



Control your world™

February 2013

## Understanding ZigBee RF4CE

## Foreword

Since its inception, the ZigBee Alliance has worked with a singular focus: create a much needed global wireless language capable of giving voices to the myriad of everyday devices that surround us as we go about our daily lives. This focus has been aimed at the little devices often overlooked in an IT-centric world, such as light switches, thermostats, electricity meters and remote controls, as well as more complex sensor devices found abundantly in the health care, commercial building and industrial automation sectors. By connecting these devices, a Machine-to-Machine (M2M) network or Internet of Things is created that offers exceptional efficiency, convenience, security and control and a whole new way for people to interact with their environment. As a result, ZigBee Alliance members have created a smart set of wireless standards that enable this new class of networks and offer extraordinary control, expandability, energy efficiency, security, ease-of-use and the ability to use ZigBee technology in any country around the world.

Today, organizations use ZigBee standards-based wireless sensor networks to deliver innovative solutions for a variety of areas including consumer electronic device control, energy management and efficiency, health care, telecom services, consumer electronic devices, home and commercial building automation, as well as industrial plant management. By choosing ZigBee, they also benefit from the Alliance's competitive and stable supply chain. With a comprehensive set of attributes, the non-profit, open membership and volunteer-driven Alliance has become a thriving ecosystem with several hundred members. As an ecosystem, the Alliance offers everything prospective product and service companies need to develop the most dynamic ZigBee products and services.

## Executive Summary

Infrared (IR) remote controls have been around since the late 1970s and have simplified the control of many devices. While widely deployed, IR remotes have a number of limitations and can prove difficult to use with large-screen, high-definition televisions because of high-intensity light emitted from the screen. Other issues with these remotes include field-of-vision limits, line-of-sight restrictions and one-way communications. With the growth of today's increasingly sophisticated consumer electronics and new trends in electronics storage, IR remotes are losing their effectiveness and limiting innovation.

Replacing decades-old IR technology with ZigBee RF4CE radio frequency technology will improve the consumer experience and enable robust products with innovative new features. Devices using the specification and its standards will free consumers from pointing a remote at an exact target, allowing them to more easily control entertainment equipment accurately and easily. Devices will confirm to the remote control that a command was executed, no longer making the consumer repeatedly hit buttons to execute a command. This two-way communication provides the consumer electronics industry with a new platform and standard designed to accommodate growth beyond traditional device control. Ultimately, these smart new capabilities will spur innovation and integration with other automation devices using ZigBee technology.

Consumer electronics based on ZigBee RF4CE will be part of a growing ZigBee presence in homes. ZigBee has already emerged as the preferred solution in several major markets: energy, home automation, lighting and health care. The ZigBee Smart Energy™, ZigBee Home Automation™ and ZigBee Health Care™ standards address each of those verticals and are focused on improving consumers' lives by enhancing comfort and convenience, helping them save time and money, improve energy efficiency and live independent longer.

## Table of Contents

High-level overview.....	5
Technical Summary .....	5
Introduction .....	5
Network Topology .....	5
Architecture .....	6
The ZigBee RF4CE NWK layer.....	6
2.4 GHz band frequencies .....	7
Channel agility.....	7
Node initialization .....	7
Power saving .....	7
NWK frames .....	8
Transmission options .....	8
Discovery.....	8
Pairing.....	9
Security .....	9
The ZigBee RF4CE application layer .....	10
Future work .....	11

## List of Figures

Figure 1 - Example ZigBee RF4CE network topology .....	6
Figure 2 - The ZigBee RF4CE specification architecture .....	6
Figure 3 - General schematic view of a NWK frame .....	8

## HIGH-LEVEL OVERVIEW

- Based on the 2.4GHz PHY/MAC IEEE 802.15.4 standard.
- The networking layer is thin, flexible and future-proof.
- Co-existence with other 2.4 GHz technologies is built-in through techniques as defined in the IEEE 802.15.4 standard and ZigBee RF4CE's advanced channel agility mechanism.
- A simple and intuitive pairing mechanism defined for establishing communication links.
- Support for multiple communication types.
- Power-management mechanism included in network layer for power-efficient implementations.
- The specification ensures that ZigBee RF4CE implementations will co-exist.
- The ZigBee RF4CE specification allows for both Alliance-developed standards and manufacturer specific profiles or transactions.
- Publicly available Alliance-developed standards include ZigBee Remote Control™ and ZigBee Input Devices™.
- Support for different applications through application layer profiles ensuring device interoperability.

## TECHNICAL SUMMARY

### Introduction

The ZigBee RF4CE specification defines a simple, robust and low-cost, low-latency communication network that allows wireless connectivity in consumer electronics applications. ZigBee RF4CE is built on the IEEE 802.15.4 standard by providing a simple networking layer and includes support for two ZigBee Alliance-developed standards, ZigBee Remote Control and ZigBee Input Device, that can be used to create multi-vendor interoperable solutions for use within the home.

Some of the characteristics of a ZigBee RF4CE network are:

- Operation in the 2.4GHz frequency band according to IEEE 802.15.4.
- Channel agile solution operating over three channels.
- Power-management mechanism for all device classes.
- Discovery mechanism with full application confirmation.
- Pairing mechanism with full application confirmation.
- Multiple star topology with inter-PAN communication.
- Various transmission options including unicast, broadcast, acknowledged, unacknowledged, secured and un-secured.
- Security key generation mechanism.
- Utilizes the industry standard AES-128 security scheme.
- Support for two publicly available standards: ZigBee Remote Control and ZigBee Input Device
- Support for custom features with manufacturer specific profiles.

### Network topology

A ZigBee RF4CE personal area network (PAN) is composed of two types of devices: a target device (or node) and a controller device (or node). A target device has full PAN coordinator capabilities and can start a network on its own. A controller device can join networks started by target devices by pairing with the target. Multiple ZigBee RF4CE PANs form a ZigBee RF4CE network and devices in the network can communicate between ZigBee RF4CE PANs. In order to communicate with a target device, a controller device first switches to the channel and assumes the PAN identifier of the destination ZigBee RF4CE PAN.

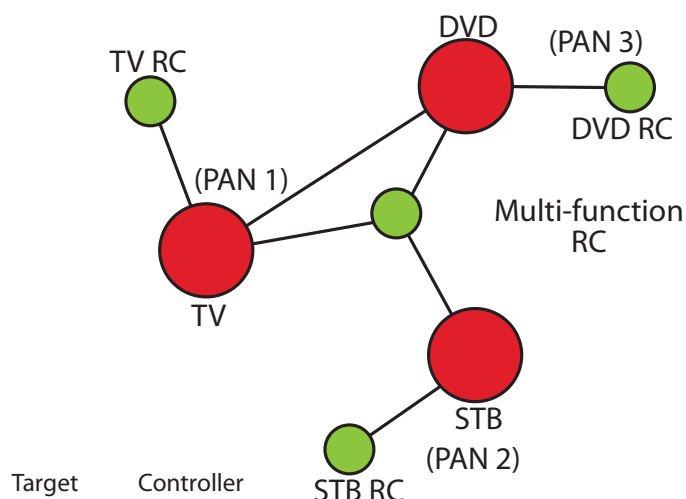


Figure 1 - Example ZigBee RF4CE network topology

It then uses the network address, allocated through the pairing procedure, to identify itself on the ZigBee RF4CE PAN and thus communicate with the desired target device.

Figure 1 illustrates an example ZigBee RF4CE topology which includes three target devices: a TV, a DVD and a Set Top Box (STB) and each target device creates its own ZigBee RF4CE PAN. The TV, DVD and STB also have dedicated remote control's which are paired to each appropriate target device. A multi-function remote control, capable of controlling all three target devices itself, is added to the network by successively pairing to the desired target devices.

As a consequence, this ZigBee RF4CE network consists of three separate ZigBee RF4CE PANs: one managed by the TV (PAN 1), containing the TV remote control and the multi-function remote control; a second managed by the STB (PAN2), containing the STB remote control and the multi-function remote control; and a third managed by the DVD (PAN3), containing the DVD remote control and the multi-function remote control.

## Architecture

The ZigBee RF4CE architecture is defined in terms of a number of blocks or layers in order to simplify the specification. Each layer is responsible for one part of the specification and offers services to the next higher layer and utilizes services from the next lower layer. The interfaces between the layers serve to define the logical links that are described in this specification. The layout of

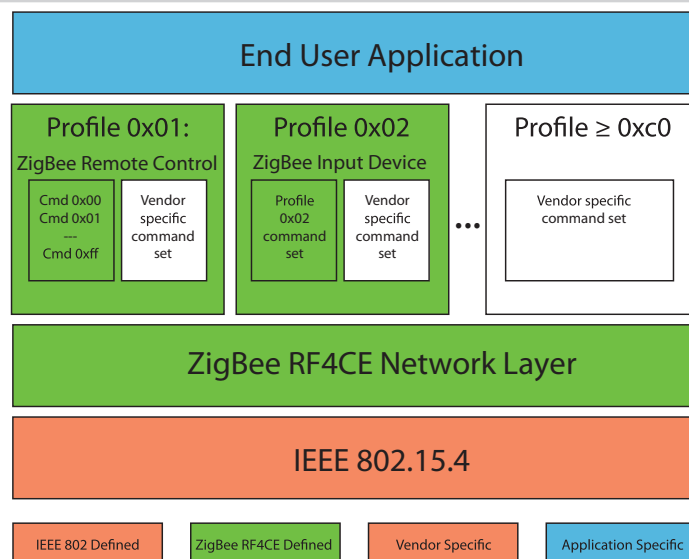


Figure 2 - The ZigBee RF4CE specification architecture

the layers is based on the open systems interconnection (OSI) seven-layer model.

Figure 2 illustrates the ZigBee RF4CE stack architecture. The ZigBee RF4CE specification is designed to be built onto the IEEE 802.15.4 standard MAC and PHY layers and provides networking functionality, while the ZigBee Remote Control and/or ZigBee Input Device can interface to the end-user application. Manufacturer specific extensions to standards can be defined by sending vendor-specific data frames within the standard. In addition, manufacturer specific profiles can also be defined.

## The ZigBee RF4CE Network layer

The ZigBee RF4CE Network (NWK) layer provides two services: the NWK layer data service, interfacing to the NWK layer data entity (NLDE) and the NWK layer management service, interfacing to the NWK layer management entity (NLME). These services are accessed through the NWK layer data entity service access point (SAP) (NLDE-SAP) and the NWK layer management entity SAP (NLME-SAP). The NWK layer data service enables the transmission and reception of NWK protocol data units (NPDU)s across the MAC data service. The NWK layer management service permits service discovery, pairing, unpairing, receiver control, device initialization and network information base (NIB) attribute manipulation.

## 2.4 GHz band frequencies

A ZigBee RF4CE device operates in the 2.4GHz frequency band, as specified by IEEE 802.15.4. However, to provide robust, low-latency service against other common sources of interference in this band, only a small subset of channels is used – channels 15, 20 and 25. A target device can choose to start its network on the best available channel at startup time and so a ZigBee RF4CE network may operate over one or more of the available three channels.

### Channel agility

All ZigBee RF4CE devices support channel agility across all three permitted channels. As described above, a target device selects its own initial channel based on the channel conditions during startup. During the course of the life of the target device, however, the channel conditions may vary and the target device can elect to switch to another channel to maintain a high quality of service.

Each device paired to the target records the channel where communication is expected. However, in the event that the target switches to another channel, the device can attempt transmission on the other channels until communication with the target is reacquired. The device can then record the new channel accordingly for the next time communication is attempted.

### Node initialization




A ZigBee RF4CE device initializes itself according to whether it is a target or a controller. Controller devices simply configure the stack according to this model and start operating normally. Target devices configure the stack and then attempt to start a network.

To do this, the target device first performs an energy detection scan that allows it to obtain information on the usage of each available channel, thereby allowing it to select a suitable channel on which to operate. The target device then performs an active scan allowing it to determine the identifiers of any other IEEE 802.15.4 PANs (ZigBee RF4CE or other ZigBee networks) operating on the selected channel, thus allowing a unique PAN identifier to be selected for its network. The target device then begins

operating normally.

### Power saving

Power saving is an important consideration for a ZigBee RF4CE device. The specification defines a power-save mechanism that allows both controller devices as well as target devices to manage their power consumption by entering a power-saving mode. The power saving mechanism is under the control of each ZigBee RF4CE standard. A device can manage its receiver in a number of ways:

-  The receiver can be enabled until further notice (e.g. when a TV comes out of standby).
-  The receiver can be enabled for a finite period (e.g. when a TV enters standby mode and wants to engage the power saving-mode).
-  The receiver can be disabled until further notice (e.g. when a remote control enters a dormant state due to none of its buttons being pressed). When the power-saving mode is engaged, the receiver is enabled for an application-defined duration (known as the active period) and then disabled. This mechanism is then repeated at an application-defined interval (known as the duty cycle). Other devices can still communicate with a device in power-saving mode by targeting the transmission during the active period. The result is a device that periodically enables its receiver for only a short time, allowing it to conserve power while remaining active on the network.



Octets: 1	4	0/1	0/2	Variable	0/4
Frame control	Frame counter	Profile identifier	Vendor identifier	Frame payload	Message integrity code
Header			Payload		Footer

## NWK frames

The ZigBee RF4CE NWK layer defines three frame types: standard data, network command and vendor-specific data. Standard data frames transport application data from either standards or manufacturer specific profiles. Network command frames transport frames that allow the network layer to accomplish certain tasks such as discovery or pairing. Vendor-specific data frames transport vendor-specific application data. The general NWK frame format is illustrated in Figure 3.

The fields of the general NWK frame are:

- Frame control: control information for the frame
- Frame counter: incrementing counter to detect duplicates and prevent replay attacks (security)
- Profile identifier: the application frame format being transported
- Vendor identifier: to allow vendor extensions
- Frame payload: contains the application frame
- Message integrity code: to provide authentication (security)

## Transmission options

The ZigBee RF4CE specification defines a number of transmission options that can be used by an application and combined as appropriate. Each transmission can be sent secured or un-secured.

- Acknowledged: Originator data is confirmed by the recipient

- Unacknowledged: Originator data is not confirmed by the recipient
- Unicast: Originator data is sent to a specific recipient
- Broadcast: Originator data is sent to all recipients
- Multiple channel: Originator attempts transmission using frequency re-acquisition mechanism
- Single channel: Originator attempts transmission on the expected channel

## Discovery

A ZigBee RF4CE device can perform discovery in an attempt to find other suitable devices for pairing. Discovery can be attempted repeatedly on all three channels for a fixed duration or until a sufficient number of responses have been received. Service discovery is only available to devices that are not currently in power-saving mode. During discovery, a number of pieces of information are exchanged between both devices. This information is passed to the application, which can then make a decision whether it should respond. The information exchanged is as follows:

- Device capabilities: The type of the device (i.e. target or controller), whether the device is mains or battery powered and level of security.
- Vendor information: The ZigBee RF4CE allocated vendor identifier and a freeform vendor string specifying vendor specific identification (e.g. a serial number).
- Application information: A short user-defined string which describes the application functionality of the device (e.g. "lounge TV"), a device type list specifying which types of device are supported (e.g. a combo device may support both "TV" and "STB" functionality)



and a profile identifier list specifying standard or manufacturer specific profiles supported by the device.

- Requested device type: The type of device being requested through the discovery (e.g. a multifunction remote control may be searching for "TV" functionality).

## Pairing

Once a device has determined, through discovery, that there is another device within communication range offering compatible services, it can set up a pairing link in order to begin communication. Nodes within a ZigBee RF4CE network may only communicate directly with other devices on the network if a pairing link exists between the originator and the target devices.

A pairing link can be established on request from the application by exchanging a similar set of information as was exchanged during discovery. The application on the target device can choose whether to accept the pair (e.g. only if it has capacity to store the pairing link) and confirms the pairing request back to the originator device.

If the pairing request was successful, both devices store a pairing link in their respective pairing tables. This allows an originator to communicate with a target and a target to communicate back to an originator. Each entry in the pairing table contains all the information necessary for the network layer to transmit a frame to the target device. This removes the burden of addressing, etc. from the application layer which can simply supply an index into the pairing table in order to communicate with another device.

Each entry in the pairing table contains the following information:

- Pairing reference
- Source network address
- Destination logical channel
- Destination IEEE address
- Destination PAN identifier
- Destination network address
- Recipient device capabilities
- Recipient frame counter
- Security link key

## Security

The ZigBee RF4CE specification provides a cryptographic mechanism to protect the transmissions. This mechanism provides the following security services:

- Data confidentiality: To ensure that the data contained in a ZigBee RF4CE transmission can only be disclosed to the intended recipient.
- Data authenticity: To ensure that the intended recipient of a ZigBee RF4CE transmission knows that the data was sent from a trusted source and not modified during transmission.
- Replay protection: To ensure that a secure transmission cannot simply be repeated by an attacking device if overheard.

128-bit cryptographic keys are generated by each end of a pairing link and stored in the pairing table for future use.

## The ZigBee RF4CE application layer

The application layer of a ZigBee RF4CE device is composed of a profile component and an application-specific component. The profile component can be thought of as a common language that devices implementing the profile exchange to accomplish certain tasks, e.g. switching the channel on a TV, and allows for interoperability between devices. The application component is provided by the end-manufacturer in order to add specific functionality to the commands request through the profile.

One important aspect of the ZigBee Alliance-developed application standards is their unified pairing mechanism. This enables controller and target devices to discover and pair in an agnostic manner as long as they share a common profile.

The ZigBee RF4CE specification defines two Alliance-developed standards, ZigBee Remote Control and ZigBee Input Device, but also permits vendors to either extend these standards or to define completely proprietary ones called manufacturer specific profiles.

### ZigBee Remote Control

The ZigBee Remote Control standard defines commands and procedures to enable consumer electronics devices (e.g. a TV, STB, DVD or CD player) to be controlled by basic control devices.

The standard's commands are based on the HDMI CEC specification and covers commands such as volume up/down, channel up/down, power on/off, mute, select, guide, ok, 0-9, etc. Consumer electronics devices can also query the control device for the list of commands that it supports. This enables a STB or a TV to customize its menu system based on the capabilities of the control device.

A command sent from the control device to the target device also contains a code indicating the specific button "action taken by the user"

- User control pressed: This code is used to specify the first command sent due to a button press on the control device.

- User control repeated: This code is used to specify that the command is sent due to a button being continually held down on the control device
- User control released: This code is used to specify that the button on the control device is released for the specific command

As an example, this allows users to hold down the volume up button to continually increase the volume to a desired level. ZigBee Remote Control specifies the timing requirements for each of the user controlled pressed/repeated/released commands.

ZigBee Remote Control provides an easy migration path from IR-based remotes to advanced control devices with little, if any, change to the user interface or remote control buttons.

### ZigBee Input Device

The ZigBee Input Device standard defines commands and procedures to enable consumer electronics devices (e.g. a TV, STB, DVD or CD player) to be controlled by the new generation of advanced input control devices. This standard is modeled after the ubiquitous USB Human Interface Device (HID) specification and enables input devices like keyboards, motion-controlled pointing devices, touchpad etc.

A controller device supporting ZigBee Input Device is referred to as an input class device, and a target device supporting the standard is referred to as a adapter class device.

Although the ZigBee Input Device is modeled after the USB HID specification, it is important to notice that the interface between an adapter and the consumer electronics equipment does not need be a physical USB interface. The standard is merely using the concepts of USB HID specification for device configuration and command reporting over the ZigBee RF4CE link.

A mandatory configuration phase is entered after a pairing between two devices is established. In this phase, the input class device will describe its capabilities and command reporting descriptors to the adapter class

device. The standard defines a collection of command reporting descriptors for commonly used input devices like a keyboard and mouse. Additionally, it provides a mechanism for the device to define its custom command reporting descriptors.

ZigBee Input Device provides three communication methods (a.k.a. pipes) between the input device and the adapter:

- **Control pipe:** This is a mandatory bi-directional pipe enabling an input device to send commands or for an adapter to poll the class device for data. Commands are sent using the unicast/acknowledged/multichannel or broadcast transmission option. Keyboard commands are typically sent using this pipe.
- **Input interrupt pipe:** This is a mandatory pipe enabling an input device to send low-latency or asynchronous commands to an adapter. Commands are sent using a combination of the unicast/unacknowledged/single channel and unicast/acknowledged/multichannel transmit options. The unicast/unacknowledged/single channel transmit option ensures low-latency delivery of commands, while the unicast/acknowledged/multichannel transmit option reacquires the ZigBee RF4CE channel in the case it is compromised and the adapter has moved to a different channel. Mouse data are typically sent using this pipe.
- **Output interrupt pipe:** This is an optional pipe enabling the adaptor to transfer low-latency or asynchronous commands to the input device.

ZigBee RF4CE enables bi-directional communication and the ZigBee Input Device standard defines a consistent way to enable adapters to send commands to input devices. This can be used to locate a lost input device such as a remote control, or send social media status, stock market alerts or real-time sports scores to be displayed on the input device.

Next-generation consumer electronics devices provide user interfaces and services that require input devices beyond a simple push-button remote controller. Among other things, consumers want to update their social media status, surf the web, search the video-on-demand catalog

or TV guide for their favorite actress/actor, or play a casual game. ZigBee Input Device enables development of input control devices that can accomplish these tasks in an easy and standardized manner.

## Future work

ZigBee Alliance members are always working to improve and extend ZigBee standards. With ZigBee RF4CE, there are several new ideas on the way to add functionality in the area of remote controls, as well as adding better bridging capabilities between ZigBee RF4CE and ZigBee Home Automation™ networks. By allowing ZigBee RF4CE-based devices to control other devices in the home environment in a standardized way, the Alliance gives consumers another way to create their own Smart Home, and also to control their world.