802.11 b/g/n USB Module

DNUR-W1

User Manual

February 2013

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.

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.

IMPORTANT NOTE:
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.

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

Country Code selection feature to be disabled for products marketed to the US/CANADA

This device is intended only for OEM integrators under the following conditions:
1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna,
3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further <u>transmitter</u> test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed

IMPORTANT NOTE
In the event that these conditions <u>can not be met</u> (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID <u>can not</u> be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling
This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: NKR-DNURW1".

Manual Information to the End User
The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.
The end user manual shall include all required regulatory information/warning as show in this manual.

IC Statement:

CAN ICES-3 (B)/NMB-3(B)

This device complies with Industry Canada licence-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.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes:

1) L'antenne doit être installée de telle sorte qu'une distance de 20 cm est respectée entre l'antenne et les utilisateurs, et
2) Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

Tant que les 2 conditions ci-dessus sont remplies, des essais supplémentaires sur l'émetteur ne seront pas nécessaires. Toutefois, l'intégrateur OEM est toujours

responsable des essais sur son produit final pour toutes exigences de conformité supplémentaires requis pour ce module installé.

IMPORTANT NOTE:

In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the Canada authorization is no longer considered valid and the IC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Canada authorization.

NOTE IMPORTANTE:

Dans le cas où ces conditions ne peuvent être satisfaites (par exemple pour certaines configurations d'ordinateur portable ou de certaines co-localisation avec un autre émetteur), l'autorisation du Canada n'est plus considéré comme valide et l'ID IC ne peut pas être utilisé sur le produit final. Dans ces circonstances, l'intégrateur OEM sera chargé de réévaluer le produit final (y compris l'émetteur) et l'obtention d'une autorisation distincte au Canada.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains IC: 4441A-DNURW1".

Plaque signalétique du produit final

Ce module émetteur est autorisé uniquement pour une utilisation dans un dispositif où l'antenne peut être installée de telle sorte qu'une distance de 20cm peut être maintenue entre l'antenne et les utilisateurs. Le produit final doit être étiqueté dans un endroit visible avec l'inscription suivante: "Contient des IC: 4441A-DNURW1".

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.
The end user manual shall include all required regulatory information/warning as show in

this manual.

Manuel d'information à l'utilisateur final

L'intégrateur OEM doit être conscient de ne pas fournir des informations à l'utilisateur final quant à la façon d'installer ou de supprimer ce module RF dans le manuel de l'utilisateur du produit final qui intègre ce module.

Le manuel de l'utilisateur final doit inclure toutes les informations réglementaires requises et avertissements comme indiqué dans ce manuel.

Table of Contents

1. Introduction

Thank you for purchasing the WLAN 802.11 b/g/n USB Adapter 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 Blueray player is shipped from the manufacturer. You can plug this adapter to your Blueray player and 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 Blueray 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 Blueray 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.

Profile Name	Identifies the configuration wireless network profile. This name must be unique. Profile names are not case sensitive.
Client Name	Identifies the client machine.
Use this profile for Access Point mode	Configures station to operate in Access Point mode.
Network Names (SSIDs)	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 Blueray 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

WPA/WPA2	Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA/WPA2 opens the WPA/WPA2 EAP drop-down menu. The options include: ● EAP-FAST ● EAP-TLS ● EAP-TTLS ● EAP-SIM ● PEAP (EAP-GTC) ● PEAP (EAP-MSCHAP V2) ● LEAP
WPA/WPA2 Passphrase	Enables WPA/WPA2 Passphrase security. Click on the Configure button and fill in the WPA/WPA2 Passphrase.
802.1x	Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include: ● EAP-FAST ● EAP-TLS ● EAP-TTLS ● EAP-SIM ● PEAP (EAP-GTC) ● PEAP (EAP-MSCHAP V2) ● LEAP
Pre-Shared Key (Static WEP)	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 Define Pre-Shared Keys window.

None	No security (not recommended).
Allow Association to Mixed Cells	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.
Limit Time for Finding Domain Controller To	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.
Group Policy Delay	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

Dimensions: 41(L) * 23(W) * 4.3(H) mm

Frequency range: USA: 2.400 ~ 2.483GHz,

Europe: 2.400 ~ 2.483GHz,

Japan: 2.400 ~ 2.497GHz,

China: 2.400 ~ 2.483GHz,

Channels support: 802.11n b/g

US/Canada: 11 (1 ~ 11)

Major European country: 13 (1 ~ 13)

France: 4 (10 ~ 13)

Japan: 11b: 14 (1~13 or 14th), 11g: 13 (1 ~ 13)

China: 13 (1 ~ 13)

Operation temperature

Host interface: USB 2.0

Operation temperature: -10° ~ 60° C

Storage temperature: -10° ~ 70° C

Antenna information:

Antenna		Peak gain (dBi)
Type	Connector	2400~2483.5MHz
PIFA	N/A	3.27

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.