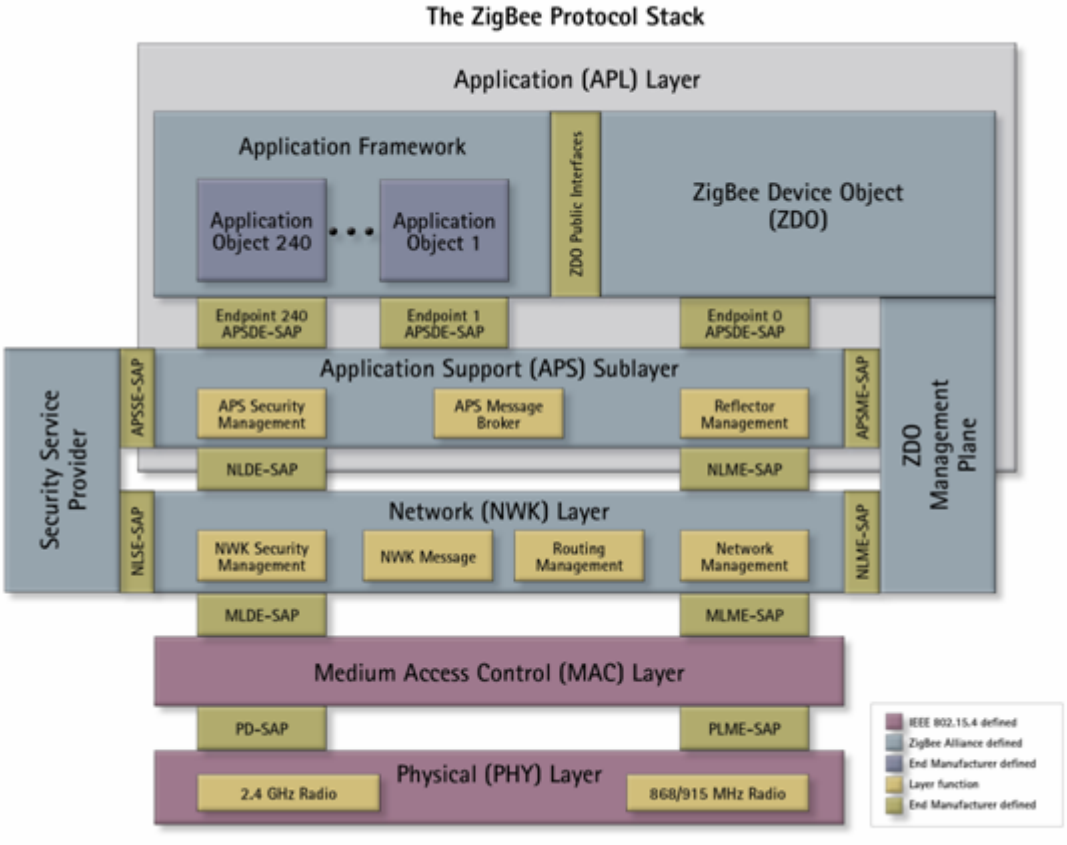
DaintreeNetworks

Getting Started with ZigBee and IEEE 802.15.4



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.

About Daintree Networks

Based in Fremont, California, Daintree Networks is a leading provider of design verification and operational support tools for wireless sensor and control networks. In a rapidly evolving industry, accelerated development and deployment cycles are key to market success. Our professional tools help OEMs, system integrators, and installers of wireless sensor and control networks speed their time to market. As an active member of the ZigBee Alliance, Daintree is playing a vital role in bringing the first wave of interoperable standards-based sensing and control products market.

Daintree's Sensor Network Analyzer family of products comprise the industry's most comprehensive solution for IEEE 802.15.4 and ZigBee development and deployment. For more information, visit www.daintree.net or email sales@daintree.net

Daintree Networks Inc
3340 Walnut Ave, Suite 275
Fremont, CA 94538 U.S.A

(w) www.daintree.net
(e) sales@daintree.net
(p) +1 (510) 505-9172

Disclaimer

This document 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 document, 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 document and the examples included.

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 reader's personal use, without the written permission of Daintree Networks.

February 2008

Contents

What is ZigBee?

ZigBee and IEEE 802.15.4 are standards-based protocols that provide the network infrastructure required for wireless sensor network applications. 802.15.4 defines the physical and MAC layers, and ZigBee defines the network and application layers.

For sensor network applications, key design requirements revolve around long battery life, low cost, small footprint, and mesh networking to support communication between large numbers of devices in an interoperable and multi-application environment.

Typical Applications

There are numerous applications that are ideal for the redundant, self-configuring and self-healing capabilities of ZigBee wireless mesh networks. Key ones include

- Energy Management and Efficiency—To provide greater information and control of energy usage, provide customers with better service and more choice, better manage resources, and help to reduce environmental impact.
- Home Automation—To provide more flexible management of lighting, heating and cooling, security, and home entertainment systems from anywhere in the home.
- Building Automation—To integrate and centralize management of lighting, heating, cooling and security.
- Industrial Automation—To extend existing manufacturing and process control systems reliability.

The interoperable nature of ZigBee means that these applications can work together, providing even greater benefits.

Motivation for ZigBee

The ZigBee standard was developed to address the following needs:

- Low cost
- Secure
- Reliable and self healing
- Flexible and extendable
- Low power consumption
- Easy and inexpensive to deploy
- Global with use of unlicensed radio bands
- Integrated intelligence for network set-up and message routing

ZigBee is the only standards-based technology that addresses the unique needs of most remote monitoring and control sensory network applications.

About the ZigBee Alliance

The ZigBee Alliance is an association of over 285 companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard. Their focus is on the following:

- Defining the network, security and application software layers
- Providing interoperability and conformance testing specifications
- Promoting the ZigBee brand globally to build market awareness
- Managing the evolution of the technology

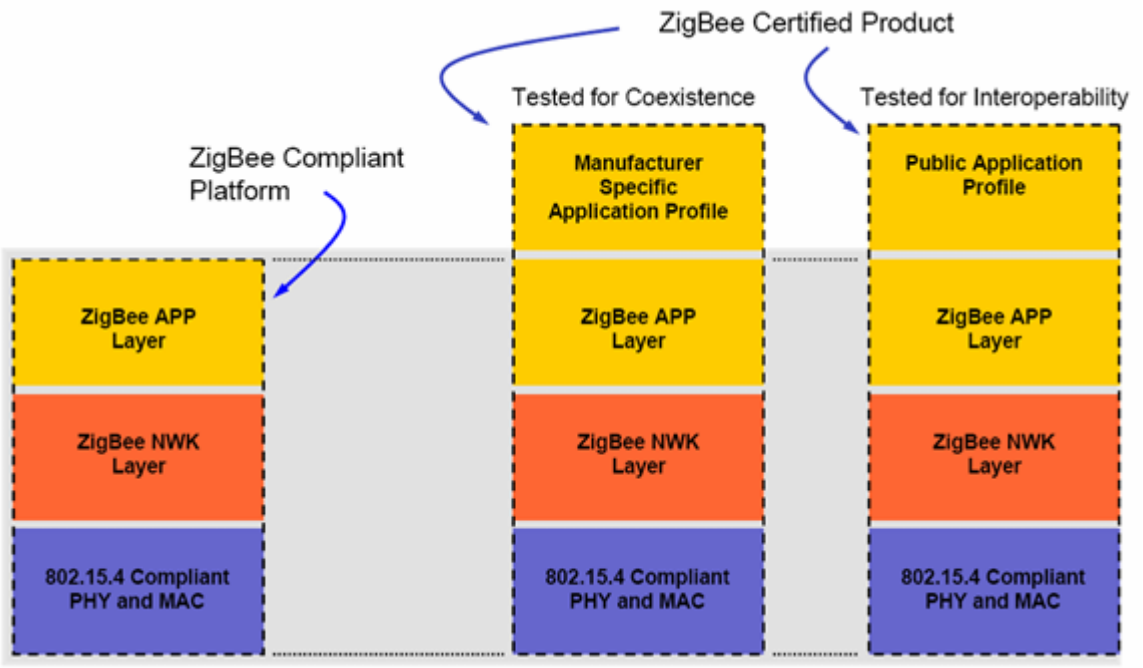
Product Certification

For a product to carry the ZigBee Alliance logo, it must first successfully complete the ZigBee Certification Program. This ensures that the product complies with the standards described in the ZigBee specification.

Only those products that pass ZigBee certification can display the ZigBee logo.

There are two ZigBee certified testing programs:

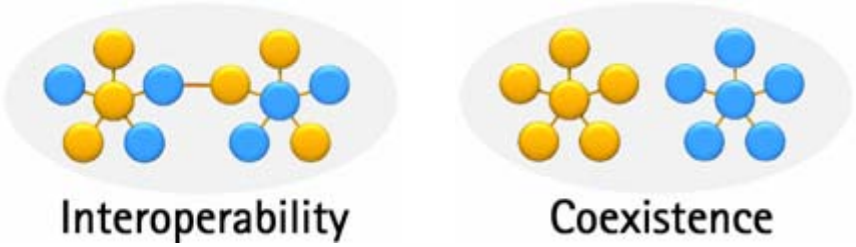
- **ZigBee Compliant Platform (ZCP)**
  The ZCP program applies to modules or platforms that are intended as building blocks for end products.
- **ZigBee Certified Products**
  This program applies to end products that are built upon a ZigBee Compliant Platform. After successful completion, these products can display the ZigBee logo.



Products that use public application profiles are tested to ensure interoperability with other ZigBee end products.

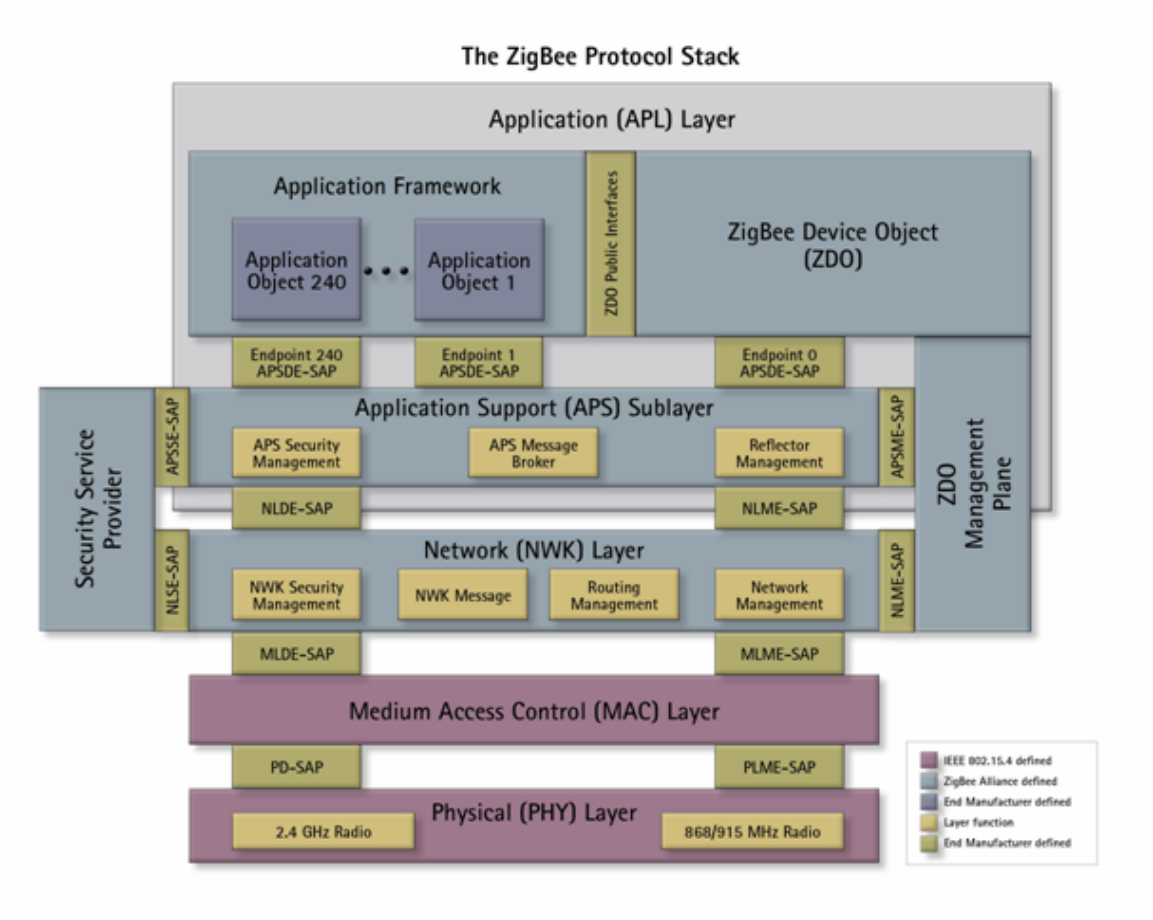
Products that use manufacturer-specific profiles, which will operate as "closed systems", are tested to ensure they can coexist with other ZigBee systems: that is, they do not adversely impact the operation of other ZigBee-certified products and networks. .

Application profiles are described later in this document.



The ZigBee Protocol Stack

ZigBee sits on top of the IEEE 802.15.4 PHY and MAC layers:



Each layer performs a specific set of services for the layer above. Each service entity provides an interface to the upper layer through a service access point (SAP).

ZigBee

Application (APL) Layer

The top layer in the ZigBee protocol stack consists of the Application Framework, ZigBee Device Object (ZDO), and Application Support (APS) Sublayer.

Application Framework

Provides a description of how to build a profile onto the ZigBee stack (to help ensure that profiles can be generated in a consistent manner). It also specifies a range of standard data types for profiles, descriptors to assist in service discovery, frame formats for transporting data, and a key value pair construct to rapidly develop simple attribute-based profiles.

Application Objects

Software at an endpoint that controls the ZigBee device. A single ZigBee node supports up to 240 application objects. Each application object supports endpoints numbered between 1 and 240 (with endpoint 0 reserved for the ZigBee Device Object (ZDO)).

ZigBee Device Object (ZDO)

Defines the role of a device within the network (coordinator, router or end device), initiates and/or responds to binding and discovery requests, and establishes a secure relationship between network devices. It also provides a rich set of management commands defined in the ZigBee Device Profile (used in ZigBee commissioning). The ZDO is always endpoint zero.

ZDO Management Plane

Facilitates communication between the APS and NWK layers with the ZDO. Allows the ZDO to deal with requests from applications for network access and security using ZDP (ZigBee Device Profile) messages.

Application Support (APS) Sublayer

Responsible for providing a data service to the application and ZigBee device profiles. It also provides a management service to maintain binding links and the storage of the binding table itself.

Security Service Provider (SSP)

Provides security mechanisms for layers that use encryption (NWK and APS). Initialized and configured through the ZDO.

Network (NWK) Layer

Handles network address and routing by invoking actions in the MAC layer. Its tasks include starting the network (coordinator), assigning network addresses, adding and removing network devices, routing messages, applying security, and implementing route discovery.

IEEE 802.15.4

Medium Access Control (MAC) Layer

Responsible for providing reliable communications between a node and its immediate neighbors, helping to avoid collisions and improve efficiency. The MAC Layer is also responsible for assembling and decomposing data packets and frames.

Physical (PHY) Layer

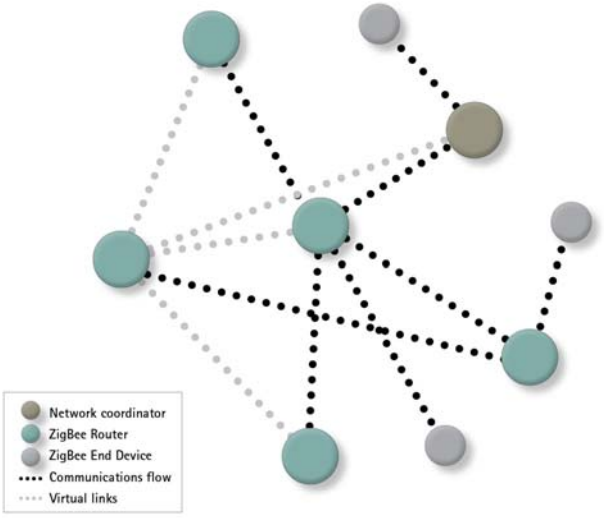
Provides the interface to the physical transmission medium (e.g. radio). The PHY layer consists of two layers that operate in two separate frequency ranges. The lower frequency PHY layer covers both the 868MHz European band and the 915MHz band used in countries such as the US and Australia. The higher frequency PHY layer (2.4GHz) is used virtually worldwide.

The ZigBee Network

Device Types

ZigBee networks include the following device types:

- Coordinators
- Routers
- End devices



Coordinator

This device starts and controls the network. The coordinator stores information about the network, which includes acting as the Trust Center and being the repository for security keys.

Router

These devices extend network area coverage, dynamically route around obstacles, and provide backup routes in case of network congestion or device failure. They can connect to the coordinator and other routers, and also support child devices.

End Devices

These devices can transmit or receive a message, but cannot perform any routing operations. They must be connected to either the coordinator or a router, and do not support child devices.

Mesh Network Topology

Mesh topology, also called peer-to-peer, consists of a mesh of interconnected routers and end devices. Each router is typically connected through at least two pathways, and can relay messages for its neighbors.

As shown in the image above, a mesh network contains a single coordinator, and multiple routers and end devices.

Mesh topology supports "multi-hop" communications, through which data is passed by hopping from device to device using the most reliable communication links and most cost-effective path until its destination is reached.

The multi-hop ability also helps to provide fault tolerance, in that if one device fails or experiences interference, the network can reroute itself using the remaining devices.

Benefits

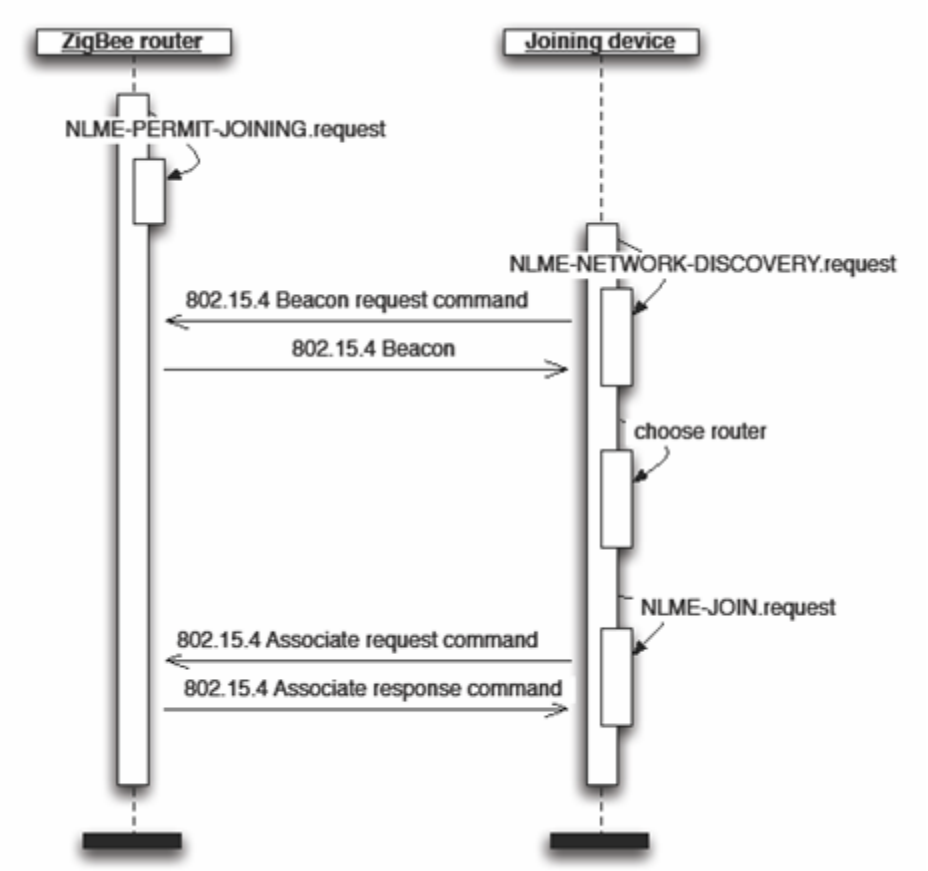
- This topology is highly reliable and robust. Should any individual router become inaccessible, alternative routes can be discovered and used.
- The use of intermediary devices in relaying data means that the range of the network can be significantly increased, making mesh networks highly scalable.
- Weak signals and dead zones can be eliminated by simply adding more routers to the network.

Joining a ZigBee Network

There are two ways to join a ZigBee network: MAC association and NWK rejoin.

MAC Association

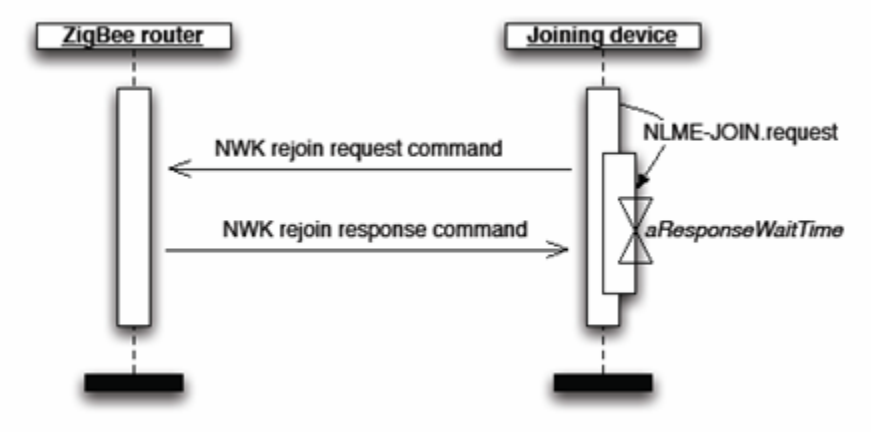
MAC association is the bare-bones default, which every ZigBee device must support, since it is actually mandated by and implemented in the underlying MAC layer. In this case, a ZigBee router or coordinator that wishes to allow other devices to join must issue a NLME-PERMIT-JOINING.request. Then the joining device, after it has discovered which network to join and to which specific device on that network it should make its request, must issue a NLME-JOIN.request with the rejoin flag set to FALSE. This last request kicks off a MAC protocol, as shown below, whereby the joining device makes a request to join the network and the receiving device issues a response, which includes an address for the device to use while associated with that network. Note that MAC association is an unsecured protocol since all the associated frames are sent in the clear (with no security).



Network Rejoin

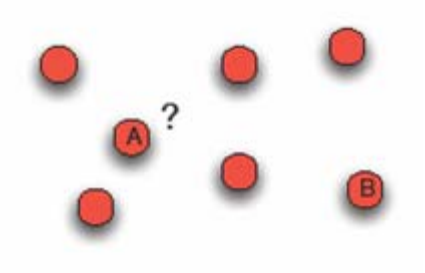
Network rejoin, which despite the name may also be used to join a network for the first time, is a NWK layer protocol. What this means, first of all, is that it is not subject to the MAC's built-in mechanism for permitting devices to join the network and can be used whether the ZigBee router has issued a NLME-PERMIT-JOINING.request or not. Second, it means that the transaction may be secured if the joining device knows the current NWK key. This could be true if the device is actually rejoining the network, or else if the device is joining for the first time but has obtained the NWK key

via some out-of-band mechanism. The figure shown below omits the optional network discovery steps shown in the previous case to stress the point that it is not necessary to discover which devices have permitted joining.

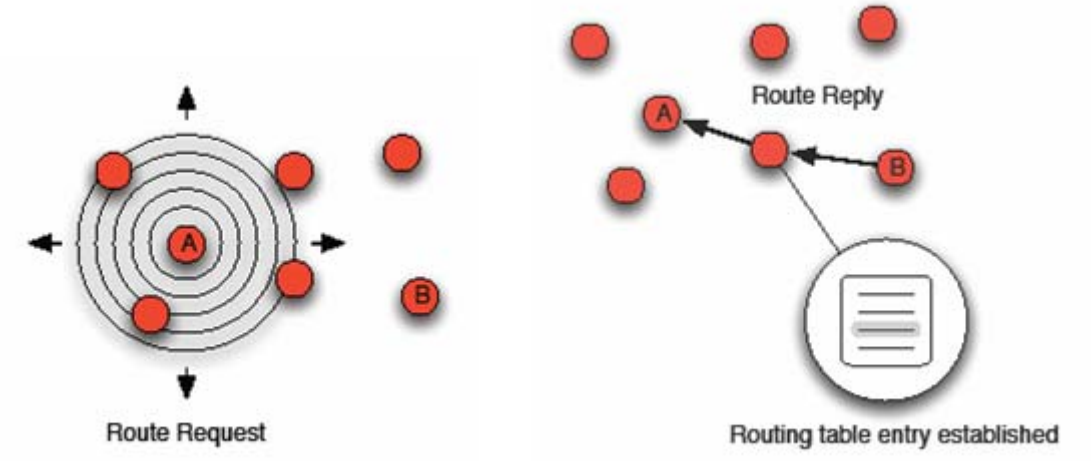


ZigBee Routing

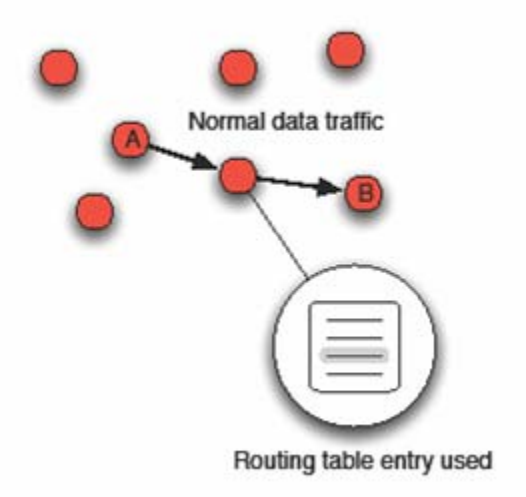
The ZigBee routing algorithm is based on the notion of "Distance Vector" (DV) routing, in which each ZigBee router that participates in the relaying of frames from a particular source to a particular destination maintains a routing table entry for the route. This entry, as a minimum, records both a "logical distance" to the destination and the address of the next router in the path to that destination.



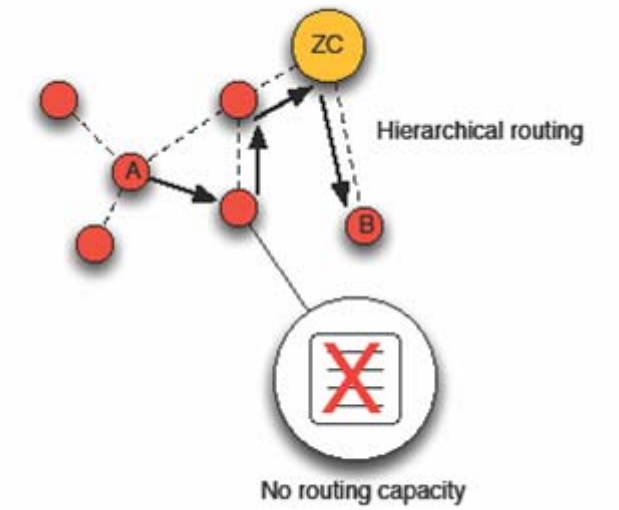
Routes are established on-demand using a route discovery process in which the originating device broadcasts a route request command and the destination device sends back a route reply.



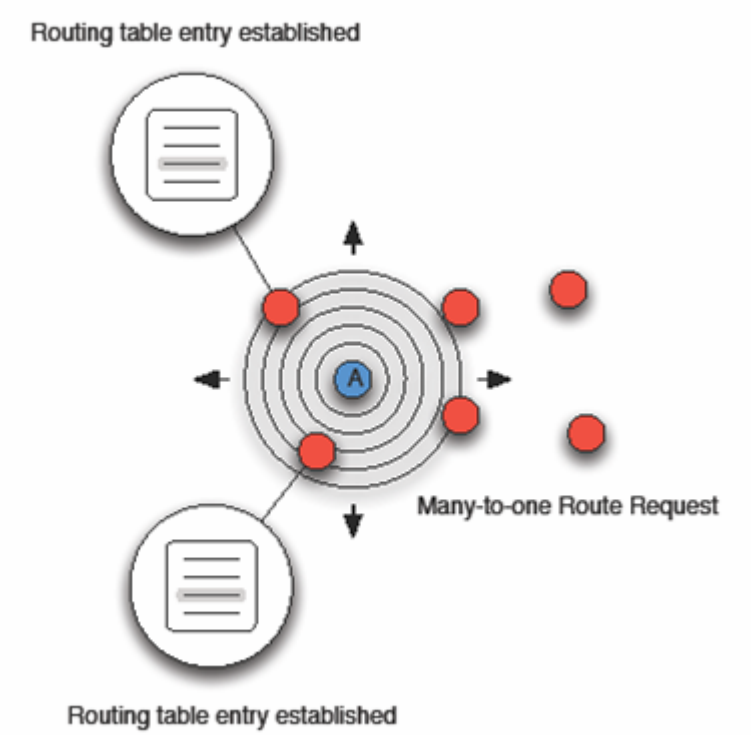
Once routing table entries are established the route may be used at will.



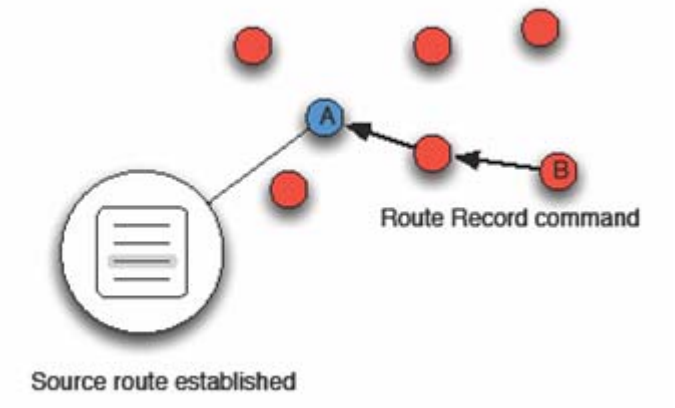
There are a number of optimizations to the basic algorithm available, which serve to reduce the RAM devoted to routing tables and, in some cases, the network traffic required to establish routes. In a device that implements the ZigBee feature set, network addresses are distributed in a hierarchical manner starting with the ZigBee coordinator (ZC). In this case, devices with little or no routing capacity, or devices whose routing capacity has been exhausted, have the option of using the address hierarchy to provide a less efficient but nonetheless usable route.



In many, perhaps in most, wireless embedded networking applications, there is a distinguished device, often called an "aggregator", to which every other device in the network must send data on a regular basis. The aggregator is shown in blue in the figure below. In order to prevent every device in the network from having to discover the aggregator separately, the ZigBee PRO feature set provides a special case of route discovery, in which a single route request broadcast from the aggregator establishes an entry with the aggregator as a destination in the routing tables of every router in the network.



In large networks, problems can also arise when the aggregator needs to address each device in the network separately. Imagine a network in which the aggregator has only a few neighbors, each of which is the next hop in the path from the aggregator to a large number of other devices. The routing tables of these few neighbors will be overburdened simply because of their proximity to the aggregator. The ZigBee PRO feature set introduces another style of routing, known as source routing, to solve this problem. Whereas in DV routing the routing information is stored in routing tables in the devices that participate in relaying the frame, source routing puts the routing information in the frame itself. Thus only the originator of the frame, in this case the aggregator, needs to maintain an entry for the route, but this routing table entry needs to store the entire path from the aggregator to the destination. ZigBee PRO uses a route record command, sent from the intended destination back to the aggregator, to record the path. Thereafter, data frames may be sent along that path using source routing.



Application Profiles, Clusters & Endpoints

An **Application Profile** describes a collection of devices employed for a specific application, and implicitly, the messaging scheme between those devices. For example, there are application profiles defined for Home Automation (HA) and Smart Energy. A profile ID is allocated to each application to uniquely identify that application.

There are two types of application profiles:

- **Public Application Profiles:** Interoperable application software developed by the ZigBee Alliance that accomplishes a specific task.
- **Manufacturer-Specific Profiles:** Private application profile developed by a company to operate a ZigBee device.

Devices within an application profile communicate with each other by means of **clusters**, which may be inputs to or outputs from the device. For example, in the HA profile there is a cluster dedicated to the control of lighting subsystems. A cluster ID uniquely identifies clusters within the scope of a particular profile.

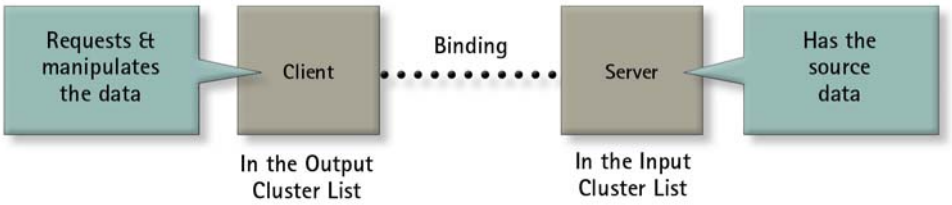
An **endpoint** defines a communication entity within a device through which a specific application is carried. For example, a remote control might allocate endpoint 6 for the control of lights in the master bedroom, endpoint 8 to manage the heating and air-conditioning system, and endpoint 12 for controlling the security system. This allows the remote control to independently communicate with these devices and identify which packets are intended for each application and device.

In all, 240 endpoints are available for use within any ZigBee device, with endpoint zero dedicated to the ZigBee Device Object (ZDO), which provides control and management commands.

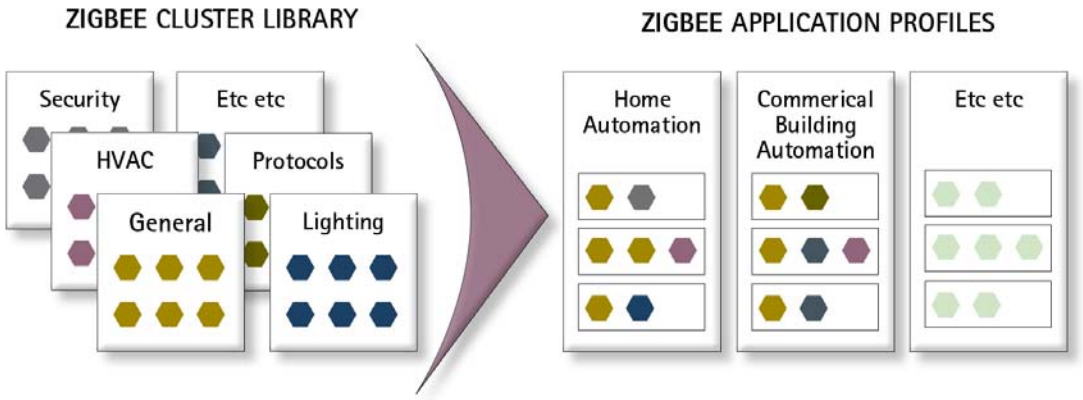
ZigBee Cluster Library (ZCL)

The ZCL is a library of clusters that can be used by any application. This allows common clusters to be reused across a number of different functional domains, for example, the same lighting clusters can be used for any application that requires lighting controls, such as home automation and commercial building automation.

Each cluster has two "ends" — client and server.



Clusters within the ZCL are organized into a number of different functional domains including Lighting, HVAC (Heating, Ventilation, Air Conditioning), Measurement and Sensing, Security and Safety, and General.



Each cluster specification defines

- Mandatory and optional attributes
- Cluster-specific commands
- Functional description

Each device specification defines

- Mandatory and optional cluster usage
- Values of "free parameters" in the ZCL
- Any additional functional description

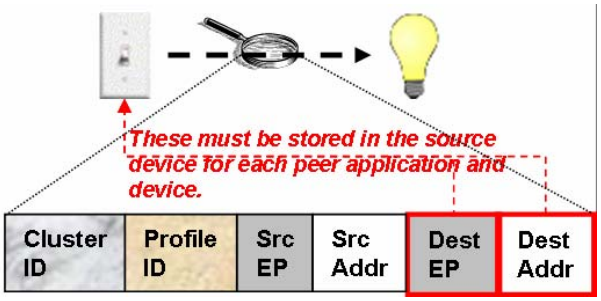
Bindings

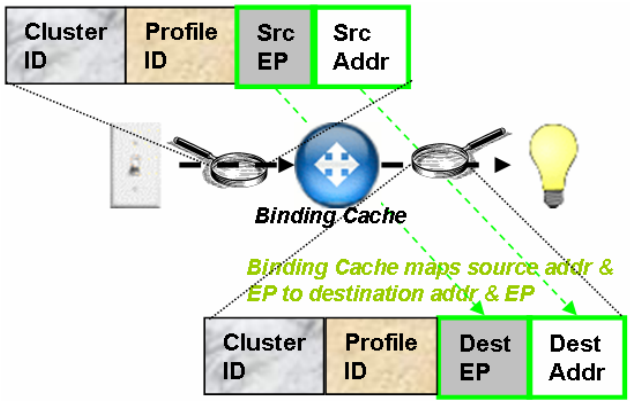
Bindings are connections between two endpoints with each binding supporting a specific application profile, and each message type represented by a cluster within that profile.

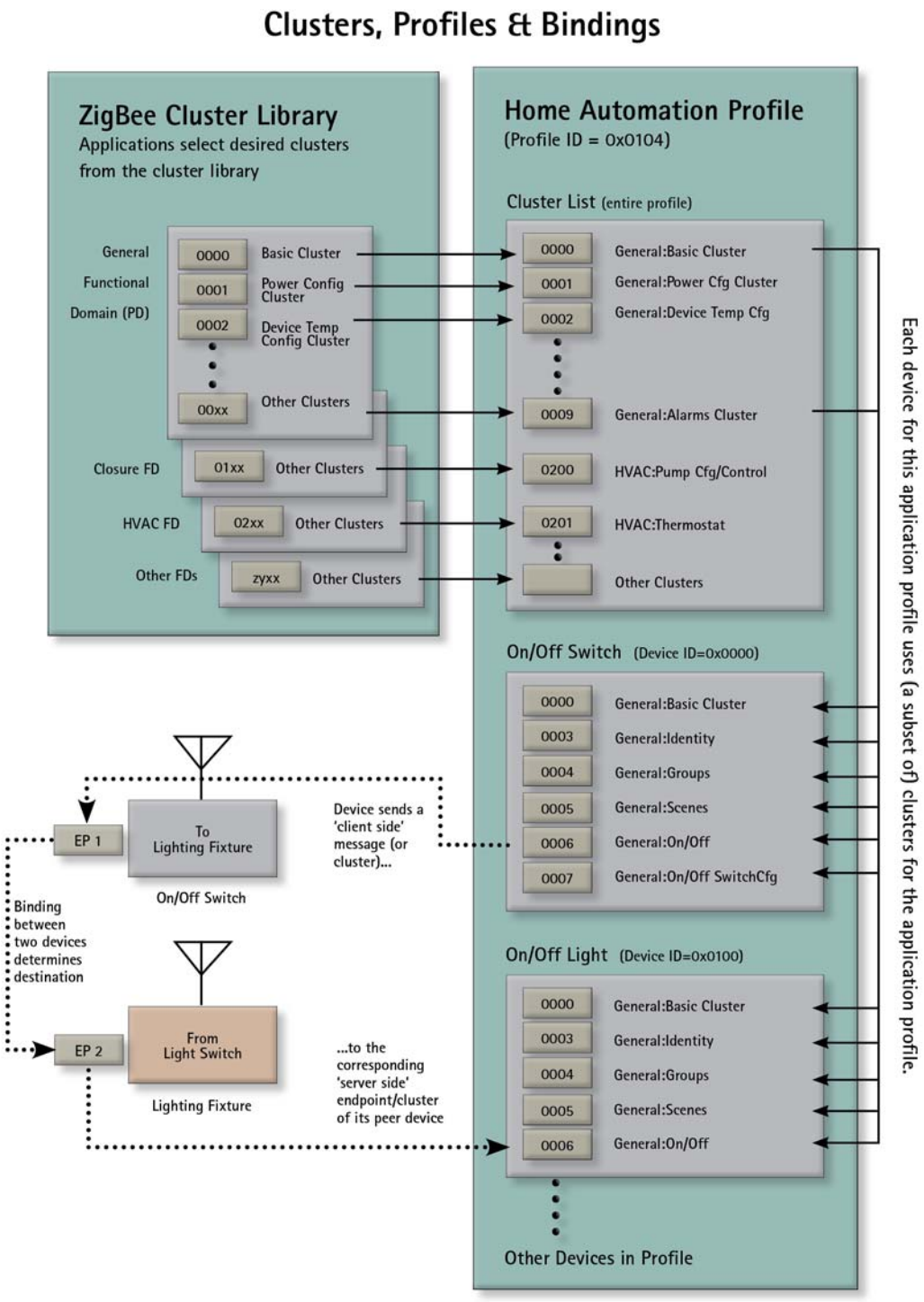
Bindings can be created between either individual or groups of endpoints, such as lights and switches, that have matching input and output clusters (that is, the same cluster IDs). ZigBee devices can have up to 240 endpoints, so each physical device can support multiple bindings.

Bindings can be stored within the source device, for example, a remote control could store the addresses and endpoint IDs of all applications it needs to communicate with. This is known as direct binding or source binding.

Binding information can also be stored in a binding cache, with an intermediary device providing a lookup table that maps all source and destination endpoints. This is known as indirect binding.






Clusters, Profiles & Bindings
ZigBee Cluster Library
Applications select desired clusters from the cluster library
General
Functional
Domain (PD)
0000
Basic Cluster
0001
Power Config Cluster
0002
Device Temp Config Cluster
00xx
Other Clusters
Closure FD
01xx
Other Clusters
HVAC FD
02xx
Other Clusters
Other FDs
zyxx
Other Clusters
Home Automation Profile
(Profile ID = 0x0104)
Cluster List (entire profile)
0000
General:Basic Cluster
0001
General:Power Cfg Cluster
0002
General:Device Temp Cfg
0009
General:Alarms Cluster
0200
HVAC:Pump Cfg/Control
0201
HVAC:Thermostat
Other Clusters
On/Off Switch (Device ID=0x0000)
0000
General:Basic Cluster
0003
General:Identity
0004
General:Groups
0005
General:Scenes
0006
General:On/Off
0007
General:On/Off SwitchCfg
On/Off Light (Device ID=0x0100)
0000
General:Basic Cluster
0003
General:Identity
0004
General:Groups
0005
General:Scenes
0006
General:On/Off
Other Devices in Profile
Each device for this application profile uses (a subset of) clusters for the application profile.
EP 1
To Lighting Fixture
On/Off Switch
Device sends a 'client side' message (or cluster)...
Binding between two devices determines destination
EP 2
From Light Switch
Lighting Fixture
...to the corresponding 'server side' endpoint/cluster of its peer device

ZigBee Security

ZigBee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. ZigBee's security services include methods for key establishment and transport, device management, and frame protection.

The ZigBee specification defines security for the MAC, NWK and APS layers. Security for applications is typically provided through Application Profiles.

Trust Center

The Trust Center decides whether to allow or disallow new devices into its network.

The Trust Center may periodically update and switch to a new Network Key. It first broadcasts the new key encrypted with the old Network Key. Later, it tells all devices to switch to the new key.

The Trust Center is usually the network coordinator, but is also able to be a dedicated device. It is responsible for the following security roles:

- Trust Manager, to authenticate devices that request to join the network
- Network Manager, to maintain and distribute network keys
- Configuration Manager, to enable end-to-end security between devices

Security Keys

ZigBee uses three types of keys to manage security: Master, Network and Link.

Master Keys

These optional keys are not used to encrypt frames. Instead, they are used as an initial shared secret between two devices when they perform the Key Establishment Procedure (SKKE) to generate Link Keys.

Keys that originate from the Trust Center are called Trust Center Master Keys, while all other keys are called Application Layer Master Keys.

Network Keys

These keys perform security Network Layer security on a ZigBee network. All devices on a ZigBee network share the same key.

High Security Network Keys must always be sent encrypted over the air, while Standard Security Network Keys can be sent either encrypted or unencrypted. Note that High Security is supported only for ZigBee PRO.

Link Keys

These optional keys secure unicast messages between two devices at the Application Layer.

Keys that originate from the Trust Center are called Trust Center Link Keys, while all other keys are called Application Layer Link Keys.

Security Modes

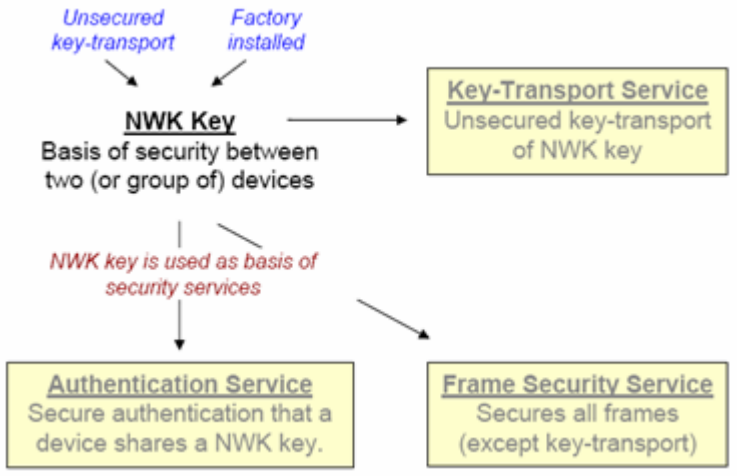
ZigBee PRO offers two different security modes: Standard and High.

Feature	Standard*	High
Network Layer security provided using a Network Key	✓	✓
APS Layer security provided using Link Keys**	✓	✓
Centralized control and update of keys	✓	✓
Ability to switch from active to secondary keys	✓	✓
Ability to derive Link Keys between devices		✓
Entity authentication and permissions table supported		✓

* Called "Residential" in ZigBee 2006
** Not supported in ZigBee 2006

Standard Security Mode

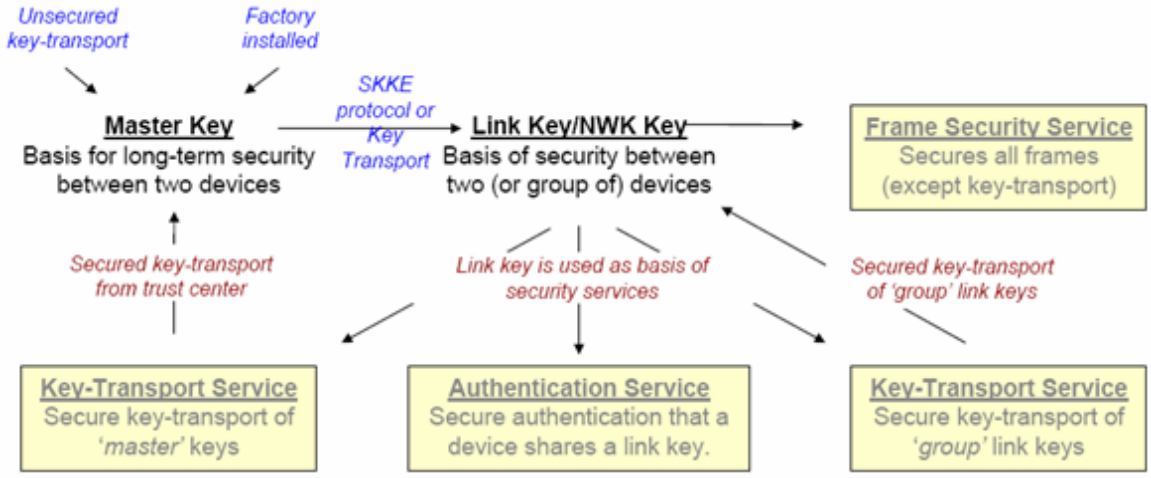
In Standard Security mode, the list of devices, master keys, link keys and network keys can be maintained by either the Trust Center or by the devices themselves. The Trust Center is still responsible for maintaining a standard network key and it controls policies of network admittance. In this mode, the memory requirements for the Trust Center are far less than they are for High Security mode.



High Security Mode

In High Security mode, the Trust Center maintains a list of devices, master keys, link keys and network keys that it needs to control and enforce the policies of network key updates and network admittance. As the number of devices in the network grows, so too does the memory required for the Trust Center.

The additional security capabilities inherent in ZigBee PRO are critical as ZigBee is used in increasingly important applications. The control of critical systems infrastructure, whether in a commercial building, utility grid, industrial plant, or a home security system must not be compromised.



Commissioning

Commissioning is the physical deployment, addressing, and logical binding of nodes to form a functional network. In its broadest sense, commissioning covers a wide range of tasks including surveying the radio and physical environment, placement of devices, configuration of parameters, application binding, optimization of network and device parameters, and testing and verification of correct operation.

Often, non- and semi-technical issues need to be considered, including the skills and workflow practices of the installer, ease and identification and accessibility of devices, and interoperability and co-existence with other wireless or wired systems.

While consideration for commissioning is often focused on installation and deployment, the ability to easily configure and commission ZigBee systems during development, testing and manufacturing is equally important.

- During development and testing, the developer often has to set up a system of devices for testing. The ability to quickly commission devices or a network using standards-based over-the-air methods can significantly improve productivity.
- During manufacturing, it may be necessary to modify device parameters (perhaps for different groups of customers), to run basic manufacturing tests or even to actually specify the ZigBee settings of devices. The ability to modify these parameters without requiring a separate firmware download provides significant flexibility to the production process.

Commissioning Tools

In a perfect world, devices would commission themselves. An installer would power them up, turn them on, and stand back and watch the devices work out which network they should join, how security worked in that network, which device (or devices) they should bind to, and which devices they should communicate with.

That perfect world may exist one day, but until then, it's up to the installer to perform all of these tasks.

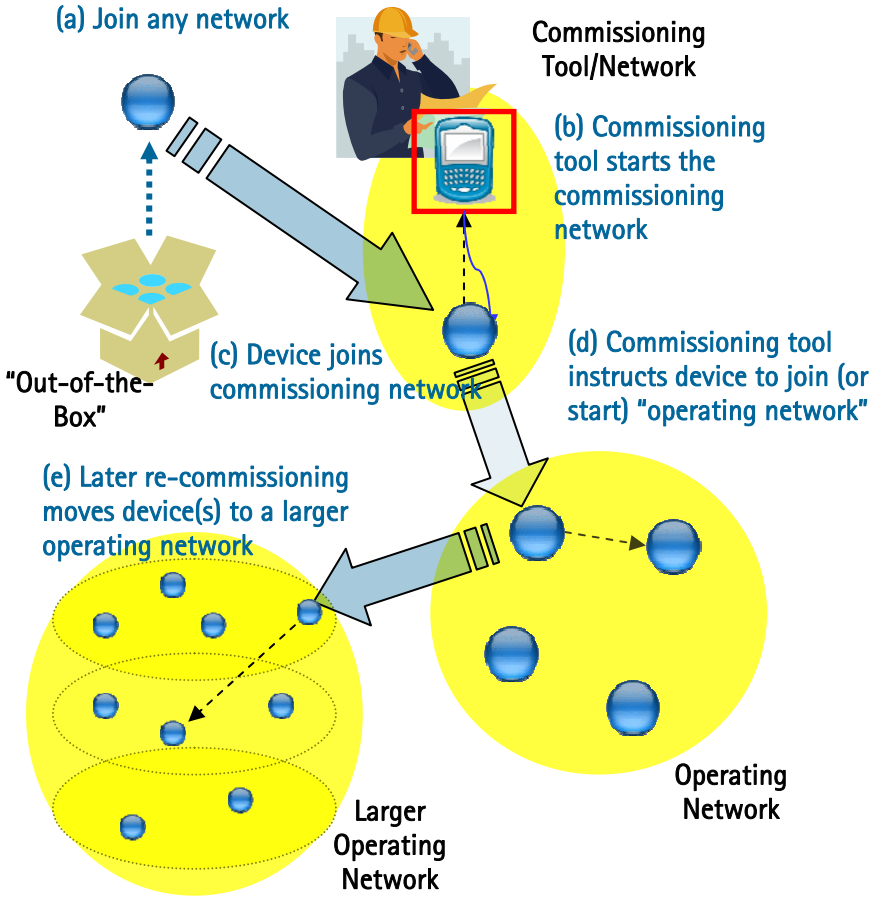
When you look at the number of tasks involved in commissioning, and consider that many installers are likely to have limited knowledge of the underlying technologies, it's easy to see the value of a commissioning tool.

These tools, which typically run on a laptop or PDA, are designed to make life easier for installers. They provide an intuitive user interface that hides the complexity of the underlying technology, and offer flexibility in allowing installers the means to visualize the network and devices, and options to configure, commission and manage the system.

Commissioning tools are generally not intended to be part of the network in its ongoing operational use, and simply facilitate commissioning or ongoing maintenance or management without being part of the primary application.

Commissioning Example

The following shows a typical commissioning scenario:



(a) A new "out-of-the-box" device is at its most flexible, and able to join any network.

(b) An installer uses a dedicated tool to starts a "Commissioning Network" through which devices can be commissioned and configured.

(c) The new device joins the Commissioning Network.

(d) The installer uses the tool to commission the device, so that it can join the correct network, using the correct security, and with the correct bindings.

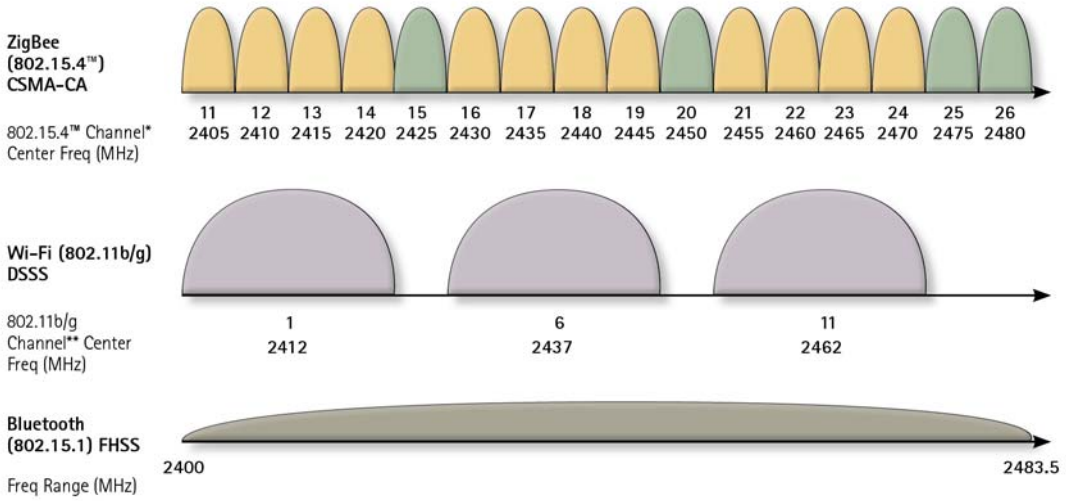
(e) If required, live networks can also be commissioned, for example to combine several smaller networks into one large one.

ZigBee Channels and Frequencies

The RF spectrums and available channels for ZigBee (802.15.4) and Wi-Fi (802.11b/g) overlap. You can avoid interference by selecting ZigBee channels that use the free space between two neighboring 802.11 channels, plus channels 25 and 26.

ZigBee, Wi-Fi & Bluetooth Channels

In the image below, 802.15.4 Orange channels have more substantial overlap with Wi-Fi channels 1, 6 & 11, while Grey channels have less overlap with Wi-Fi channels 1, 6 & 11.



Channels 1, 6 & 11 are recommended for use in the USA. Only 2.4 GHz channels are shown above. Different countries have different 802.11 b/g channels.

Channels and Frequencies

Channel Logical Sequence Num	Channel Number (Decimal)	Channel Number (Hex)	Frequency MHz
868 MHz Band			
1	0	0	868.3
915 MHz Band			
1	1	01	906
2	2	02	908
3	3	03	910
4	4	04	912
5	5	05	914
6	6	06	916
7	7	07	918
8	8	08	920

9	9	09	922
10	10	0A	924
2.4 GHz Band			
1	11	0B	2405
2	12	0C	2410
3	13	0D	2415
4	14	0E	2420
5	15	0F	2425
6	16	10	2430
7	17	11	2435
8	18	12	2440
9	19	13	2445
10	20	14	2450
11	21	15	2455
12	22	16	2460
13	23	17	2465
14	24	18	2470
15	25	19	2475
16	26	1A	2480

ZigBee 2006 and PRO

The table below shows a summary of key differences between the ZigBee (2006) and ZigBee PRO (2007) releases of the ZigBee specification. A more detailed comparison matrix is available at www.daintree.net/resources/spec-matrix.php

		2006	PRO
Interference avoidance			
	Coordinator selects best available RF channel/Network ID at startup time.	✓	✓
	RF channel and/or Network ID can be changed during operation to address interference.		✓
Automated/distributed address management			
	Addresses automatically assigned using hierarchical, distributed scheme.	✓	
	Addresses automatically assigned using stochastic scheme.		✓
Group addressing			
	Devices can be assigned to groups, which can be addressed with a single frame; thereby reducing network traffic for packets destined for groups.	✓	✓
Centralized data collection			
	Low-overhead data collection by ZigBee coordinator supported.	✓	✓
	Low-overhead data collection by other devices supported under special circumstances (e.g. with Tree Routing).	✓	✓
	Many-to-one routing allows the whole network to discover the aggregator in one pass.		✓
	Source routing allows the aggregator to respond to all senders in an economical manner.		✓
Security			
	128-bit AES encryption with 32-bit Message Integrity Code (MIC).	✓	✓
	Frame counters to assure message freshness.	✓	✓
	Security applied at the NWK layer by default, and supported at higher layers.	✓	✓
	Key rotation prevents hacking of NWK key.	✓	✓

	Trust Center operates on the ZigBee Coordinator to manage trust on behalf of network devices and act as central authority on which devices can join the network.	✓	✓
	High Security mode supported, which is selectable by Trust Center policy, and requires Application Layer Link Keys, peer-entity authentication, and peer-to-peer establishment using Master Keys.		✓
	Trust Center can run on Coordinator or any other device in the network.		✓
Network scalability			
	Addressing algorithm supports networks with tens to hundreds of devices.	✓	
	Addressing algorithm supports networks with hundreds to thousands of devices.		✓
Message size			
	< 100 bytes, with exact size depending on services employed (e.g. security).	✓	
	Large messages, up to the buffer capacity of the sending and receiving devices (supported using Fragmentation and Reassembly).		✓
Standardized commissioning			
	Standardized startup procedure and attributes support the use of commissioning tools in a multi-vendor environment.	✓	✓
Robust mesh networking			
	Fault tolerant routing algorithms respond to changes in the network and in the RF environment.	✓	
	Every device keeps track of its "neighborhood"; thereby improving reliability and robustness.		✓
Cluster Library support			
	The ZigBee Cluster Library, as an adjunct to the stack, standardizes application behavior across profiles and provides an invaluable resource for profile developers.	✓	✓