# Chung Nam Electronics (CNE)
# IEEE 802.11b/g/n MiniPCI WLAN Card
# (Model #: WLC-133NA)
# OEM Manual

# Version 0.1

June 2008

# Table of Contents

# Chapter 1 Introduction

The CNE 802.11b/g/n WLAN NIC is a complete wireless high speed Network Interface Card (NIC). It conforms to the IEEE 802.11n protocol and operates in the 2.45GHz ISM frequency bands.

- Fully compliant with the IEEE 802.11n WLAN standards
- FCC Certified Under Part 15 to Operate in the 2.45 GHz Bands
- Supporting 300Mbps
- Driver Supports LINUX

# Chapter 2 Installation Procedure

## 2.1 Get the driver

- **Get the driver LSDK-WLAN-pb44fus7.0.0.360.tar**
- **Untar LSDK-WLAN-pb44fus7.0.0.360.tar**
- **Then can see two file -- apps and wlan**

- **Apps – Some Wi-Fi application tools and encrypt tools**
- **WLAN – Linux driver in this file**

## 2.2 Compile

- 1. Go to ../../common/hal/linux
- 2. Make the file code, used the ‘make’ command
  Build a file name obj/i386-elf/hal.o
  The hal.o file is Atheros BSP
- 3. Go to ../../wlan/Linux/
- 4. Make the code, used the ‘make’ command
- 5. Install the .ko file, used the ‘make install’ command

## 2.3 Loading the driver

- The important issue on loading the driver is loading gradation.

1. Go to /lib/modules/2.6.9/net/
2. Insmod wlan.ko
3. Insmod ath_hol.ko
4. Insmod ath_dfs.ko
5. Insmod ath_rate_atheros.ko
6. Insmod ath_dev.ko
7. Insmod ath_pci.ko

## 2.4 Some Porting Issues

- 1/wlan/linux/ath_hal/ah_osdep.o /wlan/linux/ath_hal/ah_osdep.c:186: error: conflicting types for 'ath_hal_printf'/wlan/linux/ath_hal/../../common/hal/ah_internal.h:640: error: previous declaration of 'ath_hal_printf' was here
- Solve: Go to ../../common/hal/ah_internal.h:640
- Cancel the ath_hal_printf() function.
- 2 scripts/Makefile.build:13: /wlan/linux/ath/Makefile: No such file or directory
- Solve: Go to /wlan/linux/ath/
- Re-name Kbuild to Makefil

# Chapter 3 Regulatory Information

## 3.1 FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

## 3.2 FCC Guidelines for Human Exposure

*Warning:*
*The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.*

## 3.3 FCC Electronic Emission Notices

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.

## 3.4 OEM installation Guide

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.

LABEL OF THE END PRODUCT:
The final end product must be labeled in a visible area with the following
" Contains TX FCC ID: Q72WLC133NA"
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.

## 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.

This device is certified as modular radio form with the following antenna types. Change to other type requires re-evaluation/ certification

1) Dipole Antenna 1.8. dBi max

# Chapter 4 Technical Specifications

## Appendix A: Specifications

| | |
|---|---|
| **Standards** | IEEE802.11b, 802.11g, 802.11n Draft 2.0 |
| **Operating Frequency** | 2.4 GHz ~ 2.4835 GHz ISM band |
| **Channel Bandwidth** | 20/40MHz Support |
| **Protocols** | 802.11b: CCK, QPSK, BPSK<br>802.11g: OFDM<br>Draft-11n: BPSK, QPSK, 16-QAM, 64-QAM |
| **Antenna configurations** | 3T/3R Modes |
| **Security** | WPA/WP2, 64/128/152-bit WEP |
| **Receive Sensitivity** | 54Mbps@-70dBm (Typical)<br>Draft-N@-70dBm (Typical) |
| **Operating Voltage** | 3.3 VDC ± 10% |
| **Bus Interface** | 32bit Mini-PCI |
| **Antenna Connector Type** | 3 pieces of SMT ultra-miniature coaxial connectors |
| **Antenna port impedance** | 50ohm |

| Environmental and Physical | |
|---|---|
| Operating Temp | 0℃~55℃ (32℉~104℉) |
| Storage Temp | –20℃ ~ +85℃ (-40℉~158℉) |
| Humidity | 10% ~ 95% RH, Non-condensing |
| Dimensions (L×W×H) | 59.6mm (L) x 51.0mm (W) x 4.2mm (H) |

# Appendix B: Glossary

- **2x to 3x eXtended Range™ WLAN Transmission Technology -** The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, A 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.
- **802.11b -** The 802.11b standard specifies a wireless product networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **Ad-hoc Network -** An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.
- **DSSS** (**D**irect-**S**equence **S**pread **S**pectrum) **-** DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver 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. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).
- **FHSS** (**F**requency **H**opping **S**pread **S**pectrum) **-** FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.
- **Infrastructure Network -** An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless

network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

* **Spread Spectrum -** Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications 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).
* **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
* **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
* **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
* **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
* **WPA** (**W**i-Fi **P**rotected **A**ccess) **-** A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.