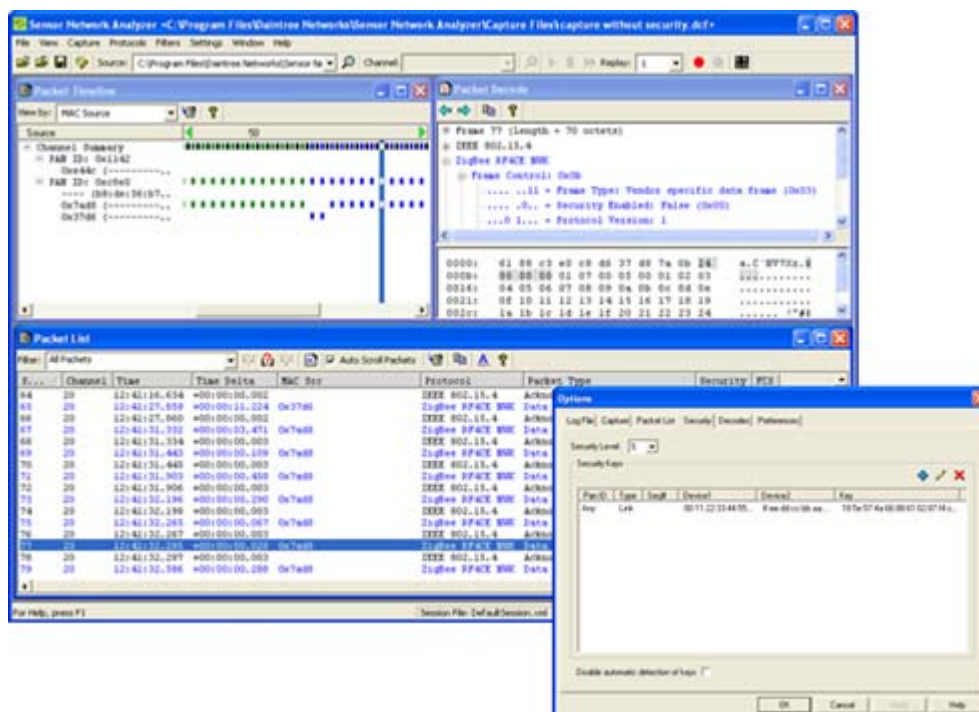


# Using the Daintree Networks Sensor Network Analyzer to decode ZigBee RF4CE

## Application Note AN035



Copyright © 2003-2009, Daintree Networks Inc  
All rights reserved

## Trademarks and acknowledgements

- ZigBee® is a registered trademark of the ZigBee Alliance.
- 802.15.4™ is a trademark of the Institute of Electrical and Electronics Engineers (IEEE).

These trademarks are registered by their respective owners in certain countries only. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

## Disclaimer

This application note and any examples it contains are provided as-is and are subject to change without notice. Except to the extent prohibited by law, Daintree Networks makes no express or implied warranty of any kind with regard to this application note, and specifically disclaims the implied warranties and conditions of merchantability and fitness for a particular purpose. Daintree Networks shall not be liable for any errors or incidental or consequential damage in connection with the furnishing, performance or use of this application note and the examples included.

The software described in this application note is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use, without the written permission of Daintree Networks.

Sensor Network Analyzer Release 3.0.0.5 (2009-04-22)

## About ZigBee RF4CE

The ZigBee RF4CE standard defines a remote control (RC) network that defines a simple, robust and low-cost communication network allowing wireless connectivity in applications for consumer electronic (CE) devices. It enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application profiles that can be used to create a multi-vendor interoperable solution for use within the home.

Characteristics of ZigBee RF4CE include the following:

- operates in the 2.4GHz frequency band according to IEEE 802.15.4
- supports frequency agility over 3 channels (15, 20, 25)
- incorporates power saving mechanisms for all device classes
- includes discovery mechanism with full application confirmation
- supports pairing mechanism with full application confirmation
- uses multiple star topology with inter-personal area network (PAN) communication
- includes various transmission options including broadcast
- provides security key generation mechanism
- uses the industry standard AES-128 security scheme
- specifies a simple RC control profile for CE products
- allows standard or vendor-specific profiles to be added

## About Daintree's Sensor Network Analyzer (SNA)

The SNA combines a powerful protocol decoder (that allows you to drill down to the packet, field, and even byte level) with advanced functionality including multi-node capture and security decryption.

To significantly accelerate troubleshooting tasks, the SNA also provides ease-of-use features such as filters, comprehensive playback controls and breakpoints, and user-definable protocol stacks and application profiles definitions using XML.

Supported by an extensive range of chipset evaluation boards, and with a flexible decode engine that provides support for most popular standards-based and proprietary wireless embedded protocols, the industry-standard SNA offers a complete toolkit for your wireless embedded development, testing and troubleshooting needs.

## About the 2400E Sensor Network Adapter

Daintree's 2400E Sensor Network Adapter is a capture accessory that acts as an observation and control point enabling the use of the SNA in live wireless embedded networks.

This adapter provides both Ethernet and USB interfaces (2.4GHz). It is portable and light-weight, making it suitable for use in remote locations.

Visit [www.daintree.net](http://www.daintree.net) to find out more about Daintree products.



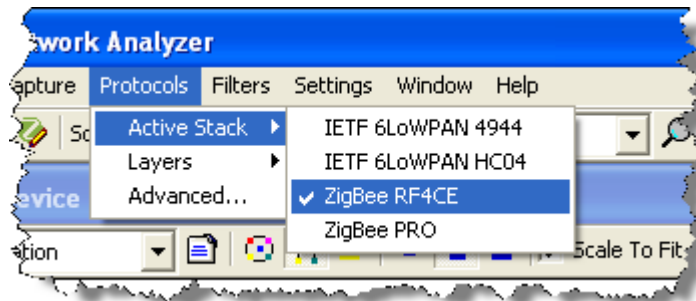
## Getting started with the SNA

This application note assumes that version 3.0.0.5 or newer of the SNA software is installed on your PC, and that you have capture hardware installed.

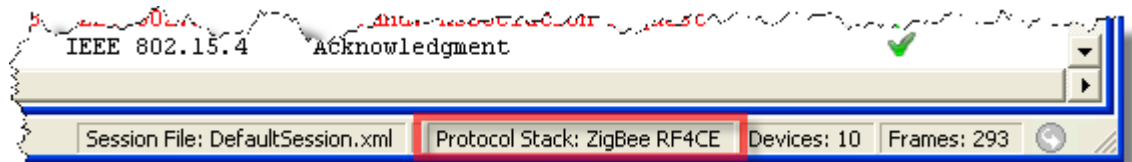
- If you are new to the SNA, please refer to the [Quick Start Guide](#), which provides full instructions for installing and starting the SNA software.
- If you need help installing capture hardware, please refer to the [SNA application notes](#), which provide instructions for setting up and using all supported capture devices.
- If you are using an older version of the SNA software (that does not provide support for ZigBee RF4CE), please [contact Daintree Networks](#) to find out how to update your software to the latest version.

## Selecting the ZigBee RF4CE network protocol

- From the **Protocols** menu, select **Active Stack**, and then select **ZigBee RF4CE**.



The currently selected protocol is shown in the Status Bar at the bottom of the main SNA window.



The SNA will immediately begin to use the stack you have selected for the protocol decodes shown in its Packet List, Packet Timeline and Packet Decode windows, and for defining Filters.

## Start capturing data

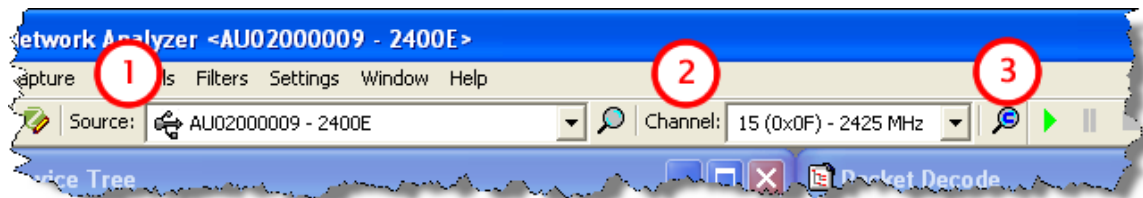
ZigBee RF4CE supports frequency agility over three channels (15, 20 and 25). What this means is that when the network first starts, target devices select the best available channel to use. If the quality of that channel degrades over time, the device can automatically switch to one of the other available channels. The controller devices know that if a target device can no longer be found on its original channel, they need to scan the other two channels to see where it has gone.

The SNA gives you the option of capturing either a single channel, or of capturing all three ZigBee RF4CE channels.

**Note** that multi-channel capture is supported only for the SNA Professional edition.

## Capturing a single channel

Capturing from a single channel is as easy as 1-2-3:

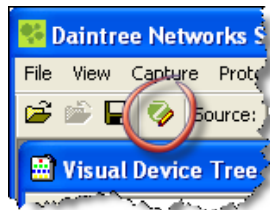


1. Select the **Source** (capture device).
2. Select the **Channel** on which to capture.
3. Click ► to start the capture.

## Capturing multiple channels (SNA Professional edition)

Capturing from multiple channels allows you to record details about all three ZigBee RF4CE channels in a single operation:

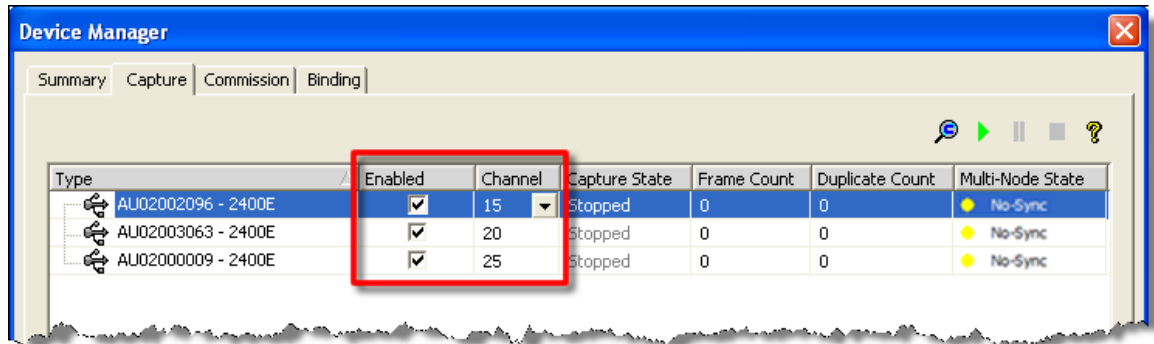
1. From the SNA's **Settings** menu, select **Device Manager**, or else click the Device Manager icon from the main SNA toolbar.




2. On the Device Manager **Summary** tab, for each device you want to include in the capture, right-click the device, and then select **Connect**. When the device is successfully connected, the Connected indicator changes to green.

Type	Connected
AU02000009 - 2400E	●

- On the **Capture** tab, ensure that each device you want to include in the capture is selected as **Enabled**. Then select the **Channels** on which you want each device to capture.



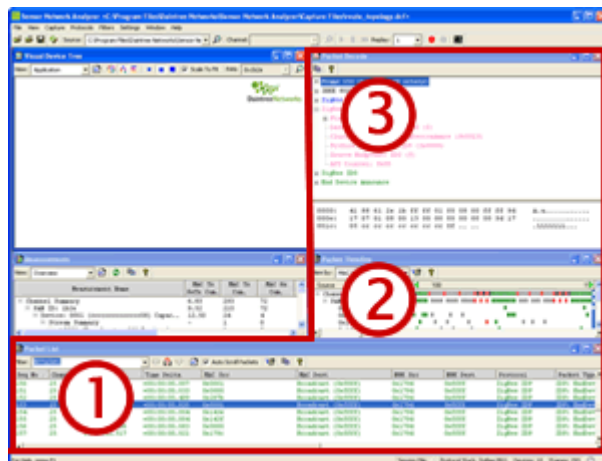
- Click  to start the capture. Measurements will automatically start when the capture starts. Packets from each of the nodes will be correlated together and presented to the SNA application as a single stream of packets for decode and analysis.

Refer to the [Multi-node and multi-channel capture with the SNA](#) application note for step-by-step instructions for performing multi-channel captures.

## Decoding captured data

The SNA shows decode details in its Packet List, Packet Timeline and Packet Decode windows. These windows are correlated, in that if you select a packet in either the Packet List or Packet Timeline window, the same packet will be displayed in all three windows:

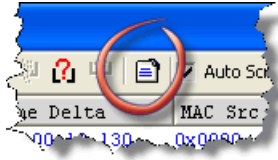
- The **Packet List** window lists all received packets sequentially with summary information.
- The **Packet Timeline** window shows packet events over time on a per-device basis.
- The **Packet Decode** window displays the decoded structure of an individual packet (selected through either the Packet List or Packet Timeline window). At the bottom of this window is a Packet Data pane, which shows bytes in hexadecimal and ASCII.



## Customizing decode details

You can customize the decode details shown to display the information that is most relevant to you in a way that makes it easy to read and understand.

1. From the Packet List toolbar, click the **Options** icon.



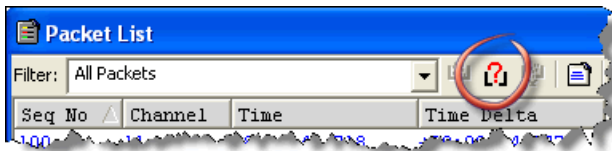
2. Use the Packet List Options dialog box to customize the display in the following ways:
  - o Select which fields to show/hide as columns.
  - o Select the order in which to display columns.
  - o Rename columns.
  - o Change the color of individual fields and entire layers (in both the Packet List and Packet Decode windows).


See the SNA's online help for detailed instructions about any of the above.

You can also quickly sort columns in the Packet List window by clicking the column headings. And if you want to remove a column from the Packet List, simply right-click the column heading, and then select **Remove Column**.

## Filtering packets

Filters allow you to quickly locate packets of interest from among thousands (or tens of thousands). The SNA provides pre-defined filters, or you can quickly create your own.



Select a filter from the **Filter** drop-down list, or click  to create a new filter. You can also right-click a field in the Packet Decode window, and then select **Add to Filter**.

Refer to the [Using filters with the SNA](#) application note for step-by-step instructions for creating and applying filters.

## Using ZigBee RF4CE security


Like any other wireless network, an RC network could be vulnerable to both passive eavesdropping and unauthorized tampering of the messages being transferred between nodes. To solve this, ZigBee RF4CE uses 128-bit cryptographic keys, which provide the following:

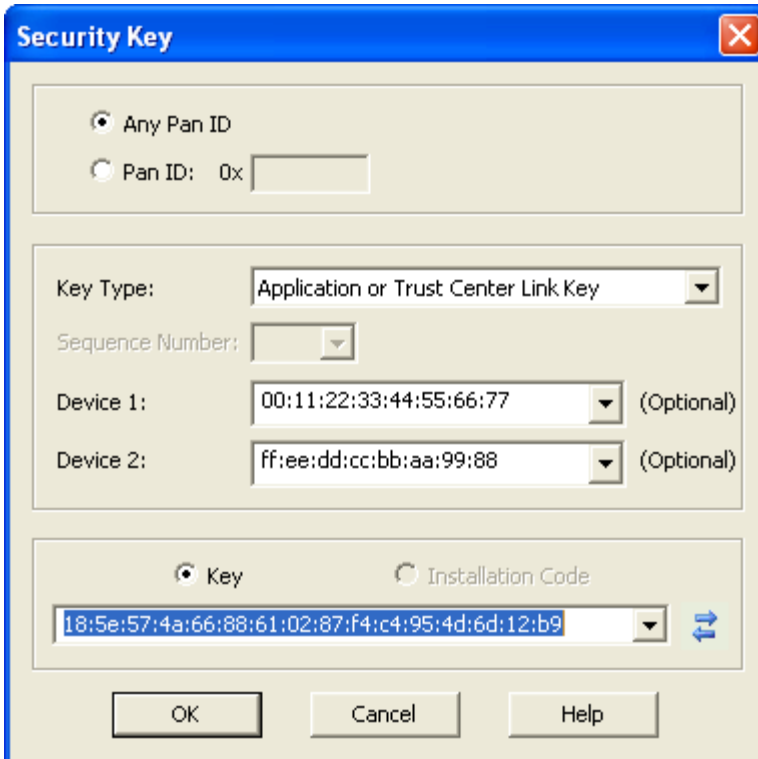
- Data confidentiality, to ensure that the data contained in an RF4CE transmission can be disclosed only to the intended recipient.
- Data authenticity, to ensure that the intended recipient of an RF4CE transmission knows that the data was sent from a trusted source and not modified during transmission.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

A security key is generated for a pairing link (between controller and target device), and stored in the pairing table for future use.


The SNA needs to have access to these keys before it can correctly decrypt secure packets. You can either manually enter the security key details, or if you have the SNA Professional edition, the SNA can automatically discover the keys for you.

### Manually adding security keys

1. From the SNA **Settings** menu, select **Options**.
2. On the Options dialog box, click the **Security** tab to access the SNA's security options.
3. Click  to add a new security key, and then enter the security key details:



- Select a **Key Type** of **Application** or **Trust Center Link Key**.
- Specify the MAC addresses of the paired devices for the key.
- Enter the 16-byte security key.

**Note** that the SNA requires keys to be entered MSB first. You can click  to reverse the order of keys entered with LSB first if required.

4. Click **OK** to save the security key details.

## Auto-discovery of security keys (SNA Professional edition)

In ZigBee RF4CE, security keys are established between a pair of devices through an exchange of messages. This starts with a Key Exchange Transfer Count, which specifies the number of messages that will be exchanged in order for the security key to be transferred. The specified number of key seed messages are then exchanged, and the security key is recovered and verified between the devices. Once the keys are verified, messages can be sent in encrypted format.

The SNA Professional edition can harvest ZigBee RF4CE security keys if it is able to observe the entire communication between two devices during which the security key is established.

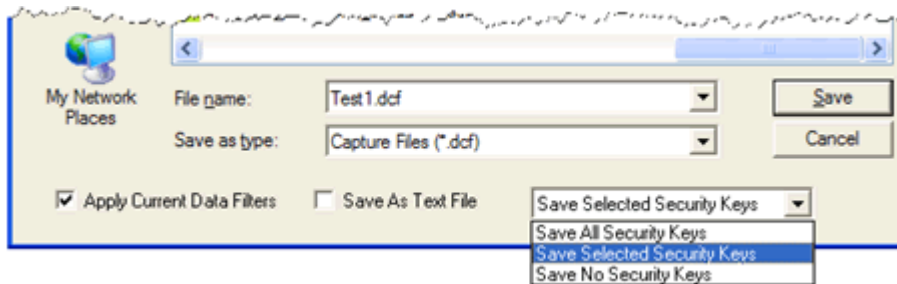
After harvesting the security keys, the SNA populates its security key table, which it then uses to decrypt secure messages.

Note that with the Professional edition, keys can also be added manually (as described previously).

## Saving security keys

If you are using security, you can select whether or not to include security keys when saving capture files. Saving keys enables the SNA to decrypt packets when the file is replayed without the need to re-discover or manually re-enter security keys, and is particularly useful in environments where capture files are shared.

1. From the SNA **File** menu, select **Save Capture File**.
2. Enter the name and file type for the capture file; then from the drop-down list at the bottom of the Save Capture File dialog box, select to save **All**, **Selected**, or **No Security Keys**.



3. If you choose to save selected keys, a Save Selected Security Keys dialog box opens through which you can select the keys you want to include with your capture file. Click **OK** to save the capture file together with the specified security keys.