Software Design Specification

Z-Wave Plus Role Type Specification

Document No.:	SDS11846
Version:	26
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;JFR;NOBRIOT;DEWASSIE
Date:	2019-04-09
Reviewed By:	NOBRIOT;COLSEN;DEWASSIE
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2019-04-09	06:24:49	NTJ	Niels Johansen	

SILICON LABS

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 5.9	Integrated approved contents from the 2016C contributions • Added Security 2 controller bootstrapping requirements • Added the NAS Role Type
15	20170102	NOBRIOT	3.11 3.4.2 3.9.2 RT sections	Integrated approved contents from the 2016D contributions: • Updated the Encapsulation order figure • Added a clarification about the default S2 key granting • Clarified requirements for the Wake Up mechanism • Changed Lifeline configuration recommendations when a controller is not the SIS, due to the new Inclusion Controller Command Class
16	20170402	NOBRIOT	3.4.1 3.9.2 4 RT Sections 5.1, 5.2, 5.3 & 5.4	Integrated approved contents from the 2017A contributions • Clarified what is allowed when S0 bootstrapping fails for S0 capable controllers. • Clarified the “heartbeat communication” is actually intended to described Wake-Up Notification mechanism only • Added Commissioning and Runtime phase definitions • Removed/updated the Wake-Up configuration requirements for inclusion controllers due to the new Inclusion Controller CC. Changed Lifeline/Wake-up recommendations for inclusion controllers to reflect the new S2 Inclusion Controller frame flow. Moved Lifeline association group section to [1]
17	20170702	NOBRIOT	3.4.2.1 3.5 Table 1 RT Sections 5.1.2.3 & 5.2.2.3 Appendix A.1 3.12	Integrated approved content from the 2017B contributions • Removed optional statements and clarified S2 bootstrapping • Removed redundant requirement for the Device Reset Locally Command Class • Removed “MUST support Security” from the Role Type Overview • (Re-)Added mains/battery and listening flag requirements in every Role Type • Clarified that optional Wake Up Interval Set Command must contain the SIS’ NodeID. • Updated Learn Mode recommended diagram Added SmartStart requirements
18	20170711	NOBRIOT	3.12	Added SmartStart controller requirements
19	20171002	NOBRIOT	3.4.2.3 3.12.2.3 5.1.2.6 3.4.1 3.12	Integrated approved content from the 2017C contributions: • Clarifications about S2 and informing the end user about security • Minor edits about Node Provisioning requirements • Rephrasing Lifeline requirement in CSC Role Type definition Added clarification for S0 bootstrapping with/without Inclusion Controller Command Class Updated some SmartStart requirements
20	20180110	NOBRIOT	Table 2 3.2.1 3.12 5.3, 5.4, 5.5, 5.7 & 5.8	Integrated approved content from the 2017D contributions: • Fixed an error in the Role Type identifiers • Added requirement for controllers to generate HomeIDs with a random number generator • Short clarifications to SmartStart requirements • Added Command Class support requirements (Wake Up and Battery) in Role Type definitions
21	20180305	BBR	All	Added Silicon Labs template
22	20180404	NOBRIOT	5.1.2.6 3.6 3.12.2.3 5	Integrated approved content from the 2018A contributions: • Removed requirement for CSC to establish Lifeline to an including RPC. • Added node interview response timeout recommendations • Clarified text for “classic” inclusion Updated network inclusion, bootstrapping and interview description
23	20180701	NOBRIOT	3.5 5.1.2.3 & 5.2.2.3 3.4.1.1	2018B Contributions: • Added requirements and guidelines for device reset • Relaxed Wake-Up Interval value requirements for PS Role Type • Added Security 0 recommendations

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
24	20181001	NOBRIOT	5.1	Contributions 2018C: - Changed the Replaced Failing Node functionality optional for the CSC Role Type
25	20190101	DEWASSIE NOBRIOT	3.3 3.4.2.3 3.12.2.3 5.1.2.5	Contributions 2018D: • Added failed node Remove and Replace functionalities and updated Learn Mode and Add Mode descriptions and requirements • Added end user notification requirements when user interface is not active during S2 bootstrapping • Removed edit requirement in the Node Provisioning List • Clarified that Replace Failing Node is always optional
26	20190401	NOBRIOT	3.4.2.1	Contributions 2019A: • Made CSA support in S2 optional for SIS controllers having the SIS role.

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
NOP	No Operation

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 [8].

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 [7].

3 Z-WAVE COMPLIANCE OVERVIEW

RT:00.11.0001.1 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 Network creation

RT:00.11.0002.1 A controller MUST generate a new HomeID using a random number generator when creating a new network.

3.2.2 Controller network roles

A controller can take the following network roles:

RT:00.11.0003.1 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.

RT:00.11.0004.1 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.

RT:00.11.0005.1 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 5

3.2.3 Portable Controllers & non-SIS capable Static Controllers

A Z-Wave 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.

RT:00.11.0006.1 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.

3.2.4 Static Controllers

RT:00.11.0007.1 All static controllers that support SIS functionality MUST accept to become SIS upon request from a Primary Controller.

RT:00.11.0008.1 A static controller operating as Primary Controller that supports SIS functionality MUST assume the SIS role when creating a new network.

3.2.5 SIS return route assignment

RT:00.11.0009.1 When the SIS is present, an including node MUST always assign SIS return route when including a slave type device.

3.3 Network Inclusion and exclusion

Learn Mode:

RT:00.11.000A.1 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. During the Learn Mode operation, the node that is being included in the network MUST receive non-zero assigned NodeID.

RT:00.11.0038.1

- If a node is included in a network, Learn Mode is used for being excluded from the network. In this case, the node that is about to be excluded from a network MUST receive the 0x00 NodeID.

RT:00.11.0039.1

Appendix A outlines the inclusion process.

Add Mode:

Add mode is used by a controller for including a new node to a network.

When a controller is in Add Mode (or NWI), it listens for Node Info Frames (NIF) and assign a non-zero NodeID to new nodes.

Remove Mode:

Remove mode is used by a controller for excluding a node from a network.

When a controller is in Remove Mode (or NEW), it listens for Node Info Frames and assign a zero NodeID to the excluded nodes.

Remove Failed Node:

Remove Failed Node is used to remove non-responsive nodes from a network.

A node is considered to be failed or non-responsive when a controller cannot reach the node, using routing and explorer frames. Sleeping nodes can be considered as failing after missing more than 2 consecutive Wake Up Periods.

RT:00.11.003A.1 Before removing a non-responsive NodeID from a network, a controller MUST issue NOP commands to the actual NodeID. If the node is not responding, the controller can proceed with removing the NodeID and updating the network.

RT:00.11.003B.1 A responding node MUST NOT be removed from the network.

Replace Failed Node:

Replace Failed Node is used to include a new node that will replace a non-responsive node in a network.

RT:00.11.003C.1 RT:00.11.003D.1 Before reusing a non-responsive NodeID to add a new node, a controller MUST issue NOP commands to the actual NodeID. If the node responds again, the Replace Failed Node MUST be aborted.

If the node does not respond, the controller will add a new node and reuse the Failed Node NodeID.

3.4 Security bootstrapping

3.4.1 Security 0 Command Class

RT:00.21.0001.1 Controllers MUST be able to perform Security 0 bootstrapping if they support the Security 0 Command Class. Refer to [1].

RT:00.21.0002.1 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.

RT:00.21.0003.1 If the SIS and the Inclusion Controller both support the Inclusion Controller Command Class, the inclusion controller MUST NOT perform S0 bootstrapping unless instructed by the SIS with an Inclusion Controller Initiate Command (S0_INCLUSION).

RT:00.21.0004.1 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.

3.4.1.1 Upgrading non-secure networks

RT:00.23.0001.1 If a controller is included in a non-secure network as an inclusion controller, it MAY start using its own S0 network key and perform S0 bootstrapping with newly included nodes.

A controller MUST NOT start using its own S0 network key if S0/S2 bootstrapping failed

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:

RT:00.21.0006.1 • It MUST support the SIS side of the Inclusion Controller Command Class

RT:00.21.0007.1 • It MUST perform Security 2 bootstrapping.

RT:00.21.0008.1 • It MUST support inclusion of nodes that implement any combination of Security 2 Security Classes

RT:00.21.0009.1 • It MUST have input and display method for support of all Security Classes.

RT:00.23.0006.1 • It MAY support inclusion using CSA

If a controller has the Inclusion Controller role:

RT:00.21.000A.1 • It MUST support the Inclusion Controller side of the Inclusion Controller Command Class

RT:00.21.000B.1 • It MUST NOT perform Security 2 bootstrapping

RT:00.23.0002.1 • It MAY have input and display method depending on supported Security Classes

If a controller has the Primary Controller role:

RT:00.23.0003.1 • It MAY perform Security 2 bootstrapping

RT:00.23.0004.1 • It MAY have input and display method depending on supported security classes

3.4.2.2 Granting Security Classes

RT:00.21.000C.1 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 (unless specified otherwise by a user).
- It MAY 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

RT:00.21.000D.1 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

RT:00.21.000E.1 RT:00.22.0001.1 If a node has been security bootstrapped with the S0 Command Class in a S2 capable network, the SIS/Primary controller MUST issue a warning message to the user informing that the node has not been included securely. The SIS/Primary controller SHOULD request a new NIF to the included node after security bootstrapping to verify if the included node supports S2 before issuing the message to the user.

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 or if a non-S2 inclusion controller bootstrapped the joining node.

RT:00.21.000F.1 If an S2 node has not been granted the highest requested S2 key during bootstrapping, the SIS/Primary controller MUST issue a warning message to the user informing that the node has not been included with the highest security. This is OPTIONAL if the user has actively chosen which keys to grant and security bootstrapping completed successfully.

In an Inclusion Controller scenario, the SIS' UI may not be active during S2 bootstrapping. In this case, the following rules apply:

RT:00.23.0005.1
- If the SIS automatically grants unauthenticated key for a node that request S2 Unauthenticated Class, it MAY notify the end user the next time it uses the UI.

RT:00.21.0010.1
- If the SIS timed out during S2 bootstrapping, it MUST instruct the end user that the node needs to be excluded and re-included.

3.5 Device Reset Locally support

RT:00.11.000B.1 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.

RT:00.11.000C.1 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.

RT:00.11.000D.1 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.

When a node is reset,

RT:00.11.000E.1
- it MUST forget its current HomeID and consider itself excluded from the network.

RT:00.13.0001.1
- The configuration of Application Command Classes [3] MAY stay unchanged (e.g. configuration parameters, Thermostat Setpoint, Clock, Door lock Timeout configuration, User codes, …)

RT:00.11.000F.1
- The configuration of other Command Classes (Management [4], Transport [5] or network [6]) MUST be reset to default (i.e. S2 keys are forgotten, Associations and Wake-Up configurations are cleared, etc…)

3.6 Node interview and response timeouts

RT:00.11.0010.1 During a node capability discovery or interview, as well as traffic generated due to user activation, a controlling nodes MUST timeout waiting for responses (reports) as part of the capability discovery or controlling scenarios.

Two timers named CommandTime and ReportTime are used for timing out during a node discovery interview. Illustrations are given for secure and non-secure cases in Figure 1 and Figure 2

- CommandTime is measured by the application

RT:00.12.0001.1
- ReportTime timeout SHOULD be set to CommandTime + 1 second.

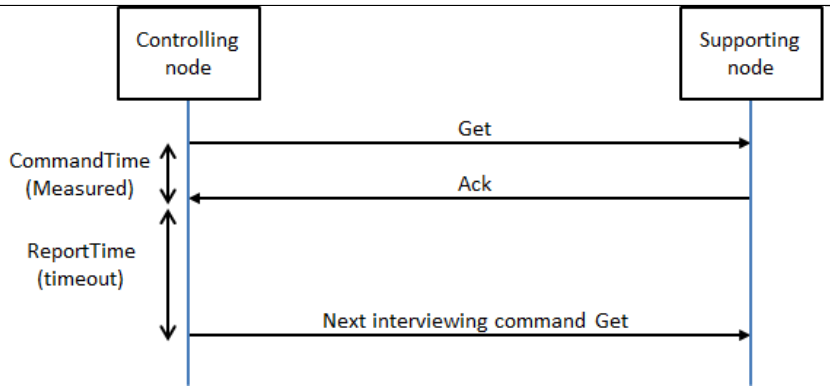

Figure 1, Node interview ReportTime timeout without security

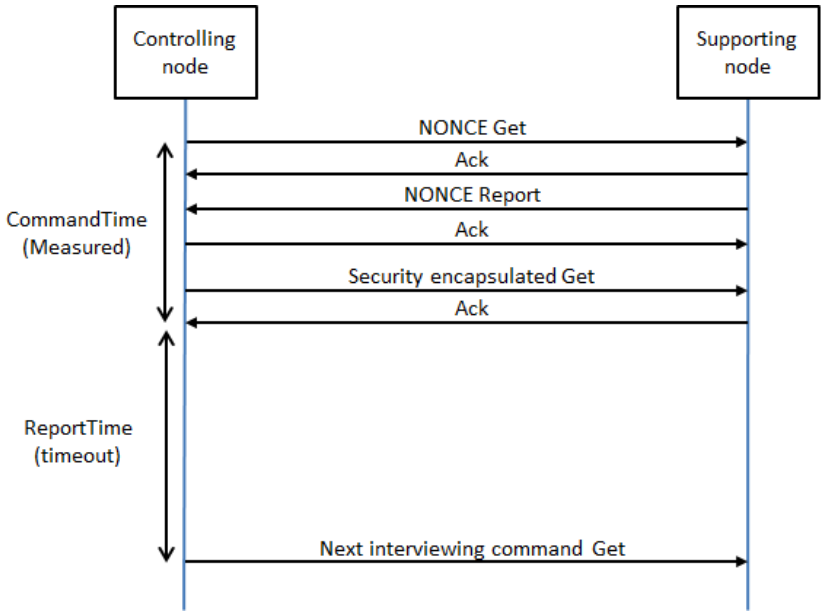

Figure 2, Node interview ReportTime timeout with security

3.7 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

RT:00.11.0011.1 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.

RT:00.11.0012.1 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 3.7.1 through 3.7.3.

RT:00.11.0013.1 Communication MUST NOT be considered as polling if:

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

3.7.1 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 3 and Figure 4

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

RT:00.11.0014.1 - CommandTime MUST be measured by the application
RT:00.11.0015.1 - The application MUST wait PollTime before polling any other node
RT:00.12.0002.1 - PollTime SHOULD be 10 seconds + CommandTime or more
RT:00.11.0016.1 - PollTime MUST NOT be less than 1 second + CommandTime

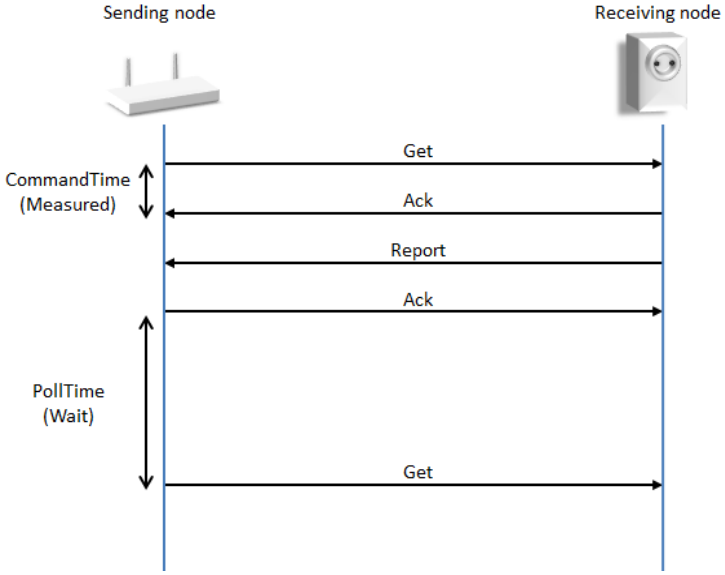

Figure 3, Polling (No errors, without security)

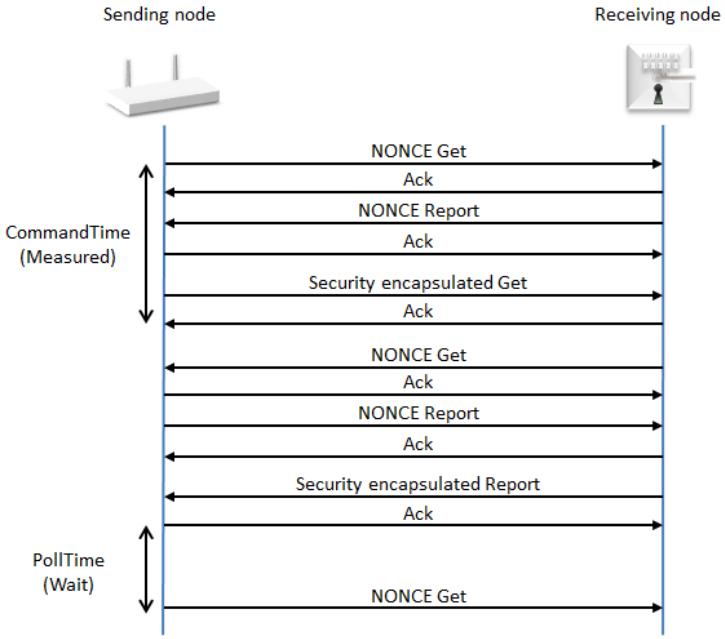

Figure 4, Polling (No errors, with security)

3.7.2 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 5 and

RT:00.11.0017.1 Figure 6. 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.

RT:00.11.0018.1

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

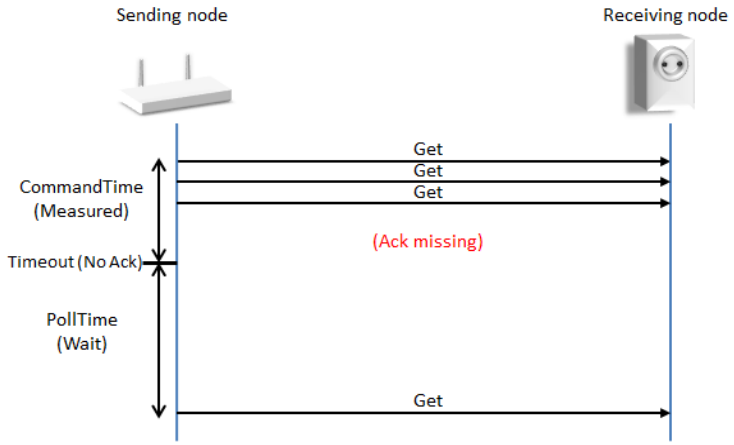

Figure 5, Polling (No Ack, without security)

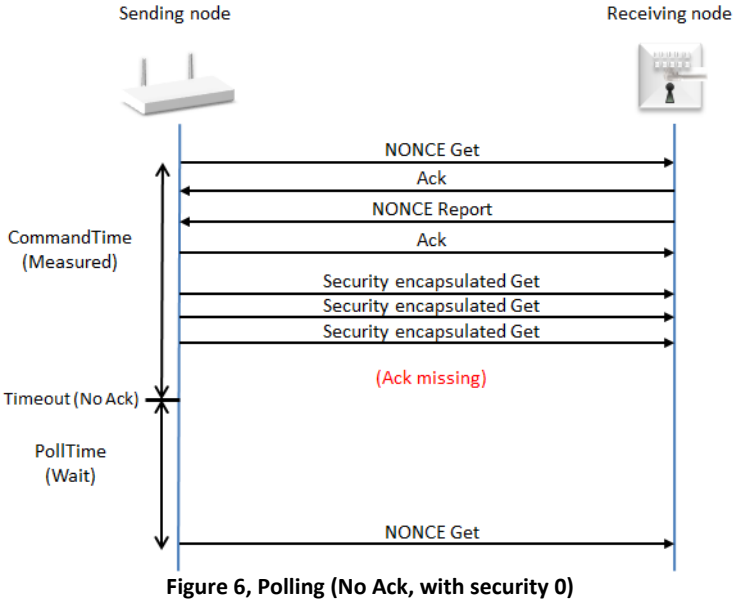

Figure 6, Polling (No Ack, with security 0)

3.7.3 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 7 and Figure 8

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

RT:00.11.0019.1
RT:00.11.001A.1

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

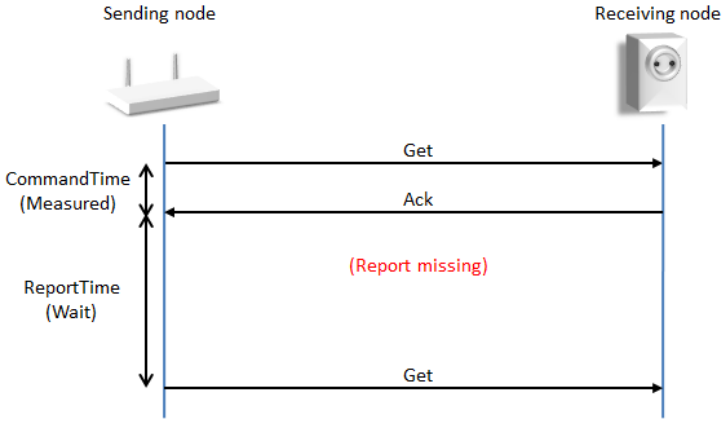

Figure 7, Polling (No Report frame, without security)

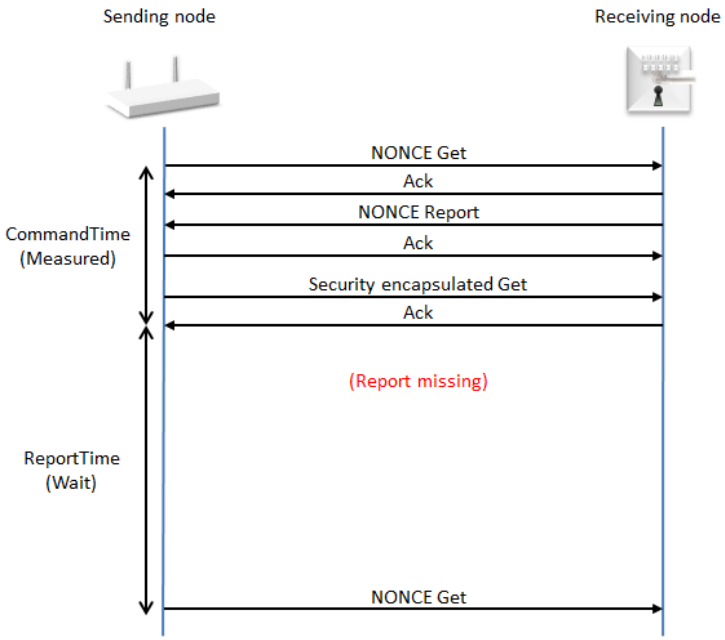

Figure 8, Polling (No Report frame, with security)

3.8 Unsolicited communication

RT:00.13.0002.1 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.

3.8.1 Unsolicited data collection communication

RT:00.11.001B.1 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.

RT:00.11.001C.1 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.

3.8.2 Unsolicited control communication

RT:00.11.001D.1 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

3.9 Runtime communication

3.9.1 Routing

RT:00.11.001E.1 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 9

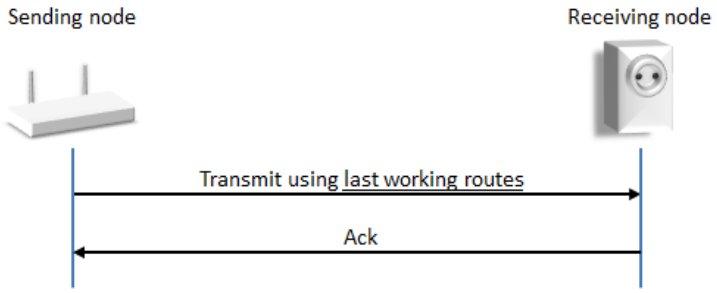

Figure 9, Successful transmission using last working routes

RT:00.11.001F.1 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 10 and Figure 11

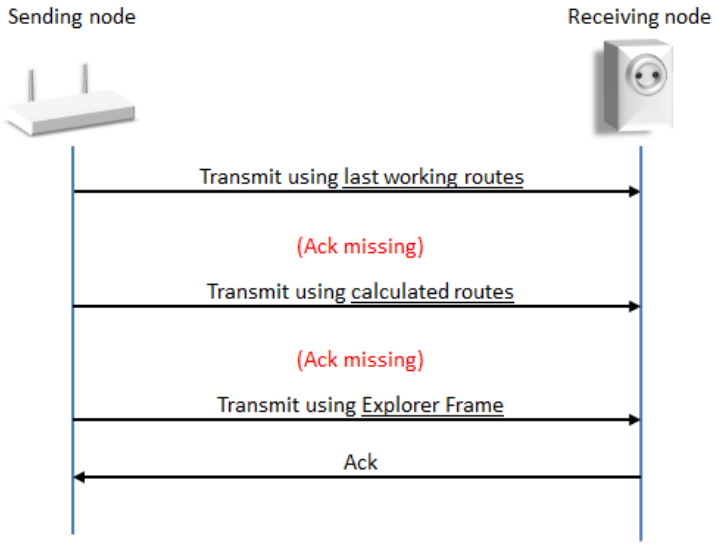

Figure 10, Successful transmission using Explorer Frame

RT:00.11.0020.1 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 10, controllers may calculate routes using the local neighbor map.

RT:00.13.0003.1 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 destination is not reachable, 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.

RT:00.13.0004.1

The steps in Figure 11 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 SHOULD give up the frame transmission.

RT:00.12.0003.1

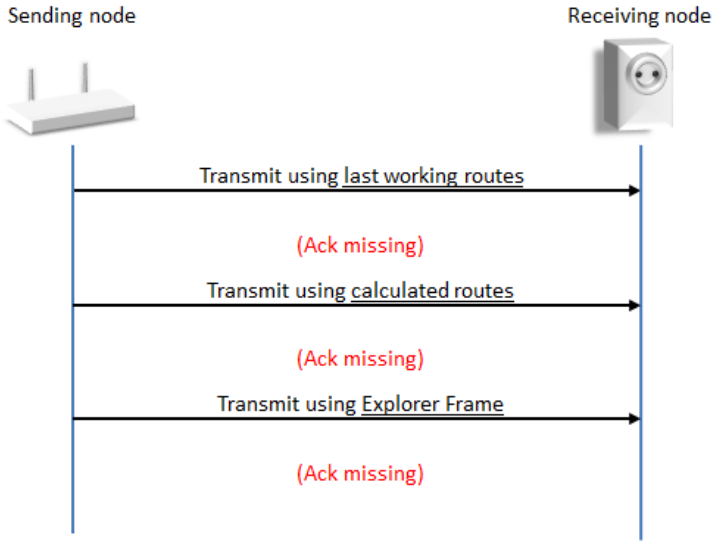

Figure 11, Unsuccessful transmission

3.9.2 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.

RT:00.12.0004.1

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.

RT:00.11.0021.1

An illustration is given in Figure 12

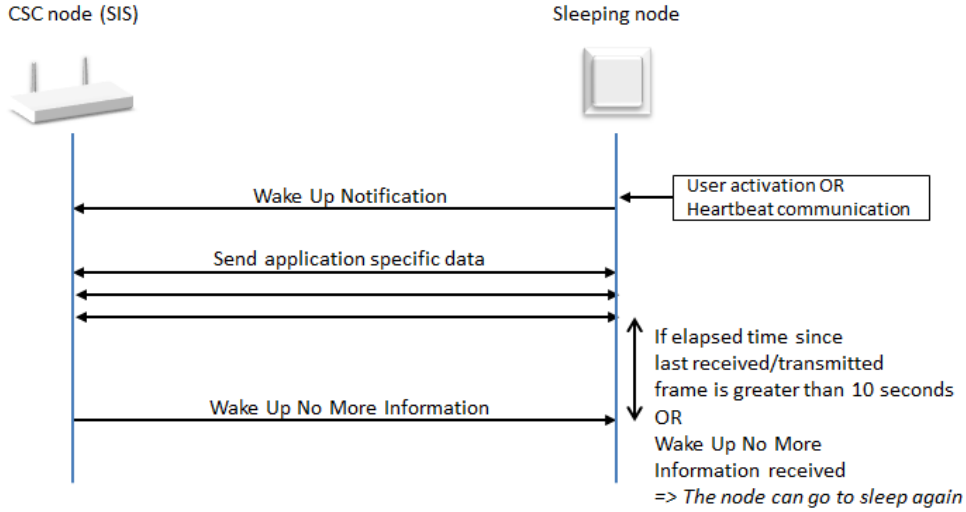

Figure 12, Wake Up Command Class

3.10 Network maintenance

RT:00.12.0005.1 The network rediscovery (Request neighbor update) feature SHOULD only be used as last resort in case the runtime communication fails.

3.11 Encapsulation order

RT:00.11.0022.1 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.

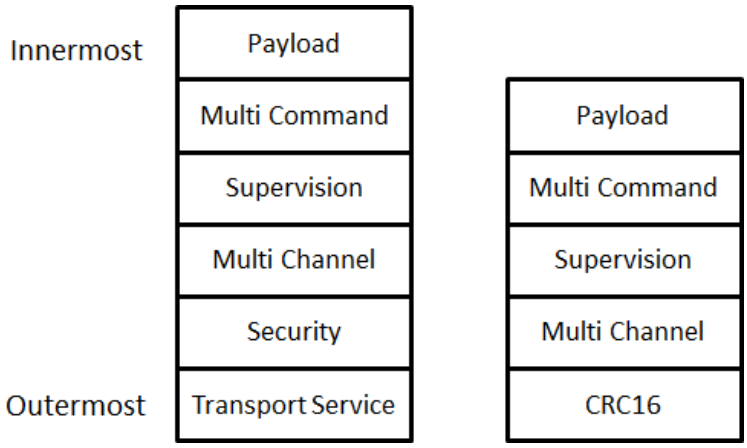

Figure 13, Encapsulation overview

Normally, responses to a given command must be carried out using the same encapsulation or lack of encapsulation as it was received, unless specified otherwise in the Command Class specifications [3], [4], [5] and [6].

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.

3.12 SmartStart requirements

3.12.1 Support requirements

3.12.1.1 SmartStart learn mode activation

RT:00.11.0023.1 A node supporting SmartStart inclusion MUST enter SmartStart Learn Mode by default when ready after powering up, regardless of network inclusion status.

RT:00.11.0024.1 A node supporting SmartStart inclusion MUST fall back on SmartStart Learn Mode after deactivating classic Learn Mode.

3.12.1.2 Higher Inclusion Request Interval

RT:00.11.0025.1 If a very power-constrained battery node is designed to settle at a higher Max Inclusion Request Interval than the default 512 seconds, this value MUST be advertised in the node's provisioning information (QR Code, refer to [1] and [9]).

3.12.1.3 Auto-reset

The SmartStart functionality may require a node to self-perform a default reset operation.

RT:00.11.0026.1 A node included via SmartStart inclusion MUST auto-reset if failing Z-Wave network inclusion or if an error occurred during S2 bootstrapping (S2 bootstrapping started and aborted).

RT:00.11.0027.1 A node included via SmartStart inclusion MUST auto-reset if S2 bootstrapping did not start.

RT:00.11.0028.1 A node included via SmartStart inclusion MUST NOT auto-reset because it is granted fewer keys or no keys at all by the controller during S2 bootstrapping.

RT:00.11.0029.1 Following auto-reset, the SmartStart node MUST automatically start requesting SmartStart inclusion again.

RT:00.11.002A.1 A SmartStart node included via classic inclusion (NWI or direct range) MUST NOT auto-reset after incomplete Z Wave inclusion or after S0/S2 bootstrapping failure.

3.12.2 Control requirements

RT:00.11.002B.1 A controller providing control of the SmartStart functionality is NOT REQUIRED to support the SmartStart functionality and support being included in a network using SmartStart inclusion.

RT:00.11.002C.1 A controller providing control of the SmartStart functionality MUST have the SIS role in a network to perform SmartStart inclusion.

RT:00.11.002D.1 A controller performing a SmartStart inclusion of another node MUST perform S2 bootstrapping even if it will grant no keys to the joining node or if the joining node does not show S2 in the NIF / Inclusion Request.

3.12.2.1 Command Class support

RT:00.11.002E.1 A Z/IP Gateway providing the SmartStart functionality MUST support the following Command Classes on the IP side:

- Network Management Inclusion Command Class, version 3 or newer
- Node Provisioning Command Class

3.12.2.2 Implementation requirements

RT:00.11.002F.1 A Provisioning List Entry MUST remain in the pending state for at least 60 minutes before being updated to the passive state.

RT:00.11.0030.1 A controller providing the SmartStart functionality MUST keep NWI enabled as long as at least 1 Provisioning List Entry is in the pending state.

RT:00.11.0031.1 A controller MUST try to include again a node that has auto-reset itself after a failed inclusion or S2 bootstrapping attempt.

3.12.2.3 User interface

RT:00.11.0032.2 A controller providing control of the SmartStart functionality MUST:

- provide a method for the end user to view the Node Provisioning List entries with their network inclusion status (included/ not included or failed).
- provide a method for the end user to manually add and remove entries in the Node Provisioning List.
- Provide a method for the end user to edit available settings for each entry in the Node Provisioning List. (e.g., Inclusion setting, Advanced joining)
- support S2 inclusion with authentication using the DSK PIN code.

RT:00.11.0033.1 If a user removes a node from the Node Provisioning List and the node is still included in the Z-Wave network, the controller MUST inform the end user that the node will stay in the network and requires to be excluded manually or reset to factory default in order to leave the Z-Wave Network.

RT:00.11.0034.1 A controller MUST inform the end user that S2 only (non-SmartStart) nodes present in the Provisioning List require to perform a classic inclusion to add them into the Z-Wave network.

3.12.2.4 QR Code scanning capability

RT:00.12.0006.1 A controller providing the SmartStart functionality SHOULD provide a QR Code scanning capability.

If the controller offers a QR Code scanning capability:

RT:00.11.0035.1
- It MUST support the addition of nodes using QR Code format defined in [10] in its Provisioning List when scanning the QR Code.

RT:00.12.0007.1
- It SHOULD support scanning of S2 only QR codes representing the DSK String prefixed with “zws2dsk:”.(example: “zws2dsk:34028-23669-20938-46346-33746-07431-56821-14553”) in order to simplify the S2 bootstrapping process.

4 ROLE TYPE OVERVIEW

Z-Wave Role Types is used as part of the Z-Wave Plus certification program. Role types define how battery and network 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.

Table 1 shows an overview of Role Types which are described in details in Chapter 5.

Table 1, Overview of Role Types

Role Type	Abbre-viation	Repea-ter	Power source	Can be SIS	Network setup	Setup lifeline	Report through lifeline	Direct controlable	Heart beat comms.
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 nodde supports 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.

Network setup: The node is capable of managing the network and inclusion/exclusion of nodes.

Setup lifeline: The node is able to configure lifeline associations.

Report through lifeline: The node 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 node is able to connect at given intervals to a central home control application to allow delivery of messages from other devices. Such a node supports the Wake Up Command Class.

4.1 Detecting the Role Type of a device

RT:00.11.0036.1

The Role Type of a node can 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 all Z-Wave Plus nodes. For details about Z-Wave Plus Info Command Class, refer to [4].

Table 2, Role Type identifiers

Role Type	Value	Identifiers
Central Static Controller (CSC)	0x00	ROLE_TYPE_CONTROLLER_CENTRAL_STATIC
Sub Static Controller (SSC)	0x01	ROLE_TYPE_CONTROLLER_SUB_STATIC
Portable Controller (PC)	0x02	ROLE_TYPE_CONTROLLER_PORTABLE
Reporting Portable Controller (RPC)	0x03	ROLE_TYPE_CONTROLLER_PORTABLE_REPORTING
Portable Slave (PS)	0x04	ROLE_TYPE_SLAVE_PORTABLE
Always On Slave (AOS)	0x05	ROLE_TYPE_SLAVE_ALWAYS_ON
Reporting Sleeping Slave (RSS)	0x06	ROLE_TYPE_SLAVE_SLEEPING_REPORTING
Listening Sleeping Slave (LSS)	0x07	ROLE_TYPE_SLAVE_SLEEPING_LISTENING
Network Aware Slave (NAS)	0x08	ROLE_TYPE_SLAVE_NETWORK_AWARE

5 ROLE TYPE DEFINITIONS

The following sections describe requirements for individual Role Types. 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 14 shows the different steps of a node setup / commissioning.

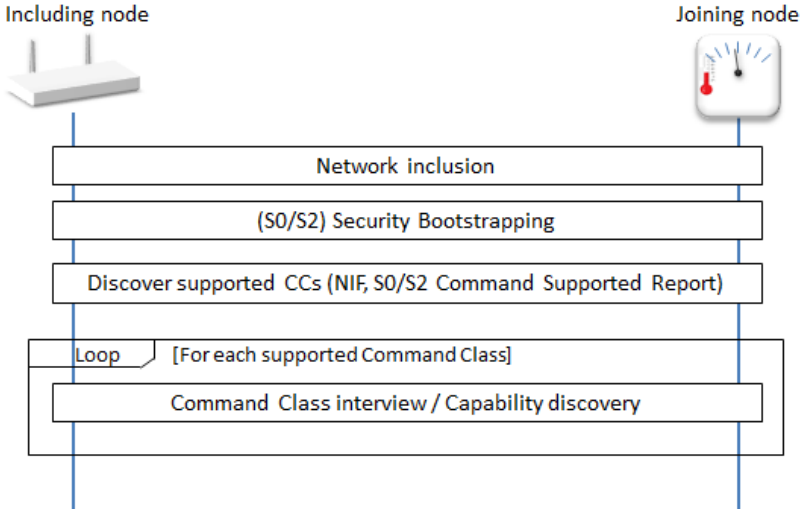

Figure 14, Node Setup / commissioning

Network inclusion

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

(S0/S2) Security bootstrapping

The security (Security 0 or Security 2) bootstrapping takes place immediately after the network inclusion. Refer to [5].

Discover supported Command Classes

The controlling node reads the supported command classes before interviewing each of them.

Command Class interview

Each role type specifies some requirements that must be observed during the Command Class interview:

- **Lifeline configuration:**

  When interviewing the Association or Multi channel association Command Class, the including controller sets up the lifeline association if it is the SIS.

RT:00.11.0037.1 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] and [2] for Lifeline group definition

- **Battery considerations**

  Some requirements apply for battery powered nodes, supporting the Wake Up Command Class. Details are given for each Role Type.

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.

RT:00.12.0008.1 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.

5.1 Central Static Controller (CSC)

The Central Static Controller Role Type is intended 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.

5.1.1 CSC Protocol Requirements

RT:01.11.0001.1 The CSC MUST respect requirements described in chapter 3.

RT:01.11.0002.1 The CSC MUST support the Static Update Controller (SUC) and SUC node ID Server (SIS) functions.

RT:01.11.0003.1 The CSC MUST be mains powered and MAY have a battery back-up.

RT:01.11.0004.1 The CSC MUST set the listening flag to 1 in its NIF.

RT:01.11.0005.1 The CSC MUST support and control the S0 and S2 Command Classes.

RT:01.11.0006.1 The CSC MUST support the following network roles:

- SIS
- Secondary controller
- Inclusion controller

5.1.1.1 If first node in the network

RT:01.11.0007.2 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

RT:01.13.0001.1 Additionally, it MAY support the following network function:

- Replace failing node

RT:01.11.0008.1 It MUST NOT be possible to activate Learn Mode if the CSC is the SIS and other nodes are included in the network.

5.1.2 CSC Setup

5.1.2.1 Inclusion process

RT:01.12.0001.1 It is RECOMMENDED to use soft buttons for activating learn mode and add mode on a CSC Role Type.

5.1.2.2 CSC including a SSC, PC, RPC or NAS

Lifeline configuration

RT:01.11.0009.1 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:

RT:01.11.000A.1
- The CSC MUST configure the Wake Up Interval Set Command destination NodeID to its NodeID.

RT:01.11.000B.1
- The CSC MUST send a Wake Up No More Information Command when the CSC has no more command to transmit.

5.1.2.3 CSC including a PS, LSS or RSS

Lifeline configuration

RT:01.11.000C.1 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

RT:01.11.000D.1 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 to its NodeID.
- 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:

RT:01.11.000E.1
- If the node advertises Wake-Up Capabilities (Wake-Up Command Class, version 2 or newer), the Wake Up Interval Set Command Seconds field MUST be within the allowed range

RT:01.11.000F.1
- If the node does not advertise Wake-Up Capabilities (Wake-Up Command Class, version 1), the Wake-Up Interval Set Command Seconds field MUST be set to 0

RT:01.12.0002.1 If the CSC is not the SIS, it SHOULD NOT send a Wake Up Interval Set Command to the included
RT:01.11.0010.1 node.
If the CSC is not the SIS and sends a Wake Up Interval Set Command, the destination NodeID MUST be the SIS' NodeID.

5.1.2.4 CSC including an AOS

Lifeline configuration

RT:01.11.0011.1 If the CSC is the SIS, it MUST set the SIS NodeID as the Association group ID 1 (Lifeline)
RT:01.11.0012.1 destination.
The CSC MUST assign a return route for the SIS.

Battery considerations

None

5.1.2.5 CSC including another CSC

RT:01.11.0013.1 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

RT:01.13.0002.1 Additionally, it MAY support the following network function:

- Replace failing node

Lifeline configuration

None

Battery considerations

None

5.1.2.6 CSC included by a PC, RPC, SSC

RT:01.11.0014.1 The CSC MUST accept to take the SIS role when a PC, RPC or SSC assigns it to the included CSC.

Lifeline configuration

RT:01.12.0003.1 If the CSC was assigned the SIS role, previously added nodes may have no lifeline associations. The CSC SHOULD create lifeline associations in all existing nodes that are directly reachable.

Battery considerations

None

5.1.3 CSC Runtime Configuration

RT:01.11.0015.1 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 12.

5.1.4 CSC Runtime Communication

No requirements

5.2 Sub Static Controller (SSC)

The Sub Static Controller Role Type is intended 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.

5.2.1 SSC Protocol Requirements

RT:02.11.0001.1 The SSC MUST respect requirements described in chapter 3

RT:02.11.0002.1 The SSC MUST be mains powered and MAY have a battery back-up.

RT:02.11.0003.1 The SSC MUST set the listening flag to 1 in its NIF.

RT:02.11.0004.1 The SSC MUST NOT support the SIS functionality.

RT:02.12.0001.1 The SSC SHOULD NOT configure lifeline associations.

RT:02.11.0005.1 The SSC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

5.2.1.1 If first node in the network

RT:02.11.0006.1 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

RT:02.11.0007.1 It MUST NOT be possible to activate Learn Mode if the SSC is the Primary Controller and other nodes are included in the network.

5.2.2 SSC Setup

5.2.2.1 Inclusion process

RT:02.12.0002.1 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.

5.2.2.2 SSC including a CSC

RT:02.11.0008.1 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.

RT:02.13.0001.1 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.

RT:02.11.0009.1 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

5.2.2.3 SSC including an RPC, PS or RSS

Lifeline configuration

None.

Battery considerations

RT:02.12.0003.1 RT:02.11.000A.1 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 a SIS in a network and the SSC sends a Wake Up Interval Set Command, the destination NodeID MUST be the SIS’ NodeID.

RT:02.12.0004.1 RT:02.11.000B.1 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:
  - RT:02.12.0005.1 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:
  - RT:02.11.000C.1 If the node advertises Wake-Up Capabilities (Wake-Up Command Class, version 2 or newer), the Wake Up Interval Set Command Seconds field MUST be within the allowed range.
  - RT:02.11.000D.1 If the node does not advertise Wake-Up Capabilities (Wake-Up Command Class, version 1), the Wake-Up Interval Set Command Seconds field MUST be set to 0

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

Lifeline configuration

None.

Battery considerations

None

5.2.3 SSC Runtime Configuration

No requirements

5.2.4 SSC Runtime communication

No requirements

5.3 Portable Controller (PC)

The Portable Controller Role Type is intended 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.

5.3.1 PC Protocol Requirements

RT:03.11.0001.1 The PC MUST respect requirements described in chapter 3

RT:03.11.0002.1 The PC MUST be battery powered and support the Battery Command Class.

RT:03.11.0003.1 The PC MUST set the listening flag to 0 in its NIF.

RT:03.12.0001.1 The PC SHOULD NOT configure lifeline associations when adding nodes to the network.

RT:03.11.0004.1 The PC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

5.3.1.1 If first node in the network

RT:03.11.0005.1 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

RT:03.11.0006.1 It MUST NOT be possible to activate Learn Mode if the PC is the Primary Controller and other nodes are included in the network.

5.3.2 PC Setup

5.3.2.1 Inclusion process

RT:03.12.0002.1 It is RECOMMENDED to use physical push buttons for activating learn mode and add mode on a PC Role Type.

5.3.2.2 PC including a CSC

RT:03.11.0007.1 If the PC is the Primary Controller and a CSC is added to the network, the PC MUST assign the SIS role to the CSC.

RT:03.11.0008.1 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

5.3.2.3 PC including an RPC, PS or RSS

Lifeline configuration

None.

Battery considerations

None.

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

Lifeline configuration

None.

Battery considerations

None

5.3.3 PC Runtime Configuration

No requirements

5.3.4 PC Runtime communication

No requirements

5.4 Reporting Portable Controller (RPC)

The Reporting Portable Controller Role Type is intended 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.

5.4.1 RPC Protocol Requirements

RT:04.11.0001.1 The RPC MUST respect requirements described in chapter 3.

RT:04.11.0002.1 The RPC MUST be battery powered and support the following Command Classes:

- Battery Command Class
- Wake Up Command Class, version 2 or newer

RT:04.11.0003.1 The RPC MUST set the listening flag to 0 in its NIF.

RT:04.12.0001.1 The RPC SHOULD NOT configure lifeline associations when adding nodes to the network.

RT:04.11.0004.1 The RPC MUST support the following network roles:

- Primary controller
- Secondary controller
- Inclusion controller

5.4.1.1 If first node in the network

RT:04.11.0005.1 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

RT:04.11.0006.1 It MUST NOT be possible to activate Learn Mode if the RPC is the Primary Controller and other nodes are included in the network.

5.4.2 RPC Setup

5.4.2.1 Inclusion process

RT:04.12.0002.1 It is RECOMMENDED to use physical push buttons for activating learn mode and add mode on an RPC Role Type.

5.4.2.2 RPC including a CSC

RT:04.11.0007.1 If the RPC is the Primary Controller and a CSC is added to the network, the RPC MUST assign the SIS role to the CSC.

RT:04.11.0008.1 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

5.4.2.3 RPC Including an RPC, PS or RSS

Lifeline configuration

RT:04.12.0003.1 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

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

Lifeline configuration

RT:04.12.0004.1 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

5.4.3 RPC runtime configuration

RT:04.11.0009.1 The RPC MUST support the Wake Up Command Class as described in 3.9.2.

RT:04.12.0005.1 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.

RT:04.11.000A.1 The RPC MUST implement a Minimum Wake Up Interval in the range 0 ..4200 (i.e. between 0 second and 70 minutes).

RT:04.11.000B.1 If the RPC’s Minimum Wake Up Interval is 0, the RPC MUST implement a Maximum Wake Up Interval greater than 0.

5.4.4 RPC runtime communication

RT:04.11.000C.1 The RPC MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

5.5 Portable Slave (PS)

The Portable Slave Role Type is intended 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. The PS allows for optimal cost, as no EEPROM is required.

5.5.1 PS Protocol Requirements

RT:05.11.0001.1 The PS MUST respect requirements described in chapter 3

RT:05.11.0002.1 The PS MUST be battery powered and support the following Command Classes:

- Battery Command Class
- Wake Up Command Class, version 2 or newer

RT:05.11.0003.1 The PS MUST set the listening flag to 0 in its NIF.

The PS can only be added to a network and has no network role requirement.

5.5.2 PS Setup

The setups of a PS by a CSC, SSC, PC or RPC are respectively described in 5.1.2.3, 5.2.2.3, 5.3.2.3 or 5.4.2.3. The PS has no additional requirement when being included.

5.5.2.1 Inclusion process

RT:05.12.0001.1 It is RECOMMENDED to use a physical push button for activating learn mode on a PS Role Type.

5.5.3 PS Runtime configuration

RT:05.11.0004.1 The PS MUST support the Wake Up Command Class as described in 3.9.2.

RT:05.12.0002.1 The PS SHOULD use a default Wake-Up interval of 0.

RT:05.12.0003.1 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.

5.5.4 PS Runtime communication

RT:05.11.0005.1 The PS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

5.6 Always On Slave (AOS)

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

5.6.1 AOS Protocol Requirements

RT:06.11.0001.1 The AOS MUST respect requirements described in chapter 3

RT:06.11.0002.1 The AOS MUST be mains powered and MAY have a battery back-up.

RT:06.11.0003.1 The AOS MUST set the listening flag to 1 in its NIF.The AOS can only be added to a network and has no network role requirement.

5.6.2 AOS Setup

The setups of an AOS by a CSC, SSC, PC or RPC are respectively described in 5.1.2.4, 5.2.2.4, 5.3.2.4 or 5.4.2.4. The AOS has no additional requirement when being included.

5.6.2.1 Inclusion process

RT:06.12.0001.1 It is RECOMMENDED to use a physical push button for activating learn mode on an AOS Role Type.

5.6.3 AOS Runtime Configuration

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

5.6.4 AOS Runtime communication

RT:06.11.0004.1 The AOS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

5.7 Reporting Sleeping Slave (RSS)

The Reporting Sleeping Slave Role Type is intended 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.

5.7.1 RSS Protocol Requirements

RT:07.11.0001.1 The RSS MUST respect requirements described in chapter 3.

RT:07.11.0002.1 The RSS MUST be battery powered and support the following Command Classes:

- Battery Command Class
- Wake Up Command Class, version 2 or newer

RT:07.11.0003.1 The RSS MUST set the listening flag to 0 in its NIF.

The RSS can only be added to a network and has no network role requirement.

5.7.2 RSS Setup

The setups of an RSS by a CSC, SSC, PC or RPC are respectively described in 5.1.2.3, 5.2.2.3, 5.3.2.3 or 5.4.2.3. The RSS has no additional requirement when being included.

5.7.2.1 Inclusion process

RT:07.12.0001.1 It is RECOMMENDED to use a physical push button for activating learn mode on an RSS Role Type.

5.7.3 RSS Runtime configuration

RT:07.11.0004.1 The RSS MUST support the Wake Up Command Class as described in 3.9.2 and in Figure 12.

RT:07.12.0002.1 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.

RT:07.11.0005.1 The RSS MUST implement a Minimum Wake Up Interval in the range 0 ..4200 (i.e. between 0 second and 70 minutes).

RT:07.11.0006.1 If the RSS's Minimum Wake Up Interval is 0, the RSS MUST implement a Maximum Wake Up Interval greater than 0.

5.7.4 RSS Runtime communication

RT:07.11.0007.1 The RSS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for details.

5.8 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.

5.8.1 LSS Protocol Requirements

RT:08.11.0001.1 The LSS MUST respect requirements described in chapter 3.

RT:08.11.0002.1 The LSS MUST be battery powered and support the Battery Command Class.

RT:08.11.0003.1 The LSS MUST set the listening flag to 0 in its NIF.

The LSS can only be added to a network and has no network role requirement

5.8.2 LSS Setup

The setups of an LSS by a CSC, SSC, PC or RPC are respectively described in 5.1.2.3, 5.2.2.3, 5.3.2.3 or 5.4.2.3. The LSS has no additional requirement when being included.

5.8.2.1 Inclusion process

RT:08.12.0001.1 It is RECOMMENDED to use a physical push button for activating learn mode on a LSS Role Type.

5.8.3 LSS Runtime configuration

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

5.8.4 LSS Runtime communication

RT:08.11.0004.1 The LSS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for details.

RT:08.11.0005.1 The LSS MUST stay awake for at least 2 seconds after communicating.

5.9 Network Aware Slave (NAS)

The Network Aware Slave Role Type is intended 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.

5.9.1 NAS Protocol Requirements

RT:09.11.0001.1 The NAS MUST respect requirements described in chapter 3.

RT:09.11.0002.1 The NAS MUST be mains powered and MAY have a battery back-up.

RT:09.11.0003.1 The NAS MUST set the listening flag to 1 in its NIF.

RT:09.11.0006.1 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.

RT:09.11.0004.1 The NAS MUST NOT provide the following network functions:

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

5.9.2 NAS Setup

The setups of an NAS by a CSC, SSC, PC or RPC are respectively described in 5.1.2.2, 5.2.2.4, 5.3.2.4 or 5.4.2.4. The NAS has no additional requirement when being included.

5.9.2.1 Inclusion process

RT:09.12.0001.1 It is RECOMMENDED to use a physical push button for activating learn mode on an NAS Role Type.

5.9.3 NAS Runtime Configuration

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

5.9.4 NAS Runtime communication

RT:09.11.0005.1 The NAS MUST communicate via the lifeline association if any lifeline association exists. Refer to [1] for more details.

APPENDIX AINCLUSION 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

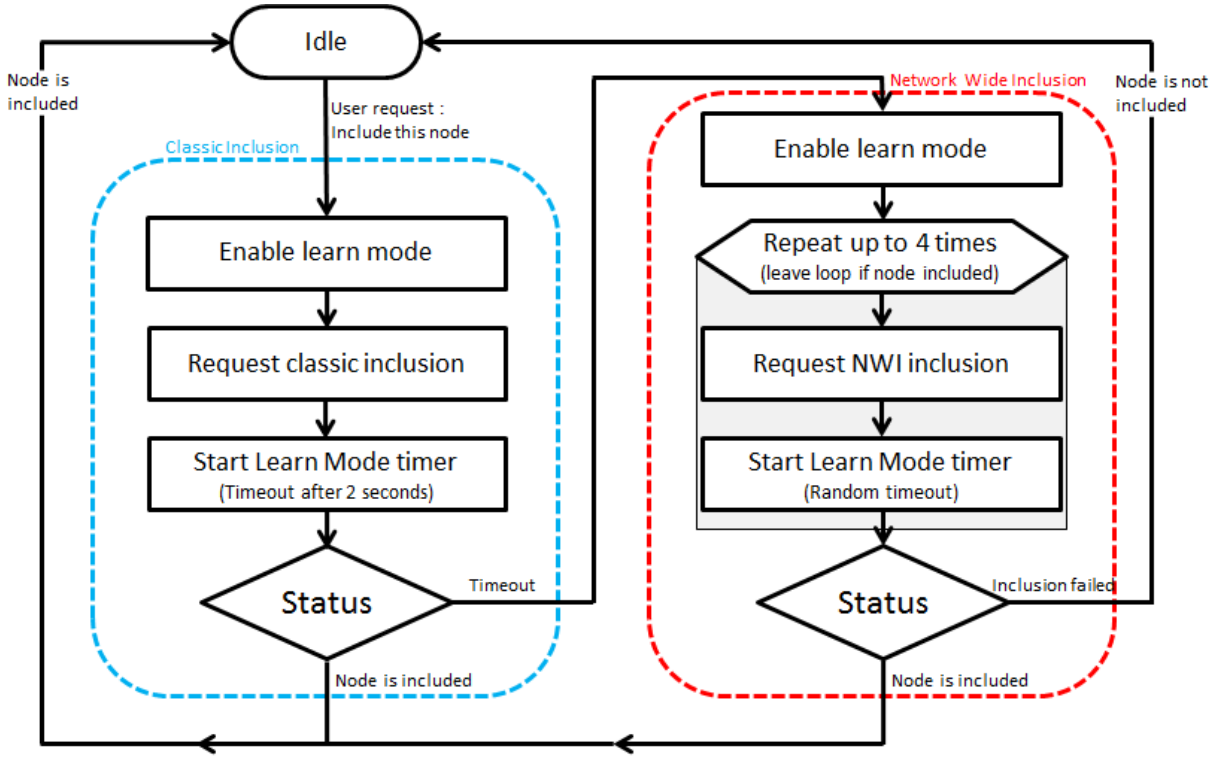

Figure 15, Inclusion process for the node being included

Appendix A.2 Including a node

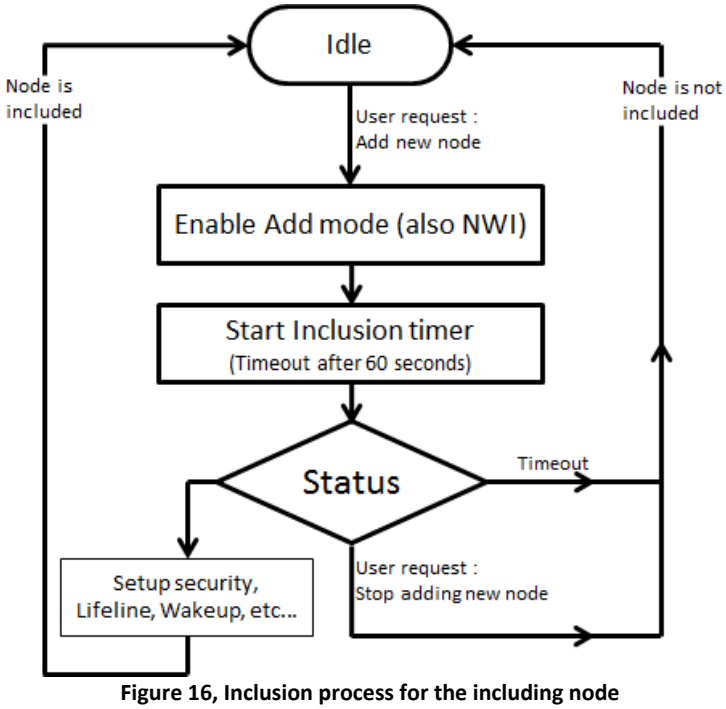

Figure 16, Inclusion process for the including node

REFERENCES

[1] Silicon Labs, SDS11847, Software Design Specification, Z-Wave Plus Device Types Specification.
[2] Silicon Labs, SDS14224, Software Design Specification, Z-Wave Plus v2 Device Types Specification.
[3] Silicon Labs, SDS13781, Z-Wave Application Command Class Specification
[4] Silicon Labs, SDS13782, Z-Wave Management Command Class Specification
[5] Silicon Labs, SDS13783, Z-Wave Transport-Encapsulation Command Class Specification
[6] Silicon Labs, SDS13784, Z-Wave Network Protocol Command 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, SDS13944, Node Provisioning Information Type Registry (QR code, Z/IP Gateway, Smart Start)
[10] Silicon Labs, SDS13937, Node Provisioning QR Code Format (S2, Smart Start)