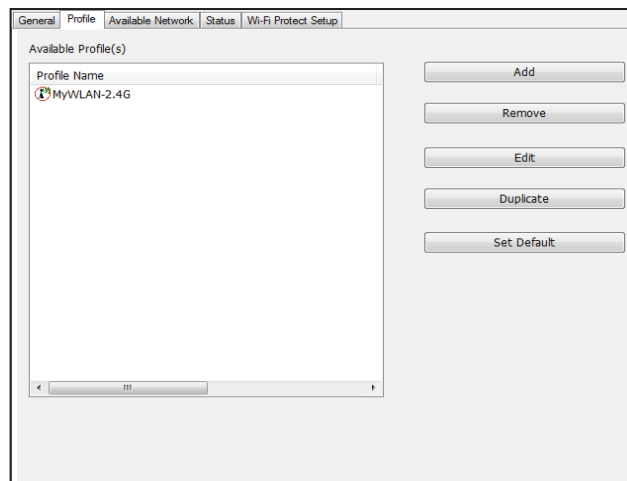
Link Quality is a measurement of receiving and transmitting performances over the radio.

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

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

5.2.2 PROFILE SETTING

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

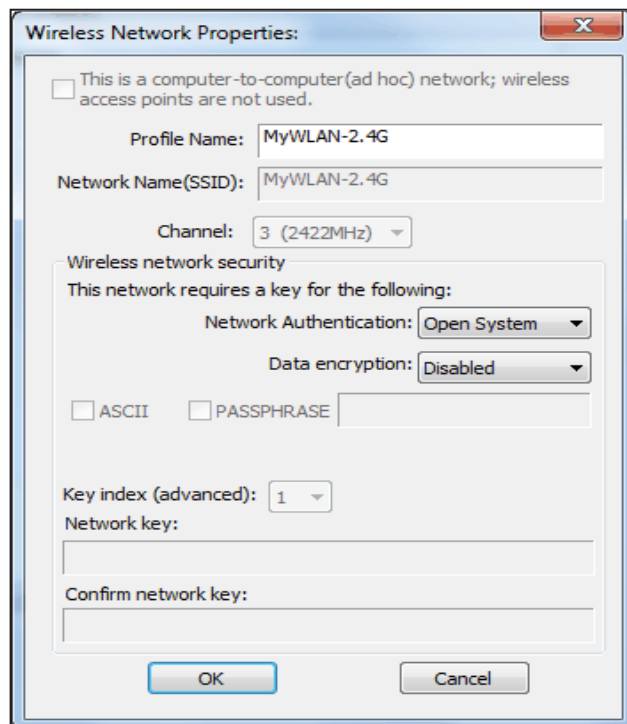
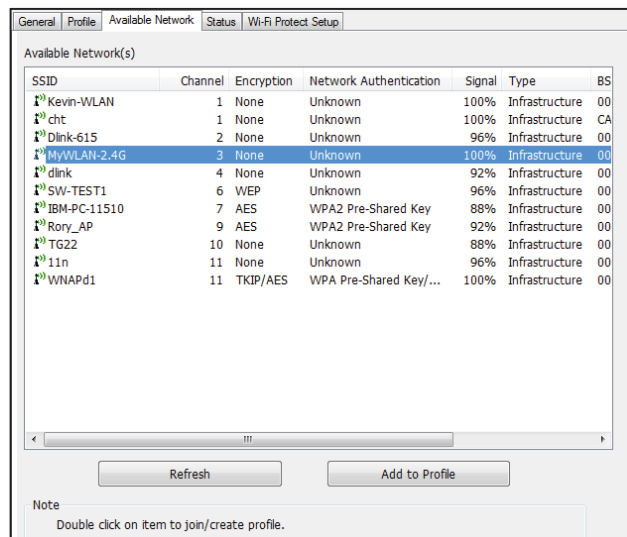


5.2.3 AVAILABLE NETWORK SETTING

Click **Available Network** tab and it will show all the available networks that the radio can reach. Select a proper SSID & BSSID you want to connect. Click the **Refresh** button to force and rescan the current available networks.

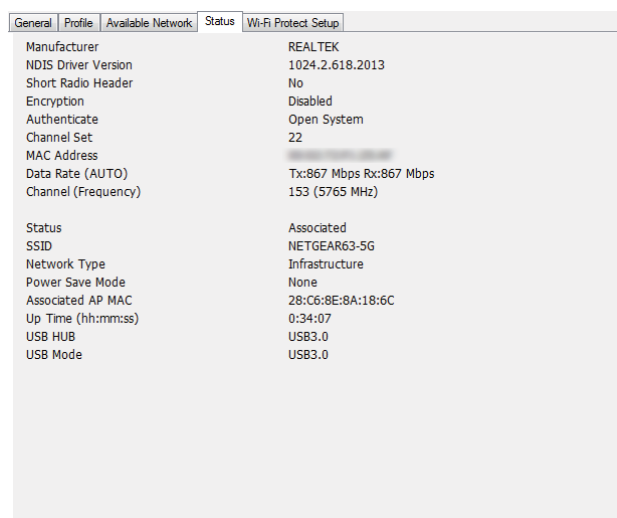
Select one of SSIDs, and click **Add to Profile** to create a profile that can be configured with more wireless parameters.

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



5.2.4 Status

This Dialog shows Manufacture, NDIS Driver Version, Short Radio Header, Encryption, Authentication, Channel Set, Mac Address... etc information



5.2.5 WiFi Protected Setup

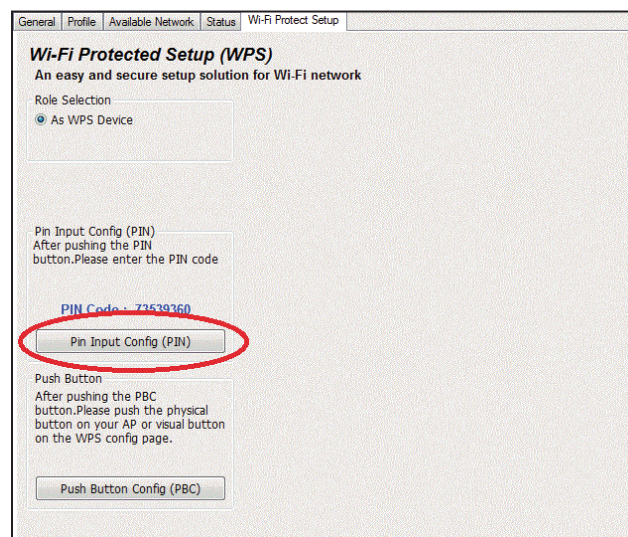
An easy and secure setup solution for a WiFi network. You can choose a PIN Code or Push Button method to connect to an AP.



■ Pin method:

Step 1 :

Press the “Pin Input Config (PIN)” button.



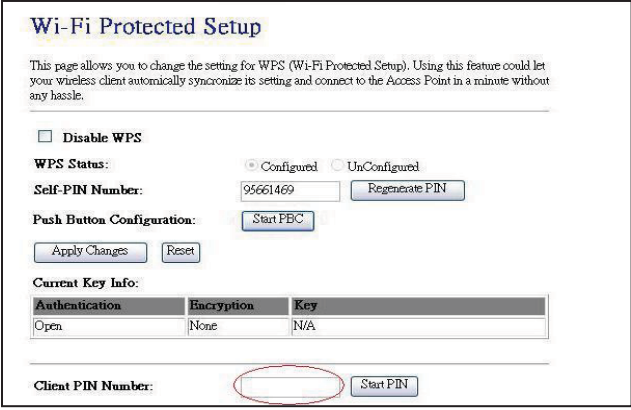
Step 2 :

Select a specific AP



Step 3 :

Enter the PIN code into your AP.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your 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: 95661469

Push Button Configuration:

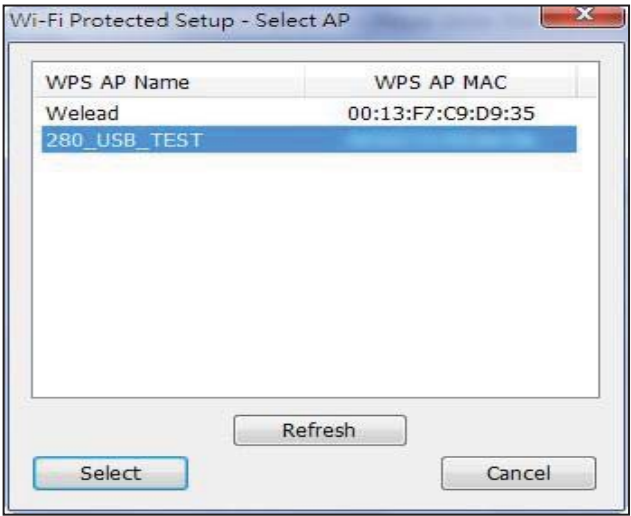
Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

Step 4 :

Select the AP that you want to configure.



Wi-Fi Protected Setup - Select AP

WPS AP Name	WPS AP MAC
Welead	00:13:F7:C9:D9:35
280_USB_TEST	

Step 5:

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



Wi-Fi Protected Setup - PIN method

Please enter the following PIN code into your AP .

PIN Code : 14909856

Status : Initial WPS ...

■ PBC method:

Step 1 :

Press “**Push Button Config (PBC)**” button

The top screenshot shows the 'Wi-Fi Protected Setup (WPS)' window. It has tabs for General, Profile, Available Network, Status, and Wi-Fi Protect Setup. The 'Wi-Fi Protect Setup' tab is active. The window title is 'Wi-Fi Protected Setup (WPS)' and the subtitle is 'An easy and secure setup solution for Wi-Fi network'. Under 'Role Selection', 'As WPS Device' is selected. Under 'Pin Input Config (PIN)', the PIN code is '73539360'. Under 'Push Button', the 'Push Button Config (PBC)' button is highlighted with a red circle. The bottom screenshot shows the 'Wi-Fi Protected Setup - PBC method' progress window. It has a title bar with a close button. The window title is 'Wi-Fi Protected Setup - PBC method'. The subtitle is 'Wi-Fi Protected Setup - PBC method'. The text says 'If there is more than one AP on the PBC mode, there will be [Session Overlap]. Please use PIN method or wait for a while and use PBC method again.' The status is 'Status : AP Sitesurvey ...'. There is a progress bar labeled 'Complete :'. At the bottom, there are two buttons: 'Push Button Config (PBC)' and 'Cancel'.

Step 2 :

Push the physical button on our AP or visual button on the WPS configuration page.

The screenshot shows the 'Wi-Fi Protected Setup' configuration page. The title is 'Wi-Fi Protected Setup'. The text says 'This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.' There is a checkbox for 'Disable WPS'. The 'WPS Status' is 'Configured'. The 'Self-PIN Number' is '95661469'. There is a 'Regenerate PIN' button. Under 'Push Button Configuration', the 'Start PBC' button is highlighted with a red circle. There are 'Apply Changes' and 'Reset' buttons. Below is a table for 'Current Key Info':

Authentication	Encryption	Key
Open	None	N/A

At the bottom, there is a 'Client PIN Number' field and a 'Start PIN' button.

5.3 Virtual WiFi Setup

Step 1 :

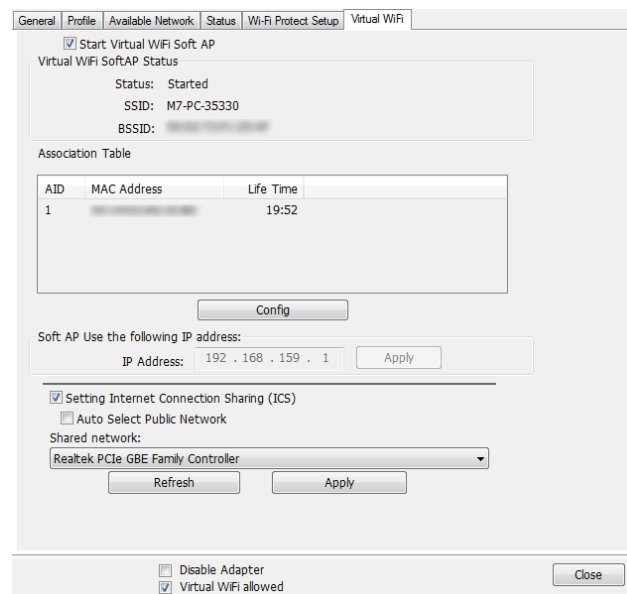
Click “**Virtual WiFi allowed**” option to enable Virtual WiFi configuration / status page.



☒ Show Tray Icon ☐ Disable Adapter
☐ Radio Off ☐ Virtual WiFi allowed

Step 2 :

Click “**Start Virtual WiFi Soft AP**” option to start



General Profile Available Network Status Wi-Fi Protect Setup Virtual WiFi

☒ Start Virtual WiFi Soft AP

Virtual WiFi SoftAP Status

Status: Started
SSID: M7-PC-35330
BSSID: [REDACTED]

Association Table

AID	MAC Address	Life Time
1	[REDACTED]	19:52

Config

Soft AP Use the following IP address:

IP Address: 192 . 168 . 159 . 1 Apply

☒ Setting Internet Connection Sharing (ICS)
☒ Auto Select Public Network

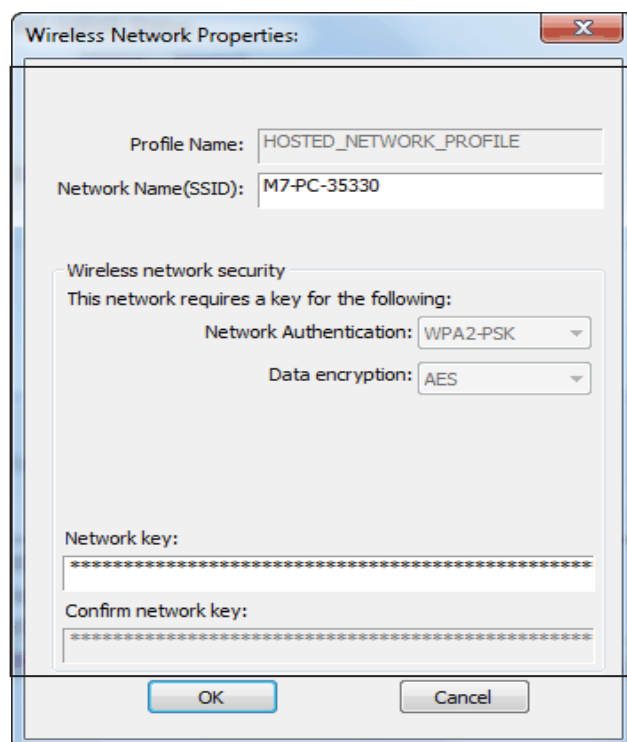
Shared network:
Realtek PCIe GBE Family Controller

Refresh Apply

☐ Disable Adapter
☒ Virtual WiFi allowed Close

Step 3 :

Click “**Config**” button to configure Soft AP SSID and Security Key.



Wireless Network Properties:

Profile Name: HOSTED_NETWORK_PROFILE

Network Name (SSID): M7-PC-35330

Wireless network security

This network requires a key for the following:

Network Authentication: WPA2-PSK

Data encryption: AES

Network key:

Confirm network key:

OK Cancel

Step 4 :

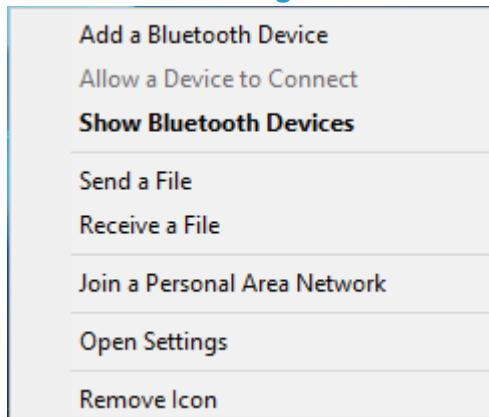
Check “**Setting Internet Connection Sharing**” and “**Auto Select Public Network**” options to enable ICS. If setup up Shared Network manually, press “**Apply**” button to re-initialization ICS.

Add a Bluetooth Enabled Device

To add a Bluetooth enabled device to your computer, you can use the [Bluetooth](#) icon located in the taskbar notification area or you can use a menu item in the [Bluetooth Devices](#) control panel.

NOTE: Before a Bluetooth device can be found, it must be within range and set to be discoverable.

To add a device using the Bluetooth icon:



Click the Bluetooth icon, click [Add a device](#), and follow the onscreen instructions. The Add a device wizard handles the pairing process.

To add a device using the Bluetooth Devices control panel:

1. Double-click the Bluetooth icon, and then click [Show Bluetooth Devices](#).

Click [Add a device](#) and follow the on-screen instructions. The Add a device wizard handles the pairing process.

NOTE:

The setup process for a Bluetooth wireless keyboard involves pairing with your computer.

- To conserve battery power, the Bluetooth wireless mouse, keyboard, or game controller goes to sleep after a specified period of inactivity. To wake up the mouse or game controller, move it around or click any of the controls. To wake up the keyboard, press any key.

After you have added a Bluetooth device to your computer, you can begin using the device.

To remove the device from your computer:

In [Bluetooth Devices](#), select the device and click [Remove device](#).

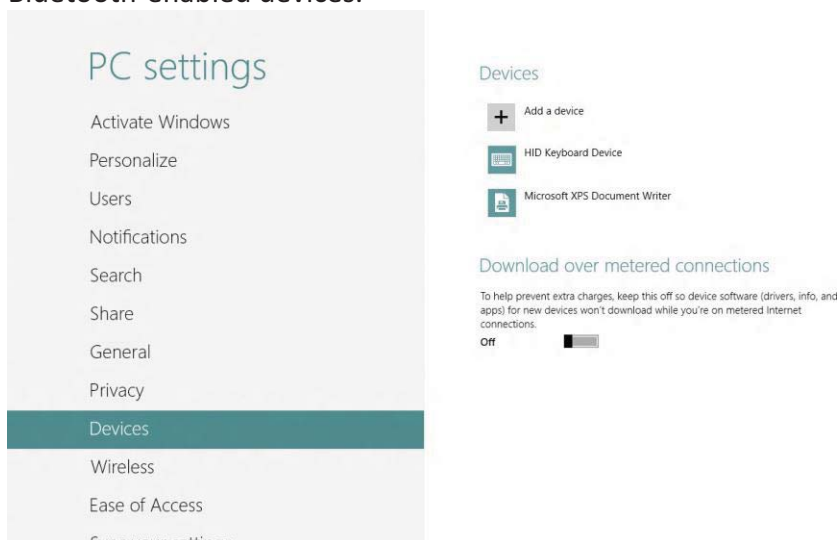
Windows 10 Setting

Use Bluetooth to facilitate wireless data transfers with other Bluetooth-enabled devices.

Pairing with other Bluetooth-enabled devices

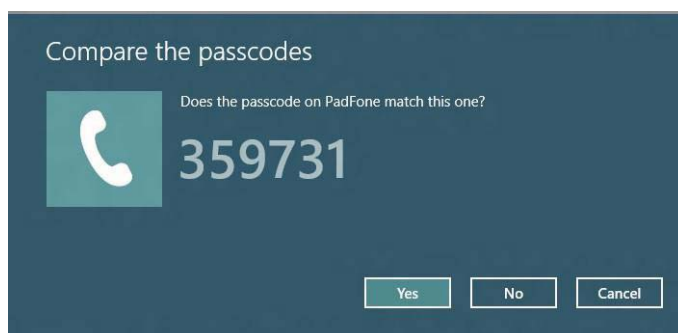
You need to pair your Notebook PC with other Bluetooth-enabled devices to enable data transfers. To do this, use your touchpad as follows:

1. Launch the Charms bar.
2. Tap, then tap Change PC Settings.
3. Under PC Settings, select Devices then tap Add a Device to search for Bluetooth-enabled devices.



4. Select a device from the list. Compare the passcode on your Notebook PC with the passcode sent to your chosen device. If they are the same, tap yes to successfully pair your Notebook PC with the device.

NOTE: For some Bluetooth-enabled devices, you may be prompted to key in the passcode of your Notebook PC.



6. Technical Specifications

Product Name	WLAN and Bluetooth combo module, USB interface
Standards	IEEE 802.11b/g/n, Bluetooth v2.1+EDR/ v3.0/ v3.0+HS/ v4.0
Data Transfer Rate	WLAN: 802.11b: 11, 5.5, 2, 1 Mbps 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11n: MCS0 to 7 for HT20MHz, MCS0 to 7 for HT40MHz Bluetooth: Basic rate: 1Mbps Enhanced data rate: 2, 3 Mbps High Speed: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulation Method	WLAN: BPSK/ QPSK/ 16-QAM/ 64-QAM/ DBPSK/ DQPSK/ CCK Bluetooth: 8DPSK, $\pi/4$ DQPSK, GFSKFSK
Frequency Range	2.4GHz ISM band
RF Output Power (tolerance ± 2 dBm)	WLAN: 17dBm – 802.11b@11Mbps 15dBm – 802.11g@54Mbps 13dBm – 802.11n@MCS0_HT20 13dBm – 802.11n@MCS7_HT20 13dBm – 802.11n@MCS0_HT40 13dBm – 802.11n@MCS7_HT40 Bluetooth: class 2
Receiver Sensitivity	WLAN: -82dBm – 802.11b@11Mbps -71dBm – 802.11g@54Mbps -67dBm – 802.11n@MCS7_HT20 -64dBm – 802.11n@MCS7_HT40 Bluetooth: -89dBm@1Mbps -90dBm@2Mbps
Antenna	Chip Antenna
Operating Temperature	-10 ~ 50° C ambient temperature 0 to 95 % (non-condensing)
Storage Temperature	-10 ~ 60°C ambient temperature 0 to 95 % (non-condensing)
Dimension	49.6 x 18 x 7.7 mm (LxWxH)

7. Troubleshooting

Symptom :

The dongle 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 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.

8. Glossary

IEEE 802.11 Standard

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

Access Point

An internet working device that seamlessly connects wired and wireless networks together.

Ad Hoc

An Ad Hoc wireless LAN is a group of personal 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). Personal 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 personal 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 personal 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 personal computer. Once a Static IP address is assigned, a personal 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.

Caution for IC (Canada)

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.



Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Please notice that if the IC identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: "Contains IC:10531A-LM811 " any similar wording that expresses the same meaning may be used.



L'étiquette d'homologation d'un module d'Innovation, Sciences et Développement économique Canada devra être posée sur le produit hôte à un endroit bien en vue, en tout temps. En l'absence d'étiquette, le produit hôte doit porter une étiquette sur laquelle figure le numéro d'homologation du module d'Innovation, Sciences et Développement économique Canada, précédé du mot « contient », ou d'une formulation similaire allant dans le même sens et qui va comme suit : Contient IC : 10531A-LM811 est le numéro d'homologation du module

Federal Communication Commission Interference Statement



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.

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

Please notice that if the FCC identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: "Contains FCC ID: VVXLM811-0451" any similar wording that expresses the same meaning may be used.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The module is limited to OEM installation ONLY.

The OEM integrator is responsible for ensuring that the end-user has no manual instruction to remove or install module.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

A separate approval is required for all other operating configurations, including portable configurations with respect to Part 2.1093 and difference antenna configurations.

There is requirement that the grantee provide guidance to the host manufacturer for compliance with Part 15B requirements.

CE Conformity



Manufacturer & Importer

LM Technologies Ltd, 19 Spectrum House, Gordon House Road, London NW5 1LP.