What's New in Zigbee 3.0

Zigbee is an industry-proven worldwide standard for low power, self-healing, robust mesh networks offering a complete and interoperable IoT solution for home and building automation. Based on the IEEE 802.15.4 standard and providing a simplified approach to commissioning devices securely, it enables users the ability to form networks involving over 250 devices for large coverage areas. Through adherence to a profile specification and ZCP (Zigbee Compliant Platform) testing, Zigbee devices can become certified for interoperability across various platforms.

Texas Instruments™ CC13x2 and CC26x2 devices are part of the SimpleLink™ microcontroller (MCU) platform. Zigbee based applications can be developed on these devices using the TI Z-Stack included with the SimpleLink™ CC13x2 and CC26x2 software development kit (SDK). This SDK includes everything needed to develop Zigbee certifiable solution including tools, application examples, documentation and source code. It uses Zigbee 3.0, the latest specification from the Zigbee Alliance which unifies former application segments under a common certification process. The following sections intend to give users an overview of all of the new features introduced in the Zigbee 3.0 specification.

1 Overview

At the core of Zigbee 3.0 is the Zigbee PRO 2017 (R22). Note that previously Zigbee Pro 2015 (R21) was required for Zigbee 3.0, which has now been replaced with the newer Zigbee Pro 2017 (R22) specification. Older implementation based on the R21 specification are still compatible with the new R22 specification.

The Zigbee PRO Specification adds child device management, improved security features, and new network topology options to Zigbee networks. Commissioning devices into networks has also been improved and made more consistent through Base Device Behavior (BDB). Zigbee 3.0 furthermore requires Green Power Basic Proxy v1.1.1 functionality in all devices to further support Green Power capabilities and compiles all profile clusters into a single specification, Zigbee Cluster Library (ZCL) v7. Finally, it formalizes common Zigbee device application architecture nomenclature, expands on the Zigbee Lighting & Occupancy Device Specification, and comments towards Zigbee 3.0 certification. The following sections address each of these attributes.

2 Zigbee PRO Specification

Zigbee PRO (2015/2017) includes the formal set of rules that all software solutions must adhere in order to become a ZCP through the Zigbee Alliance, a highly sought-after certification that ensures interoperability between devices. The following are new features that have been added to the Zigbee 2015/2017 specification that developers should be aware of. Full details can be acquired through the Zigbee PRO specification documentation and also through the Zigbee Alliance website.

2.1 Child Device Management

Child management is a procedure for which parent devices must now age out neighbor table entries for unresponsive end device children by a pre-configured default timeout. This aging timeout can be changed per end device upon request from that end device using the *End Device Timeout Request* command. MAC data polls are sent from a child end device to reset the parent's aging counter. But once the timeout value is exceeded and the child is aged out, the parent will send the device a *Leave Request* with the rejoin attribute set so that the device may be allowed to rejoin the network through a new parent device.

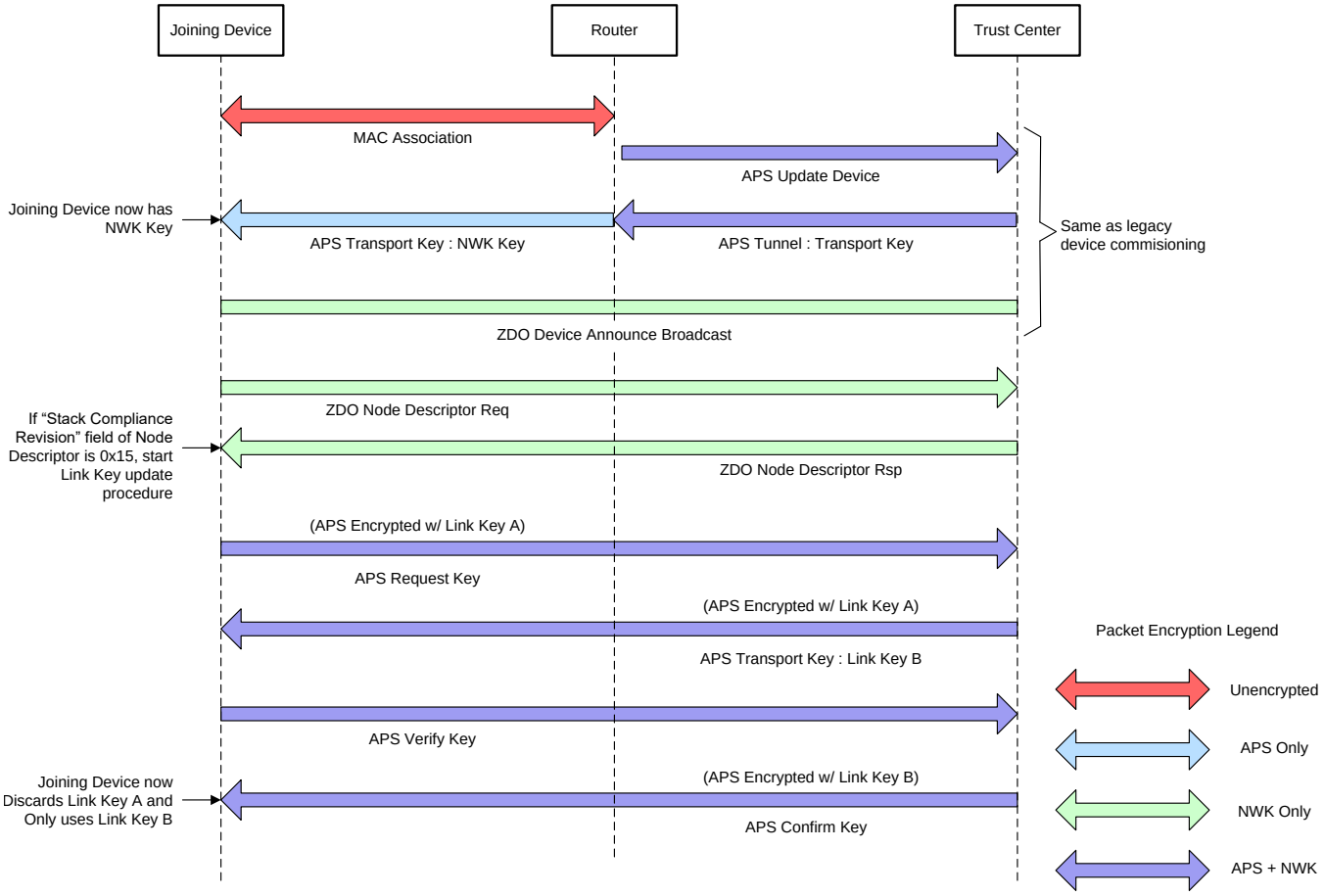
2.2 Parent Announce Command

The *Parent Announce* message is now mandatory on all routing devices (router and coordinator) and is used to notify other routing devices in a network of which child devices are known to it. The message is broadcast to 0xFFFC if a routing device previously in the network was rebooted and successfully rejoins the network. It is sent 10 to 20 seconds after this device rejoins the network.

2.3 Trust Center (TC) Link Key Updates

R21 devices joining a Zigbee 3.0 centralized network must initiate a TC Link Key update procedure upon joining the network. This unique TC Link Key is used for all encrypted APS-layer communication instead of the well-known counterpart. The *Node Descriptor* packet that is sent during network association procedure indicates the joining device's Zigbee version. R21 coordinators (acting as a trust center) can be configured to accept or reject legacy devices that do not initiate the TC Link Key update procedure. Note the mandatory unique TC Link Keys for each capable device leads to an increased flash requirement on the coordinator.

Figure 1. R21 TC Link Key Update Procedure



2.4 Install Codes

By default, the initial network key is transported to joining devices using the well-known TC Link Key. However, there is now an option of using pre-configured keys and install codes to enhance security even further. Install codes are 128 bits of random data and a 16 bit CRC which are passed through an MMO hash function to generate a TC Link Key. This derived key would be used instead of the well-known TC Link key such that no well-known key is ever used to encrypt data over-the-air. Generally, install code-derived TC link keys are hard-coded into joining devices during the manufacturing process. The corresponding install code is then included with the device and programmed into the network leader through an out-of-band method such as a user interface. High Security mode from R20 has been removed from the R21 specification due to the TC Link Key update and install code enhancements.

2.5 Outgoing NWK Frame Counter

The outgoing NWK frame counter is now persistent across all resets, including standard factory new resets and over-the-air resets, to help prevent replay attacks. The NWK frame counter will be reset if its value is greater than 0x80000000 when a NWK key update is performed.

2.6 Changes to Network Joining

Permit join can no longer be enabled forever as networks will automatically close joining after a maximum of 254 seconds. To extend the time the network is open, you may send out permit join requests periodically to restart the timer. Requests to open the network without enabling joining at the trust center are no longer supported.

2.7 New Mandatory Command Support

Processing *Mgmt-Leave* and *NWK-Leave* requests are now mandatory but handled differently depending on the Zigbee device type. Routers accept these commands from any node while end devices only accept the command from its direct parent. Coordinators ignore all leave requests. The *Mgmt_LQI_req* command is mandatory for all devices (including end devices) and provides a standard way of performing network topology discovery.

2.8 Optional Distributed Networks

Distributed networks are formed by the first router that attempts to steer a network without the existence of a coordinator. As the network does not have a coordinator for a trust center, network keys are either received from the parent upon joining through a well-known Distributed Global Link Key, pre-configured, or received out-of-band by way of an install code. Devices in distributed networks will have a lifetime of approximately 4.3 billion packets since NWK keys are fixed and cannot be updated.

3 Base Device Behavior (BDB)

Base Device Behavior (BDB) provides a consistent behavior for all nodes connecting to a Zigbee network, including a common set of mechanisms for network commissioning. It can be seen as an enhancement to EZ-Mode from the Zigbee Home Automation profile.

3.1 BDB Commissioning Modes

There are four types of commissioning modes available through BDB:

- Touchlink
- Network Steering
- Network Formation
- Finding and Binding (F&B)

Touchlink is the Zigbee Light Link profile equivalent for proximity-based commissioning. Network Steering enables permit joining (to open the network for joining), but only if the device is already on a network. If an end device or router type is not currently in a network, the device will try to join an existing network and only continue with permit joining if this procedure is successful. For coordinators (and routers if distributed networks are allowed), Network Formation will be invoked if Network Steering determines that there is not a suitable network to join. This will create a new centralized security network for coordinators or a distributed security network for router types.

F&B is invoked once the device is in a network and looks for other nodes that are also in F&B mode and interested in exchanging data from matching clusters. If matching clusters are found in other nodes, the appropriate binds are made. Once bindings are formed by the F&B procedure, any clusters with bindings that support ZCL attribute reporting will start doing so immediately to the destination set in the binding table entry. The BDB specification also mandates automatic ZCL attribute reporting for all reportable attributes. Users can configure a default reporting interval and reportable change amount.

3.2 BDB Security

Inside centralized security networks, TC link keys are used for transferring the initial and future network keys. The initial TC link key will either be the Trust Center's well-known default, derived from a pre-configured install code, or explicitly defined. As mentioned in the Trust Center Link Key Updates section, R21 devices must update their TC link key as part of the network joining procedure.

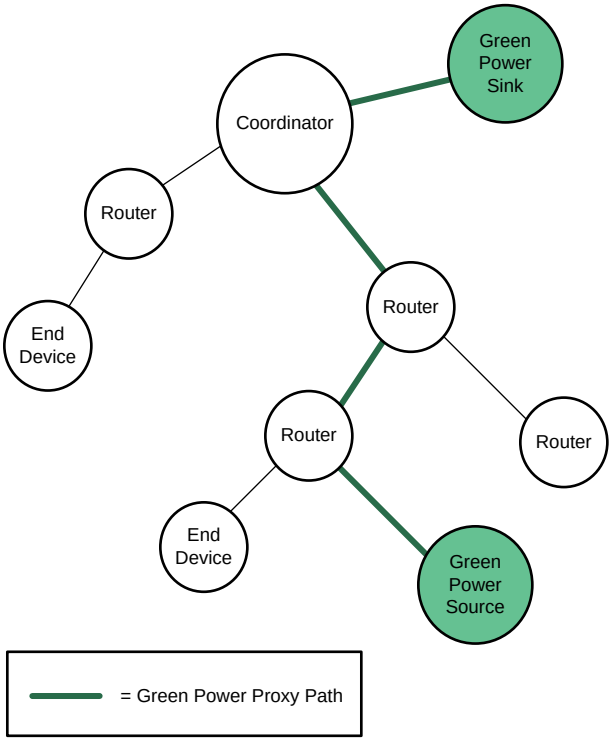
3.3 Reset Methods Available with BDB

Several reset options are made possible through BDB to perform various reset actions. This includes Basic Cluster resets through the "reset to factor defaults" instruction, in which all cluster attributes on the device are reset to their default values. Network settings, groups, and bindings are not affected. There is also "reset to factory new", where all persistent data is cleared with the exception of the outgoing NWK frame counter. It can be initiated by the *Network Leave* command with rejoin off, the *Mgmt_Leave_req* command with rejoin off, local action, or touchlink interface. Finally, there is the "complete" reset. That includes outgoing NWK frame counters and is defined by the manufacturer, as there is no standard method.

4 Green Power Basic Proxy

Every Zigbee 3.0 device with routing capabilities (router or coordinator) must implement Green Power Basic Proxy (GPBP) v1.1.1 functionality for forward compatibility. GPBP enables routing devices to tunnel Green Power Device Frames (GPDF) from Green Power Source to Sink devices, making Green Power functionality possible on any Zigbee 3.0 network, regardless of a specific device's own application.

Figure 2. Zigbee Green Power Proxy Topology



5 Zigbee Cluster Library

ZCL 7 is a single specification document that contains all cluster definitions that had previously spanned across multiple documents for multiple profiles. It conforms to a single Application Profile ID (0x0104) and no longer mandates security and encryption, as this functionality is now handled by the Zigbee PRO and BDB specifications. For further documentation details, including updates to confirmed and verified clusters, see the Zigbee Alliance website.

6 Zigbee Application Architecture

The Zigbee 3.0 Specification defines a set of rules by which the Zigbee application layer specifications will be created. As such, it provides formal definitions for the common Zigbee terms "Node", "Cluster", and "Device".

6.1 Zigbee Node

A Zigbee node represents a single testable implementation. This could be a standalone Zigbee device that runs on a single processor or application processor (ZAP) plus network processor (ZNP) that work together to form a single Zigbee device. Each node is a single Zigbee application on a single Zigbee stack, with one NWK address and one PAN ID. A Zigbee node can host multiple Zigbee device instances, where each device instance is hosted on its own endpoint. It is possible that a single physical product may support more than one Zigbee node, such as a device that bridges two separate Zigbee networks together.

6.2 Zigbee Cluster

Zigbee Clusters are defined by the ZCL specification. Each cluster specifies a set of cluster attributes, a set of commands generated and received, and other associated behavior. Attributes, commands, and behaviors for each cluster can be either mandatory or optional depending on the ZCL specification. Each Zigbee cluster has a server and client implementation. Generally, the device that supports the server side of the cluster is the one that implements the actual hardware functionality which the cluster intends to interact with. Using the example of a light and switch design, the light implements the On/Off server since it is what the On/Off command intends to control. For a Temperature Measurement cluster, the temperature sensor implements the Temperature Measurement server since it is the one that takes the actual temperature measurements using hardware. Each Zigbee cluster is defined as either a Utility or Application cluster, and either a Type 1 or Type 2 cluster.

- Utility Cluster: Not part of the functional operation of the product, for example one used for device commissioning, configuration, discovery, or diagnostic.
- Application Cluster: Generates persistent functional application transactions between client and server sides of a cluster, and the targets of these transactions are determined when binds are created between matching client/server clusters. Some examples are:
  - On/Off cluster: Switch (On/Off cluster client) sends commands to a light (On/Off cluster server)
  - Temperature Measurement cluster - Temperature sensor (Temperature Measurement cluster server) sends reports to a thermostat (Temperature Measurement cluster client)
- Type 1 Cluster: Initiates transactions from the client side of the cluster to the server side. With BDB F&B, binds are created on the client side device. This makes the client device the BDB F&B initiator. The On/Off cluster is an appropriate example as the On/Off client sends commands to the On/Off server.
- Type 2 Cluster: Initiates transactions from the server side of the cluster to the client side. With BDB F&B, binds are created on the server side device. This makes the server device the BDB F&B initiator. The Temperature Meas cluster is an example since the Temperature Measurement server sends attribute reports to the Temperature Measurement client.

6.3 Zigbee Device

Each endpoint on a Zigbee node supports a Zigbee Device type. There are three device classes for Zigbee device types:

- Node Class: Not to be confused with the previous definition of a Zigbee node, a node-class device defines an endpoint that represents the entire Zigbee node for some actions. An example of a node device endpoint would be the ZDO (Zigbee Device Object) endpoint, which is defined on endpoint 0 by the specification and is responsible for actions related to the logical Zigbee device type (ZC, ZR, ZED) like network commissioning, binding and discovery requests, and so on (all Zigbee networking-related actions). Another example of a node device endpoint would be the Green Power endpoint, which (if implemented) is defined on endpoint 242 and is another endpoint responsible for network actions. A Zigbee node can implement one or more node device endpoints and may or may not specify mandatory clusters.
- Simple Class: The most common endpoints in typical Zigbee networks. Zigbee devices like sensors, actuators, lights, and switches, are all simple devices. A simple device specifies a set of mandatory application clusters within the ZCL specification. Simple device endpoints are only operational within a Zigbee network if a bind exists for that cluster on the corresponding endpoints, otherwise it is inactive.
- Dynamic Class: This endpoint is typically found in gateway devices where there exists a higher level supervisory application above the simple device layer that can manage activities such as remote bindings, monitoring network statistics, and so on.

7 Zigbee Lighting & Occupancy (ZLO) Device Specification

The Zigbee Lighting & Occupancy Device (ZLO) Specification is a subset of the Zigbee Home Automation Profile specification that focuses specifically on Lighting & Occupancy-type Zigbee devices. It now exists as an enhancement specifically for the Zigbee 3.0 specification. This document includes Zigbee device-type definitions, required clusters for each device type, and required attributes for each cluster. More information can be found on the Zigbee Alliance website.

8 Zigbee 3.0 Certification

Zigbee 3.0 certification is now available to Zigbee Alliance members at all levels. The Zigbee Alliance provides the ZigBee Testing Tool and Green Power Test Harness to its members for compliance testing to eliminate the need of renting a test house version. More information can be found on the Zigbee Alliance website

9 References

- Zigbee Alliance website: http://www.zigbee.org/

9.1 Trademarks

Texas Instruments, SimpleLink are trademarks of Texas Instruments.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265