Software Design Specification

Z-Wave Plus Device Type Specification

Document No.:	SDS11847
Version:	32
Description:	This document defines the Z-Wave Plus Device Types, which specify how a Z-Wave Plus node are controlled and appear when included in the network.
Written By:	NTJ;BBR;JFR;NOBRIOT;DEWASSIE
Date:	2020-07-06
Reviewed By:	NOBRIOT;JFR;BBR;COLSEN;DEWASSIE
Restrictions:	Public

Approved by:				
Date	CET	Initials	Name	Justification
2020-07-06	02:41:58	NTJ	Niels Johansen	

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
16	20160823	JFR	All	Prepared for Public Z-Wave initiative
17	20161020	NOBRIOT	3.7.6 & DT sections 3.9.2 3.6.2 4.9	Integrated approved content from contributions 2016C • Added Security 2 requirements and descriptions • Added Lifeline command section • Introduced Home Control Group 13 • Added the NAS Role Type for the Gateway Device Type
18	20170102	NOBRIOT	3.5.2 3.6.2 3.7.6.1	Integrated approved content from contributions 2016D: • Clarified about controlled/supported Command Classes • Clarified minimum required HC group control when supporting other wireless technologies • Updated Security 2 requirements and descriptions
19	20170403	NOBRIOT	3.7.1 3.7.6 DT sections DT sections 3.9.1	Integrated approved content from contributions 2017A: • Added Transport Service to the list of Command Classes not covered by End Points • Rephrased some of the S2 requirements • Fixed broken “0” reference in all Device Types • Removed mandatory control of wake up command class for Remote control DTs • Added Lifeline Concept section from [1]
20	20170703	NOBRIOT	3.6.3 3.6.3.8 & 3.6.3.9 DT sections 3.9.2 4.20.5 3.7.6.4 3.10	Integrated approved content from contributions 2017B: • Introduced guidelines for Command Class Control • Clarified intentional mandatory command acceptance for S0/S2 controlling nodes • Clarified that S2 is now mandatory to support • Clarified Lifeline reporting for Multilevel Sensor Command Class • Added new Basic mapping for Notification Push Sensors Added S2 DSK label requirements Added SmartStart requirements
21	20170711	NOBRIOT	3.3.2	Added SmartStart documentation requirements
22	20171002	NOBRIOT	3.7.5 Table 2 3.6.3.9 3.7.1 3.7.6.1 DT sections 4.24 3.7.6	Integrated approved content from contributions 2017C: • Application Status Command Class is now optional to support for controller Device Types • Removed requirement to control Meter CC for HC8 controllers • Clarified Security 2 Controlling node behavior when receiving supporting commands from other nodes. • Clarified what Command Class to support for Device Types that are Multi Channel End Point • Clarified S2 bootstrapping timeout,S2 bootstrapping failure situations and how to support Command Classes based on S2 bootstrapping • Changed the mandatory Command Classes section for secure devices types (S0 and S2) Added the Sound Switch Device Type. Adjustments to the S2 and SmartStart DSK representation requirements

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
23	20180110	NOBRIOT	3.7.6 DT sections 4.35 Table 2 4.18	Integrated approved content from contributions 2017D: • Added minor clarifications in the Security 2 Command Class support requirements. • Removed Binary Switch Command Class from Window Covering DTs • Allowed different Basic Mapping for Window Covering Position/Endpoint aware DT. • Reworded requirements for HC4 and HC6 and moved Siren DT into HC8 • Added PS Role Type for the Remote control - simple
24	20180305	BBR	All	Added Silicon Labs template
25	20180405	NOBRIOT	3.3.2 3.6.1 4.2.4.1, 4.7.4.1, 4.13.4.1 & 4.13.4.1 3.7.6.3 3.7.6.4 All Device Types	Device Type Contributions 2018A: Minor changes • Updated the required documentation regarding SmartStart • Removed an interoperability guideline • Reworded S2 Access Control command class support requirements for Access Control Slave Device Types Clarifications: • Moved S0 key requirements in the S2 Command Class • Added Z-Wave alliance reference in the S2 DSK representation requirements • Added “version 2 or newer” indication for the Z-Wave Plus Info Command Class
26	20180701	NOBRIOT	3.9.2	Specification Contributions 2018B: • Removed the requirement for advertising dynamic End Point removal via the Lifeline group
27	20181003	NOBRIOT	3.7.6.4	Contributions 2018C: - Clarified that QR Codes must comply with the “Gen2” determination In [11]
28	20190401	NOBRIOT DEWASSIE	4.10 3.3.7	Contributions 2019A: • Added the IR Repeater Device Type. • Added documentation related to Notification Command Class
29	20190701	NOBRIOT	4.4 All Device Types 3.10 3.11	Contributions 2019B: • Added a Color Switch Device Type • Removed the suggested interview processes • Made DSK String representation mandatory for nodes supporting SmartStart and requesting S2 Unauthenticated as highest key • Allowed dynamic capabilities under certain conditions
30	20191001	DEWASSIE	3.7.7 3.3.8 3.10	Contributions 2019C: • Added manual wake-up functionality requirement to battery devices • Added documentation requirement related to the support of Wake Up Command Class • Allow QR Code to be present on UI for a node that supports Smart Start inclusion
31	20200101	NOBRIOT	4.30.8 3.6.3.1 3.8 Various Device Types	Contributions 2019D: • Clarified the mapping of Binary Switch/Basic for valve DT • Added control guidelines for Anti-Theft Unlock Command Class • Added Anti-Theft control rules • Added the Anti-Theft Unlock Command Class as mandatory to control for Device Type using the CSC Role type

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
32	20200701	NORBIOT DEWASSIE	3.7.6.2.2 3.7 (section removed)	Contributions 2020A: • Removed requirement to request S2 Unauthenticated when the highest request key is S2 Authenticated. • Removed bridging devices requirement.

Table of Contents

Table of Figures

Table of Tables

1 ABBREVIATIONS

Abbreviation	Explanation
AGI	Association Group Information
AOS	Always On Slave
CSC	Central Static Controller
DSK	Device Specific Key (S2 Command Class property)
DT	Device Type
GDO	Garage Door Opener
LSS	Listening Sleeping Slave
NIF	Node Information Frame
PC	Portable Controller
PS	Portable Slave
QR	Quick Response (Machine readable printed information for S2 and SmartStart)
RPC	Reporting Portable Controller
RSS	Reporting Sleeping Slave
RT	Role Type
S0	Security 0 Command Class
S2	Security 2 Command Class
SDK	Software Developer's Kit
SIS	Static or Bridge Controller getting updates regarding node changes to keep track on the latest network topology and allocating node IDs to inclusion controllers
SSC	Sub Static Controller

2 INTRODUCTION

2.1 Purpose

This document describes the details of the Z-Wave Plus Device Types. Device Types are a new definition in Z-Wave Plus and is aimed at providing greater details as to how Z-Wave device are controlled and appear when included in the network.

2.1 Precedence of definitions

In terms of reviewing products for Z-Wave Plus compliance, definitions in this document have precedence over the files distributed as part of the Software Developer's Kit (SDK). However, assignments of identifiers for all Role Types, Device Types, Device Classes and Command Classes are located in [8].

Individual Z-Wave Plus Role Type, Z-Wave Plus Device Type and Command Class Specifications approved as a final version during the type/class development process have precedence over this document temporarily until such individual specifications have been integrated into this document.

2.2 Terms used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document MUST be interpreted as described in IETF RFC 2119 [7].

3 Z-WAVE PLUS DEVICE TYPE OVERVIEW

A Z-Wave Plus Device Type defines mandatory and recommended feature for defined product categories. An actual product may omit recommended features and add other features.

Certification tests verify all mandatory features for a given combination of Z-Wave Plus Device Type and Z-Wave Plus Role Type as well as all advertised optional features.

The Z-Wave Plus Device Types add additional requirements for a device compared to the current Z-Wave Device Class specification [6] in order to strengthen interoperability and simplify the installation process.

The Z-Wave Plus Device Types are backwards compatible with the original Z-Wave Device Class [6].

The new mandatory Z-Wave Plus Info Command Class is used to advertise that a product adheres to Z-Wave Plus requirements and to advertise the Z-Wave Plus Device Type and Z-Wave Plus Role Type that the Z-Wave Plus device adheres to.

This Device Type specification SHOULD be read together with the Z-Wave Plus Role Types specification [1].

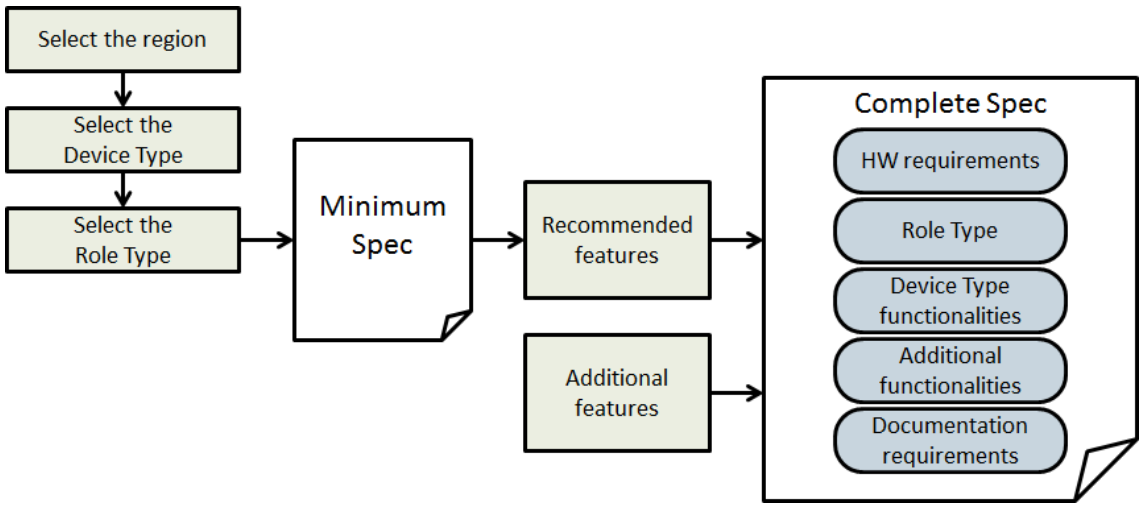


Figure 1, Z-Wave Plus selection overview

When creating a Z-Wave Plus product, the developer must choose a Z-Wave Plus Device Type depending on the intended application. The chosen Device Type MUST reflect Z-Wave functionalities and not the physical product appearance. For example if the intended product is a Gateway built into a TV, the Device Type must be Gateway and not TV. If several Device Types seem to match the product needs, the Device Type MUST be selected based on the best match. Additional Command Classes MAY be added to meet the application needs.

3.1 What does a Z-Wave Plus Device Type specify?

A Device Type specifies requirements for the following areas:

- Lifeline mandatory commands
- What role type to use
- Security requirements
- Mandatory Command classes
  - Control
  - Support
- Basic Command Class support mapping
- Association Group Information mapping
- Multi-channel considerations
- Recommended Optional Features
- Recommended interview process

3.2 How to detect a Z-Wave Plus Device

A device supports the Z-Wave Plus Info Command Class if and only if it is a Z-Wave Plus device. When supported, this Command Class MUST be placed first in the Command Class list advertised by the NIF.

Hence, a controller can identify a Z-Wave Plus certified device by looking up the first Command Class advertised in the NIF. An illustration is given in Figure 2.

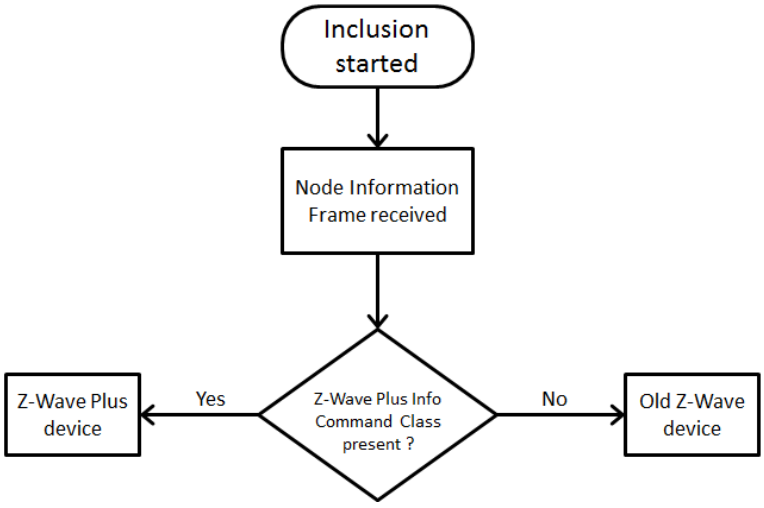


Figure 2, Detecting a Z-Wave Plus device

3.3 Required Documentation

The following requirements for end user documentation apply to all Z-Wave Plus devices regardless of the Z-Wave Plus Device Type. The documentation may be provided as product manuals, quick start guides, electronic help files, web pages, etc.

3.3.1 Documentation for Inclusion, Exclusion and Replication

For Z-Wave Plus slave Role Types, the documentation MUST describe:

- How to include and exclude the device in an existing network.

For Z-Wave Plus controller Role Types, the documentation MUST describe:

- How to include and exclude the device in an existing network.
- How to include and exclude other devices.
- How to initiate a replication of network information from the controller to another controller.
- How to put the controller into learn mode to receive network information from another controller.

3.3.2 Documentation related to SmartStart

For nodes supporting SmartStart inclusion, the documentation MUST describe:

- How to locate the DSK representation(s) on the product.
- How to access the DSK representation(s) via the UI, if available.

For nodes supporting the SmartStart inclusion, the documentation MUST include a short description of what is SmartStart. The following wording is RECOMMENDED:

> *SmartStart enabled products can be added into a Z-Wave network by scanning the Z-Wave QR Code present on the product with a controller providing SmartStart inclusion. No further action is required and the SmartStart product will be added automatically within 10 minutes of being switched on in the network vicinity.*

For controllers providing the SmartStart functionality, the documentation MUST describe:

- How to perform a secure inclusion of a SmartStart node (adding the node in the Node Provisioning List and powering up/installing the node)
- How to access and edit the Node Provisioning List.

3.3.3 Documentation related to devices from multiple manufacturers

The product documentation MUST include a section which describes how products from different manufacturers and product categories can be a part of the same Z-Wave network, and that the different non-battery powered nodes can act as repeaters regardless of manufacturers.

The following is the RECOMMENDED wording:

> *This product can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All non-battery operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.*

The manufacturer is allowed to use custom wording as long as it complies with the above guidelines.

3.3.4 Documentation for Association Command Class

If the product implements support of the Association Command Class, the documentation MUST include a description of the association groups available in the product.

Each group MUST include the following information:

- Grouping identifier
- Maximum number of devices that can be added to the group
- Description of how the association group is used and/or triggered by the product

3.3.5 Documentation for Configuration Command Class

If the product implements support of the Configuration Command Class, the documentation MUST include a description of each configuration parameter available in the product.

Each configuration parameter MUST be listed with the following information:

- Parameter number
- Description of parameter and its effect on the product
- Default value
- Size (number of bytes)
- Allowed values

Exceptions may be agreed with the Z-Wave Certification Group in certain cases (e.g. risk of damage)

3.3.6 Documentation related to Basic Command Class

If the product is based on a Device Type which does not mandate a mapping of the Basic Command Class, the product documentation MUST include information on the mapping of the Basic Command Class and the resulting product behavior.

3.3.7 Documentation related to Notification Command Class

If the product implements support of the Notification Command Class, the documentation MUST specify the implemented Notification Type(s) and Event(s).

3.3.8 Documentation for Wake Up Command Class

If the node supports the Wake Up Command Class, the product documentation MUST describe how to manually Wake Up the node.

3.3.9 Terminology

The product documentation MUST use the following terminology for Z-Wave related functionality.

Table 1, Z-Wave Plus documentation terminology

Z-Wave functionality	Documentation terminology	Example
Inclusion	Add	The process of adding a node to the Z-Wave network.
Exclusion	Remove	The process of removing a node from the Z-Wave network.
Replication	Copy	The process of copying network information from one controller to another.

3.3.10 Additional documentation required for Z-Wave Certification

In addition to the rules defined above the following technical documentation MUST be made available to the certification test lab upon submitting the product for certification:

- Documentation about how to activate any functionality available in the device related to Z-Wave behavior
- If any *special* procedures are REQUIRED to test any item in the certification form, such procedures MUST be clearly described
- If the product is a Z-Wave controller, documentation on how to send any controlled command from the controller MUST be included

If any of the above mentioned documentation is not submitted along with the product for certification, testing of the device will not be initiated.

3.4 Recommended User Interface

It is RECOMMENDED to use a dedicated button for Z-Wave network installation and maintenance providing an intuitive consumer experience. This button SHOULD NOT be the same as used for normal operation.

3.5 Terminology

3.5.1 Controllers and Home Control Groups

Nodes are controllers or slaves based on their Role Type. Refer to for [1] for details.

Z-Wave Plus Device Types are mapped into logical groups called Home Control Groups (HCG). The list is given in Table 2.These groups are used to test minimum controller functionalities.

Controllers are designed to control one or more Home Control Groups. An unknown device refers to a device which belongs to a non-supported HCG by the controller.

Controllers are classified as either Dedicated Controller or Universal Controller.

A Dedicated Controller MUST only control one Home Control Group and MAY control unknown devices via the Basic Command Class and the optional implemented controlled command classes in the controller.

A Universal Controller controls multiple Home Control Groups and MUST be able to control unknown devices with the Basic Command Class together with the optional implemented controlled command classes. A Universal Controller MUST provide individual control of unknown devices that have been included in the network.

Home Control Groups HC4 and HC6 have sub categories for sensors. A controller controlling devices in HC4 or HC6 is not required to support all types of sensors.

3.5.2 Controlled and Supported Command Classes

A node can support and/or control a given Command Class.

If a Command Class is supported:
The node implements all the Command Class functionalities and can be set and read back by other nodes. When a Command Class is supported, it is REQUIRED to implement the whole Command Class.

If a Command Class is controlled:
The node implements the ability to interview, read and/or set other nodes supporting the Command Class. Nodes controlling Command Classes MAY use only a subset of the Commands within a Command Class (for example only Set commands). Even if using a Command Class partially for control, the use MUST comply with the Command Class requirements.

Slaves nodes MAY also control command classes. For example, a Set Command sent to Association Group destinations is a form of Command Class control.

When Command Class control is mandated by the Device Type, a controlling node MUST implement the ability to interview, read and set other nodes using the given Command Class and the controlling node MUST be able to use all commands of the controlled Command Class. More details are given in 3.6.3 Command Class control mandated by the Device Type.

3.6 Controller Functionalities

A controller plays an important role in a Z-Wave network because this device hosts important functionality to create, maintain and configure the network and the home automation application. The following sections describe important rules to ensure that a controller is capable of fulfilling this important role.

3.6.1 Interoperability

To ensure interoperability a controller MUST comply with the following requirements:

1. It is not acceptable to block interoperability by any means.

2. It is not acceptable to prevent inclusion of certified devices into a system or force exclusion of non-preferred devices after inclusion.

3. It is not required to control all mandatory command classes for a given Device Type (see section 3.6.2 regarding minimal controller functionality).

4. Devices from non-preferred manufacturers MAY be placed in a special section of the user interface; this section should be referred to as “Additional Z-Wave Ecosystem Devices”. Additionally, it is acceptable to inform the user, upon inclusion of non-preferred devices that the device being included is not part of the vendors preferred ecosystem, and that control and support of the device by the vendor may be limited.

    a. It is not permitted to display additional pop-ups, ask for pin codes or implement any other blocking or discouraging behavior for inclusion or control of non-preferred devices.

    b. The Z-Wave Alliance recommends wording as follows. “You are about to include a Z-Wave compatible device that is not promoted by *‘service provider name’* for use in this application. While the device will work as expected the device may or may not support all of the features of the *‘service provider name’* recommended device.”

3.6.2 Minimal Control Functionality

If a controller product supports short range wireless non-Z-Wave technology smarthome products (e.g. light bulbs, thermostats, door locks and the like) and Z-Wave technology products, it MUST, at a minimum, provide Z-Wave minimal control functionality for HC1, HC8, HC9, HC11 and HC12 groups (see Table 2).

If a controller is designed to control a Device Type, it MUST provide at least minimal functionality for all certified devices belonging to the same Home Control Group, regardless of the manufacturer.

It is acceptable to differentiate between preferred and non-preferred devices of the same type as long as the controller provides at least minimal control of both.

Table 2 shows the minimal control functionalities, which a controller MUST provide for the different Home Control Groups.

A controller SHOULD use the information provided by NIF's Command Class list and their capability discovery Commands (such as AGI, etc.) to discover a node capabilities and provide the minimum controlled functionalities.

A controller SHOULD NOT rely on the Device Type of a node for providing minimum controlled functionalities. For example, a controller designed for controlling HC2 SHOULD be able to provide Meter CC readings for an On/Off Power Switch supporting the Meter CC.

Table 2, Minimum requirements for controlling Device Types

Home Control Group	Device Types	Minimal functionality
HC1	Door Lock – Keypad Lockbox	The application MUST be able to Lock, Unlock and check the Status (Locked/unlocked) using Door Lock Operation CC with Security 0 CC
HC2	Whole Home Meter – Simple Sub Energy Meter	The application MUST be able to query and read Meter Reports using Meter CC. Count/KWh cumulated readings MUST be available to the end user.
HC4	Notification Sensors	The application MUST be able to receive and interpret reports using Notification CC. Event/state Notifications MUST be made available to the end user and it SHOULD be possible to configure actions or rules based on the reports. Wake Up CC (version 2 or newer) MUST be controlled. Association CC MUST be controlled. Other association settings are NOT REQUIRED to be controllable by the end user.
HC6	Multilevel Sensors	The application MUST be able to receive and interpret reports using Multilevel Sensor CC. Sensor readings MUST be made available to the end user and it SHOULD be possible to configure actions or rules based on the reports. Wake Up CC (version 2 or newer) MUST be controlled Association CC MUST be controlled. Other association settings are NOT REQUIRED to be controllable by the end user.
HC8	On/Off Power Switch Power Strip Irrigation Control Siren	The application MUST be able to set the device ON/OFF and check the device's Status using Basic or Binary Switch CC.
HC9	Light Dimmer Switch Fan Switch	The application MUST be able to set the device ON/OFF and check the device's Status using Basic or Multilevel Switch CC.
HC10	Window Covering: - No Position/Endpoint - End Point Aware -Position/End Point Aware	The application MUST be able to set the device ON, OFF. at a given Level and check the Status using Basic or Multilevel Switch CC. Level setting MUST be controllable if supported by the device.
HC11	Thermostat - HVAC	The application MUST be able to Adjust Mode and Setpoints using Thermostat Mode CC and Thermostat Setpoint CC. At least Heat, Cool and OFF modes if supported by the device.
HC12	Thermostat - Setback	The application MUST be able to set the device ON/OFF and check the Status using Basic CC. It will switch between Normal/Comfort and Energy Saving.
HC13	Motorized barrier	The application MUST be able to Open/Close the barrier and read its state using the Barrier Operator CC. The application MUST be able to discover signaling capabilities, set On/Off signaling and read back the signaling status using Barrier Operator CC

Home Control Group	Device Types	Minimal functionality
None	Central Controller Display – Simple Gateway Remote Control – AV Remote Control – Multipurpose Remote Control – Simple Repeater Set Top Box Sub System Controller TV Valve – Open/Close Wall Controller	None required

3.6.3 Command Class control mandated by the Device Type

The following subsections present non-exhaustive lists of the expected behavior of a node having control of a given Command Class mandated in their Device Type definition.

3.6.3.1 Anti-Theft Unlock, version 1 or newer

If the supporting node is in the locked state and runs in restricted mode, the controlling node MUST have a UI allowing the end user to see that the supporting node is restricted and that the supporting node requires unlocking to use the full functionality.

A controlling node MAY display the information provided in [14] for the reported Z-Wave Alliance locking entity ID.

If the supporting node is in the locked state and restricted mode, the end user MUST be able send an unlock command with a user defined Magic Code.

3.6.3.2 Association Command Class, version 2 or newer

A controlling node SHOULD read the number of supported groups during node commissioning.

A controlling node SHOULD read maximum number of supported NodeID destinations and the current NodeID associations in a group before creating or removing associations.

A controlling node MUST NOT create an association if the association destination does not support the controlling commands (Set/Get type) that the actual association group will be sending.

In any case, a controlling node is allowed to create an association to any destination if the actual association group sends commands reflecting the support of a Command Class by the sending node (Report/Notification type commands).

A controlling node SHOULD NOT create an association if the source and destination nodes are bootstrapped with different security levels.

A controlling node SHOULD implement an application/UI that permits to create/remove associations between nodes.

A controlling node MUST use the Association Group Information (AGI) Command Class to probe the commands that a given association group will be sending before creating associations towards other nodes.

A controlling node SHOULD update the association group record of a node accordingly upon any received Association Report Command.

3.6.3.3 Association Group Information (AGI) Command Class

A controlling node SHOULD read the entire AGI table from supporting nodes during the node commissioning.

A controlling node MUST read the AGI table of an Association Group before establishing an association for the actual group. It means that a controlling node MUST issue the following commands for the Association Group Identifier:

- Association Group Name Get
- Association Group Info Get
- Association Group Command List Get

3.6.3.4 Basic Command Class

A controlling node MUST have an Association Group or an application/UI permitting to transmit Basic Set Commands.

A controlling node SHOULD NOT use Basic Command Class if it can actuate a node with its supported Command Classes.

A controlling node SHOULD use Supervision encapsulation or discover if a node supports the Basic Command Class (using Basic Get Command) before trying to use the Basic Set Command.

3.6.3.5 Multi Channel Command Class, version 4 or newer

A controlling node MUST discover the Multi Channel End Points and their capabilities for a supporting node.

A controlling node SHOULD understand dynamic and aggregated End Points.
A controlling node SHOULD NOT try to access non-existing End Point functionalities after dynamic End Point creation, modification or removal.

A controlling node SHOULD perform a new interview/commissioning of a Multi Channel End Point when receiving a Multi Channel End Point Report Command for a dynamic End Point.

A controlling node SHOULD use the bit addressing when issuing an identical command to several End Points.

A controlling node MUST process correctly any command received with Multi Channel encapsulation.

3.6.3.6 Multi Channel Association Command Class, version 3 or newer

A controlling node SHOULD NOT use Association Command Class and use only Multi Channel Association Command Class for managing associations in a node that supports Multi Channel Association Command Class.

A controlling node SHOULD read the number of supported groups during node commissioning.

A controlling node SHOULD read maximum number of supported destinations and the current NodeIDs/End Points associations in a group before creating or removing associations.

A controlling node SHOULD establish an End Point association towards its NodeID/End Point 0 for the Lifeline Association Group if the controlled node supports both Multi Channel Command Class and Multi Channel Association Command Class, version 3 or newer.
A controlling node SHOULD establish a NodeID association towards its NodeID for the Lifeline Association Group if the controlled node does not support the Multi Channel Command Class or Multi Channel Association Command Class, version 3 and newer.

A controlling node MUST NOT create an association if the association destination does not support the controlling commands (Set/Get type) that the actual association group will be sending.

In any case, a controlling node is allowed to create an association to any destination if the actual association group sends commands reflecting the support of a Command Class by the sending Node/End Point (Report/Notification type commands).

A controlling node SHOULD NOT create an association if the source and destination nodes are bootstrapped with different security levels.

A controlling node SHOULD correctly add/remove End Point/NodeID associations if its application/UI permits to establish associations between nodes or End Points.

A controlling node SHOULD implement an application/UI that permits to create/remove NodeID and End Point associations between nodes or End Points.

A controlling node MUST use the Association Group Information (AGI) Command Class to probe the commands that a given association group will be sending before creating associations towards other NodeIDs/End Points.

A controlling node SHOULD update the association group record of a node accordingly upon any received Multi Channel Association Report Command.

3.6.3.7 CRC-16 Encapsulation Command Class

A controlling node SHOULD use CRC-16 encapsulation to communicate with a supporting node when no security encapsulation is used and the communication speed is lower than 100 kbits/s.

A controlling node MUST support the CRC-16 Command Class and understand received commands encapsulated with CRC-16.

3.6.3.8 Security 0 (S0) Command Class

A controlling node MUST be able to perform S0 bootstrapping for newly included nodes.

A controlling node MUST read S0 capabilities (using the S0 Supported Command Get / S0 Supported Command Report Commands) before sending S0 encapsulated traffic to a supporting node.

A controlling node MUST process correctly any command received with S0 encapsulation (if the controlling node has the S0 network key).

A controlling node MUST discard a received Report/Notification type command (reflecting the support of a Command Class) if it is not received using S0 encapsulation and the corresponding Command Class is supported securely only (i.e. listed in S0 Supported Commands Report and not in the NIF).

3.6.3.9 Security 2 (S2) Command Class

A controlling node MUST be able to perform S2 bootstrapping for newly included nodes if having the SIS Role.

A controlling node MUST read S2 capabilities (using the S2 Supported Command Get / S2 Supported Command Report Commands) before sending S2 encapsulated traffic to a supporting node.

A controlling node MUST process correctly any command received with S2 encapsulation (if the controlling node has the corresponding S2 network key).

A controlling node MUST discover the highest security level granted to any supporting node if it does not have the SIS Role. It is RECOMMENDED to issue the S2 Supported Command Get Command to a supporting node starting from the highest security level downwards until the returned S2 Supported Command Report contains a non-empty Command Class list (if any).

A controlling node MUST discard a received Report/Notification type command (reflecting the support of a Command Class) if it is not received at the highest security level of the sending node and the corresponding Command Class is supported securely only (i.e. not in the NIF).

3.6.3.10 Simple AV Control Command Class

A controlling node MUST have an Association Group or an application/UI permitting to transmit Simple AV Set Commands.

A controlling node SHOULD read which AV Commands are supported by a node before issuing Simple AV Control Set Commands.

3.6.3.11 Wake up Command Class, version 2 or newer

A controlling node MUST read the capabilities of a version 2 supporting node before setting a Wake Up Interval time and destination.

A controlling node MUST set a supported Wake Up Interval time value when commissioning a version 2 supporting node.

A controlling node SHOULD verify that the Wake Up Interval Set Command executed successfully by either using Supervision encapsulation or reading back the Wake Up Interval settings.

A controlling node SHOULD read the Wake Up Interval of a supporting node when the delays between Wake Up periods are larger than what was last set at the supporting node.

3.7 Command Class support specific requirements

Certain rules must be fulfilled depending on which command classes are used. The following subsections detail the requirements of special command classes. Details about individual Command Classes can be found in [2], [3], [4] and [5]

3.7.1 Multi Channel support

It is RECOMMENDED for Z-Wave Plus multi-function devices that each individual functionality is implemented as a separate Multi Channel End Point.

For example, a power strip device may implement five End Points; one for each output.
As another example, a multi-sensor device may implement two End Points. One End Point may advertise the AGI Profile Sensor:Temperature while another End Point may advertise the AGI Profile Sensor:Humidity.

Multi Channel devices MUST support the following command classes:

- Multi Channel (version 4 or newer)
- Multi Channel Association (version 3 or newer)

A Z-Wave Plus compliant Multi Channel device MUST accept the creation of Multi Channel Associations from the Root Device.

All Controller Role Types (CSC, SSC, PC, RPC) SHOULD use Multi Channel Association to create an association for the lifeline in a Multi Channel device.
The Multi Channel Association Set command used to create the Lifeline association MUST NOT be sent Multi Channel encapsulated to the Root device of the Multi Channel device.
The Multi Channel Association Set command used to create the Lifeline association MAY specify the Multi Channel destination End Point 0 (zero).

A Multi Channel device MAY issue commands to the Lifeline destination from all of its End Points if a Multi Channel Association has been established from the Root Device Lifeline association group.

A command issued to the Lifeline destination from a Multi Channel End Point MUST be Multi Channel encapsulated if a Multi Channel Association has been established.

A command issued to the Lifeline destination by the Root Device of a Multi Channel device MUST NOT be Multi Channel encapsulated if the association destination End Point is set to 0 (zero).

The Root Device of a Multi Channel device MUST support the following command classes:

- Association, version 2
- Association Group Information (AGI), version 1 (or newer)
- Device Reset Locally, version 1
- Manufacturer Specific, version 2
- Multi Channel, version 4
- Multi Channel Association, version 3

- Powerlevel, version 1
- Security 0 (S0), version 1 (if supported by any End Point.)
- Version, version 2
- Z-Wave Plus Info, version 2

In a Multi Channel device, a Device Type MUST be assigned to each End Point. End Points within a Multi Channel device MAY have different Device Types. The list of mandatory Command Classes for an End Point is defined by its Device Type, but there may also mandatory Command Classes for the Root Device.

A Multi Channel End Point SHOULD NOT advertise any of the following command classes, which SHOULD be covered by the Root Device:

- CRC-16 Encapsulation
- Device Reset Locally
- Manufacturer Specific
- Powerlevel
- Version
- Transport Service
- Battery (unless each End Point has its own battery)

Legacy devices are unaware of Multi Channel End Points.
For compatibility with such devices, the Root Device of a Multi Channel device MUST reflect the application functionality of End Point 1.
Further, the Root Device of a Multi Channel device MAY reflect the application functionality of more End Points than End Point 1.

With regards to command handling, this means that:

The Root Device MUST forward application control commands to End Point 1.
The Root Device MAY forward application control commands to more End Points than End Point 1.
As an example, the Root Device of the before-mentioned power strip device may forward an application control command to all 5 End Points.

The Root Device MAY return one consolidated response to an application request command to represent more End Points than End Point 1.
As an example, the Root Device of the before-mentioned power strip device may report that it is turned on if just one End Point is turned on.

The Root Device MAY implement association groups which mirror the association groups of multiple End Points.
As an example, the Root Device of the before-mentioned multi-sensor device may implement two association groups which allow a legacy controller to create associations from the temperature sensor and the humidity sensor, respectively. This method of collapsing Multi Channel functionality in the Root Device may not be feasible if a device implements a number of End Points with similar functionality.

3.7.2 Configuration Command Class

If the Configuration Command Class is implemented it MUST NOT replace any existing Command Class functionality.

3.7.3 Firmware Update Command Class

It is RECOMMENDED that the Firmware Update Meta Data Command Class is supported.

3.7.4 Anti-theft Command Class

Except for the following explicitly listed Device Types, Z-Wave Plus Device Types MUST NOT support Anti Theft Command Class:

- Door Lock - Keypad
- Thermostat – HVAC
- Thermostat – Setback

3.7.5 Application Status Command Class

If a node is temporarily not capable to service a Get or Set Command request, it MUST support the Application Status Command Class and send an Application Busy Report Command to the initiator of the Get or Set.

If a node is always capable of servicing the Get and Set requests, it is OPTIONAL to support the Application Status Command Class.

3.7.6 Security 2 Command Class

All Z-Wave nodes certified after the 2nd of April 2017 MUST support the Security 2 Command Class.

Security 2 Command Class defines several Security Classes. [9]. An S2 node MUST respect the requirements associated to the highest requested S2 Security Class.

A Multi Channel Root Device and all its End Points MUST share the same highest S2 Security Class.

3.7.6.1 S2 bootstrapping and functionalities

After network inclusion, a node MUST consider S2 Bootstrapping as started after receiving the S2 KEX Get Command.

If a node times out waiting for security bootstrapping after network inclusion, it MUST NOT consider that bootstrapping failed and MUST consider that it was included non-securely.

If S2 bootstrapping started and did not complete successfully, a supporting node MAY remove support of its implemented command classes until re-included. Refer to [2] chapter 3 regarding NIF contents depending on inclusion and security bootstrapping.

A node supporting S2 MUST consider any Security Class lower than its highest granted Security Class as unsecure communication.

Certain command classes, such as Transport Service or Z-Wave Plus Info, must always be supported non-securely and present in the NIF if they are supported by a node. In this case, non-secure support requirements are specified in each individual command class definition.

By default, a node supporting S2 MUST support its Command Classes only at the highest granted Security Class. If no Security Class was granted, the node MUST support all its Command Class using non-secure communication.

This does not apply to S2 Access Control nodes, which MAY (or sometimes MUST) remove support for a given Command Class if the highest granted Security Class is lower than a minimum expected Security Class for the actual Command Class.

A node supporting S2 MAY control Command Classes at any of the granted Security Classes.

3.7.6.2 S2 Security Classes requirements

An S2 supporting node MUST comply with the requirements indicated in Table 3 associated to its highest requested Security Class during S2 bootstrapping.

Nodes requesting the S0 Security Class MUST comply with requirement indicated in 3.7.6.3.

Table 3, S2 Security Classes associated requirements

Security level	*Class Name*	*Requirements if the Security Class is the highest requested during S2 bootstrapping*
1st highest security level	S2 Access Control	Defined in 3.7.6.2.1
2nd highest security level	S2 Authenticated	Defined in 3.7.6.2.2
3rd highest security level	S2 Unauthenticated	Defined in 3.7.6.2.3

3.7.6.2.1 S2 Access Control Security Class

The S2 Access Control Class is the most trusted class and is intended for home access control devices such as door locks, garage door openers or central controllers.

A node requesting the S2 Access Control Security Class MUST carry a representation of its DSK on itself and/or make it visible on its UI at any time when Learn Mode is enabled. Refer to 3.7.6.4 for DSK format and representation.

A controller node requesting the S2 Access Control Security Class MAY decide to not support its implemented Command Classes if it has not been granted a certain minimum Security Class for a given Command Class by an S2 bootstrapping controller.

A controller requesting S2 Access Control Security Class MUST request S2 Authenticated and S2 Unauthenticated Security Classes when being S2 bootstrapped.
A slave supporting S2 Access Control Security Class MAY support any other Security Class for control purposes.

3.7.6.2.2 S2 Authenticated Security Class

The S2 Authenticated Class is the 2nd most trusted class and is intended for secure applications in home control deployments.

A node requesting the S2 Authenticated Security Class MUST carry a representation of its DSK on itself and/or make it visible on its UI at any time when Learn Mode is enabled. Refer to 3.7.6.4 for DSK format and representation.

3.7.6.2.3 S2 Unauthenticated Security Class

The S2 Unauthenticated is the 3rd most trusted class and is intended for other devices at home that do not require a high level of security as S2 Access Control or S2 Authenticated.

A node requesting the S2 Unauthenticated Security Class as its highest Class has no additional requirement.

3.7.6.3 S0 Security Class requirements

The S0 Class is the legacy Security 0 Command Class network key and is used for backwards compatibility with S0 nodes.

An S2 node MUST NOT request the S0 Security Class if it does not support the Security 0 Command Class. An S2 node MUST NOT request the S0 Security Class without requesting an S2 Security Class.

Nodes with controlling capabilities and controllers SHOULD request the S0 Security Class for application control purposes.

3.7.6.4 DSK format and representation requirements

The S2 Command Class defines a Device Specific Key (DSK) that enables authentication as part of the S2 Bootstrapping process.

The DSK can be represented with the following pre-defined formats: PIN code, DSK string and QR code.

The PIN code MUST be constructed according to Figure 3.

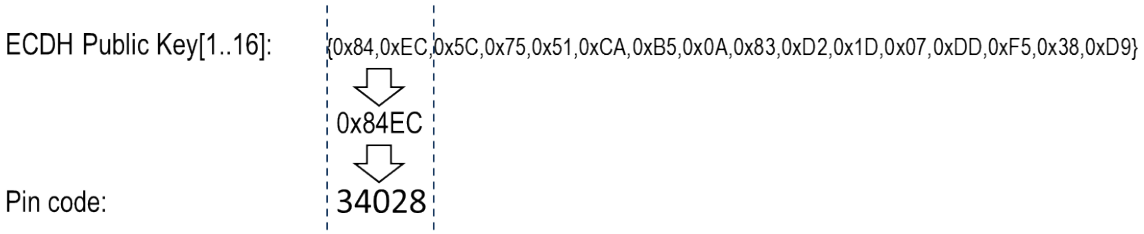


Figure 3, PIN code format

The DSK string MUST be constructed according to Figure 4.

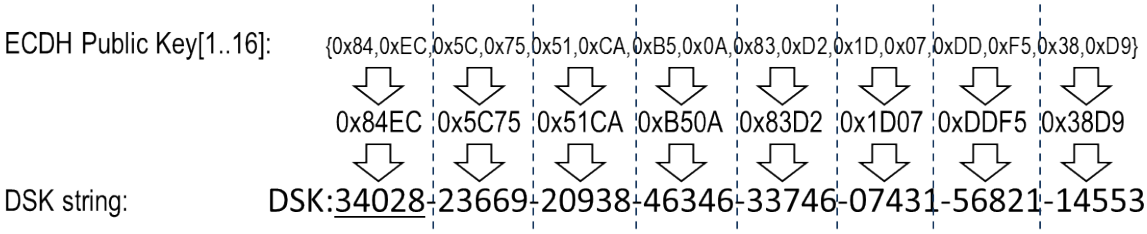


Figure 4, DSK String format

The first five digits of the DSK string MUST be underlined to help the user identify the PIN code portion of the DSK string.

The QR code format MUST comply with the “Gen2” format defined in [11]. The QR code MUST include two TLV blocks: Type 0 (Product Type) and TLV Type 1 (Product ID) as defined by [10].

Additional formatting requirements for the market certification are given by the Z-Wave Alliance, refer to [12]. The following subsections indicate the covered areas for the allowed DSK representations for a product.

3.7.6.4.1 DSK on the product or UI

A product SHOULD carry or display a QR code.

A product MUST carry or display the DSK string or PIN code.
A product carrying or displaying the PIN code MUST also carry or display a QR code.

If the product carries the PIN code representation of the DSK, the product leaflet, documentation or packaging MUST contain the DSK string.

3.7.6.4.2 DSK on documentation or leaflet

It is RECOMMENDED that a leaflet inside the product's box, advertises the QR code and the full DSK string.

3.7.6.4.3 DSK on the product's box/package

The product packaging SHOULD carry the QR code and DSK string on its outside.

3.7.7 Wake Up Command Class

If the node supports the Wake Up Command Class, the node MUST support manual Wake Up triggered by user activation.

3.8 Command Class control specific requirements

Certain rules must be fulfilled depending on which command classes are controlled. The following subsections detail the requirements of special command classes.

3.8.1 Anti-Theft Command Class

Control of this command class is limited to an entity that has been granted permission by the Z-Wave Alliance to control this Command Class and has been granted a locking entity ID. The list of granted locking entity IDs is defined in [14].

Any node controlling this Command Class locking nodes without authorization will be failed in certification.

A node controlling this Command Class MUST NOT provide access to the locking functionality feature of the Command Class to a consumer/end-user of the node; i.e. end users MUST NOT be able to lock nodes themselves.

Control of this command class by a node which is also offered in a non-service market where an end consumer has access to network control features MUST use a different Product ID and Product Type ID between the service and consumer versions of the product.

3.9 Lifeline concept and other associations

3.9.1 Lifeline association group

The Lifeline concept is a part of the Z-Wave Plus framework. The concept supports easy configuration of nodes in a centrally controlled network. The Lifeline provides a “plug-and-play” configuration experience when a node is added by a central controller.

The Association Command Class is used to establish a logical link from a node to the SIS when the node is included. Association Group 1 MUST be used for the Lifeline association.

A controlling node MAY further interview a node through the use of Association Group Information (AGI) Command Class to obtain a full list of events supported by a node. This could be events which are not mandated in a Device Type or events which are already included in the Lifeline group but are also individually available via other association groups.

3.9.2 Lifeline reporting commands (run-time reporting)

A Z-Wave Plus node MUST issue commands via the Lifeline Association Group according to Table 4 when the corresponding Command Class is supported.
Commands covered in Table 4 SHOULD NOT be provided via other association groups.

Table 4, Lifeline commands

Command Class	Command	Conditions and triggers
Barrier Operator	Barrier Operator Report	This command MUST be issued by a node when the barrier has finished a transition (e.g. from Open to Close) and reached a final state from a local activation.
Battery	Battery Report	This command MUST be issued by a node when its battery becomes low. The Battery Level field MUST be set to 0xFF to indicate a low battery warning.
Central Scene	Central Scene Notification	This command MUST be issued by a node when a user actuated a Scene Notification button on the supporting node.
Door Lock	Door Lock Operation Report	This command MUST be issued by a node when it has completed a lock/unlock operation initiated locally.
Device Reset Locally	Device Reset Locally Notification	This command MUST be issued by a node when it has been locally (or manually) reset to factory default. Refer to the Z-Wave Plus Role Type Specification [1]

Command Class	Command	Conditions and triggers
Entry Control	Entry Control Notification	This command MUST be issued by a node when a user input has exceeded key cache size or key cache timeout. Refer to the Entry Control Command Class [2].
Irrigation	Irrigation System Status Report	This command MUST be issued when a system error has been detected. Refer to Irrigation Command Class [2].
Meter	Meter Report	This command MUST be issued periodically to report the current Meter reading. The sending frequency is up to the implementation. It is RECOMMENDED to implement a minimum reporting interval (for example, every 70 minutes) and send additional reports when a measurement variation occurred
Multilevel Sensor	Multilevel Sensor Report	This command MUST be issued periodically to report the current Multilevel sensor reading. The sending frequency is up to the implementation. It is RECOMMENDED to implement a minimum reporting interval (for example, every 70 minutes) and send additional reports when a measurement variation occurred. A node supporting multiple sensor types MUST advertise readings for all of the supported types via the Lifeline Group. Each sensor type MAY have a different timing mechanism for reporting its readings.
Notification	Notification Report	This command MUST be issued by Push nodes every time a new event is detected or when a state variable has changed state. Refer to the Notification Command Class [2]
Thermostat Setpoint	Thermostat Setpoint Report	This command MUST be issued when the Thermostat Setpoint setting has been changed or updated by a local activation.

A node MAY send additional commands via the lifeline association group to reflect the state of the node. A node MUST NOT send the following via the lifeline:

- Obsoleted commands or commands belonging to an obsoleted Command Class
- Set or Get commands
- Redundant commands. (for example, if Multilevel Switch CC and Window Covering CC provide the same functionality for a node, the node MUST NOT send both Multilevel Switch Report and Window Covering Report)

3.10 SmartStart requirements

A SmartStart product documentation MUST respect the requirements described in 3.3.2 Documentation related to SmartStart.

A node supporting SmartStart inclusion MUST have a QR code printed on the product or its UI. (refer to 3.7.6.4 DSK format and representation requirements)
A node supporting SmartStart inclusion MUST have the DSK String printed on the product, leaflet, or packaging.
A node supporting SmartStart inclusion SHOULD carry a QR code on the leaflet and on the product packaging.

The QR code MUST comply with the “Gen2” format defined in [11] and indicate version 1 (SmartStart enabled nodes).
The QR code MUST include TLV block 0 (Product Type) and TLV block 1 (Product ID) as defined by [10].

A SmartStart node MUST carry and keep the same Learn Mode DSK during its entire lifetime, even if it only requests the S2 Unauthenticated Security Class. Refer to 3.7.6.2 and 3.7.6.4.

3.11 Dynamic Capabilities

Changing capabilities is not allowed while a node is included in a network. Nodes provided multiple sets of capabilities MUST be excluded and re-included before providing another set of functionalities.

However, a Z-Wave Plus node MAY alter its capabilities within a supported Command Class if it respects the following requirements:

- The NIF (or supported CCs, Device Type or Role Type) MUST NOT change
- All the changed application functionalities within Command Classes MUST be advertised with the corresponding report(s) sent unsolicited to the lifeline group destinations.

The configuration of Command Classes that are available before and after a capability change MUST remain unchanged. For instance, the Lifeline Association Group destination and Wake Up destination MUST stay identical when a node changes capabilities.

A node MUST stay compliant and observe Z-Wave Plus Device Type and Role Type requirements when and after changing capabilities.

4 Z-WAVE PLUS DEVICE TYPES

The Z-Wave Plus Device Type is communicated via the Node Information Frame (NIF). The Device Type is the two byte concatenation of the Z-Wave Generic and Specific Device Classes.

The Z-Wave Plus Info Command Class is used to differentiate between Z-Wave Plus and Z-Wave devices. For details about the Z-Wave Plus Info Command Class. Refer to [2].

Device Type identifiers are defined in [8].

An overview of how Z-Wave Plus Device Types relates to classic Z-Wave Generic and Specific Device classes is given in Table 5. New Specific Device Classes introduced in Z-Wave Plus are marked with green.

Table 5, Device Types mapping to Generic and Specific Device Classes

Generic Device Class	Specific Device Class	Device Type	Role Type
Notification	Notification Sensor	Sensor – Notification	RPC, RSS, AOS,LSS
AV Control Point	Not used	AV Control Point	AOS, LSS
	Sound Switch	Sound Switch	AOS, LSS
Binary Switch	Binary Power Switch	On/Off Power Switch	AOS, LSS
	Power Strip Switch	Power Strip	AOS
	Siren	Siren	AOS, LSS
	Valve	Valve – Open/close	AOS, LSS
	Irrigation Control	Irrigation Control	AOS
	Color Switch Tunable Binary	Color Switch	AOS
Display	Simple Display	Display – Simple	AOS, LSS
Entry Control	Secure Keypad Door Lock	Door Lock - Keypad	AOS, LSS
	Secure Door	Motorized barrier – GDO	AOS, LSS
	Secure Gate	Motorized barrier – Gate	AOS, LSS
	Secure Barrier Add-on	Motorized barrier – Add-on	AOS, LSS
	Secure Barrier Open only	Motorized barrier – Open only	AOS, LSS
	Secure Barrier Close only	Motorized barrier – Close only	AOS, LSS
	Lockbox	Lockbox	LSS; AOS;RSS; SSC, RPC
	Secure Keypad	Entry Control Keypad	AOS, LSS, RSS
Meter	Simple Meter	Sub Energy Meter	AOS, RSS
	Simple Whole Home Meter	Whole Home Meter - Simple	AOS, LSS, RSS

Generic Device Class	Specific Device Class	Device Type	Role Type
Multilevel Sensor	Routing Multilevel Sensor	Sensor - Multilevel	RPC, RSS, AOS,LSS
Multilevel Switch	Multilevel Power Switch	Light Dimmer Switch	AOS
	Motor Control A	Window Covering - No Position/Endpoint	AOS, LSS
	Motor Control B	Window Covering - End Point Aware	AOS, LSS
	Motor Control C	Window Covering - Position/End Point Aware	AOS, LSS
	Fan Switch	Fan Switch	AOS
	Color Switch Tunable Multilevel	Color Switch	AOS
Remote Controller	Portable Remote Controller	Remote Control – Multipurpose	PC
	AV Remote Control	Remote Control – AV	PS, PC
	Simple Remote Control	Remote Control – Simple	PC, PS
Repeater Slave	Repeater Slave	Repeater	AOS
	IR Repeater	IR Repeater	AOS
Static Controller	(Not recognized by client)	Gateway	CSC
	PC Controller	Central Controller	CSC
	Set Top Box	Set Top Box	CSC, SSC, PC
	TV	TV	CSC, SSC, PC
	Sub System Controller	Sub System Controller	SSC
	Gateway	Gateway	CSC, NAS
Thermostat	General Thermostat V2	Thermostat – HVAC	AOS, LSS, RSS, SSC, RPC
	Setback Thermostat	Thermostat – Setback	AOS, LSS, RSS, SSC, RPC
Wall Controller	Basic Wall Controller	Wall Controller	AOS, PS, RSS

For more details about Z-Wave Plus Role Type, refer to [1].

4.1 AV Control Point

The AV Control Point Device Type is intended for simple AV components receiving AV commands.

Table 6, AV Control Point Device Type identifiers

Device Type	Identifiers
AV Control Point	GENERIC_TYPE_AV_CONTROL_POINT
	SPECIFIC_TYPE_NOT_USED

4.1.1 What Role Type to Use

The AV Control Point Device Type MUST use one of the following Role Types:

Table 7, AV Control Point Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.1.2 Backward Compatibility

The AV Control Point Device Type is backward compatible.

4.1.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.1.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Simple AV Control
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.1.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command.

In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report in that case.

4.1.6 Recommended Optional Features

None

4.1.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.2 Motorized Barrier Devices

The Motorized Barrier Device Types support the ability for users to remotely control a barrier and monitor its state.

Table 8, Device Type identifiers for use by Barrier Operator Devices

Device Type	Identifiers
Motorized Barrier - GDO	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_DOOR
Motorized Barrier - Gate	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_GATE
Motorized Barrier – Add-ON	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE _BARRIER_ADDON
Motorized Barrier – Open Only	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_BARRIER_OPEN_ONLY
Motorized Barrier – Close Only	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_BARRIER_CLOSE_ONLY

4.2.1 What Role Type to Use

The Motorized Barrier Device Type MUST use one of the following Role Types:

Table 9, Barrier Operator Devices Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.2.2 Backwards Compatibility

The Motorized Barrier Device Types are backward compatible.

4.2.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MAY request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.2.4 Mandatory Command Classes

The Motorized Barrier Devices MUST support the following Command Classes:

- Application Status
- Association, version 2 or newer
- Association Group Information
- Barrier Operator
- Battery (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Notification, version 4 or newer
- Power level
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.2.4.1 Command Class Support and Security level

The Motorized Barrier Device MUST support its Command Classes depending on Security Bootstrapping as follows:

- If security bootstrapped, it MUST support its Command Classes only if the highest granted key is S0 or S2 Access Control Security Class. It MUST NOT support its Command Classes at all if its highest granted Security Class is any other class than S0 or S2 Access Control.
- If it timed out waiting for security bootstrapping or S0/S2 bootstrapping failed, it MUST NOT support its Command Classes non-securely.

The above requirements MUST NOT apply for Command Classes that MUST always be in the NIF.

4.2.5 Basic Command Considerations

If the device optionally supports the Binary Switch Command Class or Multilevel Switch Command Class to control a built-in light source, the Basic Command Class MUST be supported.

The Basic Command Class MUST be implemented in the following way:

- Basic Set MUST be mapped to Binary Switch Set or Multilevel Switch Set
- Basic Get MUST be mapped to Binary Switch Get or Multilevel Switch Get
- Basic Report MUST be mapped to Binary Switch Report or Multilevel Switch Report

If the device does not support the Binary Switch Command Class or Multilevel Switch Command Class, the Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.2.6 Recommended Optional Features

Motorized Barrier devices MAY feature optional command classes (support or control) that extend the capabilities of the device. It is RECOMMENDED that such features are supported securely.

- User Code Command Class - The User Code Command Class MAY be used securely to enable configuration of user codes that can unlock / activate the barrier.
- Binary Switch Command Class – The Binary Switch Command Class can be used to control a built-in lighting source in the device.
- If the device supports or requires the use of multiple proprietary sensors and the manufacture would like to provide detailed information about the sensor to the system, it is recommended that the device represents these sensors as End Points via the Multi Channel Command Class (V4). For example if the device supports both a proprietary contact sensor and a proprietary tilt sensor the Multi Channel Command Class in conjunction with the Battery Command Class would be used to provide detail battery state information to the system.

4.2.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.3 Central Controller

The Central Controller Device Type SHOULD be used for all devices operating as the central device in the network. It will also be the device that is in charge of all out of the box configuration including setting up the Z-Wave Plus Lifeline and ensuring all network requirements are met.

Table 10, Central Controller Device Type identifiers

Device Type	Identifiers
Central Controller	GENERIC_TYPE_STATIC_CONTROLLER
	SPECIFIC_TYPE_PC_CONTROLLER

4.3.1 What Role Type to Use

The Central Controller Device Type MUST use the following Role Type:

Table 11, Central Static Controller Role Type identifier

Role Type	Identifiers
Central Static Controller (CSC)	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC

4.3.2 Backward Compatibility

The Central Controller Device Type is backward compatible because it uses the same generic and Specific Device Class identifiers as before the introduction of Z-Wave Plus. Only additional requirements are introduced in Z-Wave Plus.

4.3.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MUST request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.3.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- CRC-16 Encapsulation
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Manufacturer Specific
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Power Level
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Anti-Theft Unlock, version 1
- Association, version 2 or newer
- Basic
- Multi Channel, version 4 or newer
- Multi Channel Association, version 3 or newer
- CRC-16 Encapsulation
- Security 0 (S0)
- Security 2 (S2)
- Wake up, version 2 or newer

4.3.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The Central Controller Device Type MUST control unknown devices with Basic Set = 255 (On/Open) or Basic Set = 0 (Off/Close)

4.3.6 Recommended Optional Features

For control of battery-operated devices it can be beneficial to implement the Multi Command Command Class.

4.4 Color Switch DT

The Color Switch Device Type is intended for a lighting product having the ability to change its color.

Table 12, Color Switch Device Type identifiers

Device Type	Identifiers
Color Switch	GENERIC_TYPE_SWITCH_BINARY (0x10) if supporting Binary Switch GENERIC_TYPE_SWITCH_MULTILEVEL (0x11) if supporting Multilevel Switch
	SPECIFIC_TYPE_COLOR_TUNABLE_BINARY (0x02) if supporting Binary Switch SPECIFIC_TYPE_COLOR_TUNABLE_MULTILEVEL (0x02) if supporting Multilevel Switch

4.4.1 What Role Type to Use

The Color Switch Device Type MUST use the following Role Type:

Table 13, Color Switch Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.4.2 Backward Compatibility

The Color Switch Device Type is backward compatible because it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.4.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.4.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Color Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch or Binary Switch
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.4.5 Basic Command Considerations

If supporting the Multilevel Switch Command Class, the Color Switch Device Type MUST support:

- Basic Set = 255 maps to Multilevel Switch Set = 255
- Basic Set = 0 maps to Multilevel Switch Set = 0
- Basic Set = 1-99 maps to Multilevel Switch Set = 1-99
- Basic Get/Report maps to Multilevel Switch Get/Report

If supporting the Binary Switch Command Class, the Color Switch Device Type MUST support:

- Basic Set maps to Binary Switch Set
- Basic Get maps to Binary Switch Get
- Basic Report maps to Binary Switch Report.

4.4.6 Recommended Optional Features

None

4.4.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.5 Display - Simple

The Display (simple) Device Type is intended for simple displays that can show information pushed out by the CSC. It SHOULD NOT be used for touch panel displays that allow control of other devices.

Table 14, Display (simple) Device Type identifiers

Device Type	Identifiers
Display – Simple	GENERIC_TYPE_DISPLAY
	SPECIFIC_TYPE_SIMPLE_DISPLAY

4.5.1 What Role Type to Use

The Display (simple) Device Type MUST use one of the following Role Types:

Table 15, Display (simple) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.5.2 Backward Compatibility

The Display (simple) Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.5.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.5.4 Mandatory Command Classes

Support

- Association (version 2 or newer)
- Association Group Information
- Battery – (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Screen Meta Data
- Supervision
- Transport Service, version 2 or newer
- Version (version 2 or newer)
- Z-Wave Plus Info, version 2 or newer

4.5.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.5.6 Recommended Optional Features

None

4.5.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.6 Door Lock - Keypad

The Door Lock Keypad Device Type is intended for door locks with an optional built-in keypad..

Table 16, Door Lock Keypad Device Type identifiers

Device Type	Identifiers
Door Lock – Keypad	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_KEYPAD_DOOR_LOCK

4.6.1 What Role Type to Use

The Door Lock - Keypad Device Type MUST use one of the following Role Types:

Table 17, Door Lock Keypad Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.6.2 Backward Compatibility

The Door Lock Keypad Device Type is only backward compatible on the Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.6.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MAY request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.6.4 Mandatory Command Classes

The Door Lock - Keypad MUST support the following Command Classes :

- Association, version 2 or newer
- Association Group Information
- Battery (If LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Door Lock
- Manufacturer Specific
- Power level
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- User Code (if the device has a keypad)
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.6.4.1 Command Class Support and Security level

The Door Lock - Keypad MUST support its Command Classes depending on Security bootstrapping as follows:

- If security bootstrapped, it MUST support its Command Classes only if the highest granted key is S0 or S2 Access Control Security Class. It MUST NOT support its Command Classes at all if its highest granted Security Class is any other class than S0 or S2 Access Control.
- If it timed out waiting for security bootstrapping or S0/S2 bootstrapping failed, it MUST NOT support its Command Classes non-securely.

The above requirements MUST NOT apply for Command Classes that MUST always be in the NIF.

4.6.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.6.6 Recommended Optional Features

Door Lock Keypad devices SHOULD feature optional command classes (support or control) that extend the capabilities of the device. It is important that careful consideration is taken when deciding whether a Command Class should be used securely or non-securely.

Command Classes that if supported MUST be supported using the highest Security Class only:

- Door Lock Logging and all REQUIRED command classes to support Logging
- Schedule Command Class and all REQUIRED command classes to support scheduling

4.6.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.7 Entry Control Keypad

The Entry Control Keypad Device Type is used for distributed entry control user interfaces such as a keypad, RFID reader or QR code reader. The device implements a dump terminal that sends user data to and receives status indications from a central entry control application. The central application may control services such as alarm systems or electronic locks, based on the notifications from the Entry Control Keypad.

Device Type	Identifier
Entry Control Keypad	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_KEYPAD

Table 18, Entry Control Keypad Device Type identifiers

4.7.1 What Role Type to Use

The Entry Control Keypad Device Type MUST use the following Role Type:

Table 19, Entry Control Keypad Role Type identifier

Role Type	Identifier
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING

4.7.2 Backward Compatibility

The Entry Control Keypad Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.7.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MAY request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.7.4 Mandatory Command Classes

The Entry Control Keypad MUST support the following Command Classes:

- Association, version 2 or newer
- Association Group Information
- Battery (If LSS or RSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Entry Control
- Manufacturer Specific
- Power level
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RSS)
- Z-Wave Plus Info, version 2 or newer

4.7.4.1 Command Class Support and Security level

The Entry Control Keypad MUST support its Command Classes depending on Security bootstrapping as follows:

- If security bootstrapped, it MUST support its Command Classes only if the highest granted key is S0 or S2 Access Control Security Class. It MUST NOT support its Command Classes at all if its highest granted Security Class is any other class than S0 or S2 Access Control.
- If it timed out waiting for security bootstrapping or S0/S2 bootstrapping failed, it MUST NOT support its Command Classes non-securely.

The above requirements MUST NOT apply for Command Classes that MUST always be in the NIF.

4.7.5 Basic Command Considerations

No Basic mapping is defined for the Secure Keypad Device Class. It is therefore RECOMMENDED to ignore any received basic commands.

4.7.6 Recommended Optional Features

A device MAY support one or more of the following command classes. If supported, command classes found in the following list MUST be supported securely:

- Indicator
- Screen Attributes
- Screen Meta Data

4.7.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.8 Fan Switch

The Fan Switch Device Type is used to turn on/off or control speed of fan devices. It can be incorporated into the fan itself or being an in-wall switch.

Table 20, Fan Switch Device Type identifiers

Device Type	Identifiers
Fan Switch	GENERIC_TYPE_SWITCH_MULTILEVEL
	SPECIFIC_TYPE_FAN_SWITCH

4.8.1 What Role Type to Use

The Fan Switch Device Type MUST use the following Role Type:

Table 21, Fan Switch Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.8.2 Backward Compatibility

The Fan Switch Device Type is only backward compatible with the classic Z-Wave Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.8.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.8.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.8.5 Basic Command Considerations

The Fan Switch Device Type MUST support:

- Basic Set = 255 maps to Multilevel Switch Set = 255
- Basic Set = 0 maps to Multilevel Switch Set = 0
- Basic Set = 1-99 maps to Multilevel Switch Set = 1-99
- Basic Get/Report maps to Multilevel Switch Get/Report

4.8.6 Recommended Optional Features

None

4.8.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.9 Gateway

The Gateway Device Type is intended for all gateway devices that provide access in and potentially out of the Z-Wave network. The gateway MAY be an application gateway or a transparent gateway providing transparent access (e.g. Z-Wave application Command Class level or all types of IP traffic) between two network technologies.

Table 22, Gateway Device Type identifiers

Device Type	Identifiers
Gateway	GENERIC_TYPE_STATIC_CONTROLLER
	SPECIFIC_TYPE_GATEWAY

4.9.1 What Role Type to Use

The Gateway Device Type MUST use one of the following Role Types:

Table 23, Gateway Role Type identifier

Role Type	Identifiers
Central Static Controller (CSC)	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC
Network Aware Slave (NAS)	ROLE_TYPE_NETWORK_AWARE_SLAVE

4.9.2 Backward Compatibility

The Gateway Device Type is only backward compatible on the Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus. The Gateway Device Type SHOULD be used with a GUI client.

4.9.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MUST request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.9.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- CRC-16 Encapsulation
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller (if CSC)
- Manufacturer Specific
- Power Level
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Anti-Theft Unlock, version 1
- Association, version 2 or newer
- Basic
- CRC-16 Encapsulation
- Multi Channel, version 4 or newer
- Multi Channel Association, version 3 or newer
- Security 0 (S0) (if CSC)
- Security 2 (S2) (if CSC)
- Wake up, version 2 or newer (if CSC)

4.9.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The Gateway Device Type MUST control unknown devices with Basic Set = 255 (On/Open) or Basic Set = 0 (Off/Close)

4.9.6 Recommended Optional Features

For control of battery-operated devices, it can be beneficial to implement the Multi Command Command Class.

4.10 IR Repeater

The IR Repeater Device Type is intended for IR repeater devices, which relay IR signals specified via Z-Wave Commands. They do not implement any other application functionality that can be controlled.

Table 24, Repeater Device Type identifiers

Device Type	Identifiers
IR Repeater	GENERIC_TYPE_REPEATER_SLAVE (0x0F)
	SPECIFIC_TYPE_IR_REPEATER (0x03)

4.10.1 What Role Type to use

The IR Repeater Device Type MUST use the following Role Type:

Table 25, Repeater Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.10.2 Backwards Compatibility

The IR Repeater Device Type is only backward compatible on the Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus

4.10.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.10.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Device Reset Locally (if the device can be reset, refer to [1])
- IR Repeater
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version ,version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.10.5 Basic Command Considerations

The IR Repeater Device Type MUST NOT support the Basic Command Class since there is no functionality this can be mapped to.

4.10.6 Recommended Optional Features

None

4.10.7 Suggested Interview Process

Refer to [13] interview process for each individual command class.

4.11 Irrigation Control

The Irrigation Control Device Type is used for stand-alone irrigation control devices as well as for the Root Device of Multi Channel Irrigation control devices with integrated valves.

Table 26, Irrigation Control Device Type identifiers

Device Type	Identifiers
Irrigation Control	GENERIC_TYPE_SWITCH_BINARY
	SPECIFIC_TYPE_IRRIGATION_CONTROLLER

4.11.1 What Role Type to Use

The Device Type MUST use the following Role Type:

Table 27, Irrigation Control Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.11.2 Backward Compatibility

The Irrigation Control Device Type is only backward compatible on the Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus

4.11.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.11.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Binary Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.11.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.11.6 Recommended Optional Features

None

4.11.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.12 Light Dimmer Switch

The Light Dimmer Switch Device Type is intended for lighting application that incorporates a dimming function to brighten or dim a local load light.

Table 28, Light Dimmer Switch Device Type identifiers

Device Type	Identifiers
Light Dimmer Switch	GENERIC_TYPE_SWITCH_MULTILEVEL
	SPECIFIC_TYPE_POWER_SWITCH_MULTILEVEL

4.12.1 What Role Type to Use

The Light Dimmer Switch Device Type MUST use the following Role Type:

Table 29, Light Dimmer Switch Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.12.2 Backward Compatibility

The Light Dimmer Switch Device Type is backward compatible because it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.12.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.12.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.12.5 Basic Command Considerations

The Device Type MUST support:

- Basic Set = 255 maps to Multilevel Switch Set = 255
- Basic Set = 0 maps to Multilevel Switch Set = 0
- Basic Set = 1-99 maps to Multilevel Switch Set = 1-99
- Basic Get/Report maps to Multilevel Switch Get/Report

4.12.6 Recommended Optional Features

None

4.12.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.13 Lockbox

The Lockbox Device Type is intended for devices that have Z-Wave directly built into the Lockbox. It supports the ability for users to remotely control their Lockbox.

Table 30: Device Type identifiers for use by Lockbox Devices

Device Type	Identifiers
Lockbox	GENERIC_TYPE_ENTRY_CONTROL
	SPECIFIC_TYPE_SECURE_LOCKBOX

4.13.1 What Role Type to Use

The Lockbox Device Type MUST use one of the following Role Types:

Table 31: Lockbox Role Type Identifiers

Role Type	Identifiers
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Sub Static Controller (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING

4.13.2 Backwards Compatibility

The Lockbox Device Type is only backward compatible with classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.13.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MAY request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.13.4 Mandatory Command Classes

The Lockbox MUST support the following Command Classes:

- Association, version 2 or newer
- Association Group Information
- Battery (if LSS, RSS or RPC)
- Device Reset Locally (if the device can be reset, refer to [1])
- Door Lock
- Inclusion Controller (if SSC or RPC)
- Manufacturer Specific
- Notification, version 3 or newer
- Power level
- Security 0 (S0)
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake-Up (if RSS or RPC)
- Z-Wave Plus Info, version 2 or newer

4.13.4.1 Command Class Support and Security level

The Lockbox MUST support its Command Classes depending on Security bootstrapping as follows:

- If security bootstrapped, it MUST support its Command Classes only if the highest granted key is S0 or S2 Access Control Security Class. It MUST NOT support its Command Classes at all if its highest granted Security Class is any other class than S0 or S2 Access Control.
- If it timed out waiting for security bootstrapping or S0/S2 bootstrapping failed, it MUST NOT support its Command Classes non-securely.

The above requirements MUST NOT apply for Command Classes that MUST always be in the NIF.

4.13.5 Basic Command Considerations

For security considerations the Lockbox Generic Device Class MUST NOT support the Basic Command Class.

4.13.6 Recommended Optional Features

Lockbox devices MAY feature optional command classes (support or control) that extend the capabilities of the device. It is important that careful consideration be taken when deciding whether a Command Class SHOULD be used securely or non-securely.

- User Code Command Class:-The User Code Command Class can be used when encapsulated in the Security 0 (S0) Command Class by the application to enable the configuration of user codes that can unlock / activate the Lockbox.

4.13.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.14 On/Off Power Switch

The On/Off Power Switch Device Type is used to turn on any device that is connected to power. Examples include lights, appliances etc.

Table 32, On/Off Power Switch Device Type identifiers

Device Type	Identifiers
On/Off Power Switch	GENERIC_TYPE_SWITCH_BINARY
	SPECIFIC_TYPE_POWER_SWITCH_BINARY

4.14.1 What Role Type to Use

The On/Off Power Switch Device Type MUST use one of the following Role Types:

Table 33, On/Off Power Switch Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.14.2 Backward Compatibility

The On/Off Power Switch Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.14.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.14.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Binary Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.14.5 Basic Command Considerations

The On/Off Power Switch Device Type MUST support:

- Basic Set maps to Binary Switch Set
- Basic Get maps to Binary Switch Get
- Basic Report maps to Binary Switch Report.

A supporting device MUST comply with the Binary Switch Command Class specification.

4.14.6 Recommended Optional Features

For energy management applications, it SHOULD support the Meter Command Class (version 2 or newer) for reporting energy consumption.

4.14.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.15 Power Strip

The Power Strip Device Type is intended for power strip applications. One or more outlets can be supported.

Table 34, Power Strip Device Type identifiers

Device Type	Identifiers
Power Strip	GENERIC_TYPE_SWITCH_BINARY
	SPECIFIC_TYPE_POWER_STRIP

4.15.1 What Role Type to Use

The Power Strip Device Type MUST use the following Role Type:

Table 35, Power Strip Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.15.2 Backward Compatibility

The Power Strip Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.15.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.15.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Binary Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multi Channel, version 4 or newer
- Multi Channel Association, version 3 or newer
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.15.5 Multi Channel Considerations

Each socket MUST be implemented as a separate Multi Channel Endpoint.

4.15.6 Basic Command Considerations

The Power Strip Device Type MUST support:

- Basic Set = 255 maps to Binary Switch Set = 255
- Basic Set = 0 maps to Binary Switch Set = 0
- Basic Get/Report maps to Binary Switch Get/Report

4.15.7 Recommended Optional Features

For energy management applications it SHOULD be considered to support the Meter Command Class (version 2 or newer) for reporting energy consumption. This information SHOULD be communicated through the lifeline.

4.15.8 Suggested interview process

Refer to [13] interview process for each individual command class.

4.16 Remote Control - AV

The Remote Control (AV) Device Type is intended for simple AV remotes that typically communicate directly with AV components.

Table 36, Remote Control (AV) Device Type identifiers

Device Type	Identifiers
Remote Control - AV	GENERIC_TYPE_GENERIC_CONTROLLER
	SPECIFIC_TYPE_REMOTE_CONTROL_AV

4.16.1 What Role Type to Use

The Remote Control (AV) Device Type MUST use one of the following Role Types:

Table 37, Remote Control (AV) Role Type identifier

Role Type	Identifiers
Portable Slave (PS)	ROLE_TYPE_SLAVE_PORTABLE
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE

4.16.2 Backward Compatibility

The Remote Control (AV) Device Type is only backward compatible with the classic Z-Wave Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.16.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.16.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Inclusion Controller (if PC)
- Power Level
- Security 2 (S2)
- Simple AV Control
- Supervision
- Transport Service, version 2 or newer
- Wake Up, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Basic (if PC)
- Simple AV Control

4.16.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

It is RECOMMENDED to have one of the association groups to transmit control via Basic Command Class. This will enable the control of most Z-Wave devices on a basic level.

4.16.6 Recommended Optional Features

It is RECOMMENDED to implement an Association Group for sending the Simple AV Control Set commands when a user presses, releases or holds a button for actuating associated AV devices. The Remote Control AV MAY implement several Association Groups sending Simple AV Control Set commands in order to control multiple AV devices individually.

It is RECOMMENDED to use the PC Role Type for the Remote Control – AV Device Type. If the Remote Control AV is a controller, it is able to set-up a network and control slave devices supporting Simple AV Command Class without requiring an external controller in the network.

4.16.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.17 Remote Control – Multi Purpose

The Remote Control (Multi Purpose) Device Type is intended for portable controllers that support advanced functions. This Device Type is also able to setup and configure the Z-Wave network.

Table 38, Remote Control (multi purpose) Device Type identifiers

Device Type	Identifiers
Remote Controller – Multi Purpose	GENERIC_TYPE_GENERIC_CONTROLLER
	SPECIFIC_TYPE_PORTABLE_REMOTE_CONTROLLER

4.17.1 What Role Type to Use

The Remote Control (Multi Purpose) Device Type MUST use the following Role Type:

Table 39, Remote Control (multi purpose) Role Type identifier

Role Type	Identifiers
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE

4.17.2 Backward Compatibility

The Remote Control (Multi Purpose) Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.17.3 S2 Security Classes

If the node supports the Security 2 Command Class, it MUST request at least one of the following Security Classes:

- S2 Access Control Security Class (refer to 3.7.6.2.1)
- S2 Authenticated Security Class (refer to 3.7.6.2.2)
- S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.17.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Basic

4.17.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The Remote Control (Multi Purpose) Device Type MUST be able to control unknown devices with Basic Set = 255 (On/Open) or Basic Set = 0 (Off/Close)

4.17.6 Recommended Optional Features

None

4.18 Remote Control - Simple

The Remote Control (Simple) Device Type is intended for simple remotes such as key fobs or other portable controllers with a couple of buttons. It is optimized to communicate its button status to a SIS when present. This allows for easy configuration and setup. A Simple remote control device can support 1 or more buttons.

Table 40, Remote Control (simple) Device Type identifiers

Device Type	Identifiers
Remote Control - Simple	GENERIC_TYPE_GENERIC_CONTROLLER
	SPECIFIC_TYPE_REMOTE_CONTROL_SIMPLE

4.18.1 What Role Type to Use

The Remote Control (Simple) Device Type MUST use the following Role Type:

Table 41, Remote Control (simple) Role Type identifier

Role Type	Identifiers
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE
Portable Slave (PS)	ROLE_TYPE_SLAVE_PORTABLE

4.18.2 Backward Compatibility

The Remote Control (Simple) Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.18.3 S2 Security Classes

If the node supports the Security 2 Command Class, it MUST request at least one of the following Security Classes:

- S2 Access Control Security Class (refer to 3.7.6.2.1)
- S2 Authenticated Security Class (refer to 3.7.6.2.2)
- S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.18.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery
- Central Scene
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.18.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.18.6 Recommended Optional Features

None

4.19 Repeater

The Repeater Device Type is intended for repeater devices, which do not implement any other application functionality that can be controlled. A device based on the Repeater Device Type only exists in the network to assist other nodes to reach each other.

Table 42, Repeater Device Type identifiers

Device Type	Identifiers
Repeater	GENERIC_TYPE_REPEATER_SLAVE
	SPECIFIC_TYPE_REPEATER_SLAVE

4.19.1 What Role Type to use

The Repeater Device Type MUST use the following Role Type:

Table 43, Repeater Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON

4.19.2 Backwards Compatibility

The Repeater Device Type is backwards compatible as it uses classic Z-Wave Generic and Specific Device Class.

4.19.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.19.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version ,version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.19.5 Basic Command Considerations

The Repeater Device Type MUST NOT support the Basic Command Class since there is no functionality this can be mapped to.

4.19.6 Recommended Optional Features

None

4.19.7 Suggested Interview Process

Refer to [13] interview process for each individual command class.

4.20 Sensor - Notification

The Sensor - Notification Device Type is intended for sensor devices sending notifications. Examples include door/window sensors, PIR sensors etc…

Table 44, Sensor (Notification) Device Type identifiers

Device Type	Identifiers
Sensor - Notification	GENERIC_TYPE_SENSOR_NOTIFICATION
	SPECIFIC_TYPE_NOTIFICATION_SENSOR

4.20.1 What Role Type to Use

The Sensor - Notification Device Type MUST use one of the following Role Types:

Table 45, Sensor (Notification) Role Type identifiers

Role Type	Identifiers
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.20.2 Backward Compatibility Requirements

The Sensor - Notification Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.20.3 S2 Security Classes

If the node supports the Security 2 Command Class and is a controller, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is a slave, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.20.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if RPC, RSS or LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller (if RPC)
- Manufacturer Specific
- Notification
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RPC or RSS)
- Z-Wave Plus Info, version 2 or newer

4.20.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

A push mode Notification node MAY support the Basic Command Class in order to switch the unsolicited transmission of notifications via association groups On and Off. In this case the Basic Value MUST be mapped to the Notification Status of the Notification Command Class.

- Basic Set = Enable/disable the unsolicited transmission of Notification Reports via Association groups. A node supporting several Notification Types MUST enable/disable all the Notification Types simultaneously when receiving Basic Set On/Off.
- Basic Get = Query the unsolicited transmission status of Notification Reports via Association groups.
- Basic Report = Advertise the unsolicited transmission status of Notification Reports via Association groups. A node supporting several Notification Types MUST report 0xFF (enabled) if at least one Notification Type status is enabled.

4.20.6 Recommended Optional Features

In certain sensor application it can be a benefit to use the Multi Command Command Class to save battery. However the application MUST support non Multi Command Command Class communication.

It is RECOMMENDED to have one of the association groups to transmit control via Basic Command Class. This will enable control of most Z-Wave devices on a basic level.

For door and window sensors, it is RECOMMENDED to use the Notification Type: “Access Control (0x06)“ with the events: “Door/Window Open” and ”Door/Window Closed” (respectively 0x16 and 0x17).

4.20.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.21 Sensor - Multilevel

The Sensor - Multilevel Device Type is intended for sensor devices reporting measurements. Examples include door/window sensors, temperature/humidity sensors, etc…

Table 46, Sensor (Multilevel) Device Type identifiers

Device Type	Identifiers
Sensor - Multilevel	GENERIC_TYPE_SENSOR_MULTILEVEL
	SPECIFIC_TYPE_ROUTING_MULTILEVEL_SENSOR

4.21.1 What Role Type to Use

The Sensor – Multilevel Device Type MUST use one of the following Role Types:

Table 47, Sensor (Multilevel) Role Type identifiers

Role Type	Identifiers
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.21.2 Backward Compatibility Requirements

The Sensor - Multilevel Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.21.3 S2 Security Classes

If the node supports the Security 2 Command Class and is a controller, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is a slave, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.21.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if RPC, RSS or LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller (if RPC)
- Manufacturer Specific
- Multilevel Sensor
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RPC or RSS)
- Z-Wave Plus Info, version 2 or newer

4.21.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.21.6 Recommended Optional Features

In some sensor applications, it can be beneficial to use the Multi Command Command Class to save battery life. However the application MUST support non Multi Command Command Class communication.

It is RECOMMENDED to have one of the association groups to transmit control via Basic Command Class. This will enable control of most Z-Wave devices on a basic level.

4.21.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.22 Set Top Box

The Set Top Box Device Type can have many roles. It can be used as the central gateway for the house or just a simple controller that support an AV remote or can execute simple home control commands.

Table 48, Set Top Box Device Type identifiers

Device Type	Identifiers
Set Top Box	GENERIC_TYPE_STATIC_CONTROLLER
	SPECIFIC_TYPE_SET_TOP_BOX

4.22.1 What Role Type to Use

The Set Top Box Device Type MUST use one of the following Role Types:

Table 49, Set Top Box Role Type identifiers

Role Type	Identifiers
Central Static Controller (CSC)	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC
Sub Static Control (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE

4.22.2 Backward Compatibility

The Set Top Box Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.22.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is based on the CSC role type, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MUST request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.22.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- CRC-16 Encapsulation (if CSC)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Power Level
- Manufacturer Specific
- Security 0 (S0) (if CSC)
- Security 2 (S2)
- Supervision
- Simple AV
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Anti-Theft Unlock, version 1
- Association, version 2 or newer
- Basic
- CRC-16 Encapsulation (if CSC)
- Multi Channel, version 4 or newer
- Multi Channel Association, version 3 or newer (if CSC)
- Security 0 (S0) (if CSC)
- Security 2 (S2) (if CSC)
- Wake Up, version 2 or newer (if CSC or SSC)

4.22.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The Set Top Box Device Type MUST control unknown devices with Basic Set = 255 (On/Open) or Basic Set = 0 (Off/Close)

4.22.6 Recommended Optional Features

For battery operated devices, it can be beneficial to support the Multi Command Command Class.

4.23 Siren

The Siren Device Type is intended for devices with any type of audio and/or visual notification. It is typically used with security systems.

Table 50, Siren Device Type identifiers

Device Type	Identifiers
Siren	GENERIC_TYPE_SWITCH_BINARY
	SPECIFIC_TYPE_SIREN

4.23.1 What Role Type to Use

The Siren Device Type MUST use one of the following Role Types:

Table 51, Siren Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.23.2 Backward Compatibility

The Siren Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.23.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.23.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Binary Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.23.5 Basic Command Considerations

The Siren Device Type MUST support:

- Basic Set = 255 maps to Binary Switch Set = 255
- Basic Set = 0 maps to Binary Switch Set = 0
- Basic Get/Report maps to Binary Switch Get/Report

4.23.6 Recommended Optional Features

None

4.23.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.24 Sound Switch

The Sound Switch Device Type is intended for simple speaker or sound notification system with a pre-programmed sound inventory.

Table 52, Sound Switch Device Type identifiers

Device Type	Identifiers
Sound Switch	GENERIC_TYPE_AV_CONTROL_POINT (0x03)
	SPECIFIC_TYPE_SOUND_SWITCH (0x01)

4.24.1 What Role Type to Use

The Sound Switch Device Type MUST use one of the following Role Types:

Table 53, Sound Switch Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.24.2 Backward Compatibility

The Sound Switch Device Type is only backward compatible on the Generic Device Class level. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.24.3 S2 Security Classes

During S2 bootstrapping, the Sound Switch Device Type:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class
- MUST request the S2 Unauthenticated Security Class

4.24.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Sound Switch
- Device Reset Locally (if the device can be reset)
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.24.5 Basic Command Considerations

The Sound Switch MUST support the Basic Command Class.

- Basic Set Command (value) MUST map to Sound Switch Tone Play Set Command (Tone Identifier).
- Basic Get Command MUST map to Sound Switch Tone Play Get Command
- Basic Report Command MUST map to Sound Switch Tone Play Report Command.

4.24.6 Recommended Optional Features

None

4.24.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.25 Sub Energy Meter

The Sub Energy Meter Device Type is intended for devices that provide sub energy metering data. This could be used to monitor the power consumption of e.g. the washer and/or dryer in the home. A sub meter MUST NOT support the Binary Switch Command Class. In this case the On/Off power switch MUST be used and add support for the Meter Command Class (version 2 or newer). For full home meter applications refer to Simple Whole Home Energy Meter.

Table 54, Sub Energy Meter Device Type identifiers

Device Type	Identifiers
Sub Energy Meter	GENERIC_TYPE_METER
	SPECIFIC_TYPE_SIMPLE_METER

4.25.1 What Role Type to Use

The Sub Energy Meter Device Type MUST use one of the following Role Types:

Table 55, Sub Energy Meter Role Type identifier

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING

4.25.2 Backward Compatibility

The Sub Energy Meter Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.25.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.25.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if RSS)
- CRC-16 Encapsulation
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Meter, version 2 or newer
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up (if RSS)
- Z-Wave Plus Info, version 2 or newer

4.25.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.25.6 Recommended Optional Features

None

4.25.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.26 Sub System Controller

The Sub System Controller Device Type is intended for systems that require a controller device to collect data or control sub systems. It will not be used as a central controller.

Table 56, Sub System Controller Device Type identifiers

Device Type	Identifiers
Sub System Controller	GENERIC_TYPE_STATIC_CONTROLLER
	SPECIFIC_TYPE_SUB_SYSTEM_CONTROLLER

4.26.1 What Role Type to Use

The Sub System Controller Device Type MUST use the following Role Type:

Table 57, Sub System Controller Role Type identifier

Role Type	Identifiers
Sub Static Controller (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC

4.26.2 Backward Compatibility

The Sub System Controller Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.26.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.26.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- CRC-16 Encapsulation
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Manufacturer Specific
- Power Level
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Basic
- CRC-16 Encapsulation
- Multi Channel, version 4 or newer
- Wake Up, version 2 or newer

4.26.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The Sub System Controller Device Type MUST be able to control unknown devices with Basic Set = 255 (On/open) or Basic Set = 0 (Off/Close)

4.26.6 Recommended Optional Features

For battery-operated devices, it can be beneficial to support the Multi Command Command Class.

4.27 Thermostat - HVAC

The Thermostat (HVAC) Device Type is intended by thermostats that support set points and modes. It is typically used for all mainstream thermostats that can support e.g. Heating, Cooling and Fans.

Table 58, Thermostat (HVAC) Device Type identifiers

Device Type	Identifiers
Thermostat - HVAC	GENERIC_TYPE_THERMOSTAT
	SPECIFIC_TYPE_THERMOSTAT_GENERAL_V2

4.27.1 What Role Type to Use

The Thermostat – HVAC Device Type MUST use one of the following Role Types:

Table 59, Thermostat (HVAC) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Sub Static Controller (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING

4.27.2 Backward Compatibility

The Thermostat (HVAC) Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.27.3 S2 Security Classes

If the node supports the Security 2 Command Class and is a controller, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is a slave, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.27.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if RSS, LSS or RPC)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller (if SSC or RPC)
- Manufacturer Specific
- Powerlevel
- Security 2 (S2)
- Supervision
- Thermostat Mode
- Thermostat Set Point
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RSS or RPC)
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Wake Up, version 2 or newer (if SSC)

4.27.5 Basic Command Considerations

The Thermostat HVAC Device Type MUST implement:

- Basic Set (Value = 0x00) = Set Energy Saving Mode
- Basic Set (Value = 0xFF) = Set Comfort Mode
- Basic Get = Get Report
- Basic Report (Value = 0x00) = Report Energy Saving Mode
- Basic Report (Value = 0xFF) = Report Comfort Mode

Note: The implementation of Energy Saving Mode and Comfort Mode is manufacturer specific, and MUST be documented in the User's Manual.

4.27.6 Recommended Optional Features

None

4.27.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.28 Thermostat - Setback

The Thermostat Setback Device Type is intended for thermostats that typically do not allow for actual temperature settings but rather adjust the temperature up and down to certain thresholds.

Table 60, Thermostat (Setback) Device Type identifiers

Device Type	Identifiers
Thermostat - Setback	GENERIC_TYPE_THERMOSTAT
	SPECIFIC_TYPE_SETBACK_THERMOSTAT

4.28.1 What Role Type to Use

The Thermostat Setback Device Type MUST use one of the following Role Types:

Table 61, Thermostat (Setback) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Sub Static Controller (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING

4.28.2 Backward Compatibility

The Thermostat (Setback) Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.28.3 S2 Security Classes

If the node supports the Security 2 Command Class and is a controller, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is a slave, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.28.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS, RSS or RPC)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller (if SSC or RPC)
- Manufacturer Specific
- Powerlevel
- Security 2 (S2)
- Supervision
- Thermostat Setback
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RSS or RPC)
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Wake Up, version 2 or newer (if SSC)

4.28.5 Basic Command Considerations

The Thermostat Setback Device Type MUST implement:

- Basic Set (Value = 0x00) = Set Energy Saving Mode
- Basic Set (Value = 0xFF) = Set Comfort Mode
- Basic Get = Get Report
- Basic Report (Value = 0x00) = Report Energy Saving Mode
- Basic Report (Value = 0xFF) = Report Comfort Mode

Note: The implementation of Energy Saving Mode and Comfort Mode is manufacturer specific, and MUST be documented in the User's Manual.

4.28.6 Recommended Optional Features

In certain sensor applications, it can be a benefit to use the Multi Command Command Class to save battery. However the application MUST support non Multi Command Command Class communication.

4.28.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.29 TV

The TV Device Type can take many roles. It can be used as the central gateway for the house or just a simple controller that support an AV remote or can execute simple home control commands.

Table 62, TV Device Type identifiers

Device Type	Identifiers
TV	GENERIC_TYPE_STATIC_CONTROLLER
	SPECIFIC_TYPE_TV

4.29.1 What Role Type to Use

The TV Device Type MUST use one of the following Role Types:

Table 63, TV Role Type identifiers

Role Type	Identifiers
Central Static Controller (CSC)	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC
Sub Static Control (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE

4.29.2 Backward Compatibility

The TV Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.29.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MAY request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

If the node supports the Security 2 Command Class and is based on the CSC role type, it:

- MUST request the S2 Access Control Security Class (refer to 3.7.6.2.1)
- MUST request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.29.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- CRC-16 Encapsulation (if CSC)
- Device Reset Locally (if the device can be reset, refer to [1])
- Inclusion Controller
- Manufacturer Specific
- Powerlevel
- Security 0 (S0) (if CSC)
- Security 2 (S2)
- Supervision
- Simple AV
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

Control (refer to 3.6.3)

- Anti-Theft Unlock, version1
- Association, version 2 or newer
- Association Group Information (if CSC)
- Basic
- CRC-16 Encapsulation (if CSC)
- Multi Channel, version 4 or newer
- Multi Channel Association, version 3 or newer (if CSC)
- Security 0 (S0) (if CSC)
- Security 2 (S2) (if CSC)
- Wake Up, version 2 or newer) (if CSC or SSC)

4.29.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

The TV Device Type MUST control unknown devices with Basic Set = 255 (On/open) or Basic Set = 0 (Off/Close)

4.29.6 Recommended Optional Features

None

4.30 Valve – open/close

The Valve (open/close) Device Type is intended for devices that can open and close for utility systems such as water and gas lines.

Table 64, Valve (open/close) Device Type identifiers

Device Type	Identifiers
Valve – open/close	GENERIC_TYPE_SWITCH_BINARY
	SPECIFIC_TYPE_VALVE_OPEN_CLOSE

4.30.1 What Role Type to Use

The Valve Device Type MUST use one of the following Role Types:

Table 65, Valve (open/close) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.30.2 Backward Compatibility

The Valve (open/close) Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.30.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.30.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Binary Switch
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.30.5 Basic Command Considerations

The Valve – open/close Device Type MUST support:

- Basic Set: All values (0x00 to 0xFF) map to Binary Switch Set.
- Basic Get/Report maps to Binary Switch Get/Report

4.30.6 Recommended Optional Features

None

4.30.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.30.8 Additional considerations

The mapping of the Binary Switch Command Value and Basic Command Class Value to the physical state of the valve MUST be as follows:

- The value 0 MUST represent the lowest throughput, e.g. no water runs through the valve
- The value 255 MUST represent the highest throughtput, e.g the valve is fully open and water runs throught.

However, some certified nodes have used the opposite interpretation and use 255 to block the water, 0 to let the water through.

4.31 Wall Controller

The Wall Controller Device Type is intended for devices that allow for control of the Z-Wave network from push buttons (physical or virtual) on a device. Examples include scene and zone controller, wall mounted AV controllers. Device of this type can both be battery operated or mains powered. It can also include additional support for features such as local load control of lights through the Binary Switch or Multilevel Switch Command Class. A wall controller device can support 1 or more buttons.

Table 66, Wall Controller Device Type identifiers

Device Type	Identifiers
Wall Controller	GENERIC_TYPE_WALL_CONTROLLER
	SPECIFIC_TYPE_BASIC_WALL_CONTROLLER

4.31.1 What Role Type to Use

The Wall Controller Device Type MUST use one of the following Role Types:

Table 67, Wall Controller Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Portable Slave (PS)	ROLE_TYPE_SLAVE_PORTABLE
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING

4.31.2 Backward Compatibility

The Wall Controller Device Type is not backward compatible with classic Z-Wave Generic Device Class. The Device Type uses Generic and Specific Device Class identifiers introduced in Z-Wave Plus.

4.31.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- SHOULD request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.31.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if PS or RSS)
- Central Scene
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if PS or RSS)
- Z-Wave Plus Info, version 2 or newer

4.31.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

It is RECOMMENDED to have one of the association groups to transmit control via Basic Command Class. This will enable control of most Z-Wave devices on a basic level.

4.31.6 Recommended Optional Features

None

4.31.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.32 Whole Home Meter - Simple

The Whole Home Meter (Simple) Device Type is intended for devices that provide whole home consumption data. It is typically used by devices that attaches to the home energy meter or the main utility line for a consumers home.

Table 68, Whole Home Meter (Simple) Device Type identifiers

Device Type	Identifiers
Whole Home Meter – Simple	GENERIC_TYPE_METER
	SPECIFIC_TYPE_WHOLE_HOME_METER_SIMPLE

4.32.1 What Role Type to Use

The Whole Home Meter – Simple Device Type MUST use one of the following Role Types:

Table 69, Whole Home Meter (Simple) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Reporting Sleeping Slave (RSS)	ROLE_TYPE_SLAVE_SLEEPING_REPORTING

4.32.2 Backward Compatibility

The Whole Home Meter (Simple) Device Type is only backward compatible with the classic Z-Wave Generic Device Class. The Device Type uses a Specific Device Class identifier introduced in Z-Wave Plus.

4.32.3 S2 Security Classes

If the node supports the Security 2 Command Class, it:

- MUST NOT request the S2 Access Control Security Class
- MAY request the S2 Authenticated Security Class (refer to 3.7.6.2.2)
- MUST request the S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.32.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Battery (if LSS or RSS)
- CRC-16 Encapsulation
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Meter, version 2 or newer
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Wake Up, version 2 or newer (if RSS)
- Z-Wave Plus Info, version 2 or newer

4.32.5 Basic Command Considerations

If supported, the Basic Command Class MUST be implemented in the following way:

The Basic commands can freely be mapped to another Command Class supported by the device. The mapping MUST be documented in the User's Manual. The Basic Set, Get and Report commands MUST be mapped within the same Command Class. The Basic Report MUST be in accordance with the mapped Get command. In case the manufacturer deems that no relevant commands are available for mapping, a device receiving Basic commands MUST ignore them and the device MUST NOT respond with a Basic Report under any circumstances.

4.32.6 Recommended Optional Features

None

4.32.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.33 Window Covering No Position/Endpoint

The Window Covering No Position/Endpoint Device Type is intended for applications with no indication of position or endpoints hence it is not possible for this type of device to report its position at endpoints or position between endpoints. It can be ordered to move in directions and to stop the movement.

Table 70, Window Covering (no position/endpoint) Device Type identifiers

Device Type	Identifiers
Window Covering No Position/Endpoint	GENERIC_TYPE_SWITCH_MULTILEVEL
	SPECIFIC_TYPE_CLASS_A_MOTOR_CONTROL

4.33.1 What Role Type to Use

The Window Covering No Position/Endpoint Device Type MUST use one of the following Role Types:

Table 71, Window Covering (no position/endpoint) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.33.2 Backward Compatibility

The Window Covering No Position/Endpoint Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.33.3 S2 Security Classes

If the node supports the Security 2 Command Class, it MUST request at least one of the following Security Classes:

- S2 Access Control Security Class (refer to 3.7.6.2.1)
- S2 Authenticated Security Class (refer to 3.7.6.2.2)
- S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.33.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch, version 3 or newer
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.33.5 Basic Command Considerations

The Device Type MUST support:

- Basic Set = 255 maps to Multilevel Switch = 255
- Basic Set = 0 maps to Multilevel Switch = 0
- Basic Set = 1-99 MUST be ignored
- Basic Get/Report maps to Multilevel Switch Get/Report. The value 0xFE can be reported for unknown position.

4.33.6 Recommended Optional Features

None

4.33.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.34 Window Covering Endpoint Aware

The Window Covering Endpoint Aware Device Type is intended for applications with exact knowledge of endpoints but only imprecise position knowledge when between endpoints. It MUST be possible to instruct the application to go to endpoints and to stop motion. The application MAY also respond to instructions to go to a position between the endpoints. This motor class can report its position at endpoints and also an imprecise position between endpoints. Typical application implementing Window Covering Endpoint Aware is e.g. up/down motion of window shades where the position is measured over time.

Table 72, Window Covering (endpoint aware) Device Type identifiers

Device Type	Identifiers
Window Covering Endpoint Aware	GENERIC_TYPE_SWITCH_MULTILEVEL
	SPECIFIC_TYPE_CLASS_B_MOTOR_CONTROL

4.34.1 What Role Type to Use

The Window Covering Endpoint Aware Device Type MUST use one of the following Role Types:

Table 73, Window Covering (endpoint aware) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.34.2 Backward Compatibility

The Window Covering Endpoint Aware Device Type is backward compatible as it uses classic Z-Wave Generic and Specific Device Class identifiers.

4.34.3 S2 Security Classes

If the node supports the Security 2 Command Class, it MUST request at least one of the following Security Classes:

- S2 Access Control Security Class (refer to 3.7.6.2.1)
- S2 Authenticated Security Class (refer to 3.7.6.2.2)
- S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.34.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch, version 3 or newer
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.34.5 Basic Command Considerations

The Window Covering Endpoint Aware Device Type MUST support:

- Basic Set = 255 MUST map to Multilevel Switch = 255
- Basic Set = 0 MUST map to Multilevel Switch = 0
- Basic Set = 1-99 MAY be ignored but
  SHOULD map to Multilevel Switch = 1-99 if the application can go to a specific position.

  If not mapped to Multilevel Switch = 1-99, all values in the parameter range SHOULD map to Multilevel Switch = 99.

  Other mappings MUST NOT be used
- Basic Get/Report MUST map transparently to the Multilevel Switch Get/Report. The value 0xFE MAY be reported for the unknown position.

4.34.6 Recommended Optional Features

None

4.34.7 Suggested interview process

Refer to [13] interview process for each individual command class.

4.35 Window Covering Position/Endpoint Aware

The Window Covering Position/Endpoint Aware Device Type is intended for application with knowledge of precise position i.e. the motor component provides feedback. This Device Type can be instructed to go to as well as report back its exact position and endpoints. Typical application implementing Window Covering Position/Endpoint Aware is motor controllers having feedback mechanism.

Table 74, Window Covering (position/endpoint aware) Device Type identifiers

Device Type	Identifiers
Window Covering Position/Endpoint Aware	GENERIC_TYPE_SWITCH_MULTILEVEL
	SPECIFIC_TYPE_CLASS_C_MOTOR_CONTROL

4.35.1 What Role Type to Use

The Window Covering Position/Endpoint Aware Device Type MUST use one of the following Role Types:

Table 75, Window Covering (position/endpoint aware) Role Type identifiers

Role Type	Identifiers
Always On Slave (AOS)	ROLE_TYPE_SLAVE_ALWAYS_ON
Listening Sleeping Slave (LSS)	ROLE_TYPE_SLAVE_SLEEPING_LISTENING

4.35.2 Backward Compatibility

The Window Covering Position/Endpoint Aware Device Type is backward compatible because it uses the same Generic and Specific Device Class identifiers as before the introduction of Z-Wave Plus. Only additional requirements are introduced in Z-Wave Plus.

4.35.3 S2 Security Classes

If the node supports the Security 2 Command Class, it MUST request at least one of the following Security Classes:

- S2 Access Control Security Class (refer to 3.7.6.2.1)
- S2 Authenticated Security Class (refer to 3.7.6.2.2)
- S2 Unauthenticated Security Class (refer to 3.7.6.2.3)

4.35.4 Mandatory Command Classes

Support

- Association, version 2 or newer
- Association Group Information
- Basic
- Battery (if LSS)
- Device Reset Locally (if the device can be reset, refer to [1])
- Manufacturer Specific
- Multilevel Switch, version 3 or newer
- Powerlevel
- Security 2 (S2)
- Supervision
- Transport Service, version 2 or newer
- Version, version 2 or newer
- Z-Wave Plus Info, version 2 or newer

4.35.5 Basic Command Considerations

The Window Covering Position/Endpoint Aware Device Type MUST support:

- Basic Set = 255 maps to Multilevel Switch = 255, 99 or 50.
- Basic Set = 0 maps to Multilevel Switch = 0
- Basic Set = 1-99 maps to Multilevel Switch = 1-99
- Basic Get/Report maps to Multilevel Switch Get/Report.

4.35.6 Recommended Optional Features

None

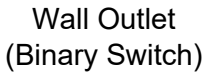
4.35.7 Suggested interview process

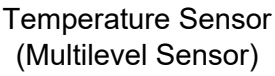
Refer to [13] interview process for each individual command class.

APPENDIX A Z-WAVE PLUS DEVICE TYPES IN A GRAPHICAL USER INTERFACE

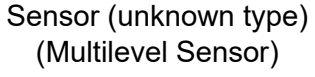
Z-Wave Plus supports the use of graphical user interfaces for installation, association and operation of Z-Wave enabled products. The general principle is that a user MUST get a meaningful representation of any product included in the network. This will not only be visually appealing to users who already use a tablet computer for many other tasks. It will also provide a more intuitive workspace to an installer that can get an immediate overview of a system.

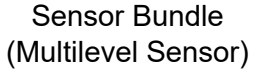
The icons below are a few examples of the icons that a Z-Wave Plus user MAY meet:





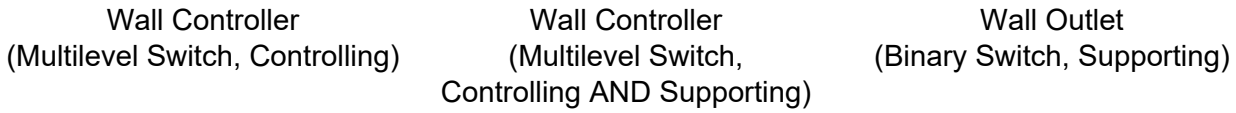
In most cases, the Z-Wave Plus Device Type maps directly to one meaningful icon. In other cases, multiple information sources MUST be combined to determine the proper icon. One such example is the Temperature Sensor shown above. The Z-Wave Plus Device Type is Multilevel Sensor. This provides no information on the actual properties of the sensor. Additional information MUST be queried from the sensor device to determine the actual sensor types and scales available.
If an unknown sensor type is detected, the generic Multilevel Sensor icon MAY be used. If multiple sensor resources are detected, the Multilevel Sensor Bundle icon MAY be used.



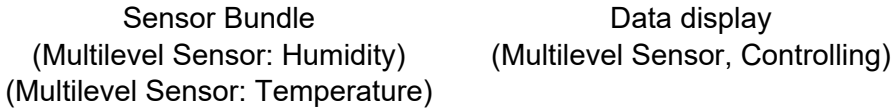


The Device Type icons serve to give a quick overview. A more detailed view is offered by attaching side icons for relevant command classes.

The first example outlines symbols related to control applications.



This second example relates to data-driven applications exchanging sensor data.



The definition and use of Command Class icons is out of scope of this document.

Any manufacturer or organization MAY create its own icon library. The icons presented in this document MAY be used by any manufacturer or organization.

REFERENCES

[1] Silicon Labs, SDS11846, Software Design Specification, Z-Wave Plus Role Types Specification.
[2] Silicon Labs, SDS13781, Z-Wave Application Command Class Specification.
[3] Silicon Labs, SDS13782, Z-Wave Management Command Class Specification.
[4] Silicon Labs, SDS13783, Z-Wave Transport-Encapsulation Command Class Specification.
[5] Silicon Labs, SDS13784, Z-Wave Network-Protocol Command Class Specification.
[6] Silicon Labs, SDS10242, Software Design Specification, Z-Wave Device Class Specification.
[7] IETF RFC 2119, Key words for use in RFC's to Indicate Requirement Levels, http://tools.ietf.org/pdf/rfc2119.pdf
[8] Silicon Labs, SDS13740, Software Design Specification, Z-Wave Device and Command Class Types and Defines Specification.
[9] Silicon Labs, SDS11274, Security 2 Command Class
[10] Silicon Labs, SDS13944, Node Provisioning Information Type Registry (QR code, Z/IP Gateway, Smart Start)
[11] Silicon Labs, SDS13937, Node Provisioning QR Code Format (S2, Smart Start)
[12] Z-Wave Alliance, Z-Wave Security 2 (S2) Product Labeling Requirements
[13] Silicon Labs, SDS14223, Z-Wave Command Class Control Specification.
[14] Silicon Labs, SDS14622, Anti-Theft Command Class, list of assigned Locking Entity IDs

INDEX

S

T

V

W