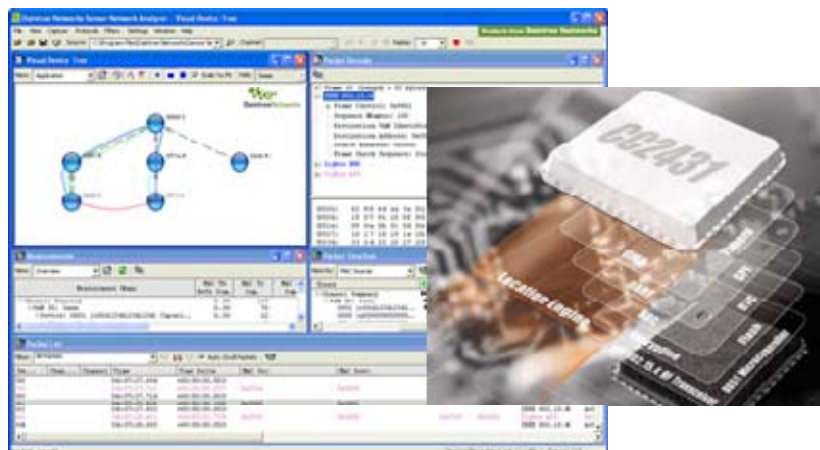


# Upgrading firmware over-the-air using TI's SoC and the Daintree Networks Sensor Network Analyzer

## Application Note AN017



Copyright © 2003-2008, 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).
- Pentium® is a registered trademark of Intel Corporation.
- Microsoft®, Windows®, and other Microsoft products mentioned herein are trademarks or registered trademarks of Microsoft Corporation.

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 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 guide, 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 guide and the examples included.

The software described in this guide 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 2.3 (2008-06-27)

## About OTA upgrades

There are many times at which you may need to upgrade the code (firmware) stored on a device, for example, to fix bugs during development and field trials, or to add new functionality during commissioning or in an already deployed network.

One way to do this is to physically connect each device via cable to a computer or PDA, and then download the code to each device in turn. This laborious and time-consuming process is prone to errors (such as some nodes being forgotten or not correctly updated), and can become completely unworkable in larger networks.

OTA upgrades, which as the name implies performs the upgrade over-the-air using ZigBee/802.15.4 connectivity, provides a faster, easier and more accurate way to upgrade firmware.

This application note provides instructions of how to use Daintree's Sensor Network Analyzer application together with the Texas Instruments CC2430 or CC2431 System on a Chip (SoC) to upgrade devices over-the-air.

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

The SNA combines a powerful protocol analyzer with network visualization, measurements and diagnostics for IEEE 802.15.4™ and ZigBee® applications. It provides automatic display of network formation, topology changes, and router and coordinator state changes allowing rapid detection of incorrect network behavior and identification of device or network failures.

It also provides a powerful commissioning tool that helps to hide the complexity of the underlying technology, and provides straight-forward configuration, testing and troubleshooting capabilities. Its graphical representations makes it fast and easy for installers to monitor network formation and measure key parameters such as link quality and bindings.

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

## About TI's CC2430/CC2431 SoC

The CC2430 and CC2431 from Texas Instruments provide a true System-on-Chip (SoC) solution specifically tailored for IEEE 802.15.4 and ZigBee applications.

The procedures described in this application note require the CC2430 or CC2431 SoC with the following:

- Rev D or later (that is, those with a date group of 0642 or later)
- OAD (Over the Air Download) Flash Board 1.0

Visit the Texas Instruments web site at [www.ti.com/zigbee](http://www.ti.com/zigbee) to find out more about the CC2540/CC2431 SoC and other TI ZigBee solutions.

## How do OTA upgrades work?

It takes two steps to upgrade the firmware on a device:

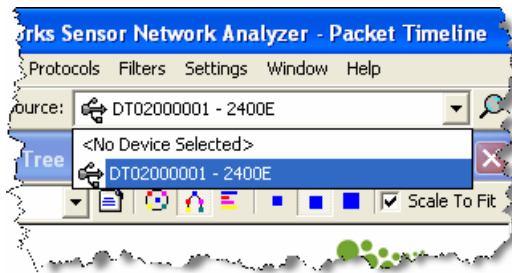
1. Download the firmware (over-the-air) to the device's external or flash memory. On completion, confirm that the firmware was successfully downloaded to memory.
2. Enable the device's firmware (copy it from memory), and then reboot the device so that it starts up using its updated firmware.

The SNA provides the ability to upgrade multiple devices in a single operation to help speed up the process.

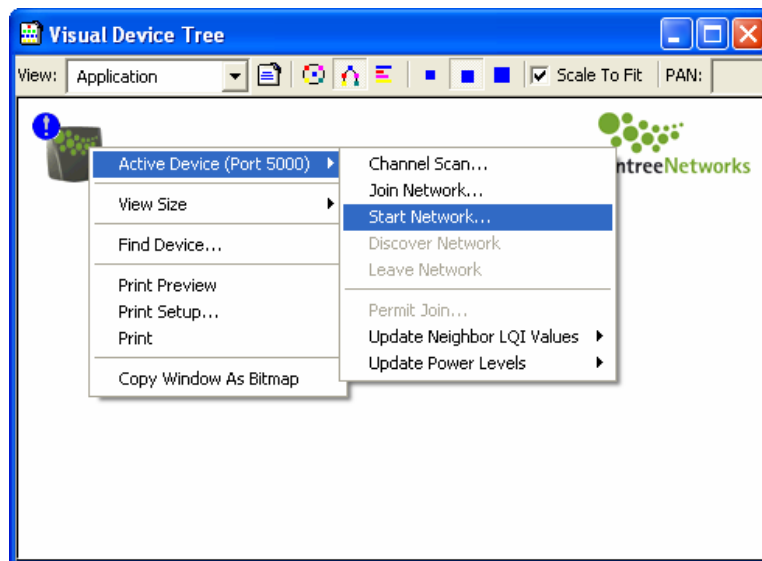
## Downloading firmware to device memory

Note that not all devices contain the external or flash memory required to perform an OTA upgrade. Therefore, the first step is to determine which devices are supported.

1. Start the SNA application and connect the 2400E Sensor Network Adapter to your computer via USB.
2. Select the 2400E from the **Source** list.



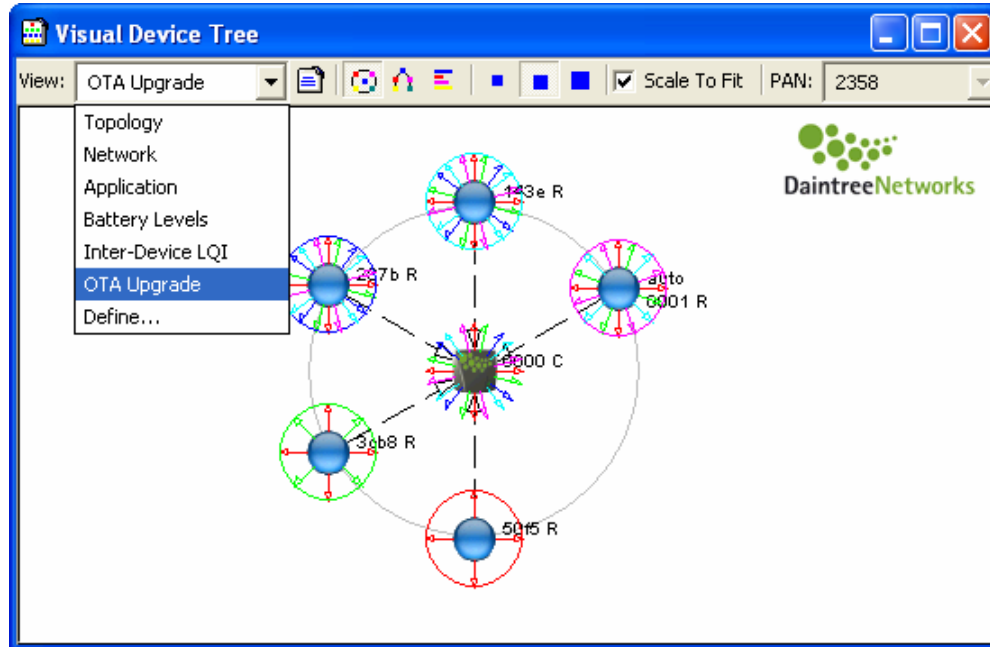
3. Right-click the 2400E on the Visual Device Tree (VDT) window, and then select **Active Device** > **Start Network**. Enter the settings required for your network (see the *SNA User Guide* if you require more instructions).



## Updating firmware over-the-air using TI's SoC and Daintree's SNA



4. If required, turn on the devices that require upgrading.
5. On the VDT window, select a View type of **OTA Upgrade**.

Note that all of the following instructions provided for the VDT window can also be performed using the Visual Device Layout (VDL) window.



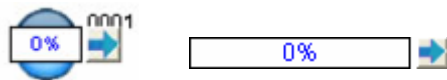
6. On the VDT window, right-click the active device, and then select **OTA Upgrade > Discover all OTA capable devices** to identify all devices that contain the external or flash memory required.

Note that you can also perform this discovery through the Device Manager:

- A. Click the  icon from the SNA toolbar to open Device Manager.
- B. Click the **Commission** tab.
- C. Click the , and select to **Discover all OTA capable devices**.


During the discovery, a message may appear asking whether you want to perform a service discovery. If this happens, answer **Yes**.


OTA-capable devices are shown with a blue arrow and progress indicator.




7. Select the device (or devices) to upgrade, and then select the file that contains the new firmware. For instructions, see
  - o [Upgrading a single device](#)
  - o [Upgrading multiple devices with the same firmware](#)

## Upgrading a single device

1. On the Device Manager or VDT window, click the  icon next to the device to upgrade, or else right-click the device and select **OTA Upgrade > Download**.
2. Select the file that contains the new firmware, and then click **Upgrade**.

When the download starts, the arrow icon changes to a . You can click this if you want to cancel the download for any reason. The progress indicator shows the progress of the download.

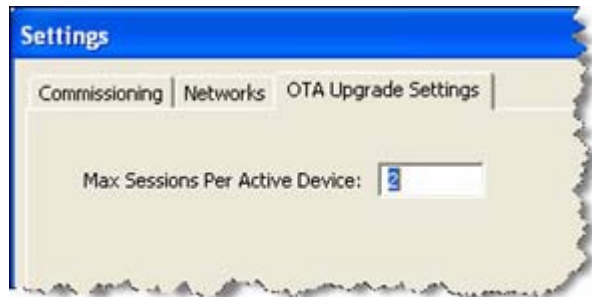
When the progress indicator reaches 100%, the SNA checks the firmware file to confirm that it was downloaded with no errors. It then displays a  to indicate that the download was successful.

3. After the firmware is successfully downloaded to the device's external or flash memory, you need to load (or enable) the firmware on the device to complete the upgrade. See page 7 for instructions.

Note that you can perform multiple single device upgrades at the same time (that is, download a different firmware file to a number of different devices). Simply repeat steps 1 and 2 above for each device you want to upgrade.


## Upgrading multiple devices with the same firmware

1. On the Device Manager or VDT window, right-click the active device, and then select **OTA Upgrade > Settings**.















2. Enter the maximum number of devices to upgrade with the same firmware file at any one time, and then click **OK**. The default (and recommended) value is 2.


Note that a higher number does not always result in faster download times. The first devices download the firmware through the active device. Once that is complete, subsequent devices are upgraded through the nearest node that contains the updated firmware, which acts as a server. Because the subsequent upgrades typically use much shorter routes, they tend to be much faster.

3. On the Device Manager or VDT window, use Ctrl+Click or Shift+Click to select the devices to upgrade.
4. Right-click the selected devices, and then select **OTA Upgrade > Download**.
  - o On Device Manager, you can also click the  icon, then and select to **Download Selected** or **Download All**.

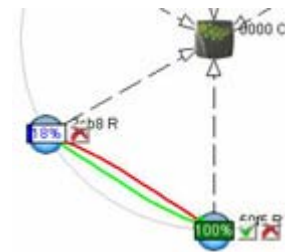
5. Select the file that contains the new firmware, and then click **Upgrade**.

The download starts for the number of devices you specified in step 1, and the arrow icon for the devices being upgraded changes to a . You can click this if you want to cancel the download for any reason. The progress indicator shows the progress of the download. A  is used to identify devices for which the upgrade is still pending.

OTA Upgrade		
100%		
89%		
90%		
0%		
0%		

When the progress indicator reaches 100%, the SNA checks the firmware file to confirm that it was downloaded with no errors. It then displays a  to indicate that the download was successful.

After the first devices are downloaded, the SNA automatically starts downloads for the next devices. You can look at the VDT window to see which route each download takes. Subsequent downloads are typically delivered from local nodes over shorter routes, and are therefore faster than the initial downloads that go through the active device.



6. After the firmware is successfully downloaded to the devices' external or flash memory, you need to load (or enable) the firmware on the devices to complete the upgrade. See page 7 for instructions.

Note that you can perform multiple upgrades at the same time (that is, download different firmware files to a number of different devices). Simply repeat steps 3 to 5 above for each group of devices you want to update.

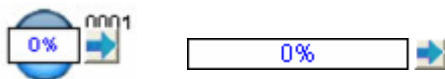
## Enabling downloaded firmware

After downloading the firmware to a device's external or flash memory, the next step is to enable (or install) that firmware on the device.


1. Click the  next to a completed download on the Device Manager or VDT window.

This causes the firmware to be copied from the memory and installed on to the device. Once successfully installed, the device is rebooted, so that it restarts using its updated firmware.

After the enable is successful (with the new firmware installed and the device restarted), the device is shown in the Device Manager and VDT window with a blue arrow and its progress bar at 0%.




2. You can also enable multiple devices in a single operation through Device Manager.

To enable ALL devices in a single operation, click  and select to **Enable All Firmware**. Note that this only enables firmware for devices that have completed downloading. Devices that are currently downloading (or waiting to download) firmware remain unaffected.

When you enable devices in this way, the SNA looks at the importance of each device within your network's routing. It restarts the least important devices first, and works its way through leaving the most important devices until last. In this way, it minimizes the impact that the restarting devices have on your network communications.

## Notes about enabling firmware

- If you click the  icon before the firmware is enabled, the downloaded firmware will be deleted from the device's external or flash memory. That means you need to re-download the firmware before the device can be enabled.
- Enabling firmware can slow down your network temporarily. Part of the enabling process causes the device to restart, which will temporarily remove it from your network.

## SNA firmware

The SNA provides a number of firmware files that can be used with TI's CC2430 and CC2431 for locationing and OAD (Over the Air Downloads).

- [Locationing node firmware used for OAD from the SNA:](#)
  - TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r5.bin (Reference node)
  - TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r6.bin (Reference node)
  - TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r5.bin (Blind node)
  - TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r6.bin (Blind node)
- [Locationing node firmware used for flashing from TI's Flash Programmer:](#)
  - TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r5.hex (Reference node)
  - TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r6.hex (Reference node)
  - TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r5.hex (Blind node)
  - TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r6.hex (Blind node)

## Notes:

- OTA Upgrades required the TI CC2430/CC2431 SoC (System on a Chip) with the following: Rev D or later (that is, those with a date group of 0642 or later) and OAD (Over the Air Download) Flash Board 1.0.
- For more information about the functionality of **Locationing** node firmware, refer to the Daintree Networks application note AN016, *Locating ZigBee nodes using TI's CC2431 location engine and Daintree's SNA*.
- For more information about (and to download) **TI's Flash Programmer**, visit [zigbee.ti.com](http://zigbee.ti.com) and select **Downloads > CC2430** or **CC2431** (depending on which you are using) > **Tools and Software > Chipcon Flash Programmer**.

## Locating node firmware used for OAD from the SNA

Firmware for Locating Nodes used for OAD (Over the Air Downloads) from the Sensor Network Analyzer (SNA):

- [Locating Reference Node firmware for OAD from the SNA](#)
- [Locating Blind Node firmware for OAD from the SNA](#)

See "Notes" on page 8 to find out more about Locating and OAD.

### Locating Reference Node firmware for OAD from the SNA

There are two firmware files provided:

- TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r5.bin
- TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r6.bin

The table below shows the features and settings for these files, most of which are common. Any variations are highlighted in **red** for easy identification.

<b>Locating Reference Node</b>	<ul style="list-style-type: none"> <li>• Security = None</li> <li>• Hardware = TI Battery boards with CC2430 or CC2431</li> </ul>
<b>Over the Air Download(OAD)</b>	<ul style="list-style-type: none"> <li>• Daintree Image version = <ul style="list-style-type: none"> <li>○ <b>0x0005</b> for TI-2430-ZBv2sp1-R-LocRef-OAD_20080612r5.bin</li> <li>○ <b>0x0006</b> for TI-2430-ZBv2sp1-R-LocRef-OAD_20080612r6.bin</li> </ul> </li> <li>• Daintree Manufacturer id = 0x103A</li> <li>• Daintree Product id = 0x00AD</li> </ul>
<b>Commissioning</b>	<ul style="list-style-type: none"> <li>• Extended PAN id = 0x0050c27710000000</li> <li>• Channels = 0x07FFF800 // all channel # Preferred Channels = 11, 14, 15, 19, 20, 24, 25</li> <li>• In Clusters # Commissioning # Basic</li> <li>• Out Cluster # Basic</li> <li>• Functionality: During network join the LED D1 is flashed until it is joined to a network or is flashing slower if join failed. Reset to default settings is done by pressing (or holding down) button S1 during joining and the LED is on for 3 sec if reset has been done. When forming a new network, or scanning to join a network, the devices scans the channels using the Preferred Channels before scanning the rest of the channels in order to avoid the most commonly used WiFi channels and to improve the user experience during installation.</li> </ul>
<b>ZDO Optional features</b>	<ul style="list-style-type: none"> <li>• Mgmt_Lqi_rsp</li> <li>• Mgmt_Leave_rsp</li> <li>• Mgmt_Permit_Joining_rsp</li> </ul>

## Locating Blind Node firmware for OAD from the SNA

There are two firmware files provided:

- TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r5.bin
- TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r6.bin

The table below shows the features and settings for these files, most of which are common. Any variations are highlighted in **red** for easy identification.

<b>Locating Blind Node</b>	<ul style="list-style-type: none"> <li>• Security = None</li> <li>• Hardware = TI Battery boards with CC2431</li> </ul>
<b>Over the Air Download(OAD)</b>	<ul style="list-style-type: none"> <li>• Daintree Image version = <ul style="list-style-type: none"> <li>○ <b>0x0005</b> for TI-2431-ZBv2sp1-R-LocBlind-OAD_20080612r5.bin</li> <li>○ <b>0x0006</b> for TI-2431-ZBv2sp1-R-LocBlind-OAD_20080612r6.bin</li> </ul> </li> <li>• Daintree Manufacturer id = 0x103A</li> <li>• Daintree Product id = 0x10AD</li> </ul>
<b>Commissioning</b>	<ul style="list-style-type: none"> <li>• Extended PAN id = 0x0050c27710000000</li> <li>• Channels = 0x07FFF800 // all channel # Preferred Channels = 11, 14, 15, 19, 20, 24, 25</li> <li>• In Clusters # Commissioning # Basic</li> <li>• Out Cluster # Basic</li> <li>• Functionality: During network join the LED D1 is flashed until it is joined to a network or is flashing slower if join failed. Reset to default settings is done by pressing (or holding down) button S1 during joining and the LED is on for 3 sec if reset has been done. When forming a new network, or scanning to join a network, the devices scans the channels using the Preferred Channels before scanning the rest of the channels in order to avoid the most commonly used WiFi channels and to improve the user experience during installation.</li> </ul>
<b>ZDO Optional features</b>	<ul style="list-style-type: none"> <li>• Mgmt_Lqi_rsp</li> <li>• Mgmt_Leave_rsp</li> <li>• Mgmt_Permit_Joining_rsp</li> </ul>

## Locating node firmware used for flashing from TI's Flash Programmer

Firmware for Locating Nodes used for flashing from TI's Flash Programmer:

- [Locating Reference Node firmware for flashing from TI's Flash Programmer](#)
- [Locating Blind Node firmware for flashing from TI's Flash Programmer](#)

See "Notes" on page 8 to find out more about Locating and OAD.

### Locating Reference Node firmware for flashing from TI's Flash Programmer

There are two firmware files provided:

- TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r5.hex
- TI-2430-ZBv2sp1-R-LocRef-OAD\_20080612r6.hex

The table below shows the features and settings for these files, most of which are common. Any variations are highlighted in **red** for easy identification.

<b>Locating Reference Node</b>	<ul style="list-style-type: none"> <li>• Security = None</li> <li>• Hardware = TI Battery boards with CC2430 or CC2431</li> </ul>
<b>Over the Air Download(OAD)</b>	<ul style="list-style-type: none"> <li>• Daintree Image version = <ul style="list-style-type: none"> <li>○ <b>0x0005</b> for TI-2430-ZBv2sp1-R-LocRef-OAD_20080612r5.hex</li> <li>○ <b>0x0006</b> for TI-2430-ZBv2sp1-R-LocRef-OAD_20080612r6.hex</li> </ul> </li> <li>• Daintree Manufacturer id = 0x103A</li> <li>• Daintree Product id = 0x00AD</li> </ul>
<b>Commissioning</b>	<ul style="list-style-type: none"> <li>• Extended PAN id = 0050c27710000000</li> <li>• Channels = 0x07FFF800 // all channel # Preferred Channels = 11, 14, 15, 19, 20, 24, 25</li> <li>• In Clusters # Commissioning # Basic</li> <li>• Out Cluster # Basic</li> <li>• Functionality: During network join the LED D1 is flashed until it is joined to a network or is flashing slower if join failed. Reset to default settings is done by pressing (or holding down) button S1 during joining and the LED is on for 3 sec if reset has been done. When forming a new network, or scanning to join a network, the devices scans the channels using the Preferred Channels before scanning the rest of the channels in order to avoid the most commonly used WiFi channels and to improve the user experience during installation.</li> </ul>
<b>ZDO Optional features</b>	<ul style="list-style-type: none"> <li>• Mgmt_Lqi_rsp</li> <li>• Mgmt_Leave_rsp</li> <li>• Mgmt_Permit_Joining_rsp</li> </ul>

## Locating Blind Node firmware for flashing from TI's Flash Programmer

There are two firmware files provided:

- TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r5.hex
- TI-2431-ZBv2sp1-R-LocBlind-OAD\_20080612r6.hex

The table below shows the features and settings for these files, most of which are common. Any variations are highlighted in **red** for easy identification.

<b>Locating Blind Node</b>	<ul style="list-style-type: none"> <li>• Security = None</li> <li>• Hardware = TI Battery boards with CC2431</li> </ul>
<b>Over the Air Download(OAD)</b>	<ul style="list-style-type: none"> <li>• Daintree Image version = <ul style="list-style-type: none"> <li>○ <b>0x0005</b> for TI-2431-ZBv2sp1-R-LocBlind-OAD_20080612r5.hex</li> <li>○ <b>0x0006</b> for TI-2431-ZBv2sp1-R-LocBlind-OAD_20080612r6.hex</li> </ul> </li> <li>• Daintree Manufacturer id = 0x103A</li> <li>• Daintree Product id = 0x10AD</li> </ul>
<b>Commissioning</b>	<ul style="list-style-type: none"> <li>• Extended PAN id = 0x0050c27710000000</li> <li>• Channels = 0x07FFF800 // all channel # Preferred Channels = 11, 14, 15, 19, 20, 24, 25</li> <li>• In Clusters # Commissioning # Basic</li> <li>• Out Cluster # Basic</li> <li>• Functionality: During network join the LED D1 is flashed until it is joined to a network or is flashing slower if join failed. Reset to default settings is done by pressing (or holding down) button S1 during joining and the LED is on for 3 sec if reset has been done. When forming a new network, or scanning to join a network, the devices scans the channels using the Preferred Channels before scanning the rest of the channels in order to avoid the most commonly used WiFi channels and to improve the user experience during installation.</li> </ul>
<b>ZDO Optional features</b>	<ul style="list-style-type: none"> <li>• Mgmt_Lqi_rsp</li> <li>• Mgmt_Leave_rsp</li> <li>• Mgmt_Permit_Joining_rsp</li> </ul>