

# **11abgn 2x2 USB WiFi module**

**SHARP Corporation**

**DNUR-SM1**

**User Manual**

## **Copyright Statement**

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the prior writing of the publisher.

Pentium is trademark of Intel.

All copyright reserved.

## **FCC Statement:**

### **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.

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

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.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is restricted to *indoor* use when operated in the 5.15 to 5.25 GHz frequency range.

- ※ FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems.
- ※ This device will not permit operations on channels 116-128 for 11na and 120-128 for 11a which overlap the 5600 -5650MHz band.

**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 user's 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 FCC ID: NKR-SM1 ". 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.

This radio module (FCC: NKR-SM1/ Model: DNUR-SM1) has been approved to operate with the antenna types listed below with its antenna type and maximum permissible gain:

Type	Gain	Remark
Printed	0.67dBi	2.4GHz band
Printed	2.15dBi	5GHz band

The two antenna connectors of this module are only for test purpose and should not be connected with any external antenna. Any other antenna is strictly prohibited for use with this module without further authorization by FCC.

For Taiwan 警語：


第十二條

經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

**Note:** 1. 本模組於取得認證後將依規定於模組本體標示審驗合格標籤 2. 系統廠商應於平台上標示「本產品內含射頻模組:  CCXXxxYYyyyZzW」字樣.

# **Table of Contents**

## **1. INTRODUCTION 6**

## **2. DRIVER/UTILITY INSTALLATION / UNINSTALLATION 6**

## **3. CONNECTING TO AN EXISTING NETWORK 6**

## **4. MODIFYING A WIRELESS NETWORK 7**

4.1 MODIFYING GENERAL SETTINGS ..... 7

4.2 MODIFYING SECURITY SETTINGS..... 8

## **5. SPECIFICATIONS 10**

## **APPENDIX A: FAQ ABOUT WLAN 11**

# 1. Introduction

Thank you for purchasing the WLAN 802.11 a/b/g/n USB Module that provides the easiest way to wireless networking. This User Manual contains detailed instructions in the operation of this product. Please keep this manual for future reference.

## System Requirements

- 128 MB of RAM or later (recommended)
- 300 MHz processor or higher

# 2. Driver/Utility Installation

The driver should have been installed before the Blu-ray player is shipped from the manufacturer. You can start using its network function without installing driver or utility.

# 3. Connecting to an Existing Network

1. Use the remote control that came with your Blu-ray player to access the network configuration settings page.
2. Select the scanning wireless network function. The system starts to scan for available network. On this list, click Refresh to refresh the list at any time
3. Select the network you want to connect to.
4. If the chosen network has security enabled, you will have to setup corresponding security parameter. Contact the network manager for the correct settings. Select the security type and fill in required parameters. The options include the following:
  - WPA/WPA2/CCKM
  - WPA/WPA2 Passphrase
  - 802.1x
  - Pre-Shared Key (Static WEP)
  - None

## 4. Modifying a Wireless Network

### 4.1 Modifying General Settings

1. Use the remote control that came with your Blu-ray player to access the network configuration settings page.
2. From the profile list, select one profile and choose the modify function.
3. Modify the settings below for your network.

<b>Profile Name</b>	Identifies the configuration wireless network profile. This name must be unique. Profile names are not case sensitive.
<b>Client Name</b>	Identifies the client machine.
<b>Use this profile for Access Point mode</b>	Configures station to operate in Access Point mode.
<b>Network Names (SSIDs)</b>	The IEEE 802.11 wireless network name. This field has a maximum limit of 32 characters. Configure up to three SSIDs (SSID1, SSID2, and SSID3).



## 4.2 Modifying Security Settings

1. Use the remote control that came with your Blu-ray player to access the network configuration settings page.
2. Select a security option of this wireless network. This product provides security options below. Contact your wireless network administrator for choosing a correct option.
  - WPA/WPA2/CCKM
  - WPA/WPA2 Passphrase
  - 802.1x
  - Pre-Shared Key (Static WEP)
  - None

<b>WPA/WPA2</b>	Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA/WPA2 opens the WPA/WPA2 EAP drop-down menu. The options include: <ul style="list-style-type: none"> <li>• EAP-FAST</li> <li>• EAP-TLS</li> <li>• EAP-TTLS</li> <li>• EAP-SIM</li> <li>• PEAP (EAP-GTC)</li> <li>• PEAP (EAP-MSCHAP V2)</li> <li>• LEAP</li> </ul>
<b>WPA/WPA2 Passphrase</b>	Enables WPA/WPA2 Passphrase security. Click on the Configure button and fill in the WPA/WPA2 Passphrase.
<b>802.1x</b>	Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include: <ul style="list-style-type: none"> <li>• EAP-FAST</li> <li>• EAP-TLS</li> <li>• EAP-TTLS</li> <li>• EAP-SIM</li> <li>• PEAP (EAP-GTC)</li> <li>• PEAP (EAP-MSCHAP V2)</li> <li>• LEAP</li> </ul>
<b>Pre-Shared Key (Static WEP)</b>	Enables the use of pre-shared keys that are defined on both the access point and the station. To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the <a href="#">Define Pre-Shared Keys window</a> .

<b>None</b>	No security (not recommended).
<b>Allow Association to Mixed Cells</b>	Check this check box if the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter. Otherwise, the client is unable to establish a connection with the access point.
<b>Limit Time for Finding Domain Controller To</b>	Check this check box and enter the number of seconds (up to 300) after which the authentication process times out when trying to find the domain controller. Entering zero is like unchecking this check box, which means no time limit is imposed for finding the domain controller. Note: The authentication process times out whenever the authentication timer times out or the time for finding the domain controller is reached.
<b>Group Policy Delay</b>	Specify how much time elapses before the Windows logon process starts group policy. Group policy is a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. Valid ranges are from 0 to 65535 seconds. The value that you set goes into effect after you reboot your computer with this profile set as the active profile. This drop-down menu is active only if you chose EAP-based authentication.

## 5. Specifications

<b>Dimensions:</b>	42(L) * 25(W) * 6(H) mm
<b>Frequency range:</b>	USA: 2.400 ~ 2.483GHz, 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz, 5.725 ~ 5.85GHz Canada: 2.400 ~ 2.483GHz, 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz, 5.725 ~ 5.85GHz Taiwan: 2.400 ~ 2.483GHz, 5.25 ~ 5.35GHz, 5.47 ~ 5.725GHz, 5.725 ~ 5.85GHz Europe: 2.400 ~ 2.483GHz, 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz Japan: 2.400 ~ 2.497GHz, 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz China: 2.400 ~ 2.483GHz, 5.725 ~ 5.85GHz

### Channels support:

- 802.11n b/g
  - US/Canada/Taiwan: 11 (1 ~ 11)
  - Major European country: 13 (1 ~ 13)
  - France: 4 (10 ~ 13)
  - Japan: 11b: 14 (1~13 or 14<sup>th</sup>), 11g: 13 (1 ~ 13)
  - China: 13 (1 ~ 13)
- 802.11na
  - 1). US/Canada/Taiwan: 12 non-overlapping channels  
(36,40,44,48,52,56,60,64; 100,104,108,112,116,  
120,124,128,132,136,140; 149,153,157,161,165)
  - 2). Europe: 19 non-overlapping channel  
(36,40,44,48,52,56,60,64; 100,104,108,112,116,120,124,128,132,136,140)
  - 3). Japan: 19 non-overlapping channels  
( 36,40,44,48,52,56,60,64; 100,104,108,112,116,120,124,128,132,136,140)
  - 4). China: 5 non-overlapping channels (149,153,157,161,165)

<b>Host interface:</b>	USB 2.0
<b>Operation temperature:</b>	0° ~ 60° C
<b>Storage temperature:</b>	-20° ~ 80° C

## Appendix A: FAQ about WLAN

### 1. What is 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).

### 2. 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, 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.

### 3. 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 offers the encryption function (WEP) to enhance security and access control.

### 4. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

### 5. What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

## 6. What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone. As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.