

---

### Implementing ZigBee™ Solutions Based on RC2200

by P. M. Evjen

---

#### Introduction

Radiocrafts offers a family of miniature modules intended for radio networks based on the ZigBee standard. This application note discusses issues related to implementing a product based on these modules. A basic knowledge of the ZigBee standard is assumed in the following discussion.

#### What does the module contain?

The RC2200 series of ZigBee modules contains all the RF circuitry needed, and provides all microcontroller resources needed for running the ZigBee stack as well as the application:

- RF front-end based on the Chipcon CC2420
- Microcontroller with 128 kB Flash, the Atmel mega128L
- Royalty fee for using the Figure 8 Wireless Z-Stack
- Optionally an antenna or an MMCX coaxial connector for use with external antenna

The module is a complete hardware platform for making a compact low power ZigBee application. It is intended for use together with the ZigBee protocol and software tools from Chipcon / Figure 8 Wireless.

As the module contains 128 kB of Flash memory and a full function device (FFD) takes approximately 64 kB of code, there is sufficient memory left for almost any application.

The module contains 4 kB RAM. A FFD (coordinator and router) use 2 – 2.5 kB RAM for the Z-Stack, hence 1.5 – 2 kB is available to the application. A RFD use approximately 1.5 kB, leaving 2.5 kB to the application.

The royalty fee per device for using the Figure 8 Wireless Z-Stack is included in the module pricing, but a license must be purchased from Chipcon in order to get access to the code and profile builders.

#### What is IEEE 802.15.4 and what is the ZigBee stack?

The physical (PHY) and medium access layers (MAC) are specified in the IEEE 802.15.4 personal Area Network (PAN) standard. The ZigBee standard is based on this and provides a standard for the network layer (NWK) as well as device profiles. Somewhat simplified it can be said that IEEE 802.15.4 provide a point-to-point link specification while ZigBee specified how to communicate in a network with multi-hops which is self-configuring and self-healing.

The ZigBee/IEEE 802.15.4 protocol stack is implemented in this way:

- PHY layer: Hardware provided in the RC2200 module
- MAC layer: Partly hardware in the module, partly firmware provided by a Chipcon licence
- Network layer: Firmware provided by Figure 8 Wireless, licensed through Chipcon
- Profile / application layer: Made by the user by using the profile/application builder provided by Figure 8 Wireless

#### How large is the ZigBee stack?

The present release of the Z-Stack from Figure 8 Wireless / Chipcon including the light control profile is approximately 64 kB using the GCC compiler implementing a full function device coordinator (as per January 2005).

It is expected that by doing some code optimization, or by using a more code efficient compiler, a FFD with application can fit into a 64 kB memory. A reduced function device (RFD) is expected to require less than 32 kB. Radiocrafts is providing cost-optimized devices with reduced memory.

### What tools do I need?

We recommend the following tools for developing a ZigBee application:

- Radiocrafts RC2200DK Demonstration Kit.
- Chipcon CC2420ZDK ZigBee Development Kit (including the MAC and Z-Stack license). Cost is approximately USD 5000, available from Chipcon ([www.chipcon.com](http://www.chipcon.com)).
- Programmers Notepad (included in the WinAVR packet) (for free)
- WinAVR GCC C-compiler (for free)
- Atmel AVR Studio for device programming and debugging (for free)
- Atmel JTAGICE mk II for USB (included in the Chipcon kit)

The Radiocrafts RC2200DK includes two RC2200DB Demonstration Boards with easy access to all the digital and analogue I/Os, JTAG and ISP interfaces for programming. The boards also contain an RS232 driver and connectors for UART communication with the module. Serial cables and battery eliminators are included.

The Chipcon CC2420ZDK also includes some demonstration board using the same MCU as in the RC2200 module. Therefore an application can be developed using the Chipcon kit and then easily transferred to the RC2200 module.

Programmers Notepad bundled with the GCC C-compiler is recommended as editor for the software development. The Z-Stack software includes scripts for running the compiler seamlessly from the Programmers Notepad. The WinAVR is freely available on the web.

The code can be ported to other C-compilers, but as it is expected that the Z-Stack will be released in updated versions in 2005Q1 and possibly 2005Q2, it should be noted that porting the source code to other compilers will require extra effort on several occasions and will not be a one-time-job only. See also comments below regarding firmware status.

The Atmel AVR studio is used to download the compiled (hex file) into the mega128 through the JTAG port. It can also be used for code debugging. The JTAGICE is connected between the PC USB port and the RC2200DB JTAG connector (standard 10 pins connector) for programming / debugging. No extra cabling is needed.

### ZigBee standard and firmware status

The ZigBee stack was released in version 1.0 in mid of December 2004. Only minor firmware updates are expected for the MAC and the Z-stack to fully comply with this release. These will be made available from Chipcon / Figure 8 Wireless shortly. Until then we call our products "ZigBee-ready". However, the physical layer is defined by IEEE 802.15.4 so the module hardware is fixed already.

The Chipcon MAC is still in a beta-release. A release for use in shipping products based is expected by February 2005.

### Profiles

The first profile to be released is the Home Lighting profile. This profile contains device specifications for light and dimmer remote controls, light and dimmer load switches, and occupancy sensors. It is not clear if this will be a part of the initial release of the standard.

These profiles are expected to be some of the first to be specified:

- Industrial Automation
- Automatic Meter Reading (AMR)
- Serial port profile

### Limitations in network topologies

The ZigBee protocol is defined with three network topologies:

- Star
- Cluster tree
- Mesh

Note that as per today the IEEE 802.15.4 does *not* support Cluster tree. This means that some of the low power mechanisms in the protocol cannot be used.

### Limitations in network size, placement of the coordinator

When implementing a certain profile (Home lighting profile, for example) be aware that there are specified limitations in how many “children” one router can support and how “deep” the network can be (maximum number of hops).

Once these limitations are set (at the stage of code compilation) they can not be changed without a device firmware upgrade of all network nodes.

The implication of this is that when installing a network, care should be taken so that the coordinator is placed in the “middle” of the mesh network. This will ensure that a minimum number of hops are needed to get to the most remote nodes.

Do also note that mobile nodes are not supported in the present ZigBee standard. This is likely to become a feature in a future upgrade.

### Low power and battery operation

In a mesh network, do note that it is only a Reduced Functionality Device (RFD), i.e. the end device, which can operate on battery power utilizing all power down features in the protocol and in the MCU itself. The network must be a non-beacon type. The coordinator and all routers must be powered all the time in a mesh network!

A non-beacon star network could also utilize power down modes in the end device (RFD).

The RC2200 includes a 32 kHz low power real-time clock (RTC) and several digital inputs with interrupt capability. These features can be used to wake the controller from sleep mode to active mode based on events. Using an interrupt pin for the light remote control is an obvious example. The start-up time of the module is in the order of 1-2 ms.

### Issues on interoperability

In order to ensure interoperability between products from different manufacturers, several important points must be handled by the system architect, which is not specified in the ZigBee protocol itself. Some of these points are discussed below.

### IEEE addressing

It is required that every node in the ZigBee network has a unique ID. This must be a 64 bit IEEE address, same as used in Ethernet. A 24-bit Unique Organisation Identifier (UOI) address can be bought from the IEEE organization and will give a virtually unlimited number of devices by providing a 40 bits serial number. The cost is approximately USD 1600.

### PAN ID

Each network must have a unique PAN ID. The ZigBee standard does not specify how this ID is chosen or given to a network. This is the sole responsibility of the application. Products from different manufactures must have the same PAN ID in order to inter-operate.

### Radio channel selection

16 different radio channels are specified in the 2.45 GHz frequency band for ZigBee. For two devices to communicate they must use the same channel. The ZigBee standard does not specify how this channel is set or chosen in a network. This is the sole responsibility of the application. Products from different manufactures must have means to select the same channel in order to inter-operate.

Products made for 2.45 GHz will not be able to communicate with products made for 868/915 MHz even if both are using the ZigBee standard. 868 / 915 MHz are not global license-free frequencies and are not likely to be supported by many manufactures.

### Security

ZigBee specify encryption based on symmetric key with AES-128. It provides authentication and encryption at MAC, NWK and application levels.

The distribution of keys is the sole responsibility of the application. Products from different manufactures must have means to select the same keys in order to inter-operate if using encryption.

### Developing your own profiles

There are three levels of profiles:

- Public profile
- Published profile
- Private profile

In order to use a private profile, a unique profile ID must be issued by the ZigBee alliance which requires an Alliance membership.

### What about adding a power amplifier?

The RC2200 output power is approximately 0 dBm. Together with excellent sensitivity (-94 dBm) this makes up a link budget that is 12 dB better than the IEEE 802.15.4 requirement. Using the ZigBee mesh network multi-hops ensure communication between nodes that cannot communicate directly. Therefore an extra power amplifier in most cases would not be necessary.

The IEEE 802.15.4 spectral mask specification and spurious emission regulations (FCC) would limit the output power to approximately 10 dBm when using an external power amplifier.

### Product approvals

There are two distinct approval regimes:

1. National regulations that must be met
2. Conformance Certification according to the ZigBee standard

First, national regulations are different from country to country. Some countries require the final product to be tested and approved by certified laboratories, while others work with self-declaration scheme. This kind of approval has nothing to do with the ZigBee standard. These regulations would not only apply for the RF transmission, but also EMC and safety of the product in general. See Chipcon AN001 by the same author for more information on this.

The RC2200 is designed to meet all national regulations for world-wide use.

Second, approval according to the ZigBee standard is required in order to make products from different manufacturers compatible.

For a two-year period only two certifying organizations can do ZigBee approval:

- NTS (offices in the US)
- TÜV (offices all over the world)

Details on the approval process are yet to be released by the ZigBee Alliance.

### Document Revision History

Document Revision	Changes
1.0	First release

### Contact Information

Web site: [www.radiocrafts.com](http://www.radiocrafts.com)

Email: [radiocrafts@radiocrafts.com](mailto:radiocrafts@radiocrafts.com)

Address:

**Radiocrafts AS**

Gunnar Schjelderups vei 11

NO-0485 OSLO

NORWAY

Tel: +47 970 86 676

Fax: +47 22 71 29 15