RF Sniffer User's Manual

Version 1.1

Revision History

Date	Revision	Description	Author
05/11/2006	1.0	Initial Release	Edward Castro
05/16/2006	1.1	Updated/Cleaned Sections	Dan Cornescu
05/24/2006	1.2	Updated Section 6 for proper FCC Statement	Trae Harrison

Table of Contents

1. Purpose and Scope of Document

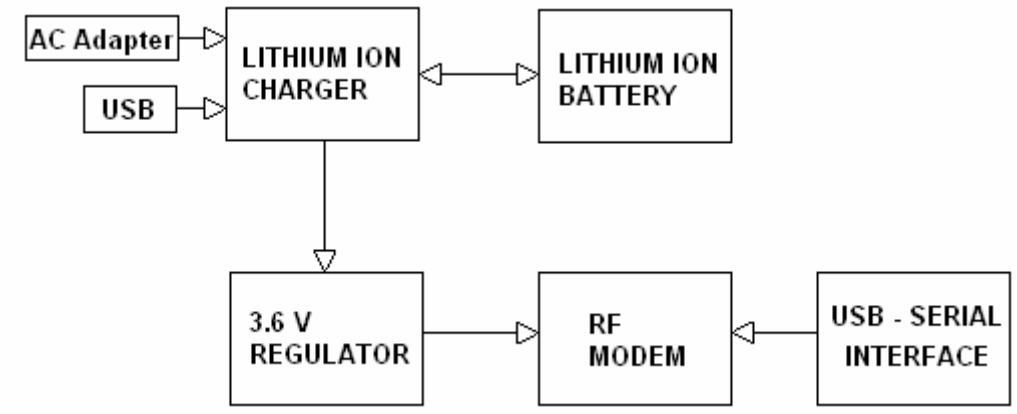
The purpose of this document is to provide the user with instructions on how to properly operate the RF Sniffer.

2. Overview of the RF Sniffer

The RF Sniffer is a 900MHz frequency-hopping self-contained deployment tool which provides a link between a device running specially designed software and the mesh network. It communicates via the 900 MHz Spread Spectrum mesh network and connects to a personal computer or PDA USB port. The Portable RF Sniffer is a battery powered device that can be re-charged from the USB port or from an optional AC adapter.

2.0 Block diagram

Below you will find the block diagram for the main functions of this device.



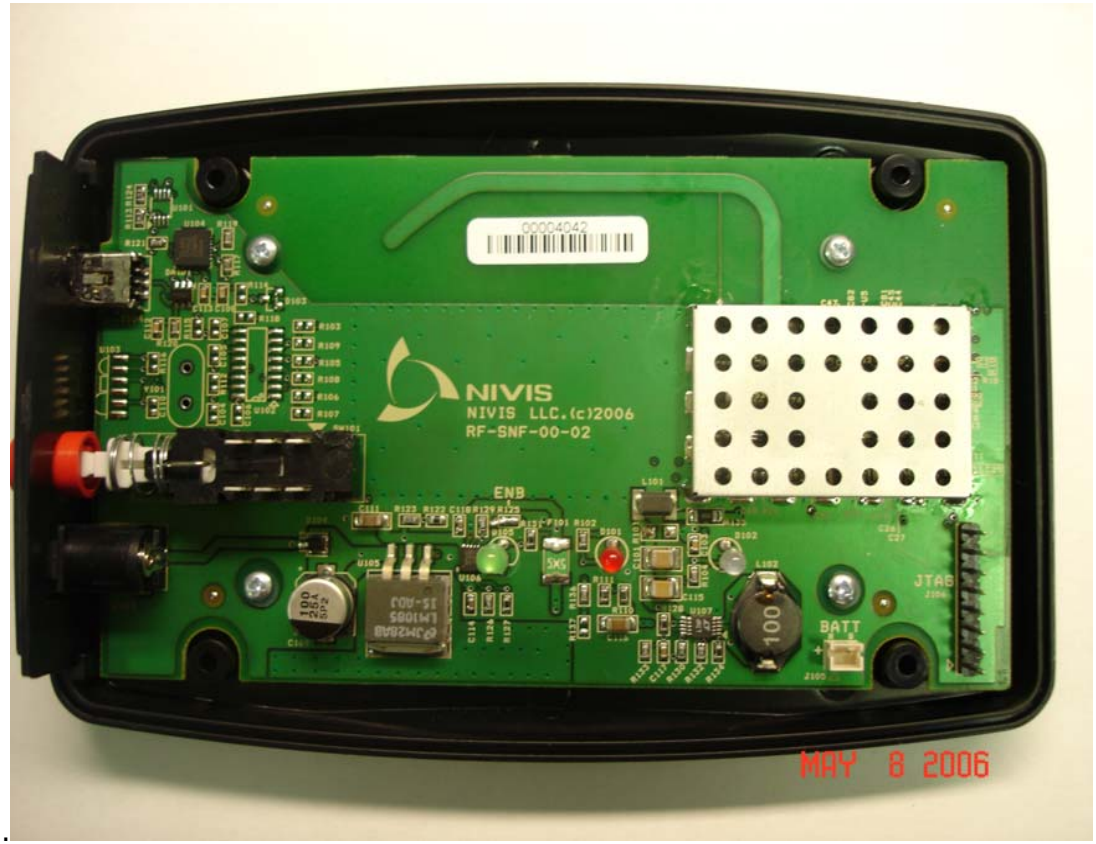
2.1 Operation

To use the RF Sniffer one only needs a connection to a USB port (PDA or PC). For limited periods of time the device can operate just by the internal Li-Ion rechargeable battery. When the device is not in use the power should be turned off to the device, then plugged into the AC Adapter for charging.

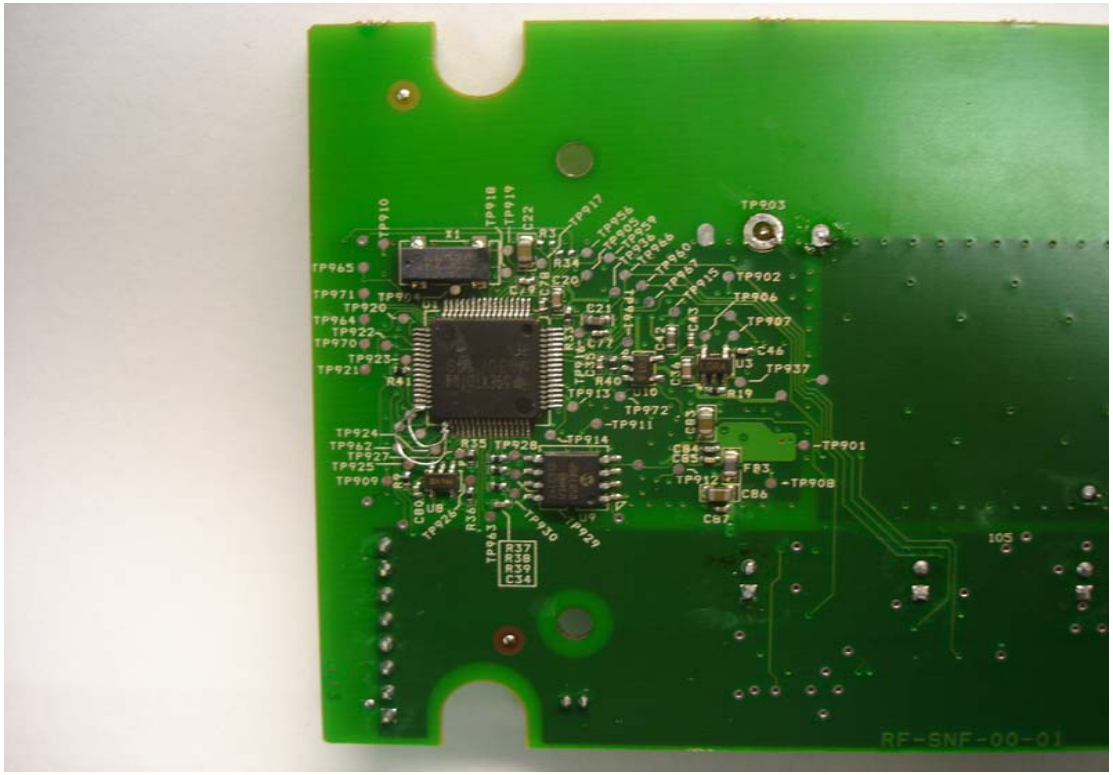
There are 3 visual indicators (LED's) on the front panel:

GREEN LED - Battery Charging LED indicator, continuously light, for periods that the device is charging the internal battery.
RED LED – Power LED indicator, continuously light if power on and the battery is charged enough. As soon as the battery is depleted and need recharging the LED start FLASHING.
BLUE LED – RF Traffic LED Indicator, lights for short periods of time when RF traffic is detected

On the left side of the picture is USB connector, in the middle-right is the Power ON/OFF button, right the AC adapter plug. Below is a picture of internal RF Sniffer circuit board



On the top side of the board (pictured above) you will find the RF components, (underneath the RF shield), the power supply section and the PCB antenna. The opposite side of the board contains the microcontroller and digital section as can be seen in the picture below.



The JTAG connector is located below and to the right of the RF shield on the front side of the circuit board. This is used for production and debugging purposes, loading firmware etc.

2.1.1 USB Interface block

The USB interface uses a serial to USB bridge controller. Device conforms to USB 2.0 standard. This chip is responsible for translating the USB protocol to the serial protocol used by the microcontroller. Connection to the PC is via a standard USB Mini B connector. The circuit is protected from damaging ESD by using a quad transient voltage suppressor. The USB interface also provides 5 volts for charging the internal Li-In battery.

2.1.2 Battery Charger block

The device uses a dual input USB / AC Li-Ion battery charger. This design allows up to 500 mA battery charge current from the AC adapter or up to 200 mA charge current from the USB interface, (supplied by the PC). The programmable charge currents are defined by the values of the two resistors.

The battery is internally protected from possible damage due to over charge / over load conditions. In addition, external protection is provided by resetable thermal fuse.

WARNING:
The input voltage from the AC adapter/charger must not exceed 15 volts or unit will be damaged.
An AC adapter of 9V - 12V is recommended. Adapter plus (+) voltage should go to center of the plug.

The battery charger circuit cannot supply charge current from both sources at the same time. With the factory soldered jumper installed, the battery will charge from the USB port when the Sniffer is turned on and will charge from the AC adapter when the Sniffer is turned off. If the jumper is removed, the battery will never charge from the USB port but will

always charge from the AC adapter, whether the Sniffer is on or off. The units are supplied from the factory with the jumper installed.

The green LED shows the charging status and is controlled by charging hardware. It is normal for the LED to cycle on and off if the Sniffer is idle for some time and the battery is fully charged.

2.1.3 Buck / Boost Regulator block

The power supply blocks uses a switch-mode regulator circuit which operates as a buck / boost regulator. This design maintains high efficiency due to a built in power switch and burst-mode control. The radio current demands can be as high a 500mA in the transmit mode. During receive, the radio typically requires 35mA. This design allows firmware control of the switching mode via microcontroller port. A high selects burst mode operation and a low selects fixed frequency operation. Fixed frequency is selected by default. Burst mode may be selected by defining port bit as an output bit high.

2.1.4 Optional IrDA Interface block

The RF Sniffer includes option for an IrDA interface. Current product does not have this option installed.

2.1.5 RF modem block

The radio modem consists of the following functional entities:

Digital section:

- includes Processor, EEPROM, LDO voltage regulators

RF section:

- includes RF transceiver, RF Power amplifier, Antenna Tx/Rx Switch

3. Diagnostic Software

The NivisLink application was developed in order to exercise the features of the Nivis Radio modem. The NivisLink application is a software application composed of a firmware hex file which is to be loaded onto the Sniffer and a GUI that controls various features of the modem.

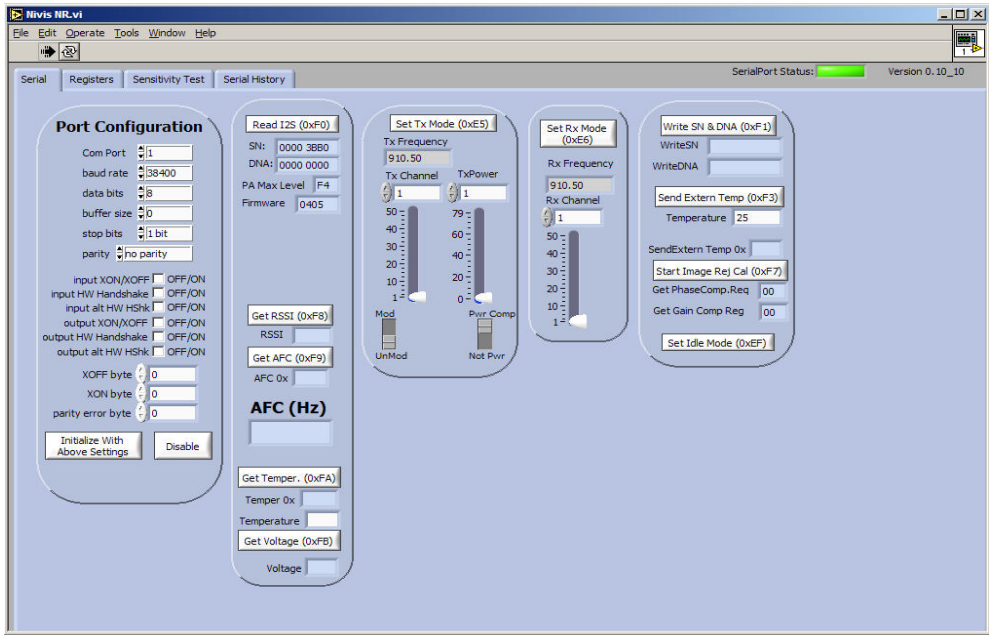
3.1. Getting started

3.1.1 Prerequisites

Install the Silicon Laboratories USB bridge drivers for CP2102 on the PC. This can be done from internet, go on the Silicon Laboratories web site *(www.silabs.com – search product CP2102 and download drivers)* or from the CD supplied together with the product.

Install the NivisLink GUI and connect the Sniffer to a USB port. When the Sniffer enumerates, Windows will assign the next available COM port number to the Sniffer. This can be verified by opening the Windows Device Manager and making a note of the new COM port number. The assigned COM port number can change each time the Sniffer is connected to the PC. This is a Windows function and the user has no control over COM port assignment.

Program the Sniffer with the NivisLink hex file provided *(Nivis_Link_4_0_6.a43)*. The figure below depicts the “Serial” tab of the NivisLink GUI. Select the appropriate COM port under ‘Port Configuration’ and click *“Initialize With Above Settings”*.



3.2 Read Calibration EEPROM

Note: The following procedure assumes that the RF Sniffer used has already undergone the calibration procedure. For tune-up and calibration procedure consult the "Tune-up Procedure" document.

The SN, DNA, PA Max level, temperature sensor calibration value and other calibration data necessary for the operation of the RF Sniffer is stored in the calibration EEPROM.

By pressing the “READ I2S” button the content of the calibration EEPROM is displayed in the tabs provided for various parameters.

The following parameters will be displayed

- Serial Number – unique identifying ID of the Sniffer
- DNA – network identification number
- Power Amplifier max level – maximum value of the power amplifier gain
- Firmware version

3.3 Transmission

In order to set the RF Sniffer in transmit mode the “SET TX MODE” button must be employed. The transmit tab will allow the user to select the TX frequency channel on which the transmission should take place. 50 frequency channels can be employed starting with the 910.5 MHz channel and than incrementing by 330 kHz up to 927.5 MHz. The user can also select the output power of the RF Sniffer by employing the TX Power knob. The MOD and UNMOD knob permits the user to select if the transmitted signal is modulated or un-modulated (carrier).

3.4 Reception

In order to set the RF Sniffer to receive the “SET RX MODE” button must be pressed. The mode will enter reception on the frequency channel selected in the adjacent tab.

3.5 Modify Register Values

The NivisLink application also gives the user the flexibility to directly control the functional registers of the RF transceiver. This gives the user complete control over every aspect of the RF functionality of the RF Sniffer. These register should only be overwritten by users that are knowledgeable of the RF transceiver. For a list and explanation of each RF register consult the datasheet of the RF transceiver.

3.6 Additional Features

The NivisLink application also permits the user to view various other parameters of the RF Sniffer.

- GET RSSI tab – displays the value present in the Received Strength Indicator register of the RF transceiver
- GET AFC - displays the value present in Automatic Frequency Correction register of the RF transceiver
- GET TEMPERATURE tab – displays the temperature value indicated by the internal temperature sensor of the MSP430 processor
- GET VOLTAGE – displays the supply voltage of the processor as read by an internal analog line of the MSP430 processor

4. RF Exposure Limit Warning

To comply with FCC's RF exposure limits for general population / uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

5. Compliance Statement (Part 15.19)

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.

6. Information to the User (Part 15.105)

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 or more 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 ratio/TV technician for help.

7. Warning (Part 15.21)

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