Software Design Specification

Z-Wave Plus Role Type Specification

Document No.:	SDS11846
Version:	16
Description:	This document defines the Z-Wave Plus Role Types, which specify how a Z-Wave Plus node must react from a network perspective.
Written By:	NTJ;BBR;ABR;JFR;NOBRIOT
Date:	2017-04-07
Reviewed By:	ABR;BBR;JFR;NTJ;NOBRIOT;TRO
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2017-04-07	14:58:31	NTJ	Niels Thybo Johansen	

DOCUMENTATION DISCLAIMER

Copyright Notice

Trademark Notice

License Restrictions Warranty/Consequential Damages Disclaimer

Warranty Disclaimer

Restricted Rights Notice

Hazardous Applications Notice

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
13	20160823	JFR	All	Prepared for Public Z-Wave initiative
14	20161020	NOBRIOT	3.4.2 4.9	Integrated contents from 2016C contributions - Added Security 2 controller bootstrapping requirements - Added the NAS Role Type
15	20170102	NOBRIOT	3.4.2, 3.8.2 & 3.10	Integrated contents from 2016D contributions
16	20170402	NOBRIOT	Various 4.1, 4.2, 4.3 & 4.4	Integrated contents from 2017A contributions - Changed Lifeline/Wake-up recommendations for inclusion controllers to reflect the new S2 Inclusion Controller frame flow. Moved Lifeline association group section to [1]

Table of Contents

Table of Figures

Table of Tables

1 ABBREVIATIONS

Abbreviation	Explanation
AOS	Always On Slave
AGI	Association Group Information
CSC	Central Static Controller
DT	Device Type
NAS	Network Aware Slave
NIF	Node Information Frame
PC	Portable Controller
RPC	Reporting Portable Controller
PS	Portable Slave
LSS	Listening Sleeping Slave
SDK	Software Developer's Kit
SIS	SUC (Node) ID Server
RSS	Reporting Sleeping Slave
SSC	Sub Static Controller
SUC	Static Update Controller

2 INTRODUCTION

2.1 Purpose

This document describes the Z-Wave Plus Role Types. The purpose of the Role Type is to provide a high level definition of how Z-Wave nodes must react from a Z-Wave networking perspective.

This document is not meant to be read in full. It is aimed at being a scalable documentation process for network specific functionality for various Z-Wave devices. It should be read together with the Device Type specification [1], which highlights what Role Types should be used for different Device Types. A device will typically have one Role Type associated with it, but in some cases there can be more than one. The developer now only needs to look at one Role Type to determine the implementation of the network specific functionality to pass certification.

It is however necessary to understand how the Central Static Controller (CSC) works as most devices will heavily depend on it for direct communication.

2.2 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 [5].

Role Type, Device Type and Command Class Specifications approved as a final version during the Type/Class development process have precedence over this document temporarily until integrated into this document.

2.3 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 [4].

3 Z-WAVE COMPLIANCE OVERVIEW

The following sections present Z-Wave properties applying to all Z-Wave Plus Role Types defined in this document. Requirements presented in this chapter MUST be respected by all Z-Wave Plus devices.

3.1 Controllers and slaves

Based on the Role Type, a node can be either a controller or a slave.

Controllers are capable of setting up and performing maintenance operations in a Z-Wave network.

Slaves do not offer any network setup or maintenance function. Slaves can only be added or removed from a network by a controller. Slaves can nevertheless send commands to other nodes and “control” others at the application level.

3.2 SIS Assignment

3.2.1 Controller network roles

A controller can take the following network roles:

Primary Controller: It is the controller that is used to set up and maintain a network. It can include/exclude nodes and knows the network topology. When no SUC/SIS is present in the network, other controllers included by the Primary Controller MUST become Secondary Controllers.

Secondary Controller: The Secondary Controller can control nodes but MUST NOT include/exclude nodes. The Secondary Controller MUST NOT provide any other network functionality than Learn Mode.

Static Update Controller (SUC): When a controller is configured as SUC, the Primary Controller automatically sends network updates to the SUC. The SUC is in charge of keeping the network topology map up to date and deliver it to any controller upon request.

SUC ID Server (SIS): When a SUC is also configured as SIS, it enables other controllers to include/exclude nodes on its behalf, by granting NodeIDs for the nodes to include. The SIS automatically becomes the Primary Controller when enabled.

Inclusion Controller: A controller included in a network with a SIS becomes an Inclusion Controller. It can include/exclude nodes on behalf of the SIS and all network management functionalities supported by the controller MUST be available.

Controllers provide network management functionalities such as Learn Mode, Network inclusion/exclusion or remove/replace failing nodes. Requirements depend on the Role Types and are detailed in Chapter 4

3.2.2 Portable Controllers & non-SIS capable Static Controllers

A Z-Wave Plus network may have no SIS capable controller. For instance this is the case if the network consists of a Portable Controller (PC) which is used to include a number of Always On Slaves (AOS). In this case, the PC acts as the Primary Controller.

If no SIS is present in the network, when including a static controller supporting SIS functionality, the Primary Controller MUST assign the SIS role to the new static controller.

3.2.3 Static Controllers

All static controllers that support SIS functionality MUST accept to become SIS upon request from a Primary Controller.

A static controller operating as Primary Controller that supports SIS functionality MUST assume the SIS role when creating a new network.

3.2.4 SIS return route assignment

When the SIS is present, an including node MUST always assign SIS return route when including a slave type device.

3.3 Inclusion

A Z-Wave Plus compliant node MUST support both Classic and Network Wide Inclusion (NWI)

All nodes (controllers and slaves) can enter Learn Mode. Learn Mode is used for several purposes:

- If a node is not included in a network (or a controller is alone in its own network), Learn Mode is used for joining a network.
- If a node is included in a network, Learn Mode is used for being excluded from the network

Appendix A outlines the inclusion process.

3.4 Security bootstrapping

3.4.1 Security 0 Command Class

Controllers MUST be able to perform Security 0 bootstrapping if they support the Security 0 Command Class. Refer to [1].

If a controller has the Inclusion Controller role in a network and includes a node that supports Security 0 Command Class only (i.e. does not support Security 2 Command Class), it MUST perform Security 0 bootstrapping immediately after including the node.

If an error happens during S0 bootstrapping of an S0 capable controller, the included controller MAY refuse to provide network functions (others than Learn Mode). In this case, the included controller MUST indicate to the user that it needs to be excluded and re-included in the Z-Wave network.

3.4.2 Security 2 Command Class

The following sections describe requirements for controllers supporting Security 2 Command Class

3.4.2.1 Bootstrapping capabilities

Security 2 mandates certain functionalities depending on the controller's role in the network.

If a controller has the SIS role:

- It MUST support the SIS side of the Inclusion Controller Command Class
- It MUST perform Security 2 bootstrapping.
- It MUST support all Security 2 Security Classes
- It MUST have input and display method for support of all Security Classes

If a controller has the Inclusion Controller role:

- It MUST support the Inclusion Controller side of the Inclusion Controller Command Class
- It MUST NOT perform Security 2 bootstrapping
- It MAY support any Security 2 Security Classes
- It MAY have input and display method depending on supported Security Classes

If a controller has the Primary Controller role:

- It MAY perform Security 2 bootstrapping
- It MAY support one or more Security 2 Security Classes
- It MAY have input and display method depending on supported security classes

3.4.2.2 Granting Security classes key

A controller with a user interface for PIN code input (and optionally a QR scanning capability) MUST comply with following when bootstrapping S2 nodes:

- It MUST grant membership of all requested Classes if the joining node requests membership of the S2 Access Control Class
- It SHOULD grant only the S2 Unauthenticated Class key by default if the joining node does not request membership of the S2 Access Control Class
- It MUST ask the user for confirmation before granting S2 Authenticated Class key if the node does not request membership of the S2 Access Control Class.
- It SHOULD provide a way to inspect and adjust the list of the Security Class memberships that will be granted to the joining node

A constrained controller with no QR scanning capability and no user interface for PIN code input MUST comply with following when bootstrapping S2 nodes:

- It MUST grant membership of the S2 Unauthenticated Class if the joining node requests membership of the S2 Unauthenticated Class.
- It MUST abort the S2 bootstrapping entirely (grant no key) if the joining node does not request membership of the S2 Unauthenticated Class.

3.4.2.3 Informing the user about security

If a node has been security bootstrapped with the S0 Command Class in a S2 capable network, the SIS MUST issue a warning message to the user informing that the node has not been included securely.

This is made to ensure that the end user is aware of which security level a node has been bootstrapped and therefore identify if a S0 downgrade attack took place during bootstrapping.

If an S2 node has not been granted the highest requested S2 key during bootstrapping, the SIS MUST issue a warning message to the user informing that the node has not been included with the highest security.

3.5 Device Reset Locally support

If a device can be reset to factory default locally on the device, the device MUST be able to issue a Device Reset Locally Command via its Lifeline to notify the Lifeline destination that the device has been reset to its factory default state. The product documentation MUST include instructions on how to perform a reset to factory default operation. The device MUST clear network settings (HomeID and NodeID) after issuing the Device Reset Locally Command.

If a device cannot be locally (or manually) reset to factory default, the device MUST NOT implement the Device Reset Locally functionality and MUST NOT list the Device Reset Locally Command Class identifier in the NIF.

If a device is reset, it MUST perform the reset operation regardless of whether or not the delivery of the Device Reset Locally Notification is successful.

It is RECOMMENDED that devices implement a mechanism that allows the user to determine when the reset operation is completed.

3.6 Polling Devices

A controlling device may monitor nodes or issue requests for status information. Communication patterns include, but are not limited to, the transmission of a:

- No Operation (NOP) Command to verify that a node is operational
- Get Command requesting status information in a Report Command
- Set Command followed by a Get Command requesting status information in a Report Command

Communication MUST be considered polling if a controlling device autonomously sends requests to one or more nodes in a repeating fashion to monitor nodes or to get information from nodes. This applies to any combination of commands.

Z-Wave is a radio technology with limited bandwidth. Therefore, it is NOT RECOMMENDED to use polling. If used, polling communication MUST comply with the requirements stated in the sections 3.6.1 through 3.6.3.

Communication MAY be considered non-polling if:

- A device issues one or more commands in a burst initiated by a user action. This applies to any combination of commands; also requests.
- A devices issues one or more commands initiated by the inclusion of a new node. This applies to any combination of commands; also requests.

3.6.1 Polling with no errors

Two timers named CommandTime and PollTime are used for polling requirements with no error. Illustrations are given for secure and non-secure cases in Figure 1 and Figure 2

The following requirements apply to the normal case where a polling request is successful.

- CommandTime MUST be measured by the application
- The application MUST wait PollTime before polling any other node
- PollTime SHOULD be 10 seconds + CommandTime or more
- PollTime MUST NOT be less than 1 second + CommandTime

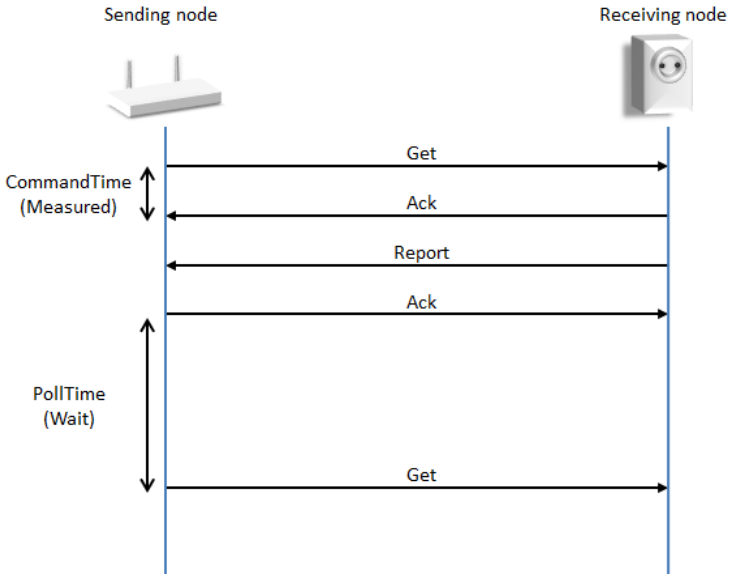

Figure 1, Polling (No errors, without security)

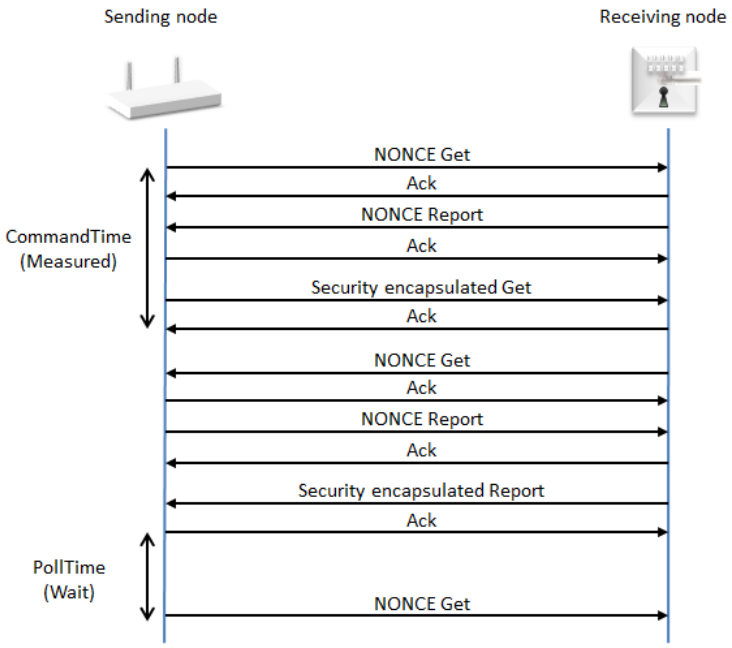

Figure 2, Polling (No errors, with security)

3.6.2 Polling with transmit error

Two timers named CommandTime and PollTime are used for polling requirements with transmission error. Illustrations are given for secure and non-secure cases in Figure 3 and Figure 4. Note that in the case of a missing Ack, the Sending node MUST transmit the Get Command 3 times before considering the Ack to be missing. CommandTime is measured from the first Get Command transmission to the timeout.

The following requirements apply to the case where a polling request is not successful.

- If the transmission fails, the application MUST wait PollTime before polling any other node. PollTime MUST be 10 seconds + CommandTime or more

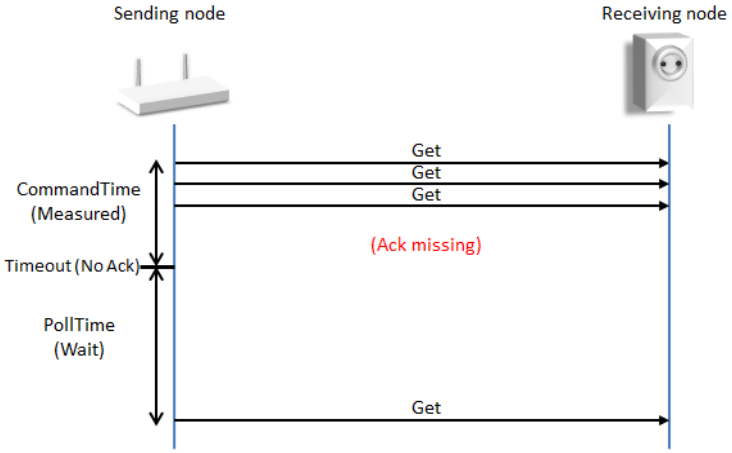

Figure 3, Polling (No Ack, without security)

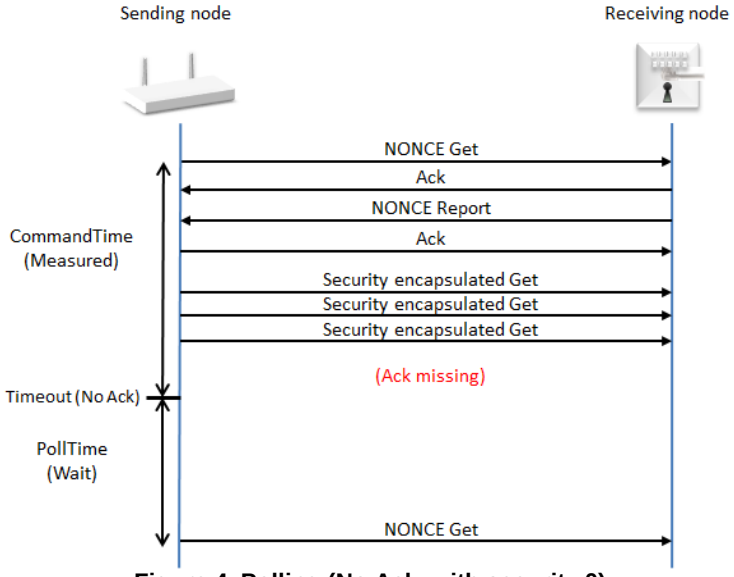

Figure 4, Polling (No Ack, with security 0)

3.6.3 Polling with missing Report frame.

Two timers named CommandTime and ReportTime are used for polling requirements when the transmission is successful but with missing report. Illustrations are given for secure and non-secure cases in Figure 5 and Figure 6

The following requirements apply to the case where a polling request is successful but no Report frame is received.

- The application MUST wait ReportTime for the reply from node X before polling any other node
- ReportTime MUST be CommandTime + 10 seconds or more

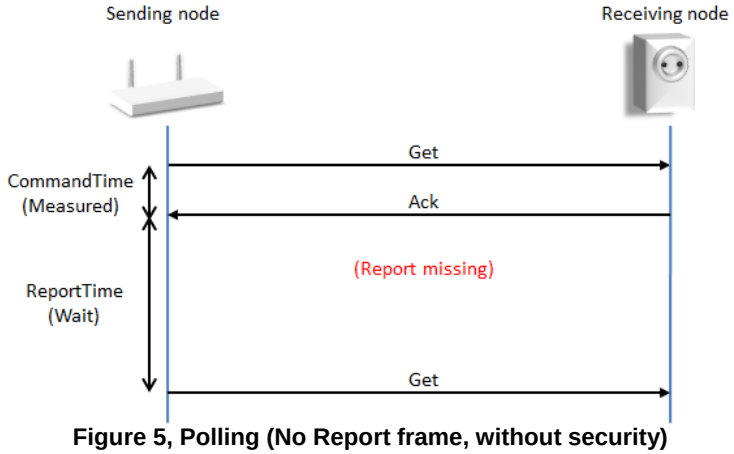

Figure 5, Polling (No Report frame, without security)

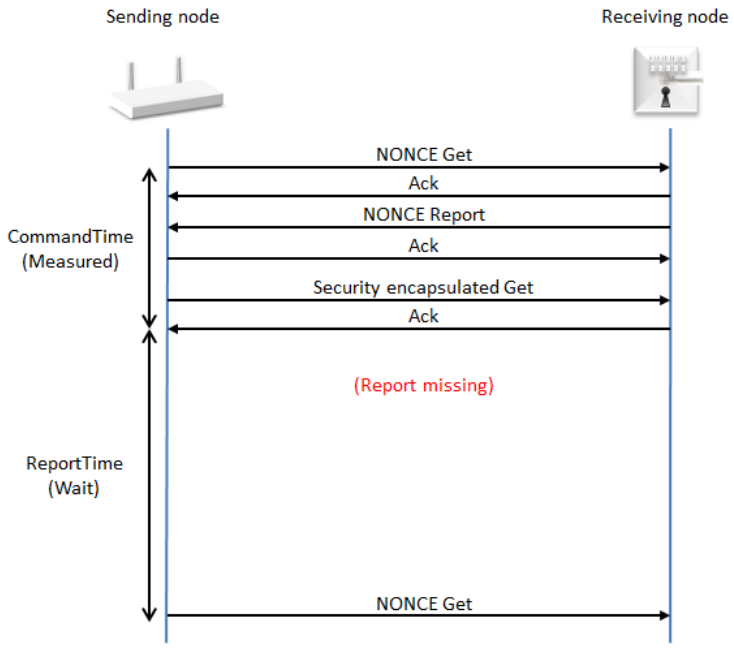

Figure 6, Polling (No Report frame, with security)

3.7 Unsolicited communication

A device MAY autonomously send control commands or status information in response to physical events or in response to a timer.

Unsolicited communication patterns include, but are not limited to, the transmission of a:

- Control command turning on light in response to a detected movement
- Power meter report sending a usage report

Different requirements apply to unsolicited data collection communication and unsolicited control communication, respectively.

3.7.1 Unsolicited data collection communication

Bursts of one or more commands which carry status information transmitted repeatedly without any user intervention MUST be considered to be unsolicited data collection communication.
Using the transmission of a control command or a NOP command as a heartbeat indication MUST also be considered unsolicited data collection communication.

To save bandwidth, data collection communication MUST comply with the following requirements.

- A device MAY issue unsolicited data collection communication in any burst size
- A device MUST NOT issue new unsolicited data collection communication less than 30 seconds since the last burst.

3.7.2 Unsolicited control communication

Bursts of one or more control commands initiated by a user action, a physical event or a time trigger MUST be considered control communication. Control communication MUST comply with the following requirements:

- A device MAY issue unsolicited control communication in any burst size.
- A device MAY issue unsolicited control communication at any interval since the last burst

3.8 Runtime communication

3.8.1 Routing

A Z-Wave Plus node MUST use by default the last working route to communicate with a target node. An illustration is given in Figure 7

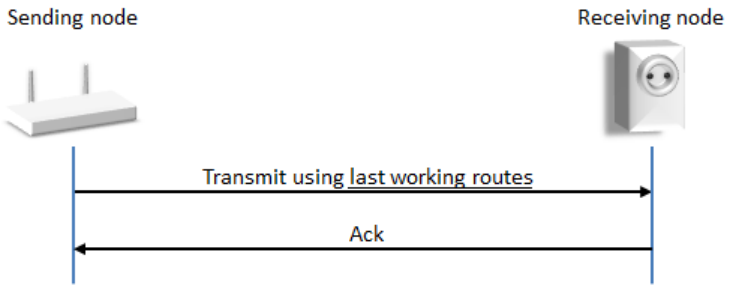

Figure 7, Successful transmission using last working routes

Over time, there is a risk that nodes are moved or stop working. To ensure that nodes adapt to changing network topology and failing repeaters, a Z-Wave Plus node MUST enable dynamic route resolution. Dynamic route resolution consists of trying the following routes:

- Last working routes
- Calculated routes
- Explorer Frame

Illustrations are given in Figure 8 and Figure 9

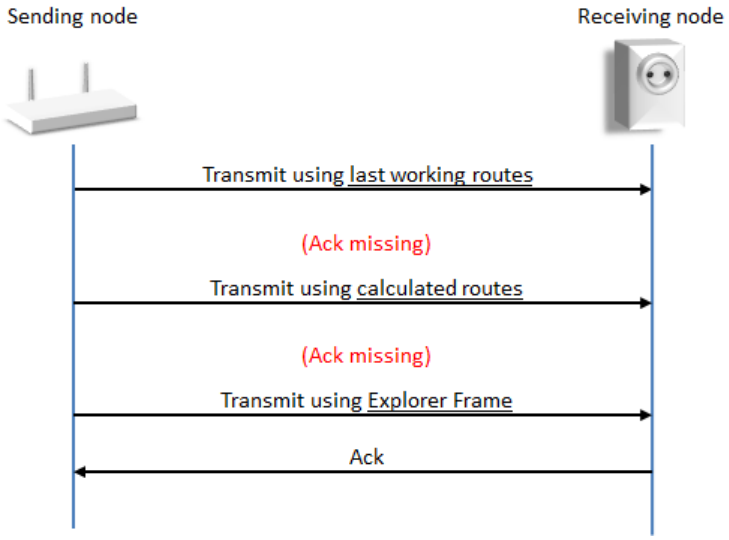

Figure 8, Successful transmission using Explorer Frame

A node MUST perform 3 routing attempts based on last working routes and/or calculated routes before sending an Explorer Frame. As outlined in Figure 8, controllers may calculate routes using the local neighbor map. Listening Sleeping Slaves (LSS) and Reporting Sleeping Slaves (RSS) MAY use return routes injected by a controller. The outlined sequence of transmission attempts is handled entirely by the routing protocol.

In case the target is not working, all routed transmission attempts will fail and ultimately, the routing protocol will have to give up delivering the frame. After a failed transmission, the application MAY try to transmit again in case a new event occurs, e.g. because the user issues a new button press.

The steps in Figure 9 involve at least three routing attempts. When all routing attempts are unsuccessful, it is very unlikely that any other transmission attempt to the same target will succeed. The sending node MAY give up the frame transmission.

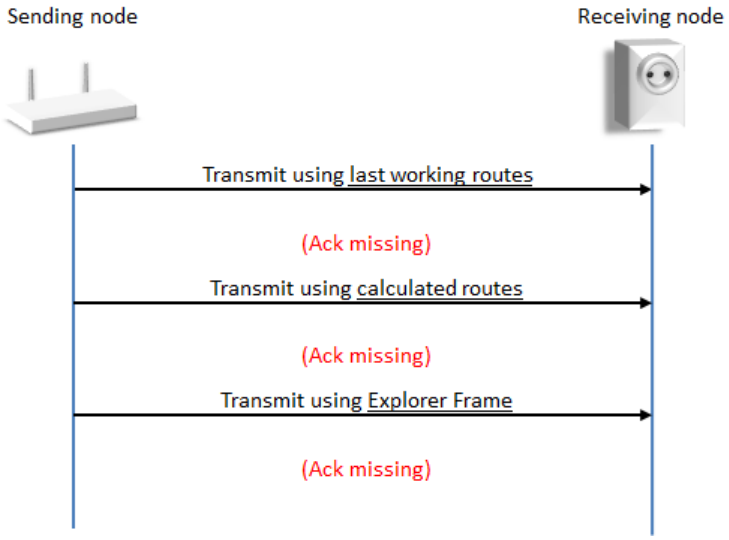

Figure 9, Unsuccessful transmission

3.8.2 Wake-Up communication timeout protection

A battery powered node supporting Wake-Up communication sends a Wake Up Notification Command to get attention when it is awake and receives a Wake Up No More Information Command when it can safely return to sleep.

A battery powered Z-Wave Plus node supporting Wake-Up communication SHOULD implement a time-out mechanism which makes the node return to sleep if the node does not receive a Wake Up No More Information Command.

If no Wake Up No More Information Command is received from the Wake Up destination, the node MUST respond to the Wake Up destination until 10 seconds have elapsed since the last transmission or reception with the Wake Up destination.

An illustration is given in Figure 10

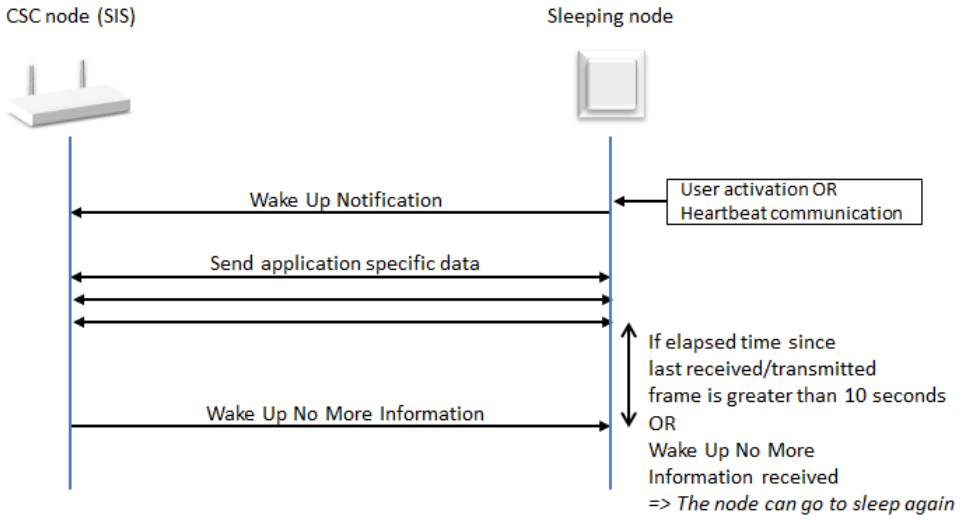

Figure 10, Wake Up Command Class

3.9 Network maintenance

The network rediscovery (Request neighbor update) feature SHOULD only be used as last resort in case the runtime communication fails.

3.10 Encapsulation order

A number of Z-Wave encapsulation Command Classes exist, they MUST be applied in the following order:

1. Any one of the following combinations:
    a. Transport Service followed by Security
    b. Transport Service
    c. Security
    d. CRC16
2. Multi Channel
3. Supervision
4. Multi Command
5. Schedule
6. Encapsulated Command Class (payload), e.g. Basic Get

Note: The Transport Service and CRC16 Command Classes are mutually exclusive as well as Security and CRC16.

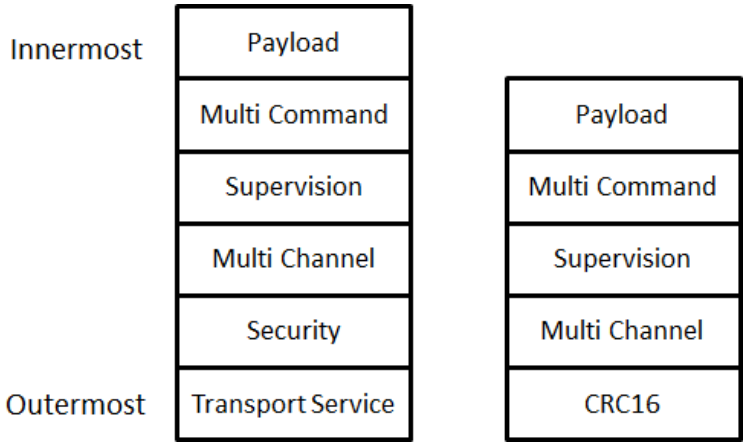

Figure 11, Encapsulation overview

Responses to a given frame must be carried out using the same encapsulation or lack of encapsulation as it was received, unless specified otherwise in the Command Class specifications [2] and [3]. An exception to this is the transport service where the response may require Transport Service encapsulation to fit the entire report. In this case it is mandatory to support the Transport Service Encapsulation when controlling a Command Class that may have to respond using Transport Service. An example of this is the Network Management Proxy Command Class which requires the Transport Service Command Class, both on the Supporting and the Controlling device.

Utilization of the Transport Service, CRC16 and Multi Command command classes can be done on all command classes reported as supported by the receiving node. However, when using Multi Channel or Security, some command classes may not be supported securely or on a specific endpoint and others may be.

Note that additional requirements may exist when using encapsulation of certain command classes. The Command Class specification for a given Command Class must always be referred to.

ROLE TYPE OVERVIEW

Z-Wave Role Types is used as part of the Z-Wave Plus certification program. Role types define how key network devices or functionalities MUST be implemented. This is to provide better uniformity and hence ensuring better interoperability between Z-Wave Plus devices.

Role types are backwards compatible with Z-Wave products certified under earlier certification programs.

The Role Types are device specific and hence the Device Type will define which Role Type(s) a given device can support.

The below matrix shows an overview of Role Types which are described in details in Chapter 4.

Table 1, Overview of Role Types

Role Type	Abbre-viation	Re-pea-ter	Power source	Can be SIS	MUST support security	Net-work setup	Setup lifeline	Report through lifeline	Direct control-able	Heart beat comms.	Push button WakeUp
Central Static Controller	CSC	✓	Mains	✓	✓	✓	✓	✓	✓	✗	✗
Sub Static Controller	SSC	✓	Mains	✗	✗	✓	✗	✓	✓	✗	✗
Portable Controller	PC	✗	Battery	✗	✗	✓	✗	✓	✗	✗	✗
Reporting Portable Controller	RPC	✗	Battery	✗	✗	✓	✗	✓	✗	✓	✓
Portable Slave	PS	✗	Battery	✗	✗	✗	✗	✓	✗	✗	✓
Always On Slave	AOS	✓	Mains	✗	✗	✗	✗	✓	✓	✗	✗
Listening Sleeping Slave	LSS	✗	Battery	✗	✗	✗	✗	✓	✓	✗	✗
Reporting Sleeping Slave	RSS	✗	Battery	✗	✗	✗	✗	✓	✗	✓	✓
Network Aware Slave	NAS	✓	Mains	✗	✗	✗	✗	✓	✓	✗	✗

The following functionalities depend on the actual Role Type:

Repeater: Indicates whether the device can act as repeater in the network. This requires an always listening device, which can accommodate any routing requests immediately.

Power source: Mains powered devices are accessible immediately and are always listening devices. Battery powered devices focus on battery lifetime extension as one of the primary objectives.

Can be SIS: The device MUST support the Static Update Controller (SUC) and SUC node ID Server (SIS) functions. When SIS functionality is enabled, the controller also takes the Primary Controller role. All other controllers operate as Inclusion Controllers, i.e. they can request that nodes are included/excluded.

If a SIS is present in the network, it is RECOMMENDED that all other devices update their network topology once a day and before configuring associations.

MUST support security: The device MUST support the Security Command Class to facilitate applications which require support of security. (For example door locks or metering devices)

Network setup: The device MUST be capable of managing the network and mastering inclusion/exclusion of nodes. In the actual context, the device MAY be operated as an inclusion controller.

Setup lifeline: The device MUST be able to configure lifeline associations to a central home control application.

Report through lifeline: The device MUST be able to report events via a lifeline association to a central home control application.

Direct controllable: Mains powered devices and battery devices configured as Frequently Listening Routing Slave (FLiRS) can be controlled at any time.

Heart beat communication: Operating as a sleeping device, the device MUST be able to connect at given intervals to a central home control application to allow delivery of messages from other devices. The device MUST support the Wake Up Command Class.

Push button wake-up: The device SHOULD have a push button for waking up a sleeping device for expedited communication. This enables interactive delivery of new configuration parameters or firmware updates.

3.11 Detecting the Role Type of a device

The Role Type can only be requested via the Z-Wave Plus Info Command Class, which MUST be listed as the first supported Command Class in the Node Information Frame (NIF) by Z-Wave Plus devices. For details about Z-Wave Plus Info Command Class, refer to [2].

Table 2, Role Type identifiers

Role Type	Identifiers
Central Static Controller (CSC)	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC
Sub Static Controller (SSC)	ROLE_TYPE_CONTROLLER_SUB_STATIC
Portable Controller (PC)	ROLE_TYPE_CONTROLLER_PORTABLE
Reporting Portable Controller (RPC)	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING
Portable Slave (PS)	ROLE_TYPE_SLAVE_PORTABLE
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
Network Aware Slave (NAS)	ROLE_TYPE_SLAVE_NETWORK_AWARE

Refer to [5] regarding the assigned values of the Role Type identifiers.

4 ROLE TYPE DEFINITIONS

The following sections describe how each of the Role Types MUST be implemented. Each Role Type has requirements categorized in the following subsections:

1. **Protocol Requirements**
2. **Setup**
3. **Runtime Configuration**
4. **Runtime Communication**

The Setup subsection describes the specific requirements for a given Role Type during and after a network inclusion. Figure 12 shows the different steps of a node setup / commissioning.

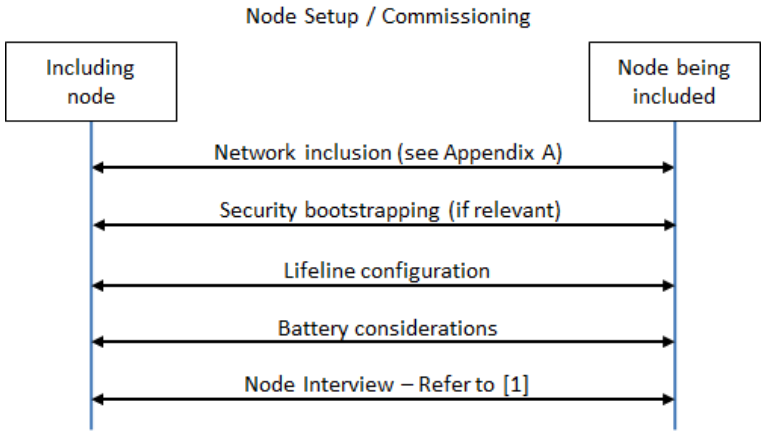

Figure 12, Node Setup / commissioning

Network inclusion

The network inclusion process is described in Appendix A. Additional recommendations are given for the different Roles Types.

Security bootstrapping

The security (Security 0 and/or Security 2) bootstrapping takes place immediately after the network inclusion. Refer to [2].

Lifeline configuration

If a SIS is present in the network, the destination NodeID of the Lifeline group MUST be the SIS NodeID. Requirements are detailed for each Role Type in the following sections. Refer to [1] for Lifeline group definition

Battery considerations

Some requirements apply for battery powered nodes. Details are given for each Role Type.

Device interview

The device interview is depending on the capabilities of the node being included. [1] provides guidelines for interviewing devices.

Commissioning and runtime phases

The commissioning phase is defined as the period after a node's inclusion during which the Security bootstrapping, Lifeline configuration, Wake Up configuration and initial device interview is made by a controller.

It is RECOMMENDED that a controller does not display a newly included node as ready to be operated during the commissioning phase.

The commissioning phase is considered over when the initial interview is completed or latest 10 minutes after the network inclusion.

Once the commissioning phase is over, a node is said to be in the runtime phase.

4.1 Central Static Controller (CSC)

The Central Static Controller Role Type SHOULD be used for always powered devices which are capable of operating as a central controller. The CSC will be the central device for most network communications and other devices will rely on it for unsolicited information via the lifeline association to the CSC (which is also the SIS). This will enable the user to receive key information without having to perform major network configuration tasks.

The CSC is typically a router, central gateway or some sort of central communication panel.

4.1.1 CSC Protocol Requirements

The CSC MUST respect requirements described in chapter 3
The CSC MUST support and control the Security Command Class.

The CSC MUST support the following network roles:

- SIS
- Secondary controller
- Inclusion controller

4.1.1.1 If first node in the network

If the CSC is the first node in the network, it MUST set itself the SIS role and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode
- Remove failing node
- Replace failing node

It MUST NOT be possible to activate Learn Mode if the CSC is the SIS and other nodes are included in the network.

4.1.2 CSC Setup

4.1.2.1 Inclusion process

It is RECOMMENDED to use soft buttons for activating learn mode and add mode on a CSC Role Type.

4.1.2.2 CSC including a SSC, PC, RPC or NAS

Lifeline configuration

If the CSC is the SIS, MUST set itself as the Association group ID 1 (Lifeline) destination.

Battery considerations

If the CSC is the SIS and the included node is of Role Type RPC:

- The CSC MUST configure the Wake Up Interval Set Command destination NodeID to its NodeID.
- The CSC MUST send a Wake Up No More Information Command when the CSC has no more command to transmit.

4.1.2.3 CSC including a PS, LSS or RSS

Lifeline configuration

If the CSC is the SIS, it MUST set itself as the Association group ID 1 (Lifeline) destination.
The CSC MUST assign a return route for the SIS.

Battery considerations

If the CSC is the SIS and the included node is of Role Type PS or RSS:

- The CSC MUST configure the Wake Up Interval Set Command destination NodeID its NodeID.
- If the CSC is the SIS, it MUST send a Wake Up No More Information Command when the CSC has no more command to transmit.

If the CSC is the SIS and the included node is of Role Type PS:

- The Wake Up Interval Set Command Seconds field MUST be equal to 0

If the CSC is not the SIS, it SHOULD NOT send a Wake Up Interval Set Command to the included node.

4.1.2.4 CSC including an AOS

Lifeline configuration

If the CSC is the SIS, it MUST set the SIS NodeID as the Association group ID 1 (Lifeline) destination.
The CSC MUST assign a return route for the SIS.

Battery considerations

None

4.1.2.5 CSC including another CSC

If the CSC is included by another CSC, the included CSC MUST take the Inclusion Controller role and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode
- Remove failing node
- Replace failing node

Lifeline configuration

None

Battery considerations

None

4.1.2.6 CSC included by a PC, RPC, SSC

The CSC MUST accept to take the SIS role when a PC, RPC or SSC assigns it to the included CSC.

Lifeline configuration

If the CSC was assigned the SIS role, previously added nodes may have no lifeline associations. The CSC SHOULD create lifeline associations in all directly reachable nodes.

If the CSC was assigned the SIS role and the including node is an RPC, the CSC MUST create a lifeline association to the RPC.

Battery considerations

None

4.1.3 CSC Runtime Configuration

The CSC MUST instruct a reporting node (RPC, RSS, PS) to return to sleep after application data has been delivered to the node. This is done by sending a Wake Up No More Information Command. An illustration is given in Figure 10

4.1.4 CSC Runtime Communication

No requirements

4.2 Sub Static Controller (SSC)

The Sub Static Controller Role Type SHOULD be used for static controllers which are not suitable as central controllers. It is aimed at applications that require a static controller to manage a subset of nodes. It is typically offered as a bundled package with e.g. sensors.

4.2.1 SSC Protocol Requirements

The SSC MUST respect requirements described in chapter 3
The SSC MUST NOT support the SIS functionality.
The SSC SHOULD NOT configure lifeline associations.

The SSC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

4.2.1.1 If first node in the network

If the SSC is the first node in the network, it MUST take the Primary Controller role and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

It MUST NOT be possible to activate Learn Mode if the SSC is the Primary Controller and other nodes are included in the network.

4.2.2 SSC Setup

4.2.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode and a soft button for activating add mode on a SSC Role Type.

4.2.2.2 SSC including a CSC

If the SSC is the Primary Controller and a CSC is added to the network, the SSC MUST assign the SIS role to the CSC.

If the SSC is the Primary Controller and has previously included some Wake Up nodes, it MAY re-assign the Wake Up destination NodeID to the CSC/SIS for the previously included Wake Up nodes at the next Wake Up Notification.

The SSC becomes an inclusion controller and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

Lifeline configuration

None

Battery considerations

None

4.2.2.3 SSC including an RPC, PS or RSS

Lifeline configuration

None.

Battery considerations

If there is a SIS in the network, the SSC SHOULD NOT send a Wake Up Interval Set Command to the included node.

If there is no SIS present in the network, the SSC SHOULD send a Wake Up Interval Set Command with its own NodeID as destination. If issuing a Wake Up interval Set Command, the SSC MUST respect the following rules:

- If the included node is of Role Type RPC, PS or RSS:
  - The SSC SHOULD set the Wake Up Interval Set Command Seconds field to the default Wake Up time advertised by the included node.
- If the included node is of Role Type PS:
  - The Wake Up Interval Set Command Seconds field MUST be equal to 0

4.2.2.4 SSC including an SSC, PC, AOS, LSS or NAS

Lifeline configuration

None.

Battery considerations

None

4.2.3 SSC Runtime Configuration

No requirements

4.2.4 SSC Runtime communication

No requirements

4.3 Portable Controller (PC)

The Portable Controller Role Type SHOULD be used for portable controllers that can setup and maintain a Z-Wave network but do not require unsolicited reporting. It is typically used by home control remotes that control a few lights.

4.3.1 PC Protocol Requirements

The PC MUST respect requirements described in chapter 3
The PC SHOULD NOT configure lifeline associations when adding nodes to the network.
The PC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

4.3.1.1 If first node in the network

If the PC is the first node in the network, it MUST take the Primary Controller role and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

It MUST NOT be possible to activate Learn Mode if the PC is the Primary Controller and other nodes are included in the network.

4.3.2 PC Setup

4.3.2.1 Inclusion process

It is RECOMMENDED to use physical push buttons for activating learn mode and add mode on a PC Role Type.

4.3.2.2 PC including a CSC

If the PC is the Primary Controller and has already included multiple nodes and a CSC is added to the network, the PC MUST assign the SIS role to the CSC.

The PC becomes an inclusion controller and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

Lifeline configuration

None

Battery considerations

None

4.3.2.3 PC including an RPC, PS or RSS

Lifeline configuration

None.

Battery considerations

- None.

4.3.2.4 PC including an SSC, PC, AOS, LSS or NAS

Lifeline configuration

None.

Battery considerations

None

4.3.3 PC Runtime Configuration

No requirements

4.3.4 PC Runtime communication

No requirements

4.4 Reporting Portable Controller (RPC)

The Reporting Portable Controller Role Type SHOULD be used for portable reporting controllers, which need to setup a Z-Wave network and also send unsolicited messages.

The RPC Role Type may for instance be used for a battery powered thermostat which can include and exclude nodes in a small network. In addition, the thermostat may be configured remotely.

4.4.1 RPC Protocol Requirements

The RPC MUST respect requirements described in chapter 3
The RPC SHOULD NOT configure lifeline associations when adding nodes to the network.

The RPC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

4.4.1.1 If first node in the network

If the RPC is the first node in the network, it MUST take the Primary Controller role and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

It MUST NOT be possible to activate Learn Mode if the RPC is the Primary Controller and other nodes are included in the network.

4.4.2 RPC Setup

4.4.2.1 Inclusion process

It is RECOMMENDED to use physical push buttons for activating learn mode and add mode on an RPC Role Type.

4.4.2.2 RPC including a CSC

If the RPC is the Primary Controller and has already included multiple nodes and a CSC is added to the network, the RPC MUST assign the SIS role to the CSC.

The RPC becomes an inclusion controller and MUST support the following network functions:

- Include new nodes (“Add mode”)
- Exclude nodes
- Learn mode

Lifeline configuration

None

Battery considerations

None

4.4.2.3 RPC Including an RPC, PS or RSS

Lifeline configuration

If a SIS is present in the network, the RPC SHOULD set the SIS NodeID as the Association group ID 1 destination.

Battery considerations

None

4.4.2.4 RPC including an SSC, PC, AOS, LSS or NAS

Lifeline configuration

If a SIS is present in the network, the RPC SHOULD set the SIS NodeID as the Association group ID 1 destination.

Battery considerations

None

4.4.3 RPC runtime configuration

The RPC MUST support the Wake Up Command Class as described in 3.8.2.

The RPC SHOULD have a physical push button for waking up the device for expedited communication. This enables interactive delivery of new configuration parameters or firmware updates.

The RPC MUST implement a Minimum Wake Up Interval in the range 0 ..4200 (i.e. between 0 second and 70 minutes).
If the RPC's Minimum Wake Up Interval is 0, the RPC MUST implement a Maximum Wake Up Interval greater than 0.The RPC MUST send Wake Up Notifications to the NodeID configured via the Wake Up Interval Set Command. The RPC MUST NOT send Wake Up Notifications if no NodeID has been configured via the Wake Up Interval Set Command.

4.4.4 RPC runtime communication

The RPC MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

4.5 Portable Slave (PS)

The Portable Slave Role Type SHOULD be used for battery powered devices that aim for the lowest possible power consumption. The PS only wakes up in response to a physical event such as a button press.

This Role Type is intended for simple AV remote controls that only need to talk to one device. The PS allows for optimal cost, as no EEPROM is required.

4.5.1 PS Protocol Requirements

The PS MUST respect requirements described in chapter 3
The PS can only be added to a network and has no network role requirement.

4.5.2 PS Setup

The setups of a PS by a CSC, SSC, PC or RPC are respectively described in 4.1.2.3, 4.2.2.3, 4.3.2.3 or 4.4.2.3. The PS has no additional requirement when being included.

4.5.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode on a PS Role Type.

4.5.3 PS Runtime configuration

The PS MUST support the Wake Up Command Class as described in 3.8.2.

The PS SHOULD have a physical push button for waking up the device for expedited communication. This enables interactive delivery of new configuration parameters or firmware updates.

4.5.4 PS Runtime communication

The PS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

4.6 Always On Slave (AOS)

The Always On Slave Role Type SHOULD be used for mains powered devices that are always reachable. One example of such a device is a light switch.

4.6.1 AOS Protocol Requirements

The AOS MUST respect requirements described in chapter 3
The AOS can only be added to a network and has no network role requirement.

4.6.2 AOS Setup

The setups of an AOS by a CSC, SSC, PC or RPC are respectively described in 4.1.2.4, 4.2.2.4, 4.3.2.4 or 4.4.2.4. The AOS has no additional requirement when being included.

4.6.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode on an AOS Role Type.

4.6.3 AOS Runtime Configuration

AOS can always be configured, as it is always listening.

4.6.4 AOS Runtime communication

The AOS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

4.7 Reporting Sleeping Slave (RSS)

The Reporting Sleeping Slave Role Type SHOULD be used for battery-powered devices that only wake up and communicates when an event has occurred. This allows to reconfigure the device remotely. Examples include sensors, wall controllers etc.

4.7.1 RSS Protocol Requirements

The RSS MUST respect requirements described in chapter 3.
The RSS can only be added to a network and has no network role requirement.

4.7.2 RSS Setup

The setups of an RSS by a CSC, SSC, PC or RPC are respectively described in 4.1.2.3, 4.2.2.3, 4.3.2.3 or 4.4.2.3. The RSS has no additional requirement when being included.

4.7.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode on an RSS Role Type.

4.7.3 RSS Runtime configuration

The RSS MUST support the Wake Up Command Class as described in 3.8.2 and in Figure 10.

The device SHOULD have a physical push button for waking up the device for expedited communication. This enables interactive delivery of new configuration parameters or firmware updates.

The RSS MUST implement a Minimum Wake Up Interval in the range 0 ..4200 (i.e. between 0 second and 70 minutes).
If the RSS's Minimum Wake Up Interval is 0, the RSS MUST implement a Maximum Wake Up Interval greater than 0.The RSS MUST send Wake Up Notifications to the NodeID configured via the Wake Up Interval Set Command.

4.7.4 RSS Runtime communication

The RSS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for details.

4.8 Listening Sleeping Slave (LSS)

The Listening Sleeping Slave Role Type is intended for battery-operated devices that can be reached even though they are sleeping thanks to Beaming (FLiRS devices). Examples include Door Locks and Battery operated Thermostats.

The LSS MUST support the lifeline unless otherwise specified in the Device type specification [1].

4.8.1 LSS Protocol Requirements

The LSS MUST respect requirements described in chapter 3.
The LSS can only be added to a network and has no network role requirement

4.8.2 LSS Setup

The setups of an LSS by a CSC, SSC, PC or RPC are respectively described in 4.1.2.3, 4.2.2.3, 4.3.2.3 or 4.4.2.3. The LSS has no additional requirement when being included.

4.8.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode on a LSS Role Type.

4.8.3 LSS Runtime configuration

A LSS can always be configured, as it is reachable via FLiRS communication.

4.8.4 LSS Runtime communication

The LSS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for details.

The LSS MUST stay awake for at least 2 seconds after communicating.

4.9 Network Aware Slave (NAS)

The Network Aware Slave Role Type is used for slaves with application controlling capabilities, which are leveraging controller functionalities to be aware of the network topology and nodes capabilities.

The SIS (or primary controller) will consider a NAS as a controller, but the NAS will not be able to include new nodes in the network.

The NAS MUST be mains powered and always reachable.

4.9.1 NAS Protocol Requirements

The NAS MUST respect requirements described in chapter 3.
The NAS can only be added to a network and MUST take the inclusion controller or the secondary controller role when added to a network.

The NAS MUST NOT provide the following network functions:

- Include new nodes
- Exclude nodes
- Remove failing node
- Replace failing node

4.9.2 NAS Setup

The setups of an NAS by a CSC, SSC, PC or RPC are respectively described in 4.1.2.2, 4.2.2.4, 4.3.2.4 or 4.4.2.4. The NAS has no additional requirement when being included.

4.9.2.1 Inclusion process

It is RECOMMENDED to use a physical push button for activating learn mode on an NAS Role Type.

4.9.3 NAS Runtime Configuration

The NAS can always be configured, as it is always listening.

4.9.4 NAS Runtime communication

The NAS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

APPENDIX A INCLUSION PROCESS

This section outlines the recommended inclusion process that all Role Types should follow. The processes for both node including and being included are covered.

Appendix A.1 Being included

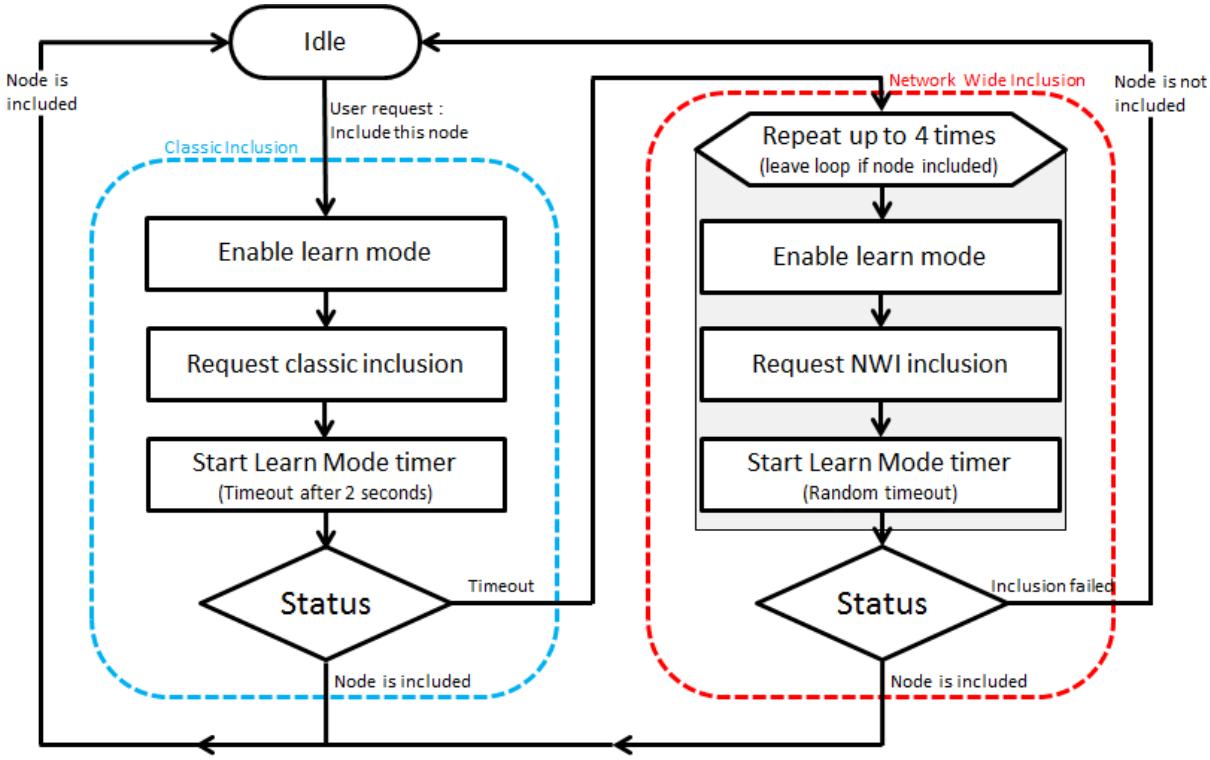

Figure 13, Inclusion process for the node being included

Appendix A.2 Including a node

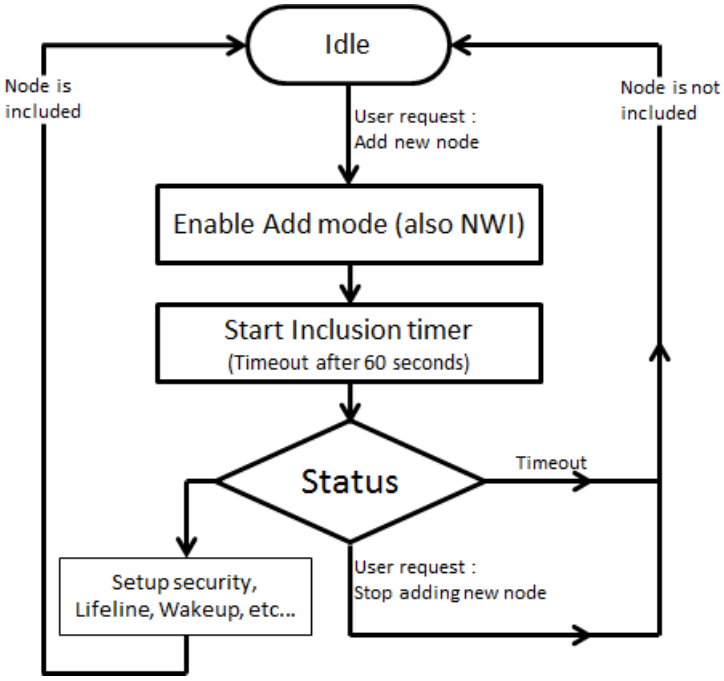

Figure 14, Inclusion process for the including node

REFERENCES

[1] Sigma Designs, SDS11847, Software Design Specification, Z-Wave Plus Device Types Specification.
[2] Sigma Designs, SDS12652, Software Design Specification, Z-Wave Command Class Specification, N-Z.
[3] Sigma Designs, SDS12657, Software Design Specification, Z-Wave Command Class Specification, A-M.
[4] IETF RFC 2119, Key words for use in RFC's to Indicate Requirement Levels, http://tools.ietf.org/pdf/rfc2119.pdf
[5] Sigma Designs, SDS13740, Software Design Specification, Z-Wave Device and Command Class Types and Defines Specification.

INDEX