ZigBee Document 053516r12

ZigBee Building Automation Standard

ZigBee Building Automation Application Profile 0x0105

Revision 12

Version 1.0

May-2011

Sponsored by:
ZigBee Alliance

Accepted for release by:
ZigBee Alliance Board of Directors.

Abstract:
This document defines the ZigBee Building Automation Application Profile.

Keywords:
ZigBee, Profile, Commercial Building Automation, ZigBee Building Automation, ZBA, CBA, Application Framework.

ZigBee Alliance, Inc.
2400 Camino Ramon, Suite 375
San Ramon, CA 94583, USA

Participants

When the document was released, the ZigBee Building Automation Profile Task Group leadership was composed of the following members:

Rudy Belliardi: *Chair*
Jerry Martocci: *Vice chair*
Cam Williams: *Technical Editor*

Contributions were made to this document by the following members:

Rudy Belliardi	Mark Hiniker	Eetay Natan
Peter Burnett	Phil Jamieson	Bob Old
Jason Choong	Tim Hirou	Dalila Pinedo
David Clark	Ted Humpal	Isaac Pinhas
Ettore Colicchio	William Keith	Phil Rudland
Kent Crouse	Jens Klostergaard Lyngsø	Zachary Smith
Christian Garcia	Chuck Lehn	Joel VanderZee
Drew Gislason	Jared Lemke	Urban Wicklander
Tim Gillman	Jerry Martocci	Cam Williams

Table of Contents

List of Figures

List of Tables

Change history

Table 1 shows the change history for this specification.

Table 1 – Document revision change history

Revision	Version	Description
0	0.1	Original version.
1	0.1	Changed the frame structure. Added more detail to the lighting device descriptions. Added support for pump devices.
2	0.1	Moved all the cluster specifications to library files. Streamlined the rest of the document accordingly.
3	0.2	Updated to correspond to latest revisions of the ZCL documents, and to be consistent with rev 16 of the Home Automation profile. Note – this revision is a working draft.
4	0.3	Added IAS device descriptions, the same as in the HA profile. Reworked Ballast device descriptions. Added scope text. Started list of *PhysicalEnvironment* constants that might be appropriate for CBA.
5	0.3	Added Alarms server cluster to most device descriptions. Added humidity sensor. Removed Scenes cluster from IAS device descriptions, as the IAS clusters do not have scene capability. Tidied up the text in many places.
6	0.4	Removed the Heating/Cooling Unit. This may be replaced by one or more other HVAC devices in the next revision. Added the following candidate ZigBee Cluster Library material as an annex:- Generic Tunnel cluster, BACnet Protocol Tunnel cluster, Generic Input, Output and Value clusters. Also reserved sections in the annex for new data types Array and Set, extensions to the attribute r/w commands to handle these new types, and an updated Alarms cluster. (NB This is an incomplete interim revision for discussion at the ZigBee Members meeting Feb. 2007)
7	0.5	Completed definition of new data types Array and Set, plus extensions to the attribute r/w commands to handle these new types. Completed definitions of Generic Tunnel cluster, BACnet Protocol Tunnel cluster, Generic Input, Output and Value clusters. Added BACnet constructed and tunneled devices.
8	0.6	Updated according to resolutions of letter ballot LB17 (document number 074863). Added commissioning details including Startup Attribute Set (SAS).
9	0.7	Updated according to resolutions of letter ballot LB27 (document number 075203). Added a list of 'deferred decisions'.
10	0.7	A few editorial corrections and clarifications.
11	0.9	Rolled errata in, major additions: Security Policy and Life Cycle
12	0.9	Addressed ZARC comments to r11 and CCBs from testing

1 Introduction

1.1 Scope

This profile defines device descriptions and standard practices for applications needed in a commercial building environment. Such an environment typically has the following characteristics:-

- Coverage of up to 100,000 square feet (approx. 10,000 m^2) or more.
- Professionally managed.
- The building may have unrestricted access, with attendant security implications.
- Interworking with installed base of existing products on other networks may be important.

The key application domains included in this initial version are lighting, closures, Intruder Alarm Systems, and some aspects of HVAC. Other applications domains may be added in future versions.

1.2 Purpose

This specification provides standard interfaces and device descriptions to allow interoperability among ZigBee devices produced by various manufacturers of commercial building automation products.

2 References

The following standards and specifications contain provisions, which through reference in this document constitute provisions of this specification. All the standards and specifications listed are normative references. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the standards and specifications indicated below.

2.1 ZigBee Alliance documents

[R1] ZigBee document 074855, ZigBee-Pro Stack Profile

[R2] ZigBee document 053474, ZigBee Specification

[R3] ZigBee document 07123, ZigBee Cluster Library Specification: General Specification chapter

[R4] ZigBee document 07123, ZigBee Cluster Library Specification: Measurement and Sensing Specification chapter

[R5] ZigBee document 07123, ZigBee Cluster Library Specification: Lighting Specification chapter

[R6] ZigBee document 07123, ZigBee Cluster Library Specification: Closures Specification chapter

[R7] ZigBee document 07123, ZigBee Cluster Library Specification: Security and Safety Specification chapter

[R8] ZigBee document 07123, ZigBee Cluster Library Specification: HVAC Specification chapter

[R9] ZigBee document 07123, ZigBee Cluster Library Specification: Foundation Specification chapter

[R10] ZigBee document 053520, Home Automation Profile Specification

[R11] ZigBee document 064309, Commissioning Framework

[R12] ZigBee document 07123, ZigBee Cluster Library Specification

2.2 European Standards Documents

[R13] EN 50131 European Standards Series for Intruder Alarm Systems

2.3 ASHRAE documents

[R14] ASHRAE 135-2004 standard, Data Communication Protocol for Building Automation and Control Networks

3 Definitions

3.1 Conformance levels

Expected: A key word used to describe the behavior of the hardware or software in the design models *assumed* by this profile. Other hardware and software design models may also be implemented.

May: A key word indicating a course of action permissible within the limits of the standard (may equals is permitted).

Shall: A key word indicating mandatory requirements to be strictly followed in order to conform to the standard; deviations from shall are prohibited (shall equals is required to).

Should: A key word indicating that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or, that (in the negative form) a certain course of action is deprecated but not prohibited (should equals is recommended that).

3.2 ZigBee Definitions

Attribute: A data entity which represents a physical quantity or state. This data is communicated to other devices using commands.

ZBA Default Settings: stack settings with ZBA default values that include the ZBA EPID, ZBA Key Material, etc.

ZBA EPID: ZBA default EPID

ZBA Link: link between ZBA endpoints on ZBA devices

ZBA SAS: ZBA default Commissioning Cluster SAS

ZBA Key Material: ZBA default ZBA Key Material

Cluster: A collection of related attributes and commands, which together define a communications interface between two devices. The devices implement server and client sides of the interface respectively.

Cluster identifier: A 16-bit number unique within the scope of an application profile which identifies a specific cluster.

Commissioning Network: a temporary network created to commission a network before the Operational Network is created. A commissioning network may have limited operational capabilities for security reasons.

Device: A device consists of one or more ZigBee device descriptions (e.g. for on/off switch, ballast etc.) and their corresponding application profile(s), each on a separate endpoint, that share a single 802.15.4 radio. Each device has a unique 64-bit IEEE address.

Device description: A collection of clusters and associated functionality implemented on a ZigBee endpoint. Device descriptions are defined in the scope of an application profile. Each device description has a unique identifier that is exchanged as part of the discovery process.

Decommission: to return to ZBA Default Settings with the default ZBA Key Material and ZBA EPID and power down the device so it is ready to put back in the box

Island Network: a network that allows nodes to join with neighbors with little or no interaction with higher level nodes, such as a Coordinator (ZC), Trust Center (TC), or Commissioning Tool (CT). Later, the island can be integrated into an Operational Network, by interaction with a TC or CT, or by doing nothing at all (passive). Passive coalescing can occur if the Stack Parameters are correct for the Operational Network. Island networks are required for the common practice of installing systems from the bottom up without a ZC or TC.

Key Material: security key and corresponding sequence number

Node: A device that runs a ZigBee stack so as to be capable of joining a ZigBee network.

Operational Network: a network defined by having an EPID in the operation range and is the normal operating state of the network.

Product: A product is a unit that is intended to be marketed. It may implement a combination of private, published, and standard application profiles.

Service discovery: The ability of a device to locate services of interest.

Stack Parameters: persistent parameters within the ZigBee stack that determine how and which network a node joins when it is reset or powered up.

ZigBee coordinator: An IEEE 802.15.4-2003 PAN coordinator.

ZigBee end device: an IEEE 802.15.4-2003 RFD (Reduced Function Device) or FFD (Full Function Device) participating in a ZigBee network, which is neither the ZigBee coordinator nor a ZigBee router.

ZigBee router: an IEEE 802.15.4-2003 FFD (Full Function Device) participating in a ZigBee network, which is not the ZigBee coordinator but may act as an IEEE 802.15.4-2003 coordinator within its personal operating space, that is capable of routing messages between devices and supporting associations.

1

4 Acronyms and abbreviations

ALK	Application Link Key
CBA	Commercial Building Automation now called ZBA
CT	Commissioning Tool
TC	Trust Center
ZC	ZigBee Coordinator
ZBA	ZigBee Building Automation (same as CBA)
ZCL	ZigBee Cluster Library
ZED	ZigBee End Device
ZR	ZigBee Router

2

5 Profile Description

5.1 ZigBee Pro stack profile

Products that conform to this specification shall use the ZigBee Pro stack profile, as defined in [R1]. In addition to the requirements specified in [R1], the following requirements are mandatory for this application profile.

- Fragmentation is permitted for any device (node), but only required if the device implements one or more clusters that require fragmentation. See 5.4 for details.
- Source binding shall be implemented (except for any device descriptions which explicitly state otherwise).
- The source binding table shall at minimum include space for one entry for every cluster (client or server), across all endpoints, that generates an unsolicited command (e.g. a request or an attribute report).
- In their normal operating state, ZigBee end devices shall poll no more frequently than once every 7.5 seconds except where this specification indicates otherwise for a particular device description (e.g. the IAS WD), or under the following conditions. ZigBee end devices may operate with a higher polling rate during commissioning, network maintenance, alarm states, and for short periods after transmitting a message to allow for acknowledgements and or responses to be received quickly, but they must return to the standard rate indicated previously during normal operation. It is recommended that ZigBee end devices poll much less frequently than once per 7.5 seconds, especially when the device normally only communicates due to user interaction (e.g. the On/Off Light Switch).

5.2 Device descriptions

Device descriptions specified in this profile are summarized in Table 2 along with their respective Device IDs. The device descriptions are organized according to the end application areas they address. A product that conforms to this specification shall implement at least one of these device descriptions and shall also include the device descriptions corresponding to all applications implemented on the product where a standard device description is specified in this profile. For example, if a product implements both a light dimmer and a light sensor application, then the Dimmable Light and Light Sensor device descriptions must both be supported.

This list will be added to in future versions of the profile as new device descriptions and clusters are developed to meet the needs of manufacturers. The reserved values shall not be used until the profile defines them. Manufacturer specific device descriptions shall reside on a separate endpoint and use a private profile ID.

Table 2 – Devices Descriptions specified in the ZBA profile

	Device Description	Device ID
Generic	On/Off Switch	0x0000
	Level Control Switch	0x0001
	On/Off Output	0x0002
	Level Controllable Output	0x0003
	Scene Selector	0x0004
	Configuration Tool	0x0005
	Remote Control	0x0006
	Combined Interface	0x0007

	Range Extender	0x0008
	Mains Power Outlet	0x0009
	Constructed BACnet Device	0x000A
	BACnet Tunneled Device	0x000B
	Reserved	0x000C – 0x00FF
Lighting	On/Off Light	0x0100
	Dimmable Light	0x0101
	Color Dimmable Light	0x0102
	On/Off Light Switch	0x0103
	Dimmer Switch	0x0104
	Color Dimmer Switch	0x0105
	Light Sensor	0x0106
	Occupancy Sensor	0x0107
	On/Off Ballast	0x0108
	Dimmable Ballast	0x0109
	Reserved	0x010A – 0x1FF
Closures	Shade	0x0200
	Shade Controller	0x0201
	Reserved	0x0202 – 0x2FF
HVAC	Reserved	0x0300
	Thermostat	0x0301
	Temperature Sensor	0x0302
	Pump	0x0303
	Pump Controller	0x0304
	Pressure Sensor	0x0305
	Flow Sensor	0x0306
	Humidity Sensor	0x0307
	Reserved	0x0308– 0x3FF
Intruder Alarm Systems	IAS Control and Indicating Equipment	0x0400
	IAS Ancillary Control Equipment	0x0401
	IAS Zone	0x0402
	IAS Warning Device	0x0403
	Reserved	0x0404 -0x4FF
	Reserved	0x0500 - 0xFFFF

1

5.3 ZigBee Cluster Library (ZCL)

This profile utilizes the clusters specified in the ZigBee Cluster Library (ZCL). The Cluster IDs used for the clusters are those given in the ZCL.

The implementation details for each cluster are given in the ZCL specifications. Further specification and clarification is given in this profile where necessary.

The minimum reporting interval specified in the ZCL [R9] shall be set to a value greater than or equal to one second. The maximum reporting interval should be set to zero by default, and if it is set to a non-zero value it shall be set to a value greater than or equal to one minute and greater than the value of the minimum reporting interval. These settings will restrict the attributes from being reported more often than once every second if the attribute is changing quickly and at least once every minute if the attribute does not change for a long time. It is recommended that the minimum reporting interval be set to a higher value whenever the application can tolerate it. It is recommended that the maximum reporting interval be set to a much greater value to avoid unnecessary traffic.

5.4 Clusters used in this profile

The clusters used in this profile, are listed in Table 3. The clusters are listed according to the functional domain they belong to in the ZCL. The corresponding cluster identifiers can be found in the ZCL Foundation specification [R9].

The functionality made available by all supported clusters shall be that given in their ZCL specifications except where a device description in this profile includes further specification, clarification or restriction as needed for a particular device.

Most clusters include optional attributes. The application designer must be aware that optional attributes may not be implemented on a particular device. It is the responsibility of a device's application to discover and deal with unsupported attributes on other devices.

It is expected that clusters will continue to be developed in the ZCL that will be useful in this profile. In many cases, new clusters will be organized into new device descriptions that are separate from those currently defined. There may also be situations where it makes sense to add clusters as new optional elements of existing device descriptions.

Adding a new mandatory cluster to a device description should not be done except by creating a new device ID and accompanying device description, as adding it to an existing device description would cause backward compatibility issues.

Manufacturer specific clusters may be added to any device description in this profile as long as they follow the specifications given in the ZCL Foundation specification [R9].

Unless otherwise stated, no clusters used or defined in this profile require fragmentation. However, if fragmentation is supported certain operations (e.g. reading all attributes) may become possible in a single command rather than multiple commands.

Table 3 – Clusters used in the ZBA profile

Functional Domain	Cluster Name
General	Basic
General	Power Configuration
General	Device Temperature Configuration
General	Identify
General	Groups

Functional Domain	Cluster Name
General	Scenes
General	On/Off
General	On/Off Switch Configuration
General	Level control
General	Alarms
General	Time
General	RSSI Location
General	Analog Input (Basic)
General	Analog Output (Basic)
General	Analog Value (Basic)
General	Binary Input (Basic)
General	Binary Output (Basic)
General	Binary Value (Basic)
General	Multistate Input (Basic)
General	Multistate Output (Basic)
General	Multistate Value (Basic)
Measurement & Sensing	Illuminance Measurement
Measurement & Sensing	Illuminance Level Sensing
Measurement & Sensing	Temperature Measurement
Measurement & Sensing	Pressure Measurement
Measurement & Sensing	Flow Measurement
Measurement & Sensing	Relative Humidity Measurement
Measurement & Sensing	Occupancy Sensing
Lighting	Ballast Configuration
Lighting	Color Control
HVAC	Pump Configuration and Control
HVAC	Thermostat
HVAC	Fan Control
HVAC	Thermostat User Interface Configuration
Closures	Shade Configuration
Security and Safety	IAS ACE
Security and Safety	IAS Zone
Security and Safety	IAS WD
Protocol Interfaces	Generic Tunnel
Protocol Interfaces	BACnet Protocol Tunnel
Protocol Interfaces	Analog Input (BACnet Regular)
Protocol Interfaces	Analog Input (BACnet Extended)
Protocol Interfaces	Analog Output (BACnet Regular)
Protocol Interfaces	Analog Output (BACnet Extended)
Protocol Interfaces	Analog Value (BACnet Regular)

Functional Domain	Cluster Name
Protocol Interfaces	Analog Value (BACnet Extended)
Protocol Interfaces	Binary Input (BACnet Regular)
Protocol Interfaces	Binary Input (BACnet Extended)
Protocol Interfaces	Binary Output (BACnet Regular)
Protocol Interfaces	Binary Output (BACnet Extended)
Protocol Interfaces	Binary Value (BACnet Regular)
Protocol Interfaces	Binary Value (BACnet Extended)
Protocol Interfaces	Multistate Input (BACnet Regular)
Protocol Interfaces	Multistate Input (BACnet Extended)
Protocol Interfaces	Multistate Output (BACnet Regular)
Protocol Interfaces	Multistate Output (BACnet Extended)
Protocol Interfaces	Multistate Value (BACnet Regular)
Protocol Interfaces	Multistate Value (BACnet Extended)

5.5 Notes on the Status of this profile

The following functionality has been deferred for consideration during development of a future version of the profile.

1. 'Heartbeat' functionality, e.g. provided by a new cluster, to provide assurance that no device has unintentionally left the network.
2. Network diagnostics, e.g. provided by means of a new cluster.
3. A means of allowing more than one cluster of the same type to be on the same endpoint, to facilitate forming devices from the Input, Output and Value clusters.
4. A means of reading / writing attributes on multiple endpoints on the same node via a single command, for efficiency and to preserve time coherency.
5. An alarm facility with functionality closer to that provided by BACnet than the functionality currently provided by the ZCL Alarms cluster [R3].

6 Constants

6.1 Profile Parameters

Profile-specific constants are shown in Table 4.

Table 4 – Constants Specific to the ZBA Profile

Constant	Description	Value
Application Link Keys	Application Link Keys are supported	true
Application Profile Identifier	Value of the Application Profile Identifier for use in the Simple Descriptor of any endpoint supporting this profile.	0x0105
Config_EndDev_Bind_Timeout	Time to visit two devices to perform E-Mode commissioning	60
minZBAGroups	Minimum number of groups that shall be supported per node, across all endpoints on that node.	16
minZBAScenes	Minimum number of scenes that shall be supported per node, across all groups on all endpoints on that node. This only applies to nodes that implement the server-side of the Scenes cluster on at least one endpoint.	16
Key Type	This is the type of key required for ZBA security policies	Trust Center Link Key
TCSendNetworkKeyInClear	A Network Key shall never be sent from a Trust Center on an operational network without using a Trust Center Link Key	false
Values of the *PhysicalEnvironment* attribute of the Basic cluster for use with this profile.	Values specified by Home Automation [R10] Break Room Cafeteria Conference Room Copy Room Corridor Cubicle Employee Entrance Janitor's Closet Lobby Machinery Room Mail Room Parking Area Restroom (toilet) Men's Room (toilet) Women's Room (toilet) Production Floor Server Room Waiting Room	0x01 – 0x4f 0x50 0x51 0x52 0x53 0x54 0x55 0x56 0x57 0x58 0x59 0x5a 0x5b 0x5c 0x5d 0x5e 0x5f 0x60 0x61 0x62

	Show Room Store Room Training Room Reserved for future additions Available for use by vendors	0x63 0x64 0x65- 0x6f 0x70 - 0x7f

6.2 APS Fragmentation Parameters

For fragmentation there are application settings from the APS IB that must be defined by the application profile. For ZBA these parameters are to be set as shown in Table 5.8.

In addition the Maximum Incoming Transfer Size Field in the Node descriptor defines the largest ASDU that can be transferred using fragmentation. Maximum ASDU size allowed is specified in [B4] and dictated by solution needs and RAM capacities of the communicating devices.

It is highly recommended all devices first query the Node Descriptor of the device it will communicate with to determine the Maximum incoming transfer . This will establish the largest ASDU that can be supported with fragmentation. The sending device must use a message size during fragmentation that is smaller than this value.

Table 6 APS Transport Parameters

Parameters	Identifier	Type	Value	Description
apsInterframeDelay	0xC9	Integer	12	Standard delay in milliseconds between sending two blocks of a fragmented transmission (see [B4] sub-clause 2.2.8.4.5)
apsMaxWindowSize	0xCD	Integer	3	Fragmentation parameter – the maximum number of unacknowledged frames that can be active at once (see [B4] sub-clause 2.2.8.4.5).

7 Security Policy

The goal of the ZBA Security policy is to allow flexibility such that each network shall be able to have its security requirements met, without sacrificing interoperability. Some vendors do not want to manage security at all. Other vendors might want rotating Network Keys and/or Application Link Keys for node-to-node communication. Others might want a hybrid with only a few secure links like a door and a controller talking with an Application Link Key.

A Trust Center (TC) Link Key is a valid Link Key that shall be shared between a node and the Trust Center.

7.1 Network Security Types

ZBA allows the use of a default and well-known Network Key and Key Sequence Number (ZBA Network Key Material) and default and well-known TC Link Key (ZBA TC Link Key). This effectively leaves the network non-secure.

There are three general types of ZBA security and they are:

Default Security – Commissioning or Operational Network

The Key Material is the ZBA Key Material. EPID is either in the commissioning or operational range.

Network Security – Network Key and TC Link Keys

All nodes have a TC Link Key and a Network Key.

Application Security – Application Link Keys

Some nodes have Application Link Keys to talk to each other. The rest of the network is as secure as the Network Key.

7.2 Node Policy

- The security mode is ZigBee Standard Security where a Network Key and TC Link Key are mandatory.
- There shall be a method to decommission a node to return to the ZBA Default Settings with the default ZBA Key Material and ZBA EPID.
- A ZBA node may support out of band pre-loading of Network, TC Link, and Application Link keys before joining an operational network.
- A ZBA node shall accept an unsolicited TC Link Key from the TC.

7.3 Trust Center Policy

- Even if a node has the proper keys to be on the network, the Trust Center may determine that a node is not authorized to be on the network.
- If the Trust Center determines that a node is not authorized to be on the network, it shall issue a Remove Device command to the parent of the node.
- All unicast APS transport key messages between a TC and a device shall be encrypted with the device's TC Link Key including those messages used to transport a Network Key to a joining or rejoining device.
- The Trust Center may allow devices that have never joined, and do not have the Network Key, to join.

- The Trust Center may allow a device to request a new TC Link Key.
- The Trust Center may broadcast or unicast a new Network Key to update the network. When broadcast, the Network Key transport message shall be encrypted with the current Network Key. When unicast, the Network Key transport message shall be encrypted with the proper TC Link. Unicast may be used to remove devices by omitting such devices from the update.
- The TC shall support ALK requests. The TC may allow all ALK requests or optionally determine which devices are authorized to make ALK requests. The TC may also constrain ALK use to particular links.

7.4 Joining Policy

A node shall never accept the Network Key sent in the clear.

7.5 Rejoining Policy

1. If the node has a Network Key, then the node shall perform a secure rejoin.
2. If the secure rejoin fails, the node shall initiate an unsecured rejoin. If the TC authorizes the node, then the TC shall tunnel the Network Key to the node, using the TC Link Key (see [R2] 3.6.1.4.2).

7.6 Application Link Key Policy

At this time, ZBA does not specify an Application Link Key Policy, because ZigBee does not specify a policy for managing Application Link Key deletion.

7.7 Commissioning Cluster Policy

After a node enters the Operational Network, which uses an Operational EPID, it shall not allow read or write access to the attributes of the Commissioning Cluster, not shall it support the Restart command.

The corresponding read or write attribute response status record, or Restart response status, shall be set to NOT_AUTHORIZED.

8 Life Cycle Flowcharts

The following flowcharts describe the life cycle of a ZBA node. There may be other transitions and/or states that are valid for a ZBA node, but these charts show typical states and transitions.

Most states are required, but some are specific to a vendor implementation. Those states, and therefore transitions to the state, that are not required, are noted as such.

8.1 Commissioning Flowchart by Network

The following flowchart (Figure 8-1) describes commissioning at a high level by the function of the network joined.

As shown, there shall always be an on-board published and non-proprietary means to get a node back to the ZBA Default Settings state.

Factory Settings are implementation dependent and may not be the ZBA Default Settings.

Darker shapes below are ZBA specific requirements. Lighter states are ZigBee specific requirements and clear shapes are vendor specific, which are up to the implementation, and therefore not required.

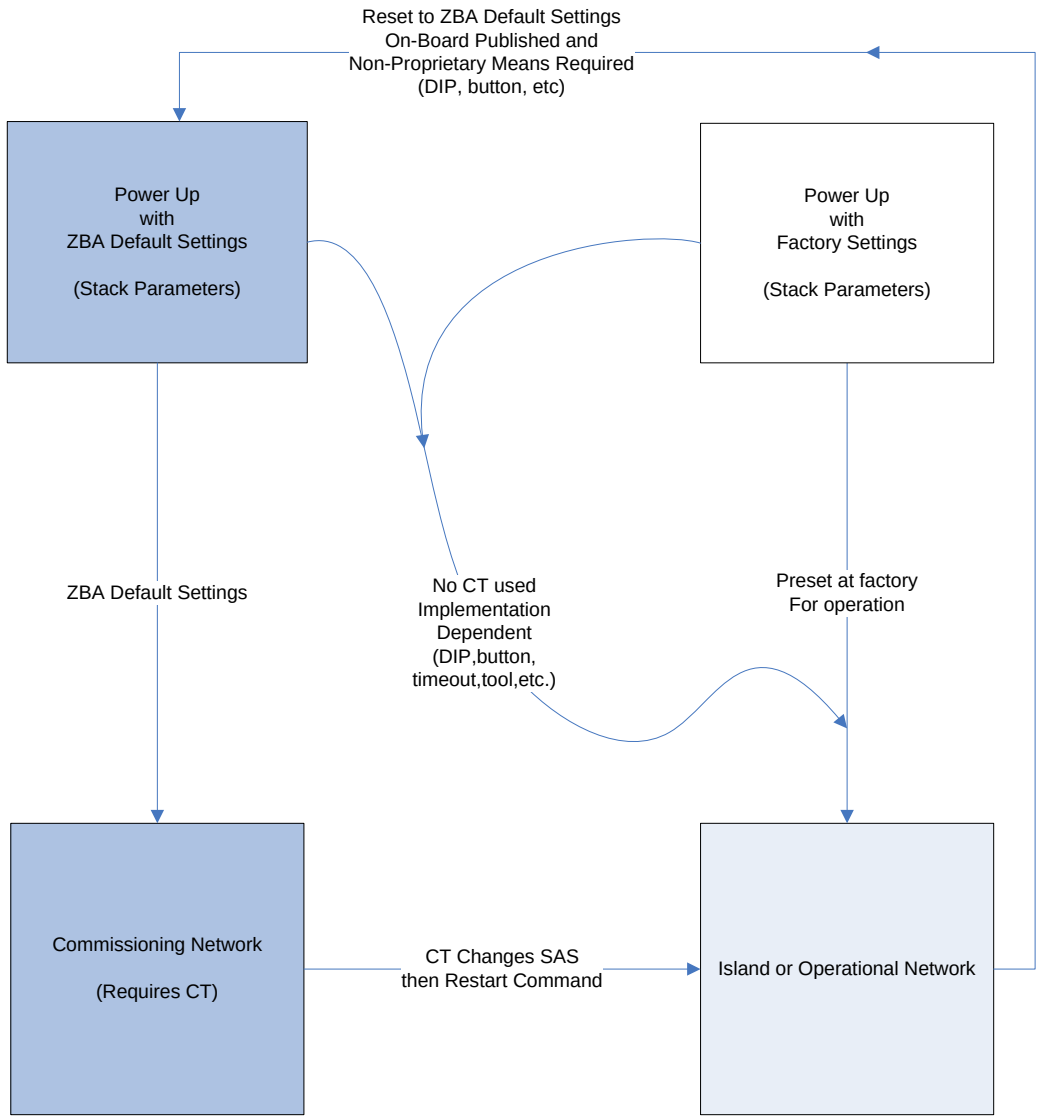

Figure 8-1

8.2 Commissioning Flowchart

The following flowchart (Figure 8-2) shows a ZBA node life cycle, from being turned on from the factory. At any point the node may be reset or lose power and then must start at Power Cycle. The same is true for Reset to ZBA Default. To passively coalesce such islands of nodes, that have no ZC, but use the same EPID, they would have to be on the same channel.

A vendor implementation may define a time out on loops that are discovery processes, such as finding a TC, or joining a network. When such a time-out occurs, it is recommended that processing restart at Power Cycle.

Darker states below are ZBA specific requirements. Lighter states are ZigBee specific requirements and clear shapes are vendor specific, which are up to the implementation, and therefore not required. If decision diamonds that are vendor specific (clear), are not implemented, take the “no” transition.

The Fall Back Network Key referenced in the ‘Check TC Start’ sub-routine shall be 0x0000000000000001.

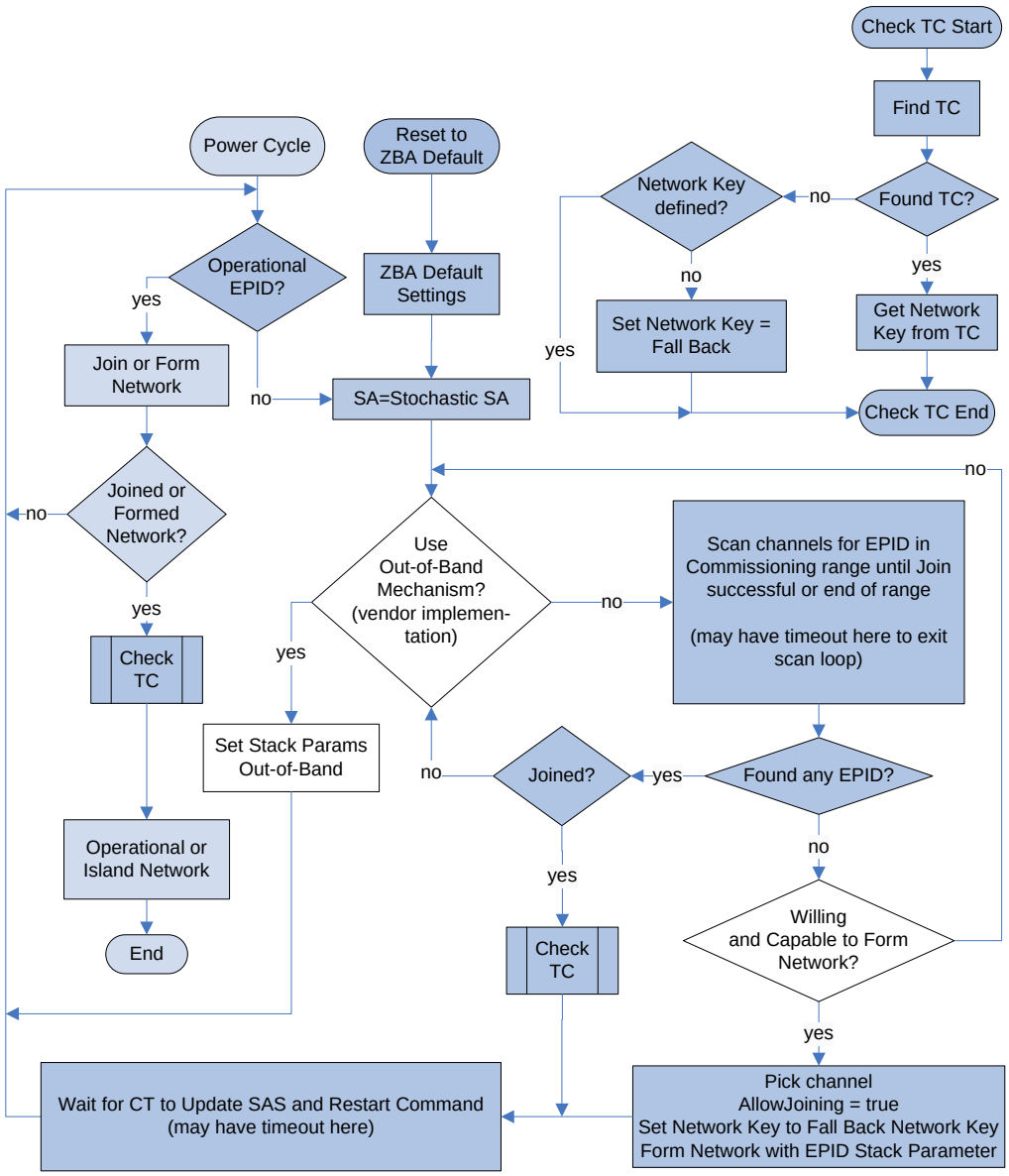

Figure 8-2

9 Device Descriptions

9.1 Terminology

The term 'device' is mainly used in this section to indicate the functionality described by a Device Description, as opposed to the physical node on which this functionality is implemented (see 3.2).

9.2 Mandatory and Optional Clusters

Each device description provides a list of mandatory clusters.

It also provides a list of optional clusters. These clusters, if implemented, have a known (and described if not obvious) role in device operation and interaction with the other clusters present in the device, and are considered part of the device from the point of view of this profile.

9.2.1 Common Clusters

Support for certain clusters is common to all the device descriptions in this profile. In order to reduce the size of the tables in the various device descriptions, these clusters are not shown in these tables, but are gathered together in Table 5. The clusters shown in Table 5 shall be supported by all devices descriptions in this profile as mandatory or optional according to the designation given here. Individual device descriptions may place further restrictions on support of the optional clusters.

Table 5 – Clusters common to all device descriptions

Server side	Client side
Mandatory	
Basic	None
Identify	
Groups[1]	
Commissioning (see [R12] for details)	
Optional	
	Basic
	Identify
	Groups
	Commissioning (see [R12] for details)
Clusters with reporting capability (See 9.2.2 for details)	Clusters with reporting capability (See 9.2.2 for details)
Power Configuration	
Device Temperature Configuration	
Alarms	

[1] *The Groups Clusters is required for ZRs and non-sleepy ZEDs. The Groups Cluster is optional for sleepy ZEDs*

Time	
RSSI Location	RSSI Location
Manufacturer specific (See for 9.2.3 details)	Manufacturer specific (See 9.2.3 for details)

9.2.2 Optional support for clusters with reporting capability

Some clusters support the ability to report changes to the value of particular attributes. These reports are typically received by the client side of the cluster. All devices in this profile may support any cluster that receives attribute reports.

9.2.3 Manufacturer specific clusters

The ZCL provides a range of cluster IDs that are reserved for manufacturer specific clusters. Manufacturer specific clusters that conform to the requirements given in the ZCL may be added to any device description specified in this profile.

9.2.4 Use of other ZCL clusters

It is allowed to add any cluster defined in the ZigBee Cluster Library as an optional cluster for any device in this profile.

Any additional cluster added shall be declared on the device PICS and shall be tested in accordance with the base network and security configurations in this document and the messaging and behavior from that specific cluster test plan.

9.3 Generic Device Descriptions

9.3.1 On/Off Switch

The On/Off Switch is capable of sending on, off and toggle commands to devices to switch them on or off. This device should only be used when a more specific device specification (e.g. a On/Off Light Switch) is not available.

9.3.1.1 Supported clusters

In addition to those clusters specified in 9.2.1, the On/Off Switch device shall support the clusters listed in Table 6.

Table 6 – Clusters Supported by the On/Off Switch

Server side	Client side
Mandatory	
	On/Off
Optional	
On/Off Switch Configuration	Scenes
	Groups
	Identify

9.3.1.2 Identify, Groups and Scenes clarification

The Identify, Groups and Scenes client clusters are included in the optional list to allow conformance to the On/Off Switch described in the Home Automation Application Profile.

9.3.2 Level Control Switch

The Level Control Switch device is capable of sending on, off and toggle commands to a wide range of devices to switch them on or off, and which can also control the level of a characteristic of such devices (e.g. brightness of a light or height of a shade). This device should only be used when a more specific device specification (e.g. a Dimmer Switch) is not available.

9.3.2.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Level Control Switch device shall support the clusters listed in Table 7.

Table 7 – Clusters supported by the Level Control Switch

Server side	Client side
Mandatory	
	On/Off
	Level Control
Optional	
On/Off Switch Configuration	Identify
	Groups
	Scenes

9.3.2.2 Identify, Groups and Scenes clarification

The Identify, Groups and Scenes client clusters are included in the optional list to allow conformance to the Level Control Switch described in the Home Automation Application Profile.

9.3.3 On/Off Output

The On/Off Output device is capable of being switched on and off. This device should only be used when a more specific device specification (e.g. a Basic Light) is not available.

9.3.3.1 Supported clusters

In addition to those clusters specified in 9.2.1, the On/Off Output device shall support the clusters listed in Table 8.

Table 8 – Clusters supported by the On/Off Output

Server side	Client side
Mandatory	
On/Off	None
Scenes	
Optional	
None	None

9.3.4 Level Controllable Output

The Level Controllable Output is a device that can be switched on and off, and the output level adjusted. This device should only be used when a more specific device specification (e.g. a Dimmable Light) is not available.

9.3.4.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Level Controllable Output device shall support the clusters listed in Table 9.

Table 9 – Clusters supported by the Level Controllable Output

Server side	Client side
Mandatory	
On/Off	None
Level Control	
Scenes	
Optional	
None	None

9.3.5 Scene Selector

The Scene Selector device is capable of setting up and selecting scenes on other (including groups of) devices.

9.3.5.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Scene Selector device shall support the clusters listed in Table 10.

Table 10 – Clusters supported by the Scene Selector

Server side	Client side
Mandatory	
None	Scenes
	Groups
Optional	
None	Identify

9.3.6 Configuration Tool

The Configuration Tool device is capable of configuring other devices. This device is intended for configuring newly installed devices and may be used for performance optimization thereafter.

The intent of this specification is to define a generic configuration device type. In future versions of the profile, new configuration devices may be specified by explicitly specifying the supported clusters.

9.3.6.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Configuration Tool device shall support all of the mandatory clusters, and may support any of the optional clusters, listed in the table below.

Both client and server (see 9.2.1) forms of the Basic cluster are mandatory, so that the device can interrogate other devices present on the network, and other devices can also interrogate the Configuration Tool device. The Identify client cluster is mandatory so that the device can ask other devices to identify themselves.

Table 11 – Clusters supported by the Configuration Tool

Server side	Client side
Mandatory	
None	Basic
	Identify
Optional	
	Scenes
	Commissioning (see [R12])
None	All other clusters used in this profile (see section 5.4)

9.3.6.2 Notes on Operation

There is potential for conflict between a Configuration Tool and other control devices there may be on the network. Such conflicts are best resolved at a system management level. Technical measures that may be taken to avoid “fighting” for control include use of the Permissions Configuration Table. Recommended practices may be added to a future version of this profile.

9.3.7 Remote Control

The Remote Control device is capable of controlling and monitoring other devices.

Typically the Remote Control device is a handheld, battery powered device, that can control devices (e.g. turn a light on/off), monitor devices (e.g. read the status of a temperature sensor) or do some user configuration (e.g. change the setpoint of a thermostat).

9.3.7.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Remote Control device shall support all of the mandatory clusters, and may support, listed in Table 12.

Both client and server (see 9.2.1) forms of the Basic cluster are mandatory, so that the device can interrogate other devices present on the network, and other devices can also interrogate the Remote Control device. The client side of the Identify cluster is mandatory so that the device can instruct other devices to identify themselves.

The intent of this specification is to define a generic remote control device type. New explicit remote control devices may be specified in future versions by (more) explicitly specifying the supported clusters.

Table 12 – Clusters supported by the Remote Control

Server side	Client side
Mandatory	
None	Basic
	Identify
Optional	
None	On/Off
	Level Control
	Groups
	Scenes
	All other clusters used in this profile (see section 5.4)

9.3.7.2 Notes on Operation

There is potential for conflict between a Remote Control device and other control devices there may be on the network. Such conflicts are best resolved at a system management level. Technical measures that may be taken to avoid “fighting” for control include use of the Permissions Configuration Table. Recommended practices may be added to a future version of this profile.

9.3.8 Combined Interface

The Combined Interface device is capable of controlling and monitoring other devices, and taking on the role of (or simulating) the functionality of clusters supported by this profile. It is typically a mains powered device like a personal computer.

9.3.8.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Combined Interface device shall support all of the mandatory clusters, and may support any of the optional clusters, listed in Table 13.

Both client and server (see 9.2.1) forms of the Basic cluster are mandatory, so that the device can interrogate other devices present on the network, and other devices can also interrogate the Remote Control device. The client side of the Identify cluster is mandatory so that the device can instruct other devices to identify themselves.

Server clusters are included in the optional list, to enable the device to take on the role of (or simulate) the functionality of clusters supported by this profile.

Table 13 – Clusters supported by the Combined Interface Device

Server side	Client side
Mandatory	
None	Basic
	Identify
Optional	
All other clusters used in this profile (see section 5.4)	On/Off
	Level Control
	Groups
	Scenes
	All other clusters used in this profile (see section 5.4)

9.3.8.2 Notes on Operation

There is potential for conflict between a Combined Interface device and other control devices there may be on the network. Such conflicts are best resolved at a system management level. Technical measures that may be taken to avoid “fighting” for control include use of the Permissions Configuration Table. Recommended practices may be added to a future version of this profile.

9.3.9 Range Extender

The Range Extender is a simple device which acts as a router for other devices. The Range Extender device shall not be a ZigBee end device. A product that implements the Range Extender device shall not implement any other devices defined in this profile. This device shall only be used if the product is not intended to have any other application, or if a private application is implemented that has not been addressed by this profile.

9.3.9.1 Supported Clusters

The Range Extender device shall support only the mandatory common clusters specified in 9.1. There are no other mandatory or optional clusters (see Table 14).

Table 14 – Clusters supported by the Range Extender

Server side	Client side
Mandatory	
None	None
Optional	
None	None

9.3.10 Mains Power Outlet

The Mains Power Outlet device is capable of being switched on and off. This device shall control a mains power outlet.

9.3.10.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Mains Power Outlet device shall support the clusters listed in Table 15.

Table 15 – Clusters supported by the Mains Power Outlet

Server side	Client side
Mandatory	
On/Off	None
Scenes	
Optional	
None	None

9.3.11 BACnet Tunneled Device

The BACnet Tunneled device is a flexible device type available to represent devices that offer BACnet functionality over the Generic Tunnel and BACnet Protocol Tunnel clusters.

9.3.11.1 Supported clusters

In addition to those clusters specified in 9.2.1, the BACnet Tunneled device shall support the clusters listed in Table 16.

Table 16 – Clusters supported by the BACnet Tunneled device

Server side	Client side
Mandatory	
Generic Tunnel	Generic Tunnel
BACnet Protocol Tunnel	BACnet Protocol Tunnel
Optional	
None	None

9.3.11.2 Group Id for BACnet Network Broadcast Receive

A unique multicast GroupID shall be associated with each BACnet network on a ZigBee network. A BACnet Tunneled Device shall be a member of the group, identified by the GroupID, associated with each BACnet network that it is connected. This allows a BACnet Tunneled Device to be able to receive BACnet broadcast messages targeting the BACnet network(s) on which it is connected.

9.3.11.3 Group Id for BACnet Network Broadcast Send

Each Generic Tunnel and BACnet Protocol Tunnel clusters pair on an endpoint shall be associated with a BACnet network. For each associated BACnet network, group bindings shall be created for both clusters to the GroupID associated with the BACnet network. This allows the BACnet Tunneled Device to send to the Generic and BACnet Protocol clusters on an endpoint, which in turn sends a group multicast message using the associated GroupID.Constructed BACnet Device

The Constructed BACnet device is a flexible device type available to represent devices constructed from the Generic Input, Output and Value clusters. The physical implementation is manufacturer dependent, and the usage of each cluster may be discovered by reading the ApplicationType and/or other attributes of the relevant cluster, or in other ways.

9.3.11.4 Supported clusters

In addition to those clusters specified in 9.2.1, the Constructed BACnet device shall support at least one of the the clusters listed in Table 17.

1 **Table 17 – Clusters supported by the Constructed BACnet device**

Server side	Client side
Mandatory	
None	None
Optional	
Analog Input (Basic, BACnet Regular, BACnet Extended)	Analog Input (Basic, BACnet Regular, BACnet Extended)
Analog Output (Basic, BACnet Regular, BACnet Extended)	Analog Output (Basic, BACnet Regular, BACnet Extended)
Analog Value (Basic, BACnet Regular, BACnet Extended)	Analog Value (Basic, BACnet Regular, BACnet Extended)
Binary Input (Basic, BACnet Regular, BACnet Extended)	Binary Input (Basic, BACnet Regular, BACnet Extended)
Binary Output (Basic, BACnet Regular, BACnet Extended)	Binary Output (Basic, BACnet Regular, BACnet Extended)
Binary Value (Basic, BACnet Regular, BACnet Extended)	Binary Value (Basic, BACnet Regular, BACnet Extended)
Multistate Input (Basic, BACnet Regular, BACnet Extended)	Multistate Input (Basic, BACnet Regular, BACnet Extended)
Multistate Output (Basic, BACnet Regular, BACnet Extended)	Multistate Output (Basic, BACnet Regular, BACnet Extended)
Multistate Value (Basic, BACnet Regular, BACnet Extended)	Multistate Value (Basic, BACnet Regular, BACnet Extended)

2

3

9.4 Lighting Device Descriptions

9.4.1 On/Off Light

The On/Off Light device is a light that can be switched on and off.

9.4.1.1 Supported clusters

In addition to those clusters specified in 9.2.1, the On/Off Light device shall support the clusters listed in Table 18.

Table 18 – Clusters supported by the On/Off Light

Server side	Client side
Mandatory	
On/Off	None
Scenes	
Optional	
None	Occupancy Sensing

9.4.1.2 Occupancy Sensing cluster support

If an On/Off Light supports the Occupancy Sensing cluster, the action taken upon receipt of a report (indicating a change in state of the *Occupancy* attribute) is left up to the manufacturer. The ability to configure this behavior may be included in a future version of this application profile.

9.4.2 Dimmable Light

The Dimmable Light device is a light that can be switched on and off, and whose luminance level may be controlled.

9.4.2.1 Supported clusters

In addition to those clusters specified in 9.2.1, the dimmable light device shall support the clusters listed in Table 19.

Table 19 – Clusters supported by the Dimmable Light

Server side	Client side
Mandatory	
On/Off	None
Level Control	
Scenes	
Optional	
None	Occupancy Sensing

9.4.2.2 Level Control cluster (server) clarification

The level control cluster shall allow control over the luminance level of the light. The functionality made available by this cluster shall be that given in its specification [R3].

When the Level is set to 0, the light shall be turned fully off. When the level is set to 254, the light shall be turned on to the maximum level possible for the device.

It is recommended that the luminance is interpreted as a logarithmic scale, according to what is given in specification [R13].

9.4.2.3 Occupancy Sensing cluster support

If a Dimmable Light supports the Occupancy Sensing cluster, the action taken upon receipt of a report (indicating a change in state of the *Occupancy* attribute) is left up to the manufacturer. The ability to configure this behavior may be included in a future version of this application profile.

9.4.3 Color Dimmable Light

The Color Dimmable Light device is a light that can be switched on and off, and its luminance, hue, and saturation levels may be controlled.

9.4.3.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Color Dimmable Light device shall support the mandatory clusters, and any of the optional clusters listed in Table 20.

Table 20 – Clusters supported by the Color Dimmable Light

Server side	Client side
Mandatory	
On/Off	None
Level Control	
Color Control	
Scenes	
Optional	
None	Occupancy Sensing

9.4.3.2 Level Control cluster (server) clarification

The level control cluster shall allow control over the luminance level of the light. The functionality made available by this cluster shall be that given in its specification [R3].

When the Level is set to 0, the light shall be turned fully off. When the level is set to 254, the light shall be turned on to the maximum level possible for the device.

It is recommended that the luminance is interpreted as a logarithmic scale, according to what is given in specification [R13].

9.4.3.3 Occupancy Sensing cluster support

If a Color Dimmable Light supports the Occupancy Sensing cluster, the action taken upon receipt of a report (indicating a change in state of the *Occupancy* attribute) is left up to the manufacturer. The ability to configure this behavior may be included in a future version of this application profile.

9.4.4 On/Off Light Switch

The On/Off Light Switch device can send on, off and toggle commands to devices (typically lights) to switch them on or off.

The On/Off Light Switch is identical in functionality to the On/Off Switch (see 9.3.1), and supports the same clusters.

It has a different Device ID (see Table 2) to enable more detailed matching if required, and a more specific icon to be drawn where needed.

9.4.4.1 Supported clusters

In addition to those clusters specified in 9.2.1, the On/Off Light Switch shall support the clusters listed in Table 21.

Table 21 – Clusters Supported by the On/Off Light Switch

Server side	Client side
Mandatory	
Optional	
On/Off Switch Configuration	On/Off
	Scenes
	Groups
	Identify

9.4.5 Dimmer Switch

The Dimmer Switch device can send on, off and toggle commands to devices (typically lights) to switch them on or off, and can also control the level of a characteristic of such devices (typically the brightness of lights).

The Dimmer Switch is identical in functionality to the Level Control Switch 9.3.2 and supports the same clusters.

It has a different Device ID (see Table 2) to enable more detailed matching if required, and a more specific icon to be drawn where needed.

9.4.5.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Dimmer Switch device shall support the clusters listed in Table 22.

Table 22 – Clusters supported by the Dimmer Switch

Server side	Client side
Mandatory	
	On/Off
	Level Control
Optional	
On/Off Switch Configuration	Identify
	Groups
	Scenes

9.4.5.2 Identify, Groups and Scenes clarification

The Identify, Groups and Scenes client clusters are included in the optional list to allow conformance to the Dimmer Switch described in the Home Automation Application Profile.

9.4.6 Color Dimmer switch

The Color Dimmer Switch device can turn a light (or multi-color light) on and off, and control the luminance, hue and saturation levels of a multi-color light.

9.4.6.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Dimmer Switch device shall support the mandatory clusters, and any of the optional clusters, listed in Table 23.

Table 23 – Clusters supported by the Color Dimmer Switch

Server side	Client side
Mandatory	
	On/Off
	Level Control
	Color Control
Optional	
On/Off Switch Configuration	Identify
	Groups
	Scenes

9.4.6.2 Identify, Groups and Scenes clarification

The Identify, Groups and Scenes client clusters are included in the optional client list to allow conformance to the Color Dimmer Switch described in the Home Automation Application Profile.

9.4.7 Light Sensor

The Light Sensor device measures, and may periodically report, the illuminance of an area.

9.4.7.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Light Sensor device shall support the clusters listed in Table 24.

Table 24 – Clusters supported by the Light Sensor

Server side	Client side
Mandatory	
Illuminance Measurement	None
Optional	
None	Groups

9.4.8 Light Level Sensor

The Light Sensor device reports whether the illuminance detected by the sensor is within, above or below a configurable target level range.

9.4.8.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Light Sensor device shall support the clusters listed in Table 25.

Table 25 – Clusters supported by the Light Level Sensor

Server side	Client side
Mandatory	
Illuminance Level Sensing	None
Optional	
None	Groups

9.4.9 Occupancy Sensor

The Occupancy Sensor device reports the occupancy state of an area.

9.4.9.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Occupancy Sensor device shall support the clusters listed in Table 26.

Table 26 – Clusters supported by the Occupancy Sensor

Server side	Client side
Mandatory	
Occupancy sensing	None
Optional	
None	Groups

9.4.10 On/Off Ballast

The On/Off Ballast is a device for starting and regulating fluorescent and discharge lamps, which can be switched on and off, but not dimmed.

9.4.10.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Ballast device shall support the clusters listed in Table 27.

Table 27 – Clusters supported by the On/Off Ballast

Server side	Client side
Mandatory	
On/off	None
Ballast Configuration	
Device temperature configuration	
Power configuration	
Scenes	
Optional	
Illuminance level sensing	Occupancy sensing
	Illuminance level sensing
	Illuminance Measurement

9.4.10.2 On/Off cluster clarification

The *OnOff* attribute of this cluster represents whether the lamps are currently ignited (On) or not (Off).

9.4.10.3 Ballast Configuration cluster clarification

The *MinLevel* and *MaxLevel* attributes of this cluster are lower and upper limits to the *CurrentLevel* attribute of the Level Control cluster. When, during the action of a Move to Level, Move, or Step command, *CurrentLevel* reaches one of these limits, the action shall be terminated (see relevant paragraphs of the Level Control cluster specification).

9.4.10.4 Identify cluster clarification

It is recommended that the identification procedure employed by this device is as follows.

Upon starting the identification procedure, the ballast device should store the value of the *CurrentLevel* attribute of the Level Control cluster. It should then alternate the value of this attribute (and thus the actual light output) between a low and high level, for example *PhysicalMinLevel* and *PhysicalMaxLevel* , remaining on each level for 1 second, for the length of time that the identification procedure is in operation.

Upon termination of the identification procedure, the ballast device should restore *CurrentLightLevel* to the value previously stored when the identify procedure was started.

9.4.10.5 Occupancy sensing cluster clarification

The ballast device shall be configured to receive attribute reports of the *Occupancy* attribute.

The rate of reporting and the action to be taken upon receipt of a report is manufacturer and context dependent. Typically, upon receipt of a report with value "Occupied", the ballast should be turned on. Typically, upon receipt of a report with the value "Unoccupied", the ballast should be turned off.

9.4.10.6 Illuminance level sensing cluster clarification

The ballast device shall be configured to receive attribute reports of the *LevelStatus* attribute.

The rate of reporting and the amount of increase / decrease per report is manufacturer and context dependent. Typically, upon receipt of a report with value "Illuminance below target", the ballast shall be switched on. Upon receipt of a report with value "Illuminance above target", the ballast shall be switched off. Upon receipt of a report with value "Illuminance on target", no action shall be taken.

An illuminance level sensing (server) cluster may optionally be implemented, to allow control of the light by a built in level sensor rather than a remote level sensing device.

9.4.10.7 Illuminance measurement cluster clarification

The illuminance measurement cluster shall optionally be implemented, to receive from a remote light measurement sensor light measurements that input into the optional illuminance level sensing (server) cluster.

9.4.11 Dimmable Ballast

The Ballast is a device for starting and regulating fluorescent and discharge lamps.

9.4.11.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Ballast device shall support the clusters listed in Table 28.

Table 28 – Clusters supported by the Dimmable Ballast

Server side	Client side
Mandatory	
On/off	None
Ballast Configuration	
Device temperature configuration	
Power configuration	
Scenes	
Optional	
Illuminance level sensing	Occupancy sensing
	Illuminance level sensing
	Illuminance Measurement

9.4.11.2 On/Off cluster clarification

The *OnOff* attribute of this cluster represents whether the lamps are currently ignited (On) or not (Off).

9.4.11.3 Level Control cluster clarification

The *CurrentLevel* attribute of this cluster represents the current light level of the ballast device, as given by the dimming light curve described in the Ballast Configuration cluster.

9.4.11.4 Ballast Configuration cluster clarification

The *MinLevel* and *MaxLevel* attributes of this cluster are lower and upper limits to the *CurrentLevel* attribute of the Level Control cluster. When, during the action of a Move to Level, Move, or Step command, *CurrentLevel* reaches one of these limits, the action shall be terminated (see relevant paragraphs of the Level Control cluster specification).

9.4.11.5 Identify cluster clarification

It is recommended that the identification procedure employed by this device is as follows.

Upon starting the identification procedure, the ballast device shall store the value of the *CurrentLevel* attribute of the Level Control cluster. It shall then alternate the value of this attribute (and thus the actual light output) between a low and high level, for example *PhysicalMinLevel* and *PhysicalMaxLevel* , remaining on each level for 1 second, for the length of time that the identification procedure is in operation.

Upon termination of the identification procedure, the ballast device shall restore *CurrentLightLevel* to the value previously stored when the identify procedure was started.

9.4.11.6 Occupancy sensing cluster clarification

The ballast device shall be configured to receive attribute reports of the *Occupancy* attribute.

The rate of reporting and the action to be taken upon receipt of a report is manufacturer and context dependent. Typically, upon receipt of a report with value "Occupied", the ballast should be turned on, or the light level increased. Typically, upon receipt of a report with the value "Unoccupied", the ballast should be turned off, or the light level decreased.

9.4.11.7 Illuminance level sensing cluster clarification

The ballast device shall be configured to receive attribute reports of the *LevelStatus* attribute.

Upon receipt of a report with value "Illuminance below target", the CurrentLevel attribute of the Level Control cluster shall be increased. Upon receipt of a report with value "Illuminance above target", the CurrentLevel attribute of the Level Control cluster shall be decreased. Upon receipt of a report with value "Illuminance on target", no action shall be taken.

The rate of reporting and the amount of increase / decrease per report is manufacturer and context dependent.

An illuminance level sensing (server) cluster may optionally be implemented, to allow control of the light by a built in level sensor rather than a remote level sensing device.

9.4.11.8 Illuminance measurement cluster clarification

The illuminance measurement cluster shall optionally be implemented, to receive from a remote light measurement sensor light measurements that input into the optional illuminance level sensing (server) cluster.

9.5 Closure Device Descriptions

9.5.1 Shade

The Shade provides the ability to open or close window coverings including setting partially open or partially closed states. This device description is applicable to roller shades, drapes, and tilt-only blinds.

9.5.1.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Shade shall support the clusters listed in Table 29.

Table 29 – Clusters supported by the Shade

Server side	Client side
Mandatory	
Shade Configuration	None
On/Off	
Level Control	
Scenes	
Optional	
None	None

9.5.1.2 On/Off cluster (server) clarification

The functionality of the supported On/Off cluster follows the specifications in the dependencies section of the Level Control cluster specification [R3]. For this device, “On” shall mean that the shade is open and “Off” shall mean that the shade is closed (i.e. at the level corresponding to the *ClosedLimit* attribute of the Shade Configuration cluster).

9.5.1.3 Level Control cluster (server) clarification

The level control cluster shall allow control over the position of the shade. The functionality made available shall be that given in its specification [R3].

The position of the shade shall correspond to the level by the following relationship:

Shade position = *ClosedLimit* x (254 – *Level*) /254

When *Level* is 0 the shade is at the *ClosedLimit* and is closed. When *Level* is 254 the shade is at position 0 and is fully open.

9.5.2 Shade Controller

The Shade Controller device can control the level of a shade, and put it into configuration mode so that the user may adjust its limits.

9.5.2.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Shade Controller shall support the clusters listed in Table 30.

Table 30 – Clusters supported by the Shade Controller

Server side	Client side
Mandatory	
None	On/Off
	Level Control
Optional	
None	Shade Configuration
	Scenes
	Groups
	Identify

9.6 HVAC Device Descriptions

9.6.1 Thermostat

The Thermostat device can have either built-in or separate sensors for temperature, humidity or occupancy. It allows the desired temperature to be set either remotely or locally. The thermostat may send heating and/or cooling requirement notifications to a heating/cooling unit (e.g. an indoor air handler) or may include a mechanism to control a heating or cooling unit directly.

9.6.1.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Thermostat device shall support the clusters listed in Table 31.

Table 31 – Clusters supported by the Thermostat

Server side	Client side
Mandatory	
Thermostat	None
Scenes	
Optional	
Thermostat User Interface Configuration	Fan Control
	Temperature Measurement
	Occupancy Sensing
	Relative Humidity Measurement

9.6.1.2 Temperature Measurement cluster (client)

The functionality made available by the Temperature Measurement client cluster shall be that given in its specification [R4]. It is used to receive temperature measurements when either the local or outdoor temperature for the thermostat cluster is designated to be sensed remotely.

9.6.1.3 Occupancy Sensing cluster (client)

The functionality made available by the Occupancy Sensing client cluster shall be that given in its specification [R4]. It is used to receive occupancy notifications when occupancy for the thermostat cluster is designated to be sensed remotely.

9.6.1.4 Relative Humidity Measurement cluster (client)

The functionality made available by the Relative Humidity Measurement client cluster shall be that given in its specification [R4]. It is used to receive humidity measurements when humidity for the thermostat cluster is designated to be sensed remotely.

9.6.1.5 Scene table extensions

The following extension fields shall be added to the Scenes table for the Thermostat cluster:

OccupiedCoolingSetpoint , OccupiedHeatingSetpoint , SystemMode

9.6.2 Temperature Sensor

The Temperature Sensor device reports measurements of temperature.

9.6.2.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Temperature Sensor device shall support the clusters listed in Table 32.

Table 32 – Clusters supported by the Temperature Sensor

Server side	Client side
Mandatory	
Temperature Measurement	None
Optional	
None	Groups

9.6.3 Pump

The Pump device is a pump that may have variable speed. It may have optional built in sensors and a regulation mechanism. It is typically used for pumping water.

9.6.3.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Pump shall support the clusters listed in Table 33.

Table 33 – Clusters supported by the Pump

Server side	Client side
Mandatory	
Pump Configuration and Control	None
On/Off	
Scenes	
Optional	
Pressure Measurement	Pressure Measurement
Temperature Measurement	Temperature Measurement
Flow Measurement	Flow Measurement
Level Control	
Alarm	

9.6.3.2 On/Off cluster (server) clarifications

The actions carried out by the pump on receipt of commands are shown in Table 34.

Table 34 – Pump Actions on Receipt for On/Off Commands

Command	Action on receipt
Off	If the pump is powered on, store the current level then immediately power it off.
On	If the pump is powered off, power it on and move immediately to the level stored by a previous Off command. If no such level has been stored, move immediately to the maximum level allowed for the pump. The level is related to the setpoint as described in section 9.6.3.3. Note that the pump may ramp its speed up until its performance meets the setpoint. This speed ramping is manufacturer specific.
Toggle	If the pump is powered on, proceed as for the Off command. If the device is powered off, proceed as for the On command.

9.6.3.3 Level Control cluster (server) clarifications

The level control cluster shall allow controlling the pump setpoints as specified in [R3], however the transition time is always ignored.

The Setpoint of the pump is a percentage related to the Level according to Table 35

Table 35 – Relationship between Level and Setpoint for the Pump

Level	Setpoint	Meaning
0	0.0 %	Pump is stopped
1 – 200	Level / 2 (0.5 – 100.0 %)	Pump setpoint in percent
201 – 254	100.0 %	Pump setpoint is 100.0 %

9.6.3.4 Pressure Measurement(server)

This cluster allows serving of internal pressure measurement if available. This is independent of the Pressure Measurement client cluster, which connects to an external networked pressure sensor.

The pressure measurement is a differential pressure measurement over the flanges of the pump.

9.6.3.5 Temperature Measurement(server)

This cluster allows serving of internal temperature measurement if available. This is independent of the Temperature Measurement client cluster, which connects to an external networked temperature sensor.

9.6.3.6 Flow Measurement (server)

This cluster allows serving of internal flow measurement if available. This is independent of the Flow Measurement client cluster, which connects to an external networked flow sensor.

9.6.4 Pump Controller

The Pump Controller device can configure and control a Pump device.

9.6.4.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Pump Controller device shall support the clusters listed in Table 36.

Table 36 – Clusters supported by the Pump Controller

Server side	Client side
Mandatory	
	Pump Configuration and Control
	On/Off
Optional	
None	Pressure Measurement
	Temperature Measurement
	Flow Measurement
	Level Control
	Scenes
	Groups
	Identify

9.6.4.2 Pressure Measurement (client)

This cluster allows configuration and monitoring of the Pressure Sensor internal to a Pump device.

9.6.4.3 Temperature Measurement Notification (client)

This cluster allows configuration and monitoring of the Temperature Sensor internal to a Pump device.

9.6.4.4 Flow Measurement Notification (client)

This cluster allows configuration and monitoring of the Flow Sensor internal to a Pump device.

9.6.5 Pressure Sensor

The Pressure Sensor device measures, and may periodically report, the pressure of a liquid (typically water).

9.6.5.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Pressure Sensor device shall support the clusters listed in Table 37.

Table 37 – Clusters supported by the Pressure Sensor

Server side	Client side
Mandatory	
Pressure Measurement	None
Optional	
None	Groups

9.6.6 Flow Sensor

The Flow Sensor device measures, and may periodically report, the flow rate of a liquid (typically water).

9.6.6.1 Supported clusters

In addition to those clusters specified in 9.2.1, the Flow Sensor device shall support the clusters listed in Table 38.

Table 38 – Clusters supported by the Flow Sensor

Server side	Client side
Mandatory	
Flow Measurement	None
Optional	
None	Groups

9.6.7 Humidity Sensor

The Humidity Sensor device measures, and may periodically report, the percentage of relative humidity.

9.6.7.1 Supported clusters

In addition to those clusters specified in 7.3, the Humidity Sensor device shall support the clusters listed in Table 39.

Table 39 – Clusters supported by the Humidity Sensor

Server side	Client side
Mandatory	
Relative Humidity Measurement	None
Optional	
None	None

9.7 Intruder Alarm System (IAS) Device Descriptions

9.7.1 IAS Control and Indicating Equipment (CIE)

The IAS CIE device is the central Control and Indicating Equipment for an Intruder Alarm System. It receives inputs from IAS Zone devices (see 9.7.3) and Ancillary Control Equipment (ACE - see 9.7.2), and sends output to a warning device (WD - see 9.7.4).

9.7.1.1 Supported clusters

In addition to those clusters specified in 9.2.1, the IAS CIE shall support the clusters listed in Table 39.

Table 39 – Clusters supported by the IAS CIE

Server side	Client side
Mandatory	
IAS ACE	IAS WD
	IAS Zone
Optional	
None	Groups
	Scenes

9.7.1.2 Basic cluster (server) restrictions

The ability to disable the device shall not be provided. That is, the *DeviceEnabled* attribute shall be read only and set to 1 (enabled).

9.7.2 IAS Ancillary Control Equipment (ACE)

The IAS ACE device is a remote control for an Intruder Alarm System. A Zigbee enabled ACE device can access an IAS CIE device and manipulate the IAS system, on behalf of a level-2 user (see [R13]). The device can also act as a Zone sensor.

9.7.2.1 Supported clusters

In addition to those clusters specified in 9.2.1, the IAS ACE shall support the clusters listed in Table 40.

Table 40 – Clusters supported by the IAS ACE

Server side	Client side
Mandatory	
IAS Zone	IAS ACE
Optional	
None	Identify

9.7.2.2 Basic cluster (server) restrictions

The ability to disable the device shall not be provided. That is, the *DeviceEnabled* attribute shall be read only and set to 1 (enabled).

9.7.3 IAS Zone

An IAS Zone device detects alarm conditions (e.g. intrusion, fire) and signals them to the Control and Indicating Equipment (CIE) of an IAS system. An IAS Zone device supports up to two alarm types, low battery reports and supervision of the IAS network.

9.7.3.1 Supported clusters

In addition to those clusters specified in 9.2.1, the IAS Zone device shall support the clusters listed in Table 41.

Table 41 – Clusters supported by the IAS Zone

Server side	Client side
Mandatory	
IAS Zone	None
Optional	
None	None

9.7.3.2 Basic cluster (server) restrictions

The ability to disable the device shall not be provided. That is, the *DeviceEnabled* attribute shall be read only and set to 1 (enabled).

9.7.4 IAS Warning Device (WD)

An IAS WD device can produce audible and visible warning indications (siren, strobe lighting, etc) when instructed to by an IAS Central Indicating Equipment (CIE) on detection of a system alarm condition. The IAS WD can also act as a sensor (Zone).

9.7.4.1 Supported clusters

In addition to those clusters specified in 9.2.1, the IAS WD shall support the clusters listed in Table 42.

Table 42 – Clusters supported by the IAS WD

Server side	Client side
Mandatory	
IAS WD	None
IAS Zone	
Optional	
Scenes	None

9.7.4.2 Basic cluster (server) restrictions

The ability to disable the device shall not be provided. That is, the *DeviceEnabled* attribute shall be read only and set to 1 (enabled).

9.7.4.3 Polling rate exception

The IAS WD may poll at a maximum rate of once per second when it is implemented as a battery-powered ZigBee end device that sleeps. It is recommended that this exception be used cautiously, and that the number of devices installed in a network that make use of this be kept to a minimum.

10 Commissioning

Commissioning is the process of initializing the devices on a network to work together - for example, a control device needs to be bound to a suitable target (or targets) for it to control. The required initializations may be done after installation, or they may be done at the factory before the device is sold. The operations involved in the two cases are very similar.

The ZigBee Alliance has recognized the importance of commissioning and, in particular, the importance of specifications for commissioning in a multi-vendor environment. A general commissioning framework specification may be found in [R11], and a commissioning cluster is specified in [R12].

This section gives details of how the general techniques described in these documents are applied to the ZBA domain.

10.1 Support for commissioning modes

Three different commissioning modes are discussed in [R11]. They are denoted A, E and S-mode. All ZBA devices shall support S-mode. Devices may also optionally support E-mode.

For devices that support E-mode, it is recommended that the practices described in section 5.9.3 “Commissioning Documentation” of the Home Automation Profile Specification [R10] are followed.

10.2 Forming the network (Start-up sequence)

When a ZBA device is started ‘out of the box’, i.e. before it is fully commissioned, the default Startup Attribute Set (SAS) it uses is described in 10.2.1. This SAS results in the device joining a commissioning network with the ZigBee global commissioning EPID.

This default ZBA SAS shall be available on every device conforming to the ZBA profile. However, a vendor may supply a different vendor- specific SAS that the device starts with ‘out of the box’ as long as a simple means is provided to select the default ZBA SAS instead.

On startup ‘out of the box’, each ZBA device shall attempt to join the network specified by the startup SAS (default or vendor specific) on all channels at least once.

Note that the result of commissioning, i.e. the operating network, must have an EPID that is different from the reserved Global Commissioning EPID.

With respect to notification of installers and users, the following practices are recommended:

- A device should be able to indicate to the user, that it has decided to become the coordinator of a network.
- A device should be able to indicate to the user, that it has successfully joined a network.
- A device should be able to indicate to the user, that it is in the process of searching for or joining a network.

These indications can be implemented in a number of ways including indicator light(s) or an audible indicator. Blinking a green indicator light is the recommended method.

10.2.1 Startup Attribute Set

All ZigBee nodes supporting the ZBA profile shall support the Commissioning server cluster (see [R12]) on one of its endpoints. The default Startup Attribute Set (SAS) used by the Commissioning cluster on all nodes shall be as detailed in Table 43. Every node shall either startup automatically with this default SAS, or a simple means shall be provided (e.g. a button) to allow a user to cause it to start up with this SAS.

1 **Table 43 – Startup Attribute Values for ZBA**

Attribute	Value	Notes
ShortAddress	0xFFFF	This means that the device has not been allocated a network address.
ExtendedPANId	0x0050C27710000000	This is the global commissioning_EPID reserved by the ZigBee Alliance.
PANId	0xFFFF	This means that the device has not yet joined a network.
Channel Mask	All channels supported by the device	-
ProtocolVersion	0x02	ZigBee 2007
StackProfile	0x02	ZigBee Pro
StartupControl	0x03	The device shall perform an unsecure join using MAC association.
TrustCenterAddress	0x0000000000000000	This means that the trust center address is not initially specified, but will be communicated to the device when it joins (or rejoins) the network.
MasterKey	0x0000000000000000	Not used
NetworkKey	0x0000000000000000	Undefined Network Key
UseInsecureJoin	Enabled	This setting enables the device to join a network that uses the ZigBee stack profile, e.g. a Home Automation network. It shall be set to Disabled (by the commissioning tool) in an operational ZBA network.
PreconfiguredLinkKey	'ZigBeeAlliance09'	Default Trust Center Link Key
NetworkKeySeqNum	0x00	(See note for NetworkKey)
NetworkKeyType	0x01	Standard Security mode
NetworkManagerAddress	0x0000	This means that the Network Layer Function Manager address is by default that of the ZigBee Coordinator.

2 ## 10.3 Identify mode support

3 The server side of the Identify cluster is supported by all device descriptions and provides a
4 utility, accessible over the air in S mode (which is mandatory) and (optionally) locally, to aid in
5 the commissioning of devices. The Identify cluster plays a particularly important role when
6 setting up groups and scenes in commissioning.

7 In the (optional) case of E mode commissioning, each device should provide a user interface
8 to enter identify mode unless the ability for a user to interface with the device is not possible
9 (e.g. it would be unsafe). Devices that support the Identify client cluster should provide a user
10 interface to issue commands to put other devices in identify mode.

10.4 Commissioning Group Membership

A description of the principles underlying group commissioning can be found in reference [R11]. There are two steps to commissioning groups – first identify the devices that are to be grouped (e.g. by using the Identify cluster), then allocate them to a group via over-the-air command(s).

In S-mode, selecting devices may be done in any desired way, typically via a commissioning tool and without direct user interaction with the target device.

The following are some guidelines for commissioning group membership in (optional) E mode.

It should be possible to:

- Set matching devices in identify mode.
- Perform group allocation for the selected matching devices.

For example, when configuring a multicast group, the device could perform the following:

- Find devices on the network with matching cluster services.
- Put the matched devices in identify mode one at a time.
- When a user action is performed, the device currently identifying becomes a member of a group binding.

Similarly, for an On/Off Light Switch, the process could be:

- User flips the physical switch 4 times rapidly. The switch (implementing the On/Off client cluster) searches for devices on the network with matching services (implementing the On/Off server cluster).
- The matched devices are put in identify mode for a short period one at a time. For On/Off Lights, the light bulb could be flashing.
- When a device that the user wants to be a part of this group is identifying, the user flips the switch once. The switch initiates a group binding to the light currently identifying.

10.5 Commissioning Scenes

Where supported, scenes may be commissioned using the Scenes cluster, as described in reference [R3].

Scenes may be added or modified by:

- Setting the relevant devices to their intended values, and then storing this as a specified scene number.
- Directly configuring the values to be used for a specified scene number.

Scenes may be removed by directly removing the specified scene number. Also, where a scene is related to a specified group, the scene is also removed by removing the device from the relevant group.

10.6 Commissioning Bindings

Bindings should be commissioned using the mechanisms specified in the ZDO (see [R2]).

10.7 Commissioning Security Permissions

The security Permissions Configuration Table is described in references [R2] and [R12]. It provides a mechanism by which certain commands can be restricted to specified authorized devices. If the application requires this level of security for certain devices, and particularly if application link keys are to be used, the following approach should be used.

Configuration of groups via the Groups cluster should use the ApplicationSettings permissions entry to specify from which devices group configuration commands may be received, and whether a link key is required.

Regarding security options at the application level, all devices described in this profile should use the ApplicationCommands permissions entry to determine how commands may be exchanged.