300N Dual Band
Wireless LAN USB Module

User Manual

Version: 1.0

(OCT., 2012)

COPYRIGHT

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 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:

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

FCC Caution

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

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.

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

Statement

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

IMPORTANT NOTE:

This module is intended for OEM integrator. The OEM integrator is still responsible for the FCC compliance requirement of the end product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

USERS MANUAL OF THE END PRODUCT:

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of 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.

LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX FCC ID: LNQ802RUN ". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of 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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC 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)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

C A T A L O G

Chapter I: Product Information

1-1 Introduction and safety information

Thank you for purchasing this high-speed wireless dual band network module! This network module can operate in 2.4GHz or 5GHz wireless network. Excepting common wireless standards 802.11a/b/g, this wireless network module is also able to access 802.11n wireless networks - data transfer rate is 300Mbps, and that's six times faster than 802.11g wireless network!

With easy-to-install USB 2.0 interface - a very common expansion port of computers - plug this wireless network module into any empty USB port of your computer, just that simple!

Other features of this router including:

- IEEE 802.11a/b/g/n compatible.
- High transfer data rate – up to 300Mbps.
- Support WMM wireless QoS feature.
- Support 64/128-bit WEP, WPA, WPA2 with IEEE 802.1x functions for high level of security.
- Support the most popular operating system: Windows XP/Vista/7.
- Support WPS (Wi-Fi Protected Setup) hardware button for easy connection.
- Support software AP function.
- Support USB 2.0/1.1 interface.
- Portable and tiny size design.
- **Green Power Saving**: it supports the smart transmit power control and auto-idle state adjustment.

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the following safety instructions:

1. This USB wireless network module is designed for internal box use only. DO NOT expose this network module to direct sun light, rain, or snow.

2. DO NOT put this network module at or near hot or humid places, like kitchen or bathroom. Also, do not left this wireless network module in the car in summer.

3. This network module is small enough to put in a child's mouth, and it could cause serious injury or could be fatal. If they throw the network module, the module will be damaged. PLEASE KEEP THIS NETWORK MODULE OUT THE REACH OF CHILDREN!

4. This network module will become hot when being used for long time (***This is normal and is not a malfunction)***. DO NOT put the network module on a paper, cloth, or other flammable objects after the network module has been used for a long time.

5. There's no user-serviceable part inside the network module. If you found that the network module is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the network module and device by yourself, warranty will be void.

6. If the network module falls into water, DO NOT USE IT AGAIN BEFORE YOU SEND THE MODULE TO THE DEALER OF PURCHASE FOR INSPECTION.

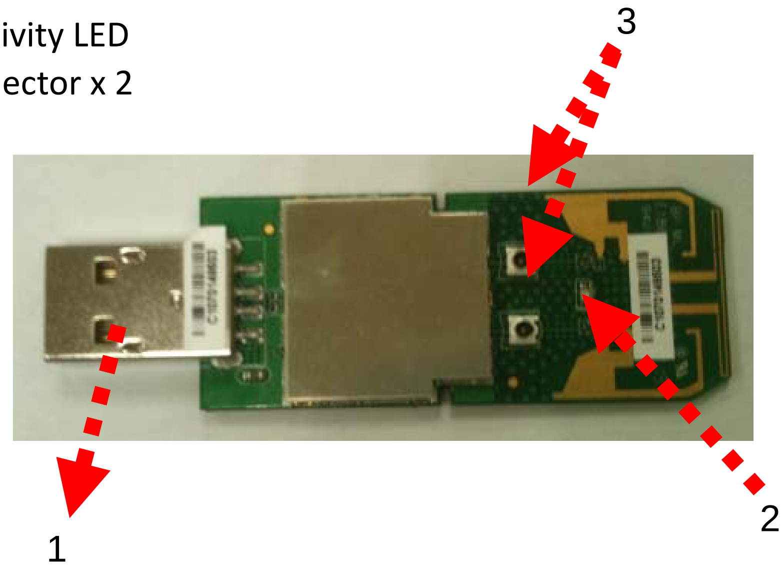
7. If you smell something strange or even see some smoke coming out from the network module, switch the device off immediately, and call dealer of purchase for help.

1-3 System Requirements

- An empty USB 2.0 port (May not be able work with USB 1.1 port, and performance will be greatly reduced)
- Operating system: Linux

1-4 Familiar with your new wireless network Module

1. USB Connector
2. Link/Activity LED
3. RF Connector x 2



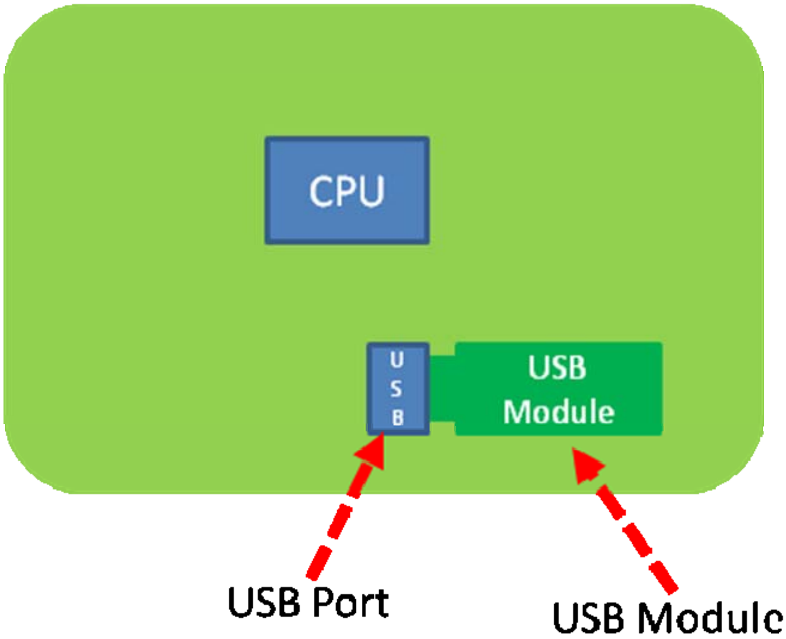
LED Name	Color	Light Status	Description
Radio Off	Green	Off	Wireless LAN function is disabled.
Radio On (No Link)	Green	Off	No link to wireless AP or Router
		Slow blinking	Transmitting management information.
Radio On (Link to AP or Router)	Green	On	Link to wireless AP or Router
		Blinking	Transmitting data or management information. If user activates WPS mode (hold WPS button for 3 seconds), the LED will be still blinking.

CHAPTER II: Driver Installation and Configuration

2-1 Network Module Installation

Please follow the following instructions to install your new wireless network module:

1. Insert the USB wireless module into an empty USB 2.0 port of your device when device is switched on. Never use force to insert the module, if you feel it's stuck, flip the module over and try again.



2-2 Network Module Driver Installation

Introduction

In this document, we introduce two ways to compile and install our Wi-Fi driver: 1) Using install.sh script for PC-Linux and 2) Step by step manually. The former targets for end users who are not familiar with Linux system, while the later for engineers who want to port our Wi-Fi driver onto different platforms.

2-2-1. Using install.sh Script for PC-Linux

For driver compilation and installation in PC-Linux, we provide an install.sh script to do the duties automatically. If you want to use our Wi-Fi solutions to access network on PC-Linux, you can just run install.sh script and then control Wi-Fi with utilities such as Network Manager. For further information about Wi-Fi station mode, please refer to:

document/Quick_Start_Guide_for_Station_Mode.pdf.

If you want to apply our Wi-Fi solutions on other embedded platforms, you should read and check the following paragraphs.

2-2-2. Decompress the driver source tar ball

The driver source tar ball is located in the driver folder of our software package. For example, to decompress rtl8188C_8192C_8192D_usb_linux_v3.3.0_2920.20111123.tar.gz:

root@driver/# tar zxvf rtl8188C_8192C_8192D_usb_linux_v3.3.0_2920.20111123.tar.gz2

2-3. Selecting Chip Type with make_drv Script (for compound release)

Our driver source release has two types: 1) single release, which can build out driver only for single chip type, and 2) compound release, which can build out drivers for multiple chip types separately.

For compound release driver, you will see make_drv script after you decompress the driver tar ball located in driver folder. Before compiling driver source, executing the make_drv to select the target chip type to compile. For example:

```
root@rtl8188C_8192C_8192D_usb_linux_v3.3.0_2920.20111123# ./make_drv
Please select chip type(1/2):
1) RTL8192cu
2) RTL8192du
#? 1
You have selected RTL8192cu
```

2-4. Compilation Settings in Makefile

2-4.1. Adding or Selecting Target Platform

The default target platform is PC-Linux, if you do not want to compile driver for other platforms you can skip this section.

To add or select target platform for compilation, we provide two sections in Makefile: 1) platform selection section and 2) platform setting section. First, you should look at the platform selection section of Makefile:

```
CONFIG_PLATFORM_I386_PC = y
CONFIG_PLATFORM_ANDROID_X86 = n
CONFIG_PLATFORM_ARM_S3C2K4 = n
CONFIG_PLATFORM_ARM_PXA2XX = n
CONFIG_PLATFORM_ARM_S3C6K4 = n
CONFIG_PLATFORM_MIPS_RMI = n
CONFIG_PLATFORM_RTD2880B = n
CONFIG_PLATFORM_MIPS_AR9132 = n
CONFIG_PLATFORM_MT53XX = n
CONFIG_PLATFORM_RTK_DMP = n
```

The platform selection section consists of entries with 'CONFIG_PLATFORM_' prefix. Only one entry is allowed to be set with value 'y' and others with 'n'. The 3

'CONFIG_PLATFORM_I386_PC' is selected by default.

We can select an existing entry or add a new entry for your target platform. For example, to add and select a new entry, 'CONFIG_PLATFORM_NEW':

```
CONFIG_PLATFORM_I386_PC = n
CONFIG_PLATFORM_NEW = y
```

Second, you should create and/or modify the corresponding entry inside platform setting section. For example, adding the following entry in platform setting section for 'CONFIG_PLATFORM_NEW' we just add:

```
ifeq ($(CONFIG_PLATFORM_NEW), y)
EXTRA_CFLAGS += -DCONFIG_LITTLE_ENDIAN
ARCH := arm
CROSS_COMPILE := /opt/ new/toolchain/arm-eabi-4.4.3/bin/arm-eabi-
KSRC := /opt /new/kernel
endif
```

2.4.2. Platform Setting Section in Detail

EXTRA_CFLAGS

The EXTRA_CFLAGS is usually used to carry some additional settings at compilation time through macro definitions.

Macro	Effect
CONFIG_BIG_ENDIAN	Define some internal data structure as big endian.
CONFIG_LITTLE_ENDIAN	Define some internal data structure as little endian.
CONFIG_MINIMAL_MEMORY_USAGE	For better performance in powerful platform, we allocate large physical continuous memory as TX/RX IO buffers. In some embedded platform, there is chance to fail to allocate memory. Define this macro to prevent this situation.
CONFIG_PLATFORM_ANDROID	Older Android kernel do not has CONFIG_ANDROID defined. Define this macro to force the Android corresponding code inside our driver to be compiled. For newer Android kernel, it has no need to define this macro, otherwise, warning message about redefinition will show up

2-3 Glossary

1. **What is the IEEE 802.11g standard?**

   802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

   The standard specifically calls for:

   A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

   B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard?**

   The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support?**

   The product supports the following IEEE 802.11 functions:

   - CSMA/CA plus Acknowledge Protocol
   - Multi-Channel Roaming
   - Automatic Rate Selection
   - RTS/CTS Feature
   - Fragmentation
   - Power Management

4. **What is Ad-hoc?**

   An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN module, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. **What is Infrastructure?**

   An integrated wireless and 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.

6. **What is BSS ID?**

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

7. **What is WEP?**

   WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. **What is TKIP?**

   TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. **What is AES?**

   AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. **Can Wireless products support printer sharing?**

    Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. **Would the information be intercepted while transmitting on air?**

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. **What is DSSS? What is FHSS? And what are their differences?**
Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. **What is Spread Spectrum?**
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. **What is WPS?**
WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access point automatically. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.