Instruction

Z-Wave PC based Controller v5 User Guide

Document No.:	INS13114
Version:	24
Description:	-
Written By:	JFR;SEROMAN1;SCBROWNI;VOSAVOST
Date:	2022-12-07
Reviewed By:	JKA;COLSEN;JSI;ABUENDIA;RREYES;SEROMAN1;SCBROWNI;JFR;JCC;CAOWENS
Restrictions:	Public

Approved by:

Date	CET	Initials	Name	Justification
2022-12-07	16:37:41	JFR	Jorgen Franck	on behalf of NTJ
2022-12-07	16:37:30	JFR	Jorgen Franck	on behalf of NTJ

SILICON LABS

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
1	20141217	SRO;AVA;VSA	All	Initial version based on INS10240-13
	20150226	SRO;AVA;VSA	All	Updated all screenshots, Updated Association, Command Class, Encrypt/Decrypt, Firmware Update, Backup/Restore NVM topics Added IMA, Settings Trace Capturing, Polling functionality, Setup Route functionality topic
	20150226	SRO	4.21.1	Added Power shell script example
2	20160128	SRO;VSA	All	Update all screenshots
			3.1.1	Added new settings view Updated description for Security S0 test settings and added description for Security S2 keys and test settings
			0	Update list of views available from start screen
			3.2	Described 'Floating View' option
			3.2.3	Added screenshot for additional Bridge Controller actions (Add, Remove virtual) Updated description of the available nodes' actions including Security S2-related actions
			3.2.4	Added screenshot for additional Bridge Controller action (Virtual Learn Mode) Updated description of the available controller actions Added description of the Set Node Information action.
			3.4	Updated description of the available options on the Command Classes view
			3.10	Added Security S2 Encrypt/Decrypt description
			3.14, 4.15	Added: Configuration Command Class support
			3.15,	Added: UL Monitor Tool
			4.1	Update Table1
			4.2.2	Added: Nodes with Endpoints
			4.2.5	Added: NWE
			4.2.10	Added warning screenshot if SIS already present in network
			4.2.22	Added: Select Security scheme
			4.2.20	Added: Reset SPAN
3	20160224	SRO	All	Update all screenshots
			3.1.1	Updated: Settings also contains connection arguments input field
			4.2.1	Changed: added secure S2 node inclusion dialogs description
4	20160708	SRO	3.1.1	Updated Tab S2 Security Test Scheme topic (new test settings and CSA option)
			3.2	Updated screenshot
			3.2.4	Updated screenshot and added MPAN table description
			3.3	Updated Association view screenshot and description
			3.1, 3.2, 3.2.3	Added screenshots for Z/IP controller
			3.2.4	Added screenshots for Z/IP controller, Unsolicited destination description
	20160708	SRO	4.5	Updated topic
5	20160726	AVASILEVSKY	4, 4.2.1	Added reminders to set up unsolicited destination for Z/IP Gateway
	20160726	AVASILEVSKY	3.4	Update command classes view screenshot Added description of 'Auto increment' session id functionality for supervision encapsulation
	20160805	AVASILEVSKY	4.14	Added clarifications on how NVM restores from zip and hex files
6	20160912	AVASILEVSKY	3.1, 3.2, 3.11, 4.2	Updated screenshots Added description for new buttons and views
	20160913	AVASILEVSKY	4.7	Added explanations how to configure security test schema

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
	20160927	JFR	1.3	Updated necessary tools for PC-based Controller build environment.
7	20161206	SRO	2.3	Updated installation steps
			All	Updated screenshots
				Removed "Start the Z-Wave PC Controller" section
			3.1.1.4	Updated section: Security Test Schema Button
	20161212	SRO	4.7	Updated section: Security Test Schema view
			4.12	Added S2 message encapsulation frame decrypt description
			4.14	Include mention of the wake-up settings of the Sensor PIR nodes
8	20170922	VSAVOSTIANENKO		Removed image "Node settings pop-up window"
			3.1.1.4	Added property "Is Broadcast"
			4.7.2	Added property "Is Broadcast" explanation
				Removed "UL Tool Monitor View" section
				Removed "UL Tool Monitor" Section
			3.15	Added "Smart Start View" section
			4.16	Added "Smart Start" section
			All	Updated screenshots
			4.7.3	Added description of "Applied Action" and updated examples
9	20180305	BBR	All	Added Silicon Labs template
10	20180531	SRO	1.3	Updated to .Net Framework 4.5
11	20180601	VSAVOSTIANENKO	All	Updated all screenshots
	20180601	VSAVOSTIANENKO	3.2.4	Updated selection learn mode
	20180601	VSAVOSTIANENKO	3.4	Added additional buttons
	20180601	VSAVOSTIANENKO	4.16	Updated view description
	20190315	JFR	All	Fixed page numbers
12	20190320	AYurttas	All	Tech Pub reviewed revision
13	20190520	VOSAVOST	All	Updated all screenshots
			3.2.3	Added Identify button
			4.2.18	Added Identify button description
			3.17	Added Transmit Settings UI
			4.17	Added Transmit Settings UI description
	20190520	SEROMAN1	1.3 & 2.1	Updated sections
14	20190523	SCBROWNI	2.1 & 4.17	Typos
15	20190613	VOSAVOST	2.2	Updated section "Required Z-Wave Hardware"
			3.17	Updated screenshot and description table
			4.17	Updated section "Transmit Settings" and screenshot
	20190621	VOSAVOST	4.3	Remove Set Node Info from Controller View functionality section
			0	Added section "Set Node Information View" section
			4.17	Added section "Set Node Information" section
			4.1	Updated table
16	20190923	SEROMAN1	3.1.1.1	Updated table and figure
			3.1.1.3	Added Section
			All	Updated Sections and screenshots
	20191203	VOSAVOST	3.1.1.1	Updated Table
			3.2.4	Updated "unsolicited destination view" description
			All	Updated screenshots
	20200326	VOSAVOST	All	Added and updated List of tables and Indexes
	20200327	VOSAVOST	All	Review changes, updated references and punctuation
17	20200528	SCBROWNI	All	Technical Publications Review
	20200603	VOSAVOST	4.5.1	Fixed typo
18	20200618	SEROMAN1	All	Updated screenshots related to Long Range feature

REVISION RECORD

Doc. Rev	Date	By	Pages affected	Brief description of changes
			3.2.1, 3.15, 4.16	Added 'LR flag', added 'Node Options'
19	20201124	VOSAVOST	All	Updated sections and screenshots
			3.1.1.4	Added Long Range Network Keys
			3.1.2	Updated list of content Main View
			3.4	Added Send Data History and removed Last Used and Repeat List from Command Class View
			3.17	Added 'Set LR Channel'
			4.2.1	Added Smart Start Long Range inclusion description
			3.15	Added 'Updated' button
19	20201124	SCBROWNI	All new sections	Review all new or revised sections since last Tech Pub's review
20	20201201	OBOIKO	3.15	Added 'LR flag' for Z/IP connected Controller
21	20200122	VOSAVOST	3.17, 4.18	Added 'DCDC Config' controls and description
			3.18, 4.19	Added new 'Network Statistics' view and description
			3.1.1.3	Added 'Inclusion Controller Initiate Request Timeout'
22	20210604	VOSAVOST	1	Added abbreviations
			3.1.1.3	Added 'Supervision Report Status Response' option
			3.2.4	Added description for Select Learn Mode View Items
			3.11, 4.13	Added 'Stop transmitting bulk reports on missing acknowledge'
			3.17, 4.18	Added 'Max LR Tx Power' and 'Radio PTI'
			All	Updated figures
23	20220418	VOSAVOST	3.4	Added 'Predefined Commands' and 'Recent Commands' view description
			3.11	Updated Screenshot and table
			3.18	Added 'Background RSSI' and updated Screenshots and table
24	20221108	VOSAVOST	1.3, 2.1	Updated to .Net Framework 4.8
			1.1, 2.2, 3.1.1.4, 3.2.1, 3.2.4, 3.4, 3.17, 4.1, 4.3	Updated description of Serial API End Device
			All	Updated figures

Table of Contents

List of Figures

List of Tables

1. ABBREVIATIONS

Abbreviation	Explanation
API	Application Programming Interface
DLL	Dynamic Link Library
IMA	Installation and Maintenance Application
NVM	Non-volatile memory
OTA	Over-the-air
OTW	Over-the-wire
SC	Static Controller
SUC	Static Update Controller
SIS	SUC ID Server
ERTT	Enhanced Reliability Test Tool
DSK	Device-Specific Key
LR	Long Range
RF	Radio Frequency
PTI	Packet Trace Interface
WSTK	Wireless Starter Kit

1 INTRODUCTION

1.1 Purpose

The Z-Wave PC-based Controller application is an example on how Static/Bridge Controller and End Device Serial API functionality can be used to implement a Z-Wave-enabled PC application.

1.2 Audience and Prerequisites

The audience is Z-Wave partners and Silicon Labs. It is assumed that the Z-Wave partner is already familiar with the current Z-Wave Developer's Kit.

1.3 Implementation

The Z-Wave PC-based Controller application requires the .NET Framework 4.8 or higher.

2   THE Z-WAVE PC-BASED CONTROLLER

The Z-Wave PC-based Controller is an application designed for the Windows platform that can communicate with Z-Wave nodes like switches and sensors through a Static Controller (SC).
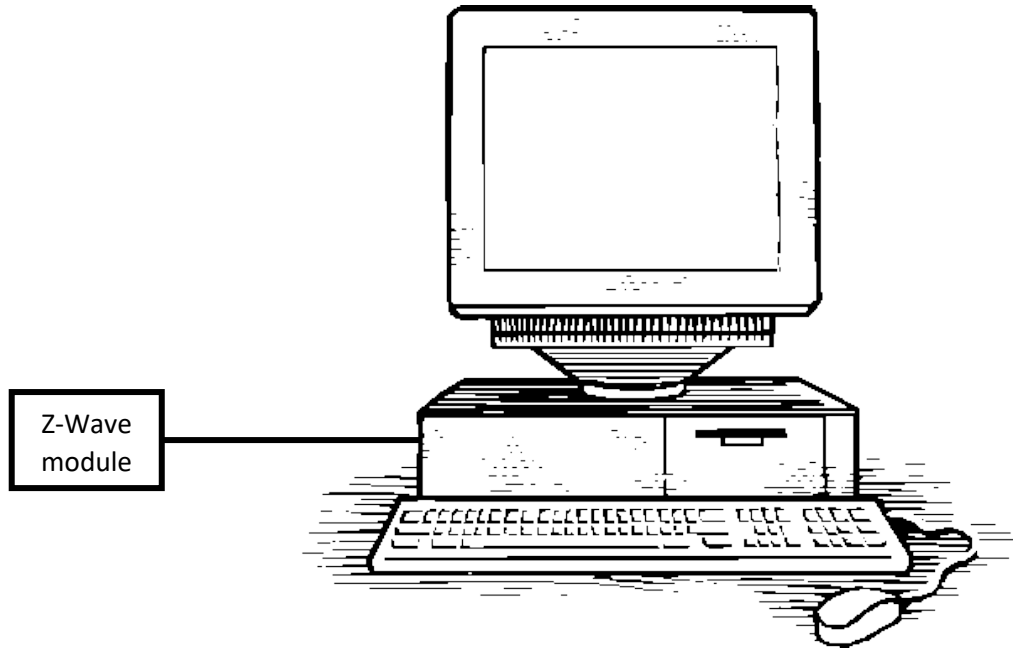
Figure 1. PC with a Z-Wave Module Connected

2.1   Check the Prerequisites

The .NET Framework 4.8 or later must be installed on the machine to run the Z-Wave PC-based Controller Windows application.

Limitation: Z-Wave PC Controller has been verified on Windows 10.

Important: Ensure that you have the latest service pack and critical updates for the version of Windows that you are running.

2.2   Required Z-Wave Hardware

Z-Wave PC Controller application requires a Z-Wave module programmed with a Serial API application, including next library types: Static Controller, Bridge Controller, Portable Controller, End Device and connected to the appropriate serial or USB port.

To program the Z-Wave module, use the firmware HEX file and additional programming tool:

-    Simplicity Studio and choose needed application from latest available Z-Wave SDK demos.
-    For devices with chip series ZW050x and older use Z-Wave Programmer tool and file by next name pattern: `serialapi_<Lib_Type>_ZW050x_XX.hex` (USB version has USBVCP in

its name) located in the directory 'C:\DevKit_X_YY\SDK\ProductPlus\Bin\
SerialAPI_Controller_Static\'

Finally, connect the Z-Wave device to the COM or WSTK Virtual COM port on the PC.

UZB is the Z-Wave USB Adapter. It is a USB-based Static Controller.

As the device exports a USB CDC/ACM class-compliant interface, it appears as a serial port, reusing existing standard drivers on the most popular PC operating systems. As such, there is no vendor driver required. Over the serial port, the Z-Wave Serial API is exported.

UZB.INF is provided that reuses the standard Windows usbser.sys or usbser64.sys driver. The device appears in the Device Manager under the Ports section, and is accessible through the Windows CreateFile API by applications as "//.//COMxxx" where xxx is the COM Port number assigned by the OS.

For more information on UZB, see INS11850, Instruction, UZB User Manual.

2.3   Install the Z-Wave PC Controller

Perform the following steps to install the Z-Wave PC Controller:

1. Exit all programs.

2. Run the installation file of the Z-Wave PC Controller application and follow the installation wizard.

3. The actual installation procedure will pass with progress indicator and final confirmation appears.

4. Click **Finish** to complete the installation.

2.4   Remove Z-Wave PC Controller

You can uninstall Z-Wave PC Controller from your computer if you no longer use it.

1. Open "**Add or Remove Programs"** in Control Panel.
2. Click the program in the list and then click the "**Remove"** button.
3. Standard confirmation dialog appears. Click "**Yes"** to continue the removal of the Z-Wave PC Controller software.
4. Z-Wave PC Controller and its settings will be removed.

3   USER INTERFACE

3.1   Main Menu View

The Z-Wave PC Controller application's Main menu view consists of the following items:

- Title bar
- Content view (current view depends on selected button on Main menu view)
- Log bar
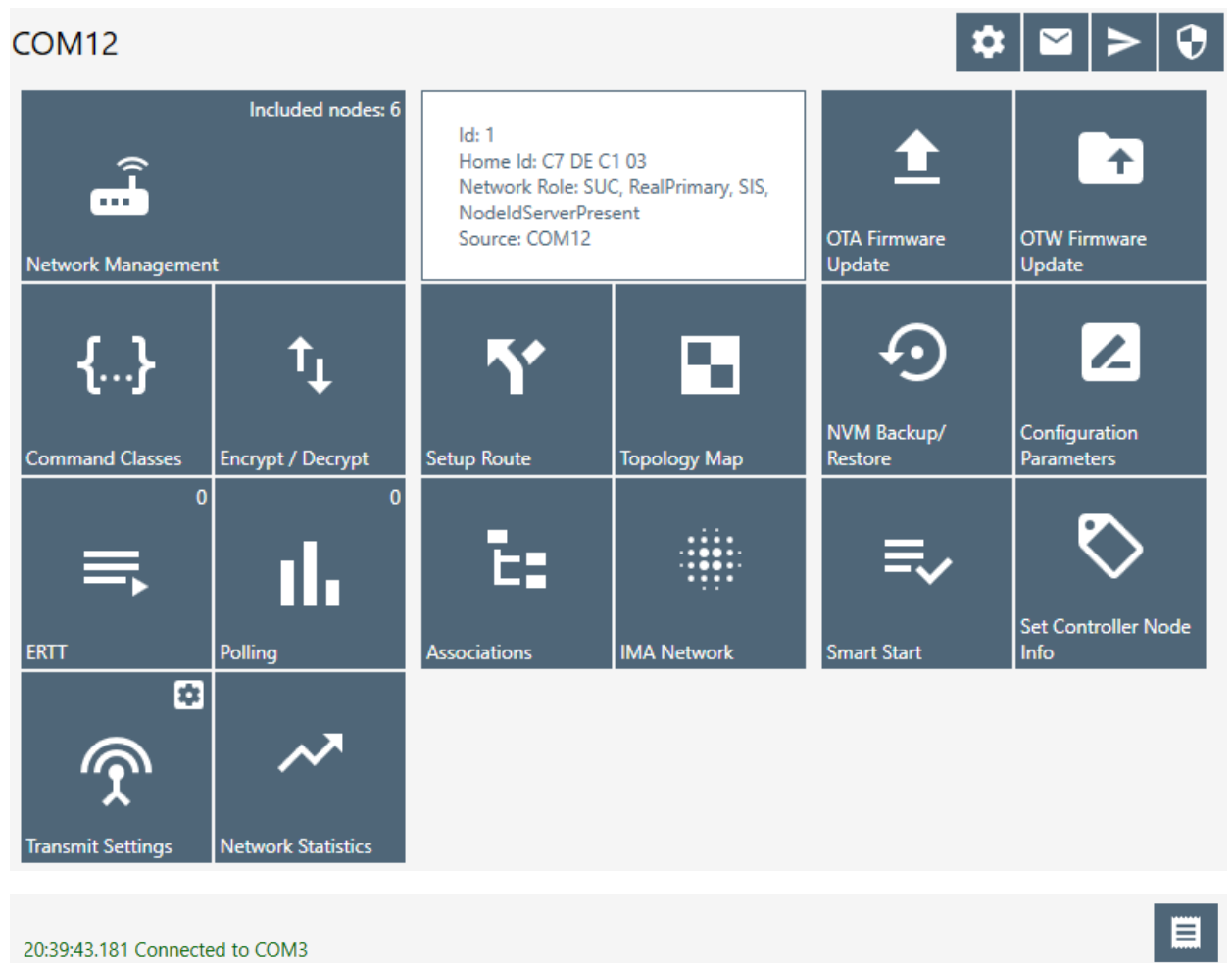
Figure 2. Main Menu View

The availability of a menu item depends on the library type of connected device.

3.1.1   Title Bar

The Title bar is located on top of the Main Menu View. It is accessible from any view. It has the following items:

3.1.1.1 Settings

Pressing on the Settings button opens a new window in which a controller device can be selected. Additionally, users can set up trace capture settings in this window.

Figure 3. Settings View

Table 1. Settings View Items

Menu item	Description
Detect	Detects library type for available devices.
Refresh	Refreshes list of connected devices.
Clear All	Clears list of Socket Data Sources.
Discover	Detects available Socket Data Sources. ZIP Gateway and WSTK boards connected via IP.
Add	Adds custom IP Address to list.
Enable Watchdog	Turn On/Off Watchdog command for ZW070x devices.
Capture communication trace to	Enables trace capturing.

… (Browse for Folder)	Selects folder for saving files of capture.
Auto split	Enables splitting files by size and/or duration and count of file parts.
Ok	Selects chosen COM port as controller and closes the window and applies changes of trace capturing.
Cancel	Closes the window without changes.

3.1.1.2 Commands Queue Button

Pressing the "Commands Queue" button shows the queue commands for nodes in the new window. Each node has its own group.
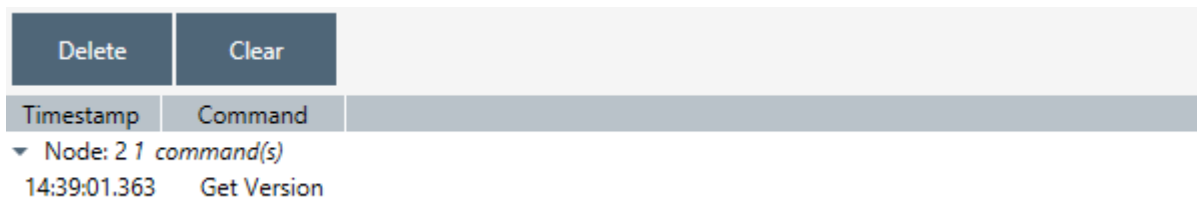
Figure 4. Commands Queue View

Table 2. Commands Queue View Items

Menu item	Description
Delete	Deletes selected command from queue.
Clear	Clears queue.

3.1.1.3 Send Data Settings

Opens view with Send Data options for easy navigation and setup data from any other view

Figure 5. Send Data Settings

Table 3. Send Data Settings Items

Menu item	Description
Delay 'Wake Up No More Information'	Sets additional delay in ms to respond with Wake Up No More after releasing commands queue for non-listening receiver.
Max bytes in encrypted (S0) packet's fragment	Sets the maximum length in encrypted packet fragments.
Transport service max segment size	Sets the Transport service maximum segment size. Reads max payload length from device. Default value is taken from the connected device and equal to Max Payload Size.
Request Timeout	Changes wait time in ms for request commands responds.
Delay Response	Sets additional delay in ms to respond on any received data.
Inclusion Controller Initiate Request Timeout	Sets wait time for Initiate Inclusion Controller request completes in ms
Supervision Report Status Response	Sets reported 'Status byte' in response to Supervision Get, by default 'SUCCESS'
Ok	Apply options and close the dialog.
Cancel	Close the dialog with changes.
Apply	Applies set options without closing.

3.1.1.4　Security Test Schema Button

Pressing on the Security Test Schema button opens a new window Security Settings which contains the list of security network keys and the list of test properties for Security and Security Version 2.

Disabled for the Serial API End Device and controlled by the device.
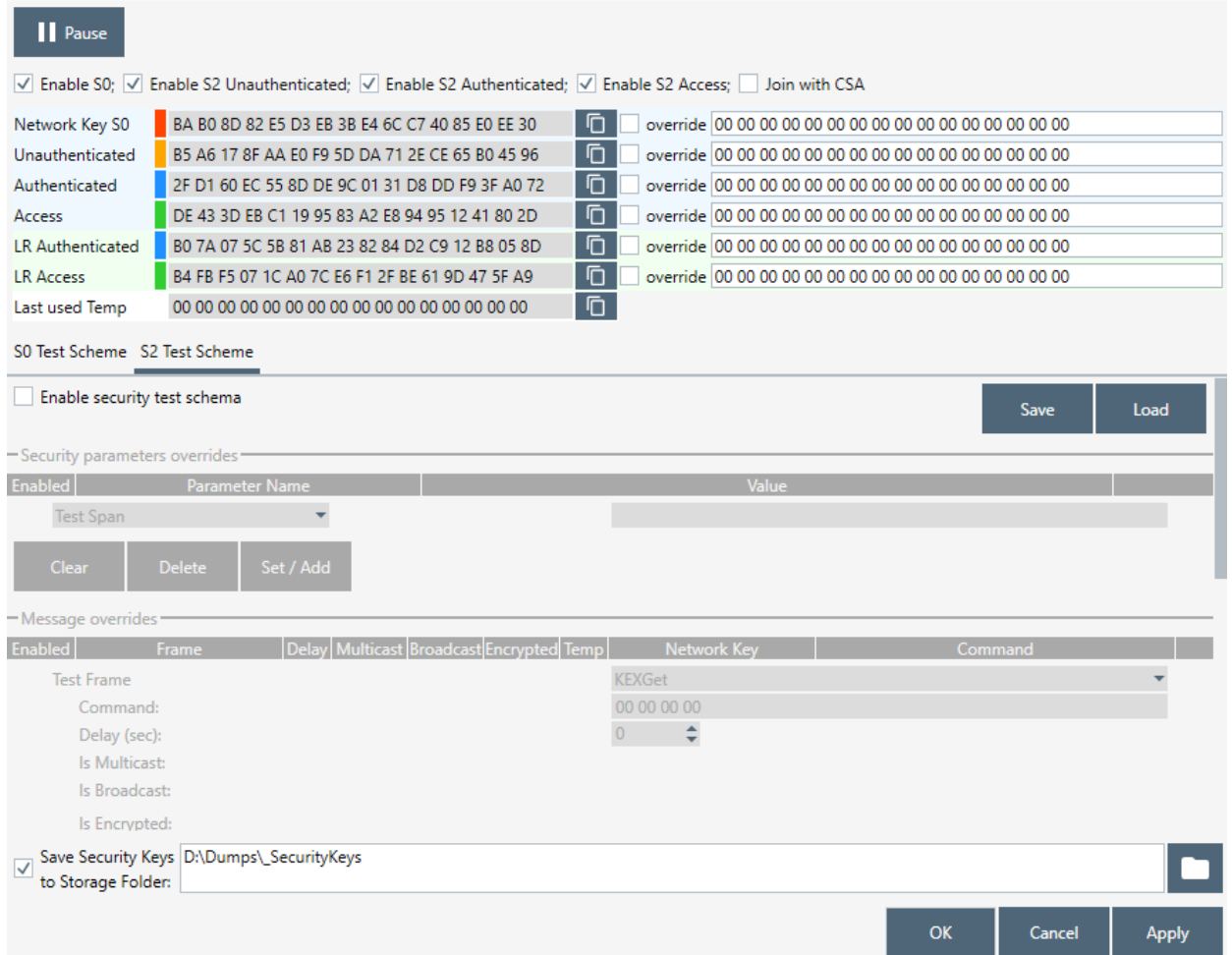
Figure 6. Security Test Settings

Table 4. Security Test Settings View Items

Menu item	Description
Save	Saves the current Security S2 test schema to file.
Load	Loads the Security S2 test schema from file.
OK	Applies current Security settings and Security Test Settings if enabled and closes the Security Settings dialog.
Cancel	Closes the Security Settings dialog without applying

	changes.
Apply	Applies current Security settings and Security Test Settings if enabled without closing the Security Settings dialog.

The Security Test Schema functionality is available to test secure networks for failures if the device malfunctions.

Checkboxes "Enable S0", "Enable S2 Unauthenticated", "Enable S2 Authenticated", and "Enable S2 Access" turns on/off corresponding security class.

Checkbox "Join with CSA" allows the PC Controller to send KEX Report with CSA flag set to 1. This flag will only be set when the PC Controller is included in the network as a secondary controller.

Current Network Keys are shown in grey (disabled editing) textboxes according to security level: Network Key S0, Unauthenticated, Authenticated, Access and LR Authenticated, LR Access for Long Range, and Last Used Temp. Near each network key are buttons to copy the value to clipboard and checkboxes to use the Permanent Key from the white (enabled editing) textbox.

Save Security Keys to Storage checkbox enables saving network keys to file when applying settings, resetting the controller and when adding the controller to another network. The button "…" changes the storage folder path. Values will be added to file with the current network home ID name.

Tab S0 Security Test Scheme

Security Test Schema S0 can be configured for both Including Controller and Included Node. To enable Schema, check the "Enable security test schema" checkbox.

All changes made on this view are applied after clicking the "OK" or "Apply" button.

Tab S2 Security Test Scheme

To enable Schema, check the "Enable security test schema" checkbox. See [4] for more details.

All changes made on this view are applied after clicking the "OK" or "Apply" button.

Group "**Security parameters overrides**" allows changing encryption parameters:
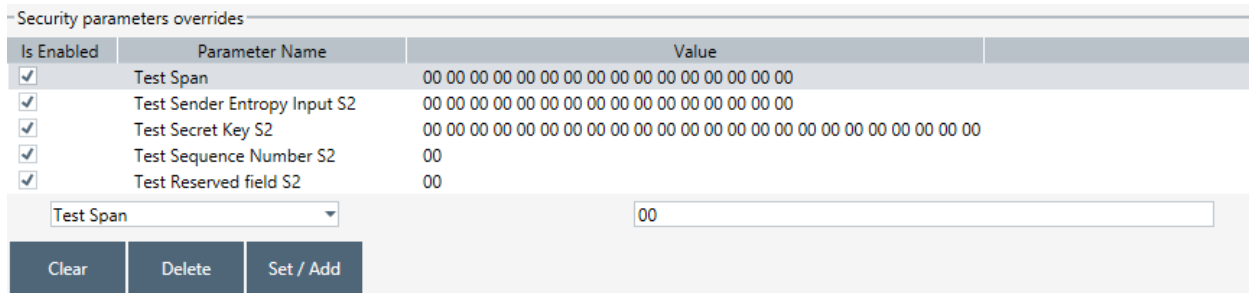
Figure 7. Security Parameter Overrides

- Test Span replaces the current SPAN with a specified value during data encryption.

- Test Sender Entropy Input S2 replaces the sender Entropy Input with a specified value during data encryption.
- Test Secret Key S2 replaces the current secret key of the S2 keypair. DSK value will be calculated based on the secret key.
- Test Sequence Number S2 replaces the current Sequence Number with a specified value during data encryption.
- Test Reserved field S2 replaces the Reserved field with a specified value during data encryption.

Group "**Message overrides**" contains a set of test frames with properties: "Command", "Delay", "Is Encrypted", "Is Multicast", "Is Broadcast", "Network Key", and "Is Temp Network Key". Click a corresponding checkbox to activate the parameter override and specify a new value. If the parameter override is not active, the PC Controller will use a valid specific frame parameter value. For example, "KEXGet" is not encrypted but KEXGetEcho is encrypted if "IsEncrypted" parameter is not active.

Figure 8. Security Message Overrides

Test Frame types:

- InjectCommand
- KEXGet
- KEXReport
- KEXSet
- PublicKeyReportB – joining node's Public Key Report frame
- PublicKeyReportA – including controller's Public Key Report frame
- KEXSetEcho
- KEXReportEcho
- NetworkKeyGet_S0
- NetworkKeyReport_S0
- NetworkKeyVerify_S0
- NetworkKeyGet_S2Unauthenticated
- NetworkKeyReport_S2 Unauthenticated
- NetworkKeyVerify_S2 Unauthenticated
- NetworkKeyGet_S2 Authenticated
- NetworkKeyReport_S2 Authenticated

- NetworkKeyVerify_S2 Authenticated
- NetworkKeyGet_S2Access
- NetworkKeyReport_S2 Access
- NetworkKeyVerify_S2 Access
- TransferEndA_S0 – including controller
- TransferEndA_S2Unauthenticated– including controller
- TransferEndA_S2Authenticated – including controller
- TransferEndA_S2 Access – including controller
- TransferEndB – joining node
- NonceGet
- NonceReport
- MessageEncapsulation
- CommandsSupportedReport
- InclusionInitiate1
- InclusionInitiate2
- InclusionComplete1
- InclusionComplete2

The Group "**Extension overrides**" table allows users to set custom extensions for any S2 Message encapsulation. Message type filters are as follows: "SinglecastAll", "SinglecastWithSPAN", "SinglecastWithMPAN", "SinglecastWithMPANGrp", "SinglecastWithMOS", and "MulticastAll". Extension types are as follows: "SPAN", "MPAN", "MPANGrp", "MOS", and "Test". Other parameters are as follows: "Is Encrypted", "Extension Length", "More to Follow", "Is Critical", and "Number of usages". Click a corresponding checkbox to activate the parameter override and specify a new value. If the parameter override is not active, the PC Controller uses a valid specific extension parameter value. For example, Extension Length will be calculated based on the Extension value unless a specific parameter value is activated.

Figure 9. Security Extension Overrides

The Checkbox "Cleanup existing extensions first" overrides existing extensions in selected message type when applying test extensions. When this checkbox is not set, test extension will be added to default extensions.

3.1.2 Content View

The Content View consists of command buttons and one Information item:

- Network Management
- Command Classes
- Encrypt/Decrypt
- ERTT
- Polling
- Transmit Settings
- Network Statistics
- Setup Route
- Topology Map
- Associations
- IMA Network
- Firmware Update (OTA)
- Firmware Update (OTW)
- Backup/Restore (NVM)
- Configuration Parameters
- Smart Start
- Set Controller Node Information (active when the controller is selected and active)
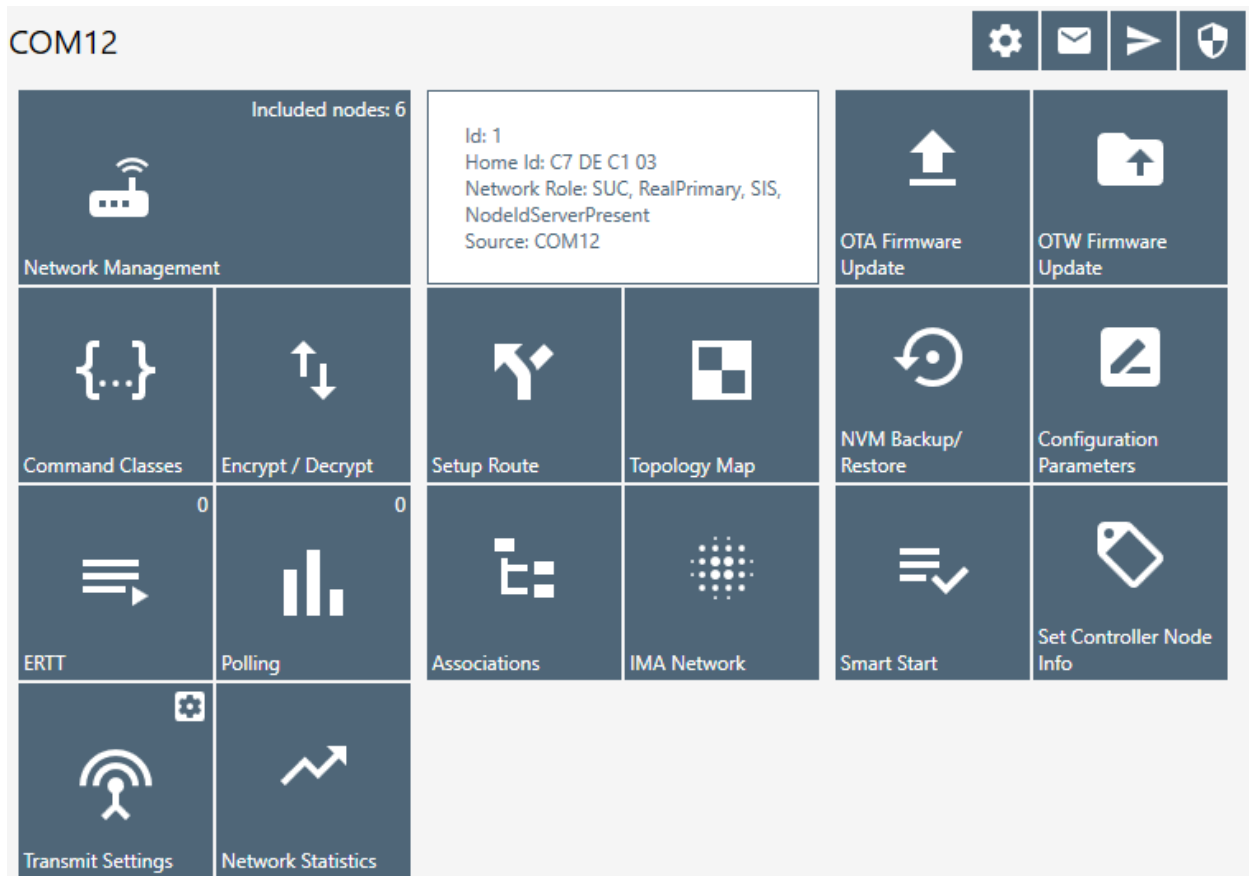
Figure 10. Content View
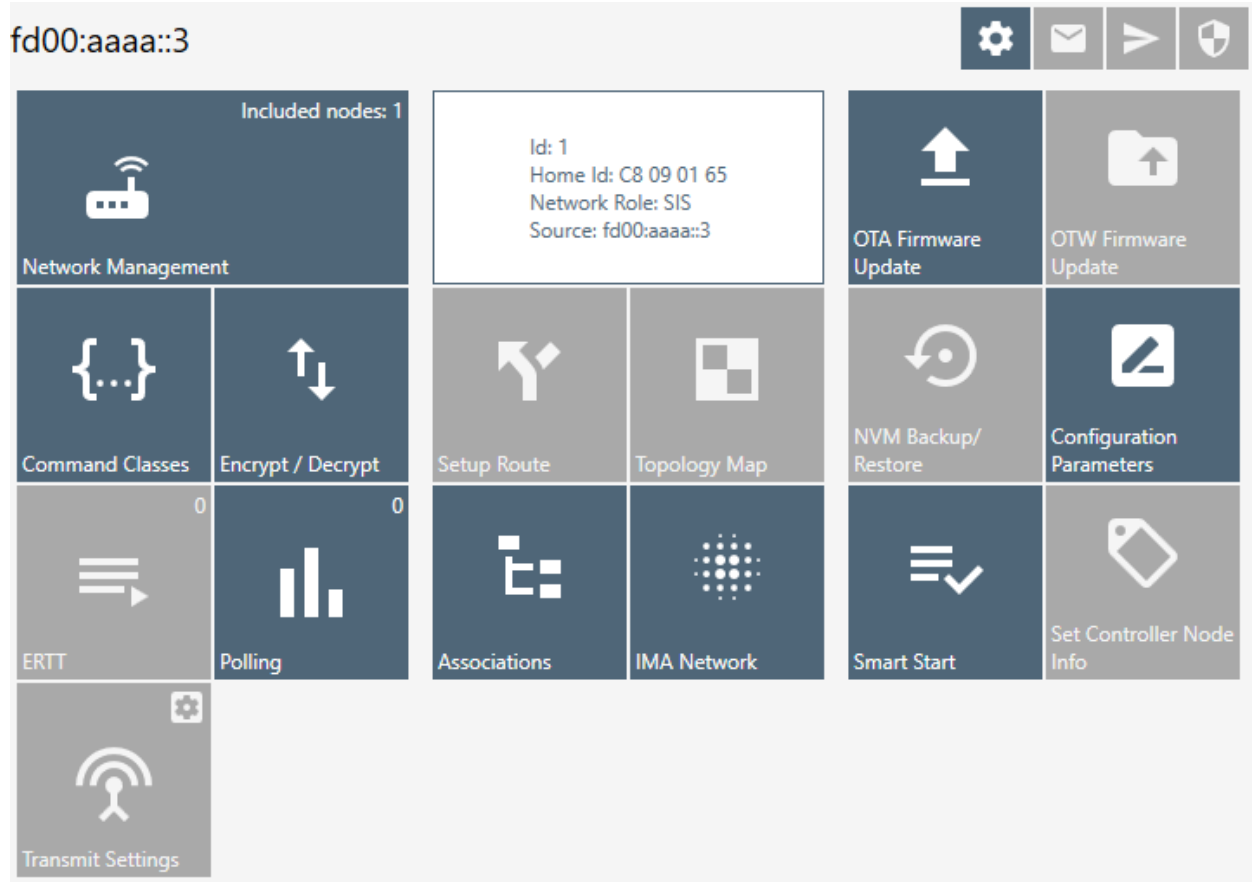
Figure 11. Content View with Z/IP Controller Connected

COM31

Included nodes: 20

Network Management

{ Id = 0, HomeId = DE CF D2 25, SourceName = COM31 }

OTA Firmware Update

OTW Firmware Update

Command Classes

Encrypt / Decrypt

Setup Route

Topology Map

NVM Backup/ Restore

Configuration Parameters

ERTT

Polling

Associations

IMA Network

Smart Start

Set Controller Node Info

Transmit Settings

Network Statistics
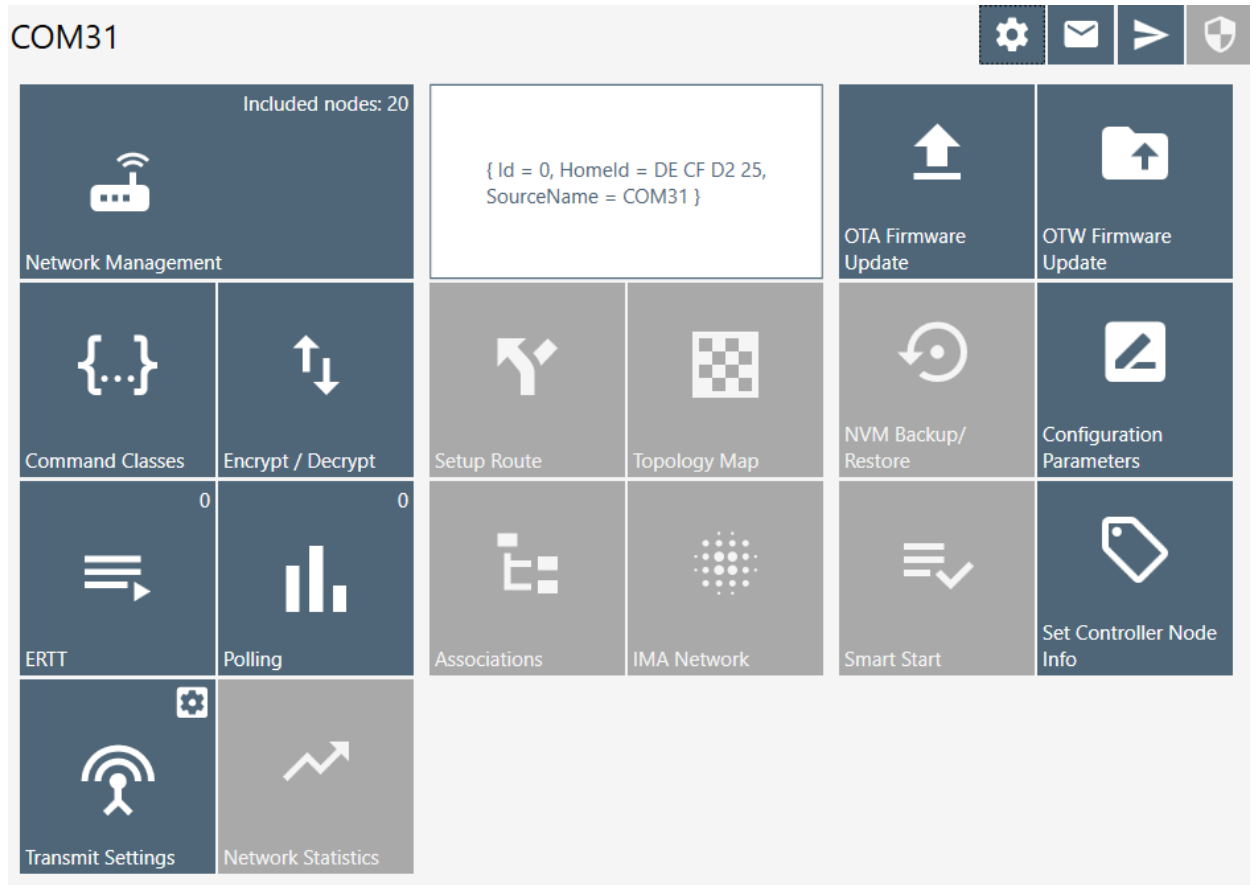
Figure 12. Content View with Serial API End Device Connected

3.1.3 Log Bar

The Log bar contains information about the last action and a **Show Log button**.

16:31:21.513 'Send Node Information' Completed
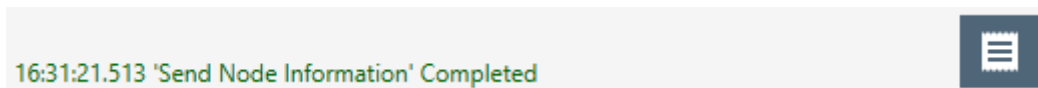
Figure 13. Log Bar View

Pressing the **Show Log button** opens a new window with brief information about the action and its time.

Clear		☑ Auto Scroll
Timestamp	**Message**	
16:34:33.326	'Reset Controller' Started	
16:34:36.207	Setup Security Manager Info	
16:34:36.571	**'Reset Controller' Completed**	
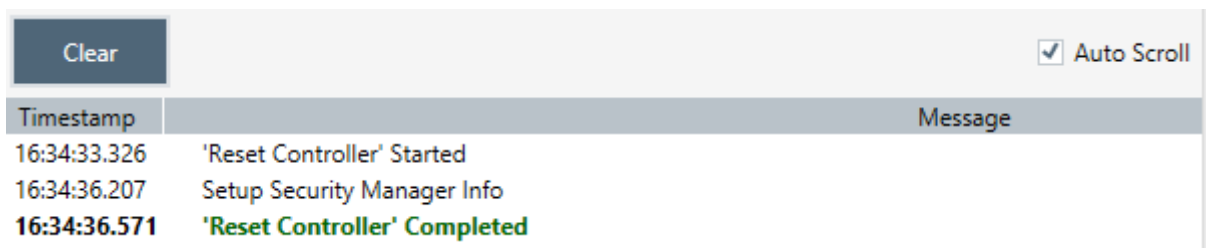
Figure 14. Log Window View

Table 5. Log View Items

Menu item	Description
Clear	Clears log items.
Auto Scroll	Enables auto scroll.

3.2   Network Management View

The **Network Management View** contains *Node List* and *Node information* for the selected node, *Nodes Actions,* and *Controller Actions*. It is used for operations with nodes and basic controller actions.

If checked, the 'Floating View' checkbox Network Management View will be shown in the other window.

Figure 15. Network Management View
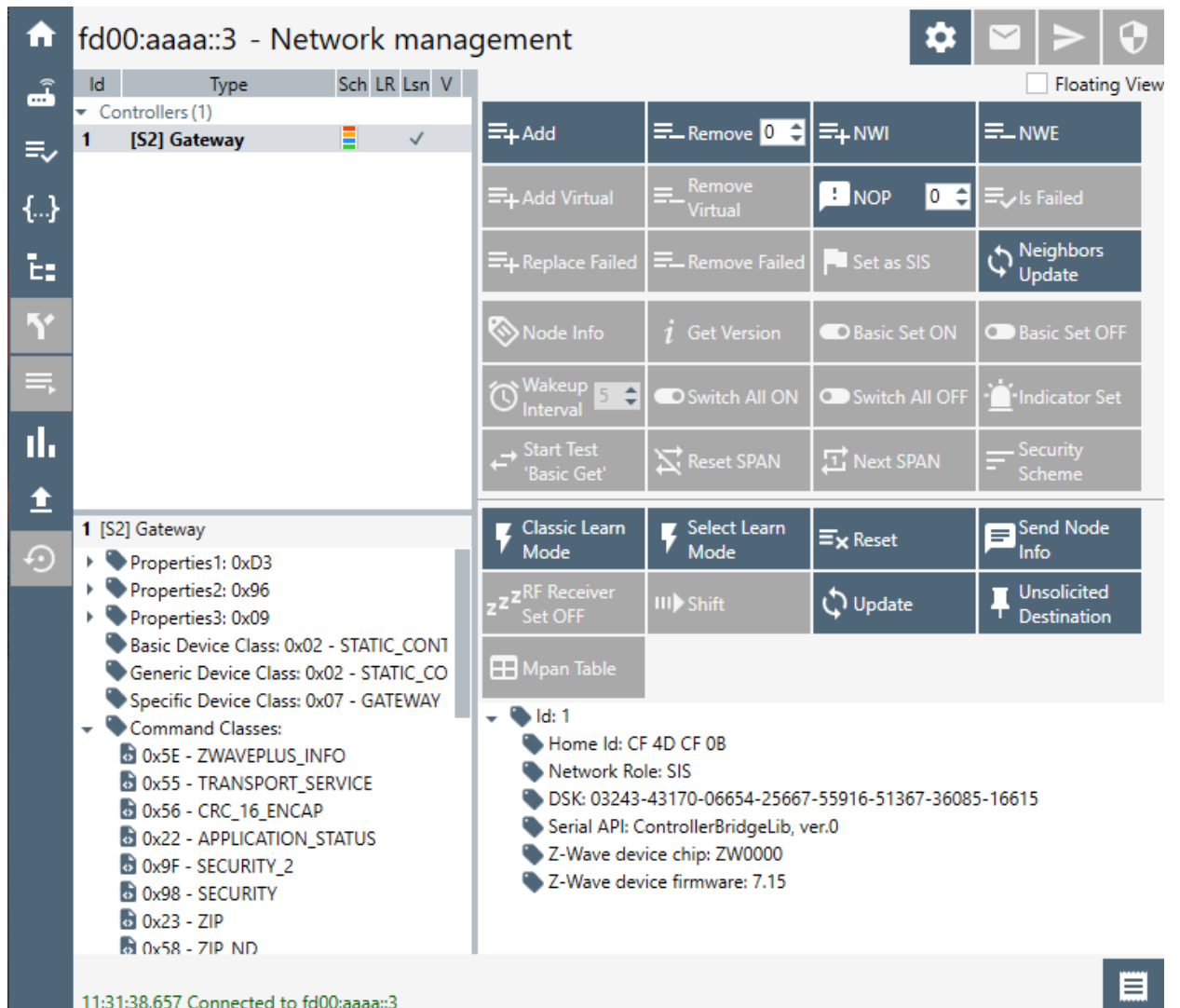
Figure 16. Network Management View with Z/IP Controller Connected

Figure 17. Network Management View with Serial API End Device Connected

3.2.1 Node List View

Figure 18. Nodes View

Used for view and selecting *Nodes*, contains next columns:
- ID – shows the node numbers of all nodes in the network
- Type – device type - shows description of the type of every node in the network

- Sch – security scheme granted
- LR – long range capability
- Lsn – checked if node is a listening node
- V – checked if node is a virtual node

The currently connected device highlights with bold font.

For Serial API End Node impossible to get the node list from the connected device so it always shows 20 included nodes. Adds one item if a current ID is greater than 20. ID = 0 in default state or after reset.

The button on the bottom line is to return to the 'Network Management View' from other views.

3.2.2   Node Information View
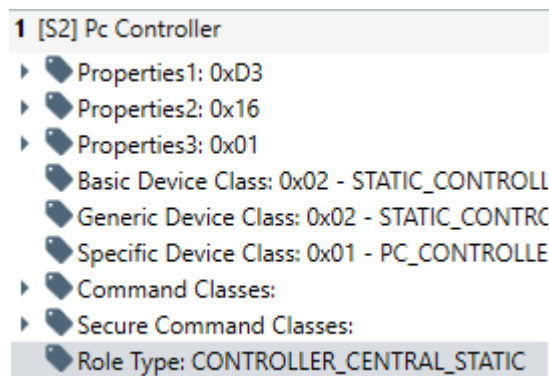
Figure 19. Node Information View

The *Node Info* section gives structured information about the selected node. For more information, see the Z-Wave Device Class Specification documentation.

Navigate to the 'Command Classes View' by double clicking on an item from Command Classes or Securely S0/S2 Supported Command Classes lists.

3.2.3 Nodes Actions View

Figure 20. Nodes Actions View

Figure 21. Nodes Actions View when Z/IP Controller Connected
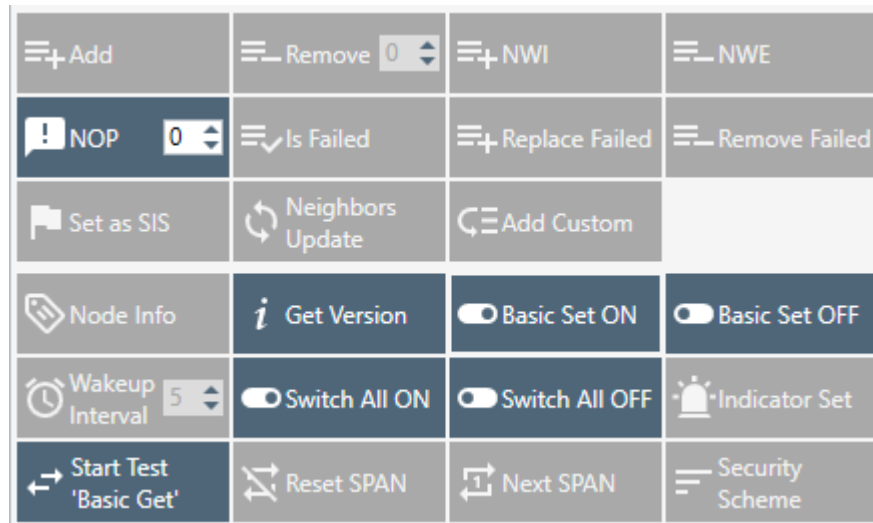
Figure 22. Nodes Actions View when Serial API End Device Connected

This view contains all available actions for a selected node. An action button is greyed out if the current action is not available for a selected node.

Additional buttons for the Bridge Controller:

Figure 23. Bridge Controller Additional Actions

Table 6. Node Actions View Items

Menu item	Description
Add	Start inclusion mode with default settings.
Remove	Removes a node.
NWI (Network Wide Inclusion)	Network Wide Inclusion includes all nodes into network once they have been reset and given power.
NWE (Network Wide Exclusion)	Network Wide Exclusion excludes all nodes from network once they have been reset and given power.
Add Virtual	Adds a virtual node for the Bridge Controller.
Remove Virtual	Remove a selected virtual node added by/from connected Bridge Controller.
NOP (Send NOP)	'No Operation' to send a frame not carrying any functional info to a node.
Is Failed	Sends a Failure signal to a node.
Replace failed	Replaces a failed node.
Remove Failed	Removes a failed node.
Set SIS	Sets the "Set SIS" command to the selected Controller.
Neighbor Update (Request Node Neighbor Update)	Gets the neighbors from the specified node.
Add Custom	Add node using custom settings.
Node Info	Requests Node information from a node.
Version Get	Sends Version Get command to the selected node.
Basic Set On	Sends the BASIC SET ON command to Switch a selected node(s) ON.
Basic Set Off	Sends the BASIC SET OFF command to Switch a selected node(s) OFF.

Wake Up Interval	Sets up the Wake-Up Interval for a non-listening node.
Switch All On	Switches all nodes in the network ON.
Switch All Off	Switches all nodes in the network OFF.
Start Basic Test/ Stop Basic Test	Starts and stops the basic test functionality to the selected item.
Node Settings	Opens a pop-up with following actions for selected node 'Reset SPAN', 'Next SPAN', 'Security Scheme'.
Reset SPAN	Clears SPAN table for selected node.
Next SPAN	Rolls SPAN record one time on each click for selected node.
Security Scheme	Sets active security scheme for selected node.

Add Node Custom dialog:
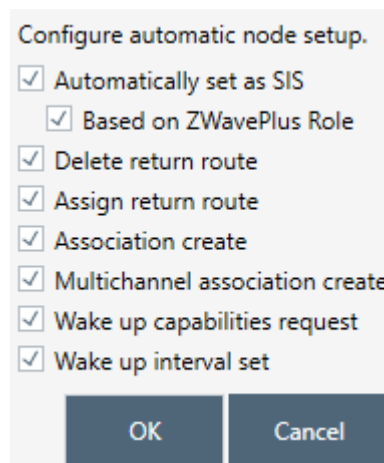
Figure 24. Add Custom

3.2.4   Controller View

The *Controller view* includes *Network Role Option, Controller Actions,* and *Controller Information* sections. This view is used for operations with controllers.
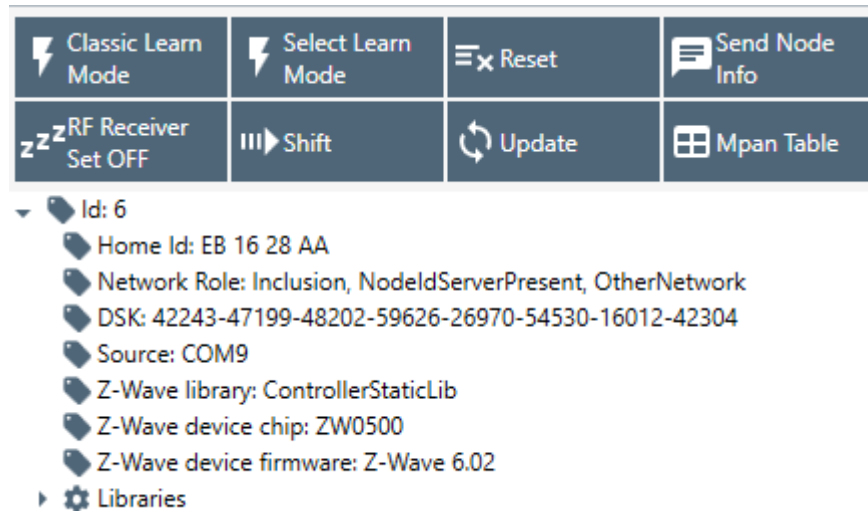
Figure 25. Controller View
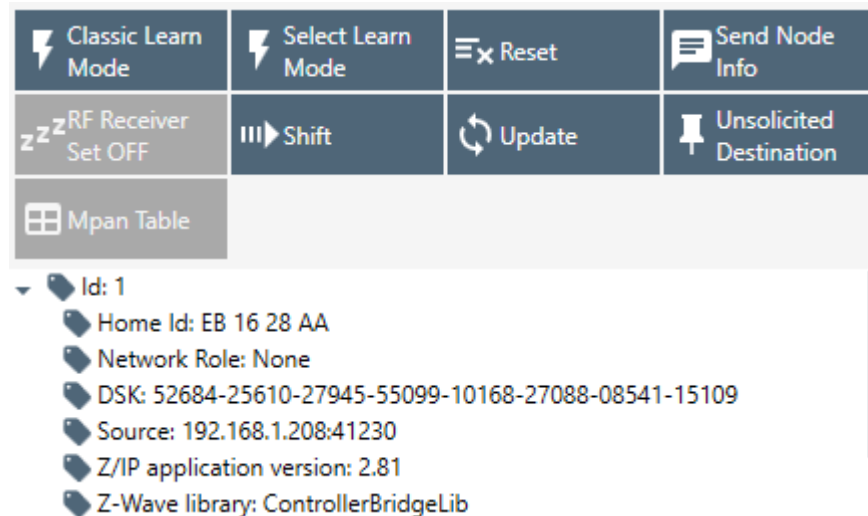
Figure 26. Z/IP Controller View

Id: 4
Home Id: CB AE 51 FD
DSK: 15310-57545-53326-29151-57411-38745-07580-51176
Serial API: EndDeviceLib, ver.9
Z-Wave device chip: ZW0800
Z-Wave device firmware: Z-Wave 7.18
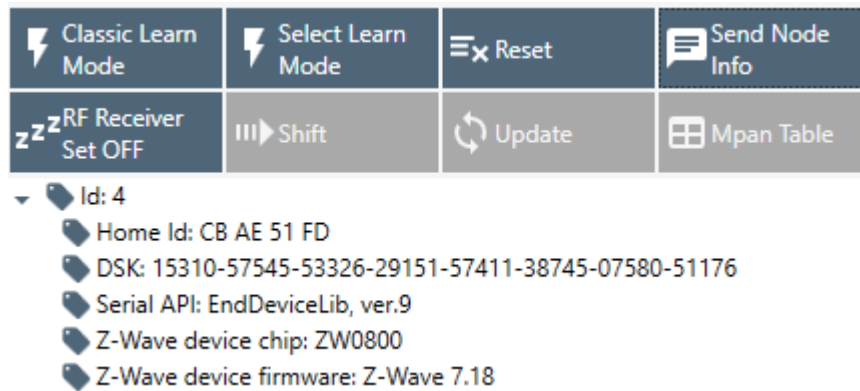
Figure 27. Serial API End Device Controller View

Select the Controller learn modes dialog:
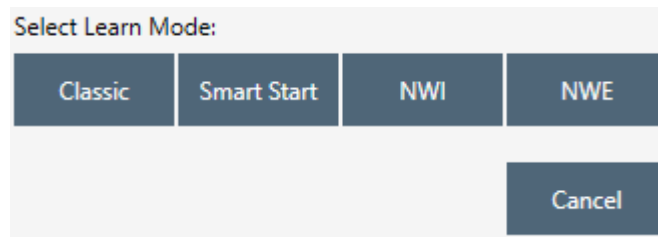
Figure 28. Select Learn Mode

Additional button for the Bridge Controller:
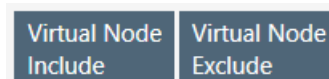
Figure 29. Bridge Controller Additional Action

Table 7. Select Learn Mode View Items

Menu item	Description
Classic	Activates Learn mode with Classic mode option
Smart Start	Activate Smart Start Learn mode for joining device or exclusion of included Smart Start LR device for connected Serial API End Device Libraries
NWI	Activate Network Wide Inclusion mode
NEW	Activate Network Wide Exclusion mode
Virtual Node Include	Add virtual node in learning mode, only Bridge Library
Virtual Node Exclude	Remove selected virtual node in learning mode, only Bridge Library

The Controller view has the following actions:

Table 8. Controller Actions View Items

Menu item	Description
Learn Mode (Start Learn Mode)	Starts classic learn mode for the controller if it is needed to include it in another controller's network.
Select Learn Mode	Opens Select learn mode dialog.
Reset	Resets a controller.
Send Node Info	Broadcasts node info from controller.
RF Receiver Set OFF	Disables radio transmission on connected device. Auto enables when send operation is initiated.
Set Node Info	Changes node information for controller.
Shift	Shifts the primary role to another controller in the network.
Update (Request Update)	An Inclusion controller can request network updates from a SIS.
MPAN Table	Modifies an existing MPAN table in PC Controller.
Unsolicited Destination	Gets and sets unsolicited destination for Z/IP Gateway.

The *Network Role Option* section has controls to assign the role of the SC in the network:

- SIS – Static Update Controller with ID server
- None

General information regarding the SC is displayed in the *Controller Information* section in the following items:

Table 9. General Information View Items

Section	Description
Controller ID	Displays the node ID of the PC-based SC.
Controller Home ID	Displays the current Home ID of the PC-based SC.
Controller Network Role	Displays the PC-based SC network role.
Serial Port	Displays the serial port in use.
Source	Displays connection address (for Z/IP Controller).
DSK	Displays DSK of current controller.
Z/IP application version	Displays current firmware version of Z/IP Gateway application.

MPAN Table View

Call from the Controller View by clicking on "MPAN Table" button opens a new window "MPAN Table configurations". Group ID, Owner ID, MOS state, MPAN, Node IDs list will be listed for each record in the table after pressing "Load MPANs" button.

Figure 30. MPAN Table Configurations View

Table 10. MPAN View Items

Buttons	Description
Load MPANs	Retrieves current state of MPAN table of PC Controller.
Clear	Deletes all entries in MPAN table.
Add/Update	Create new or updates data in MPAN table for entered Group id and Owner ID. If data wasn't present in the table, a new record will be created.
Remove	Removes the selected item from MPAN table.
Next MPAN	Calculates next MPAN for selected item in table.

Unsolicited destination

Call from the Controller View by clicking on 'Unsolicited Destination' button opens a new window 'Z/IP Unsolicited Destination'. Pressing the "Start/Stop" button will update the unsolicited destination address on the Z/IP Gateway and restart an unsolicited listener in the PC Controller for a selected port.
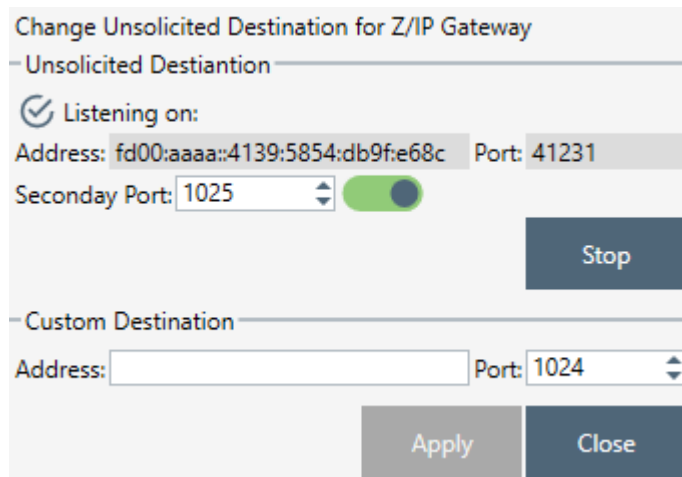
Figure 31. Unsolicited Destination View

Table 11. Unsolicited View Items

Button	Description
Start/Stop	Set current unsolicited destination state.
Secondary enable Toggle	Display and change secondary port state.
Apply	Set custom settings and sends unsolicited destination set command to Z/IP Gateway.
Close	Closes the window.

Button "Apply" triggers the "Unsolicited address" view from text input to drop down list selector with list of all IP Addresses of the current machine.

3.3 Associations View

The **Associations** view has a *Nodes List View, Node Information View,* and *Association Actions View*. It is used to set up associations between nodes.
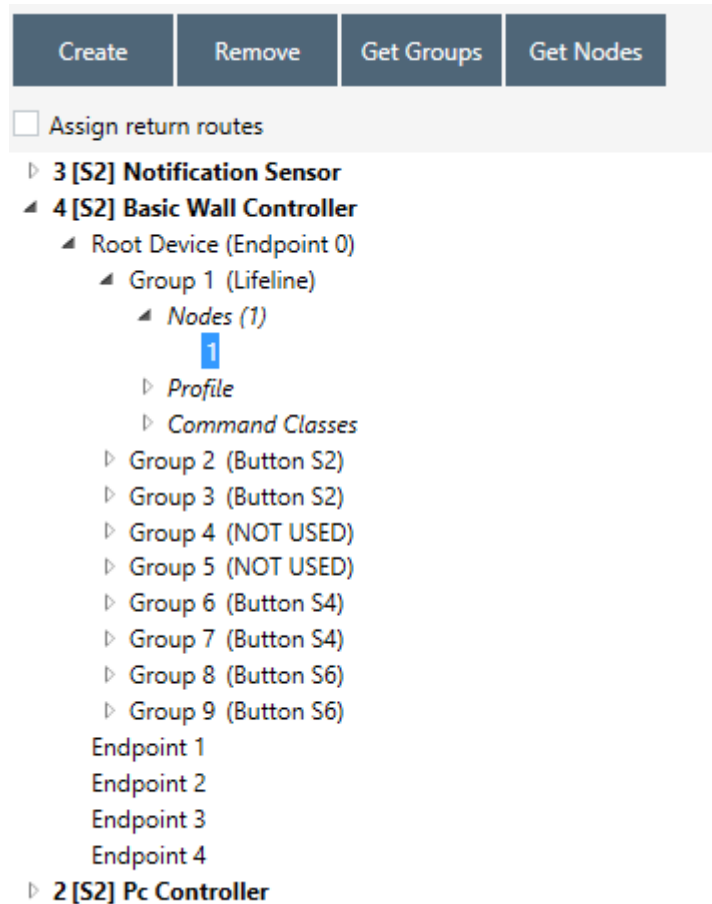
Figure 32. Associations View

Table 12. Association View Items

Menu item	Description
Create	Creates an association between selected nodes.
Remove	Removes a selected association.
Get Groups Info	Returns groups for selected nodes in the association's tree view with information about group's Profile and group's supported command classes.
Get Nodes	Return nodes for a selected group in the association's tree view.

The Associations View shows a tree of available source nodes that support the Association command class, e.g., Binary sensor.

The Groups node shows the association groups that can be or have been created, information based on Association Group Info command class, and profile and supported command classes for each group.

The "Assign Return Routes" checkbox is to define whether the Controller should assign return routes together with setting the association.

3.4   Command Class View

The **Command Class view** uses to send a specified command class to a selected node with parameters.

The view of Command Classes can be displayed in a separate window when the Floating View is checked.

Figure 33. Command Classes View

Command Classes View consists of the following items:

1) Nodes and Node Info views (on the left)

2) Group of checkboxes for wrapping selected command with another (on the top)

3) Command selection view (in the middle, includes command class selection and send data text box) and buttons to open 'Predefined commands' and 'Recent commands' views

4) Send Data section: Send Data field – current payload and Drop-down list of expected commands (if enabled)

5) Sending mode radio buttons and control buttons (on the bottom)

6) Security commands references (disabled for Serial API End Devices)

Table 13. Send Data View Items

Item	Description
CRC16	Wraps the selected command with a CRC16 command.
Suppress Multicast Follow up	Disables follow up Singlecast frames after a multicast frame.
Force Multicast	Uses multicast even if only one frame is selected.
Supervision Get	Wraps the selected command with a Supervision command.
Session ID	Session ID will be present in the Supervision encapsulated command. Can be set manually or auto incremented by enabling the 'Auto increment' checkbox (set by default).
Multi-Channel	Enables multi-channel wrapping.
End Point (SRC)	Sets the Source End Point when a wrapping multi-channel is enabled.
End Point (DST)	Sets the Destination End Point when a wrapping multi-channel is enabled.
Bit Address	Sets the Bit Address flag for a Multi-Channel Command.
Command class	Shows the selected command class.
Command	Selects a command from the selected Command Class and shows selected command from the 'Select Command View'.
Select	Open the 'Select command' view (Figure 34) to choose a command.
Predefined Commands	Open the 'Predefined commands' view to manage sets of send data
Recent	Open the 'Recent Commands' view with a list of recently sent commands.
Send data	List of recently sent commands. A click on item automatically inserts data in Send Data control.
Expect command	Shows a list of commands that is filtered by currently selected Command Class control. PC Controller will wait for a node to respond with selected command. Timeout for this expect defined in 'Send Data Settings' view. When enabled 'Send'

	button changes its label to 'Request'.
Default	Radio button to set security mode to default (Secure for securely included nodes, non-secure for normally included nodes).
Secure	Radio button to enable force secure command sending.
Non-secure	Radio button to enable force non-secure command sending.
Broadcast	Radio button to enable force broadcast sending.
Serial API	Radio button to send bytes directly to Serial API of connected controller device.
Reload XML	Reloads XML from the local machine if changes were made in it.
Send/Request	Button to send a command or request if enabled 'Expect command' to a selected node.
Node Info	Gets the node information from a selected node.
Reset SPAN	Clears the SPAN table for a selected node.
Next SPAN	Rolls the SPAN record one time on each click for a selected node.
Security Scheme	Sets the active security scheme for a selected node.
MPAN Table	Opens the MPAN settings dialog.

The **Select Command view** used to show and select all available commands with information about a selected node. This consist of the following:

- List of Command classes and commands (on the left)

- Information about a selected command (on the right)
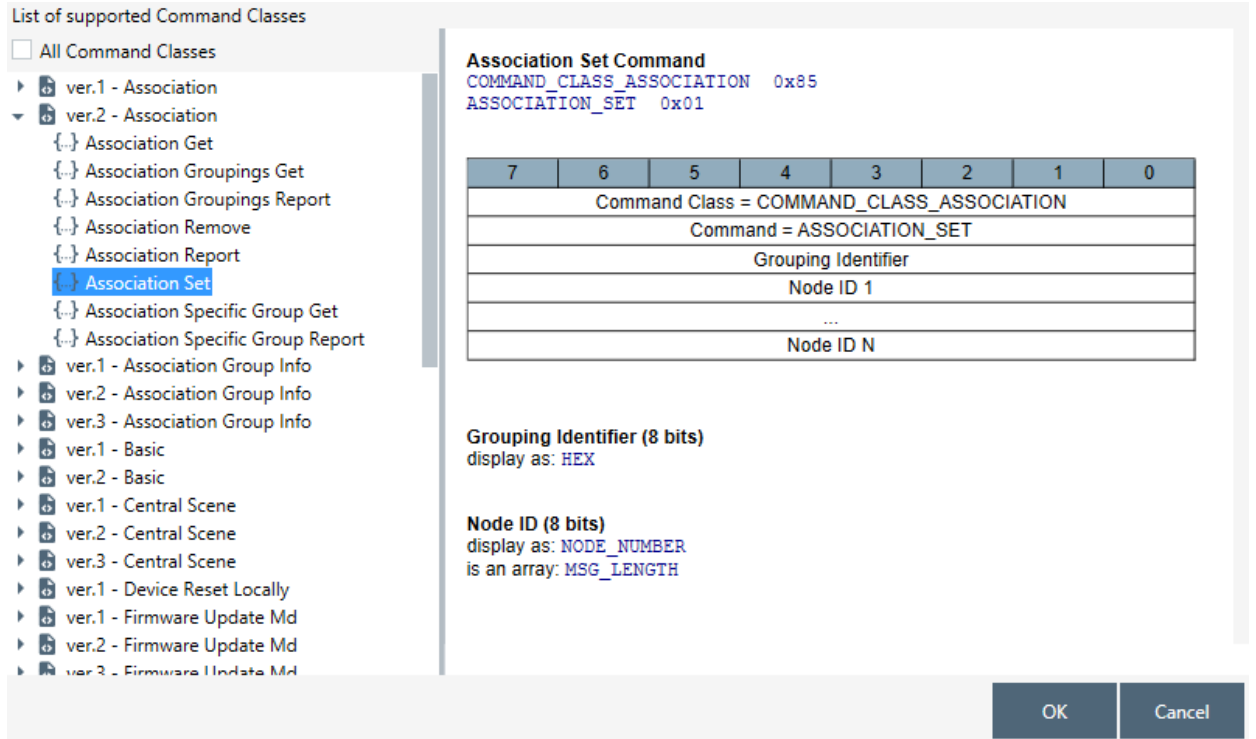
Figure 34. Select Command View

Table 14. Select Command View Items

Item	Description
All Command Classes	Allows choosing all command classes and not only supported by device.
Ok	Confirms a selection.
Cancel	Closes a window without selection.

The **Predefined Commands Manager** is an additional tool view to create, edit and send sets of predefined commands. A double-click on an item automatically inserts data into Send Data control and fills the selected command the Command Classes view. At the bottom of the view is an info box - displays parsed data of a selected item.

Figure 35. Predefined Commands Manager

Table 15.Predefined Commands View Items

Item	Description
New	Add a new group with name from the "Name" field
Open	Import a new group from XML file.
Copy Group	Make a copy of selected group with items
Rename	Change name of selected group
Save	Exports selected group to new file.
Name	Selected group name, editable field
Groups	Container of available groups
Navigation buttons group	Up – move selected item above in the selected list Down – move selected item bellow in the selected list Copy – make a copy of selected item Delete – remove selected item from the list Add – add an added item to predefined list from the Command Classes View
Send List	Consistently send items from the select group of predefined commands.
Info box	Displays parsed data of selected item

The **Recent Commands** contains list of last sent commands. A double-click on an item automatically inserts data into Send Data control and fills the selected command the Command Classes view. At the bottom of the view is an info box - displays parsed data of a selected item.

Time	Name	Ver	Data	CRC	MF
13:42:10	Version Z-Wave Software Get	3	86 17		
13:42:07	Version Capabilities Get	3	86 15		
13:42:03	Version Command Class Get	3	86 13 86		
13:41:50	Version Get	3	86 11		
13:41:43	Z-Wave Plus Info Get	2	5E 01		
13:41:34	Z-Wave Plus Info Report	2	5E 02 02 00 00 00 04 00 02		

Command Details:

Z-Wave Plus Info Report
   Z-Wave+ Version: 0x02
   Role Type: ROLE_TYPE_CONTROLLER_CENTRAL_STATIC=0x00
   Node Type: NODE_TYPE_ZWAVEPLUS_NODE=0x00
   Installer Icon Type: 00 04
   User Icon Type: 00 02

Figure 36. Recent Commands View

3.5   Setup Route View

Setup Route View allows assigning or deleting routes between nodes.

○ Return Route	○ Priority Return Route	● Get/Set Priority Route	Priority Route:	00 00 00 00
○ SUC Retrun Route	○ Priority SUC Return Route		Route Speed:	100 KBit/s ▼

Id	Type		Id	Type	
1	[S2] Pc Controller		1	[S2] Pc Controller	
3	[S2] Notification Sensor		3	[S2] Notification Sensor	
4	[S2] Basic Wall Controller		4	[S2] Basic Wall Controller	
2	[S2] Pc Controller		2	[S2] Pc Controller	

Get Priority Route   Set Priority Route   Assign   Delete

Figure 37. Setup Route View

Setups in the top of the view are change modes for assigning a route.

Source Node list(left) and *Destination Node list(right)* show lists of source and destination nodes in a routed network, respectively.

Table 16. Setup Route View Items

Item	Description
Return Route	Enables 'Return Route' mode.
Priority Return Route	Enables 'Priority Return Route' mode.
SUC Return Route	Enables 'SUC Return Route' mode.
Priority SUC Return Route	Enables 'Priority SUC Return Route' mode.
Get/Set Priority Route	Enables 'Get/Set Priority Route' mode.
Priority Route	Repeaters array from route.
Route Speed	Selects Route Speed.
Get Priority Route	Gets a priority route for selected node.
Set Priority Route	Sets a priority route for selected node.
Assign	Assigns routes via selected nodes.
Delete	Deletes assigned routes for selected node.

3.6 ERTT View

ERTT (Enhanced Reliability Test Tool) View allows configuring the test scenario and shows status of the test running.

Figure 38. **ERTT View**

ERTT View itself consists of following items:

1) Nodes and Node Info views (on the left)

2) ERTT configuration view (in the middle)

Table 17. ERTT View Items

Item	Description
Test Iterations	Repeats the test selected number of times.

Run forever	Repeats the test infinite times with 100ms delay between requests.
Low power	Send frames with low power when selected.
Test Mode	Sends basic set with a selected value by radio buttons.
TX Controlled by Module	Enable TX mode to start test from device, only for supported devices.
Stop on Error	Stops the test if error occurs.
Start/Stop	Starts or stops running test.
Retransmission	When checked, enables frame retransmission. Only if supported TX Controlled by module.

3.7　Polling View

Polling View allows enabling polling for all available nodes in the network.

Figure 39. **Polling View**

Table 18. Polling View Items

Item	Description
Start button	Runs the Polling for all nodes in the list.

Stop button	Stops the process.
Edit buttons	On list items allows setting **Poll Time, sec.** and **Report Time, sec** parameters for polling.
Done button	Used to finish editing parameters and exit Edit mode.

3.8   Topology Map View

This view shows a graphical representation of the node network and access between.

Figure 40. Topology Map

The Topology Map view consists of:

- The Graphical topology scheme itself
- Node Type Colors section

Table 19. Topology Map View Items

Item	Description
Graphical topology scheme	Graphically represents the network scheme, showing the nodes of all types differentiated through colorization, and the link statuses between the Installer controller and end device nodes.
Reload Topology	Reloads the topology.

Node Type Colors

Node Type Colors is a list of node types with colors assigned for graphical representation on the Topology Scheme. It is possible to select a special color for each node type.

3.9 IMA Network View

The **IMA Network** view has a *Network Actions View Nodes, Nodes View, IMA Details View, and Network Layout Properties View*. Installation and Maintenance Application (IMA) is designed to perform analysis of network health.
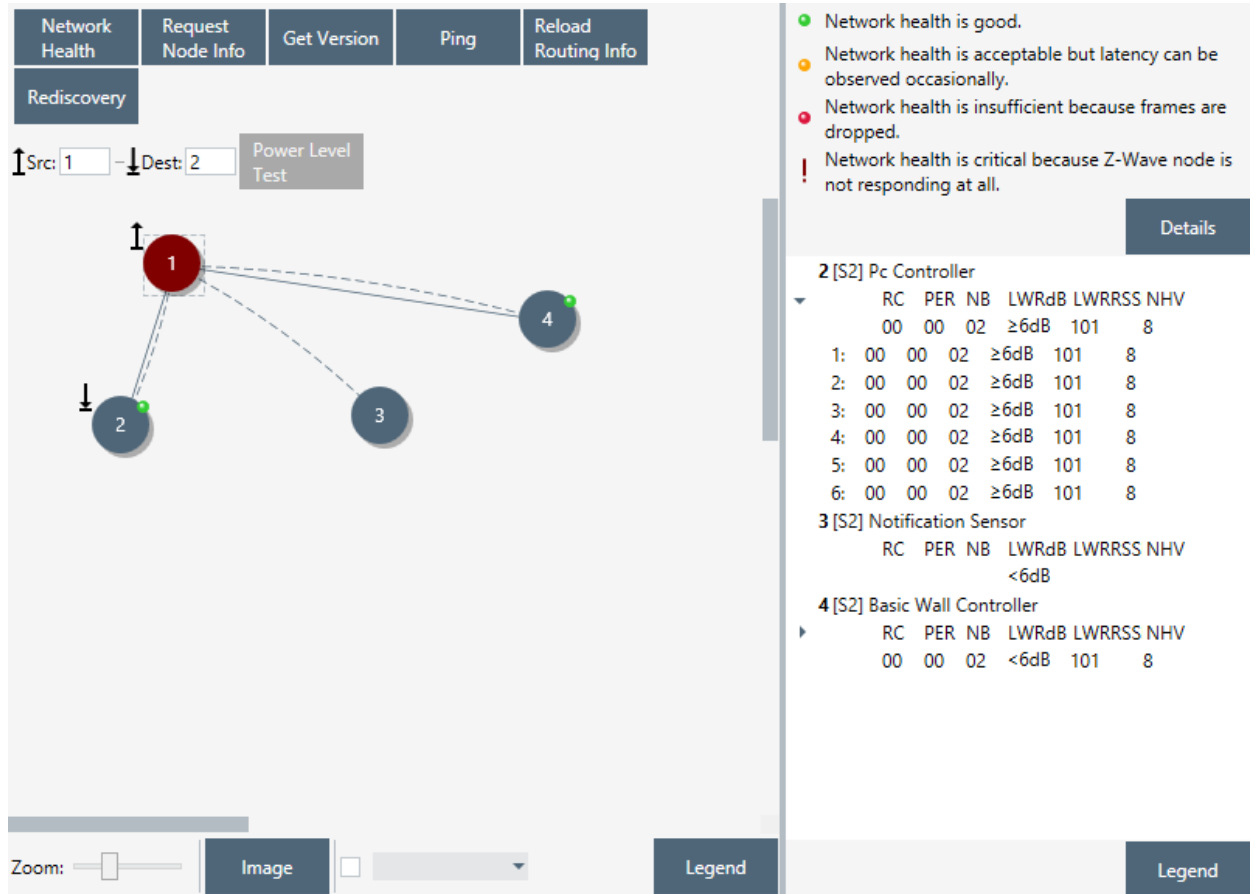
Figure 41. IMA Network View

Table 20. IMA Network View Items

Menu item	Description
Network Health	Performs an algorithm for gathering measurements to calculate the Network Health Value. These measurements are RC, PER, NB, LWRdB, and LWRRSSI.
Request Node Info	Sends the Node information get command.
Get Version	Sends the Version get command.
Ping Node(s)	Sends the NOP command and waits for Ack from the node.
Reload Routing Info	Executes the Get routing information command and rebuilds the neighbors list.
Rediscovery	Sends "Get Nodes In Range" command.
Src / Dest	Specifies the source and destination node for commands with source and destination arguments.
Power Level Test	Performs a power level test (only for selected nodes Src and Dest).

The *Nodes View* shows the nodes in the network and controller. It also shows the neighbor's connections of selected node and, after the Network health completed, the connections between nodes. Each node can be moved on canvas. Multiple nodes can be selected.

To move the canvas use ALT + drag.

To zoom in/out the canvas use CTRL + scroll.

The *IMA Details View* contains detailed information about each step of the Network Health algorithm. Empty entries show that this measurement cannot be calculated for a selected node.

Table 21. IMA Details View Items

Menu item	Description
Details	Shows the list of recommended actions according to the Network Health status. See Figure 42.
Legend	Opens a popup window with information about the measurements. See Figure 43.

Figure 42. IMA Network Health Status Description (Details)

RC	Route Change
	Number of times the protocol needed additional routes

PER	Packet Error Rate
	Number of failed transmitions

NB	Neighbors count
	Number of repeater neighbors

LWRdB	Last Working Route Powerlevel
	The maximum reduction in transmit power where the LWR still works

LWR_RSSI	Estimation of the signal-to-noise ratio
	The difference between LWR RSSI and background RSSI

NHV: Network Health Value

- 10: PER = 0 AND RC = 0 AND NB > 2 AND LWRdB ≥ 6dB AND LWR_RSSI ≥ 6dB 17dB
  - 9: PER = 0 AND RC = 1 AND NB > 2 AND LWRdB ≥ 6dB AND LWR_RSSI ≥ 6dB 17dB
  - 8: PER = 0 AND RC ≤ 1 AND NB ≤ 2 AND LWRdB ≥ 6dB AND LWR_RSSI ≥ 6dB 17dB

- 7: PER = 0 AND RC ≤ 1 AND NB > 2 AND (LWRdB < 6dB OR LWR_RSSI < 17dB)
  - 6: PER = 0 AND RC ≤ 1 AND NB ≤ 2 AND (LWRdB < 6dB OR LWR_RSSI < 17dB)
  - 5: PER = 0 AND 1 < RC ≤ 4
  - 4: PER = 0 AND RC > 4

- 3: PER = 1
  - 2: PER = 2
  - 1: 2 < PER < 10

! 0: PER = 10

- Network health is good.
- Network health is acceptable but latency can be observed occasionally.
- Network health is insufficient because frames are dropped.
! Network health is critical because Z-Wave node is not responding at all.

[Details]

2 [S2] Pc Controller

	RC	PER	NB	LWRdB	LWRRSS	NHV
	00	00	02	≥6dB	101	8
1:	00	00	02	≥6dB	101	8
2:	00	00	02	≥6dB	101	8
3:	00	00	02	≥6dB	101	8
4:	00	00	02	≥6dB	101	8
5:	00	00	02	≥6dB	101	8
6:	00	00	02	≥6dB	101	8

3 [S2] Notification Sensor

RC	PER	NB	LWRdB	LWRRSS	NHV
00	00	02	≥6dB	101	8

4 [S2] Basic Wall Controller

RC	PER	NB	LWRdB	LWRRSS	NHV
00	00	02	<6dB	101	8

[Legend] [Legend]

Figure 43. IMA Network Health Value Description (Legend)

The *Network Layout Properties View* allows changing the view of the Nodes, its scale, and background.
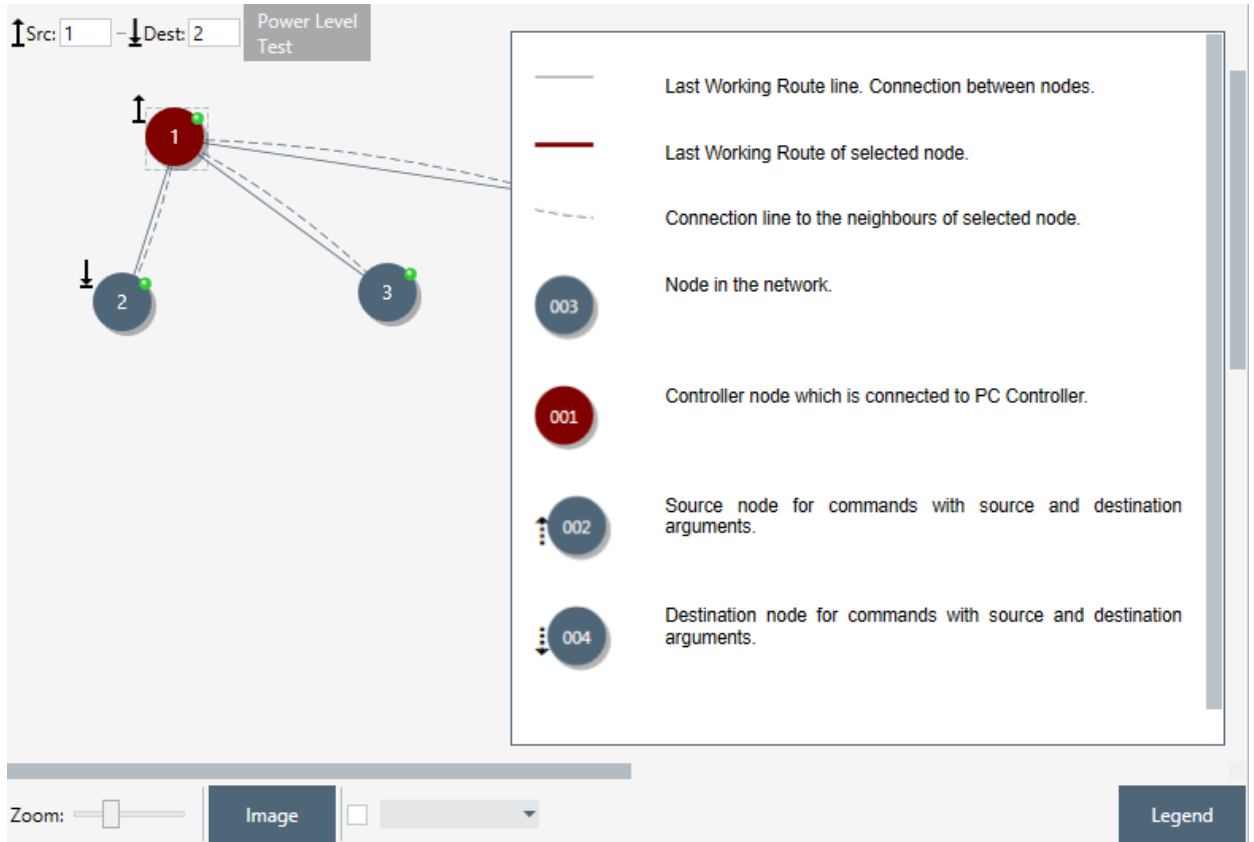
Figure 44. IMA Nodes View Description (Legend)

Table 22. IMA Nodes View Items

Menu item	Description
Zoom	Changes the scale of the canvas.
Image	Opens a dialog window to choose the picture background for the canvas.
Fill	A color of filling can be chosen when the checkbox is activated.
Legend	Opens a popup window with information about the elements shown on *Nodes View*. See Figure 44.

3.10 Encrypt/Decrypt View

Encrypt/Decrypt Message View allows to either Encrypt or Decrypt message.

S0 Tab to use Security S0 encrypt algorithms

Figure 45. Encrypt/Decrypt View S0 Tab

Table 23. Encrypt/Decrypt S0 View Items

Item	Description
Use Current	Inserts the current network key to a field from the security scheme.
Decrypt	Decrypts the message set in the **Encrypted message** with parameters from input fields.
Encrypt	Encrypts the message set in the **Decrypted message** with parameters from input fields.

S2 Tab to use Security S2 encrypt algorithms

Figure 46. Encrypt/Decrypt View S2 Tab

Table 24. Encrypt/Decrypt S2 View Items

Item	Description
Decrypt	Decrypts the message set in the **Encrypted message** with parameters from input fields.
Encrypt	Encrypts the message set in the **Decrypted message** with parameters from input fields.

3.11 Firmware Update (OTA) View

Firmware Update (Over the Air) View provides functionality to update devices over the air.

Figure 47. **Firmware Update (OTA) View**

Firmware Update View consists of the following items:

- Nodes and Node Info views (on the left)
- Firmware configuration view (in the middle)

Table 25. Firmware Update OTA View Items

Item	Description
Get	Gets the information about the current firmware of a selected node.
File selection	Allows selecting a file with *.hex or any other extension.
Stop transmitting bulk reports on missing acknowledge	Discard transmitting reports in case of multiple reports requested by a destination node if not received acknowledge from it and wait for the next request.
Limit number of reports	Amount or reports in case of used multiple report
Discard last reports count	Stop transmitting bulk reports on missing acknowledge receive in case of multiple reports requested
Update	Starts the update process on a selected node.
Activate	Sends Firmware Update Activation Set command to start the delayed activation process. Button available only for Firmware Update MD Command Class Version 4.
Download	Get firmware from the device

3.12   Firmware Update (OTW) View

Firmware Update (Over the Wire) View provides functionality to update devices that are connected to the PC. It opens a file dialog window to choose the update file.
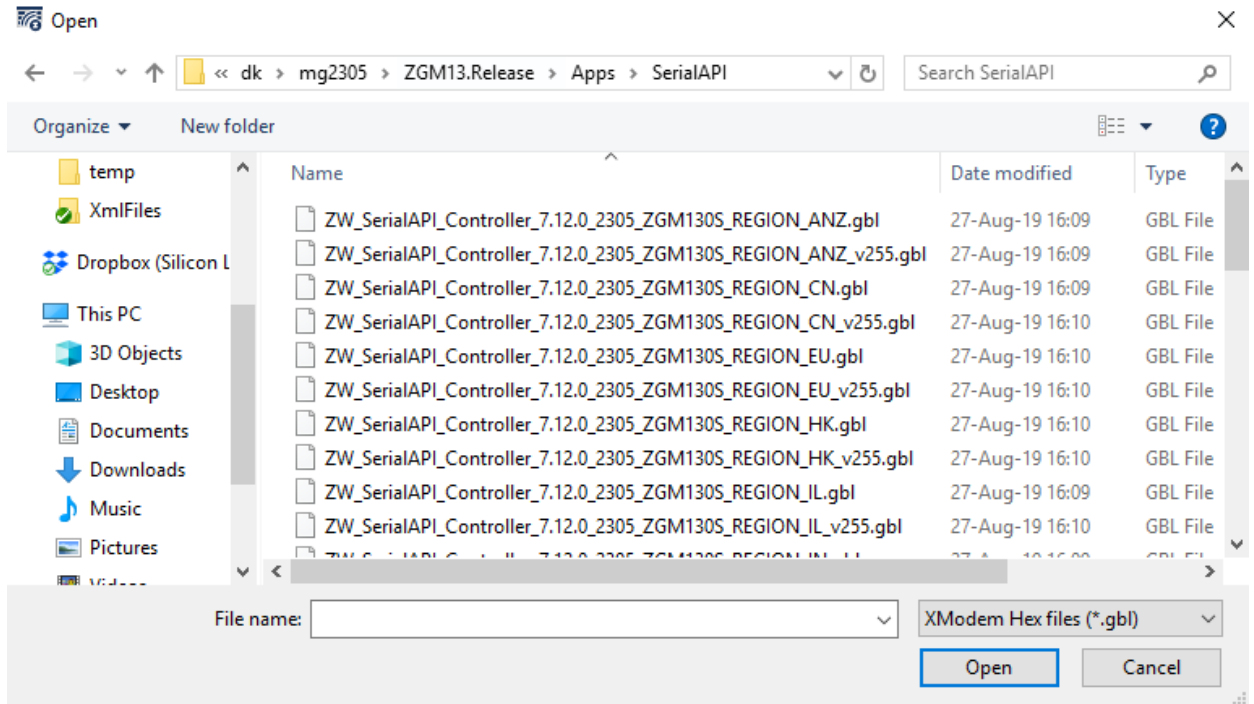
Figure 48. File Dialog View

3.13   Backup/Restore NVM

NVM (Non-volatile Memory) Backup/Restore View provides functionality to save and upload non-volatile memory content of the device.
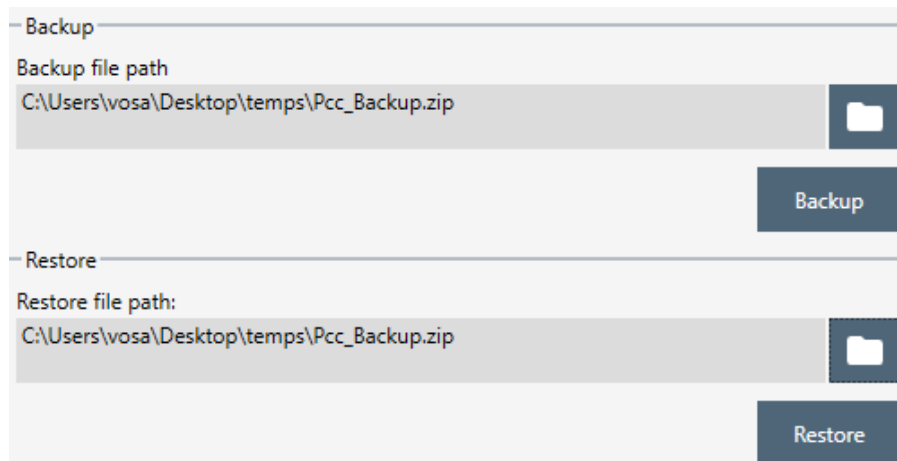
Figure 49. NVM Backup/Restore View

Item	Description
… (Save As)	Selects a destination file to save data.
Backup	Starts backup to file.
… (Open)	Selects a source file of NVM.
Restore	Starts a restore file to device.

3.14 Configuration Parameters

Configuration Parameters View to manage node settings using the Configuration Command Class for selected Node from the list in case of supported command class.

Figure 50. Configuration Parameters View

Table 27. Configuration Parameters View Items

Item	Description
Get List	Gets list of configuration parameters for a selected controller.
Set	Sets configuration parameters.

3.15 Smart Start View

Smart Start View contains a provisioning list of DSKs provided by the PC Controller and enables managing it**.**

Provisioning List:

257	DSK: 28132-34146-31801-22818-18299-16229-01407-4196
258	DSK: 32294-00016-25479-56384-38447-09260-15601-4293
256	DSK: 41256-64296-09957-41572-11835-20871-11564-3488

Refresh List	Scan DSK	Import DSKs	Export DSKs

DSK Value

Grant Schemes: ☑ S0; ☑ S2 Unauthenticated; ☑ S2 Authenticated; ☑ S2 Acce

Node Options: ☐ Long Range; ☑ Network Wide; ☐ Normal Power;

☐ Auto remove DSK on Device Reset Locally Notification

Add	Update		Remove	Remove All

Figure 51. Smart Start View

Provisioning List:

▼ DSK: 00794-20909-13989-27643-56039-48160-33896-14574
  Name: testL2
  Location: testN2
▼ DSK: 00794-20569-13009-27333-56129-00160-11896-13554
  BootstrappingMode: 0x02

Refresh List	Scan DSK	Import DSKs	Export DSKs

DSK Value 00794-20569-13009-27333-56129-00160-11896-13554

Node Options: ☑ Long Range;

☐ Auto remove DSK on Device Reset Locally Notification

Add	Update		Remove	Remove All

Metadata Type - Name:

Metadata Type - Location:

Figure 52. Z/IP Controller Connected Smart Start View

Table 28. Smart Start View Items

Item	Description
Refresh List	Reloads the provisioning list.
Scan DSK	Open dialog which gives opportunity to scan QR-Code using special scanner or connected camera.
Import DSKs	Load provisioning list from special XML file.
Export DSKs	Save provisioning list to file.
Grant Schemes	Select which security schemes to be granted if requested
Node Options	Select which node options to be used during smart start inclusion process. Only Long-range or only normal smart start requests will be accepted depending on 'Long Range' node option.
Auto remove DSK on Device Reset Locally Notification	Option to enable/disable removing node included to network using DSK from the provisioning list on receiving 'Device Reset Locally' notification from it.
Add	Adds a new DSK to the provisioning list.
Updated	Change selected item from the provisioning list.
Remove	Removes the selected DSK from a provisioning list.
Remove All	Clears the provisioning list.

Figure 53. Scan DSK View

The "Scan DSK" dialogue gives the opportunity to enter new DSK values from reading the QR code by camera or text input in case of "Keyboard Entry" marked. The scanned value will be automatically parsed to the corresponding TLV fields, and incorrect value highlights.

3.16   Set Node Information View

Set Node Information view allows to change PC Controller list of command classes for node information, setup device options and Z-Wave Plus Info Report.

Figure 54. Set Node Info View

Table 29. Set Node Info View Items

Item	Description
Command Classes list	Select supported command classes for connected device, bold fold highlights supported/controlled classes by application.
Default	Automatically set checkbox only for default command classes.
Clear	Clear selected items in the list.
Role Type	Select value for Z-Wave Plus Info Report Role Type.
Node Type	Select value for Z-Wave Plus Info Report Node Type.
Listening	Option to Enable/Disable listening property.
Device Option	Select value for Basic Device Class in Application Node Info.
Generic	Select value for Generic Device Class in Application Node Info.
Specific	Select value for Specific Device Class in Application Node Info.
Set	Apply changes.

3.17 Transmit Settings View

Transmit Settings View provides functionality to adjust the TX power on Z-Wave 700 and above Controller devices.

Figure 55. Transmit Settings View

Table 30. Transmit Settings View Items

Item	Description
Set 'Tx Power Level'	Configure of default Tx Power level settings in Deci dBm in range from -100 to +130, where value 100 equal to 10 dBm, and values greater than 100 are for test purposes.
Set 'Max LR Tx Power'	Set the maximum LR power
Set 'RF Region'	Configure of RF Region settings with selected item from the "Region" combo box.
Set 'LR Channel'	Configure Channel in use for Serial API Controllers only if Rf Region is US_LR.
Set 'DCDC Mode'	The current DCDC configuration can be updated or retrieved using Set DCDC Configuration and Get DCDC Configuration Commands, respectively.
Set 'Radio PTI'	Enable/Disabled Radio PTI support mode – enable Zniffer on the connected device, except End Device.

3.18 Network Statistics View

Displays and clears Tx Timers and collected statistics by Z-Wave protocol.

Figure 56. Network Statistics View

Table 31. Network Statistics View Items

Item	Description
Clear 'Network Stats'	Calls function to clear current Network Statistics collected by Z-Wave protocol
Get 'Network Stats'	Retrieves the current Network Statistics as collected by the Z-Wave protocol.
Clear 'Tx Timers'	Clears the protocols internal Tx timers.
Get 'Tx Timers'	Gets the protocols internal Tx timer for each channel. The returned value is in milli seconds
Get 'Background RSSI'	Get current values for each channel
Start Jamming Detection	Start polling Get Background RSSI from a connected device, add warnings to log
Stop Jamming Detection	Stop polling Get Background RSSI

4 FUNCTIONALITY

For each SC in the network, a separate instance of the PC-based Controller application must be started.

Note: For correct behavior of the Z/IP Gateway as SIS in network and for support of the Inclusion controller command class, set up unsolicited destination. For more information, see Section 3.2.4.

The SC can be configured to one of the following controller types:

- **Primary SC**
- **Secondary SC**
- **Primary SC with SUC and node ID Server functionality (SIS)**
- **Inclusion SC**

Primary SC

When configured as primary, the SC can be used to include/exclude nodes in the Z-Wave network. The primary SC will automatically update an SUC if present in the Z-Wave network. Only one primary controller is allowed in the Z-Wave network.

Secondary SC

When configured as secondary, the SC cannot include/exclude nodes in the Z-Wave network. Several secondary controllers are allowed in the Z-Wave network.

Primary SC with SUC and node ID Server functionality (SIS)

The SIS enables other controllers to include/exclude nodes in the network on its behalf. The SIS is the primary controller in the network because it has the latest update of the network topology and capability to include/exclude nodes in the network. When including additional controllers to the network, they become inclusion controllers because they have can include/exclude nodes in the network on behalf of the SIS. The SIS cannot shift its primary role to other controllers in the network.

To read more about SIS functionality, see reference [2].

Inclusion SC

The inclusion SC can include/exclude nodes in the network on behalf of the SIS. The inclusion SC's network topology is dated from the last time a node was included or it requested a network update from the SIS and therefore it can't be classified as a primary controller.

4.1   The SC Properties

Depending on the functionality required in the network, the PC-based Controller (SC and BC) can shift roles to obtain the desired functionality.

<u>Primary</u>

If the SC is the first node in a network, it will automatically be configured to act as a primary controller.

<u>Secondary</u>

If the SC is not the first node in a network, it will automatically be configured to act as a secondary controller.

<u>SIS</u>

It is possible to set the Network Role Option by clicking Set as SIS command.

The table below shows which functionality is available for the PC-based SC depending on the configuration on the controller.

Table 32. Overview of the Static Controller Properties

	Primary	Inclusion	SIS	Secondary	End Device
Node:					
Add Node	X	X	X	-	-
Add Node with DSK	X	X	X	-	-
Remove Node	X	X	X	-	-
Network Wide Inclusion	X	X	X	-	-
Network Wide Exclusion	X	X	X	-	-
NOP	X	X	X	X	X
Mark Node as Failed	X	X	X	X	-
Replace Failed Node	X	X	X	-	-
Remove Failed Node	X	X	X	-	-
Set as SIS	X	X	X	-	-
Neighbors Update	X	X	X	X	-
Request Node Info	X	X	X	X	-
Basic Set On	X	X	X	X	X
Basic Set Off	X	X	X	X	X
Set wake Up Interval	X	-	-	-	-
Switch All On	X	X	X	X	X
Switch All Off	X	X	X	X	X
Identify	X	X	X	X	X
Start Test 'Basic Get'	X	X	X	X	X
Change Security Scheme	X	X	X	X	-
Reset SPAN	X	X	X	X	-
Controller:					
Receive Information	X	X	-	X	-
Send Information	X	X	X	-	-
Create New Primary	-	-	-	-	-
Controller Shift	X	-	-	-	-
Reset Controller	X	X	X	X	X
Request Update	-	X	-	-	-
Command Class:					
Send	X	X	X	X	X
Association:					
Create Association	X	X	X	X	-

Remove Association	X	X	X	X	-
Get Associations	X	X	X	X	-
Setup Route:					
Assign Route	X	X	X	X	-
Delete Route	X	X	X	X	-
Get Priority Route	X	X	X	X	-
Set Priority Route	X	X	X	X	-
General:					
All On	X	X	X	X	-
All Off	X	X	X	X	-
Abort	X	X	X	X	-
OTA Firmware Update	X	X	X	X	-
OTA Firmware Update	X	X	X	X	-
IMA Network	X	X	X	X	-
NWM Backup/Restore	X	X	X	X	-
Configure Parameters	X	X	X	X	-
Smart Start	X	X	X	-	-
Set Node Information (Reset State)	X	X	X	-	X
Transmit Settings (ZW070x and above)	X	X	X	X	X

4.2   Node View

4.2.1   How to Add a Node

PC-based SC is Primary / Inclusion / SIS

To add a node to the Z-Wave network, activate the button 'Add' in the 'Network Management' view. When activating this button, the Status popup message will display 'Press shortly the pushbutton on the node to be included in the network'. Select the node that should be added to the Z-Wave network by activating the node's button. During the inclusion process, the node must be located at its final position, so that it can obtain the correct neighbors within its range. If the operation was successful, information regarding the node type will be displayed in the node list. The PC-based controller reduces the RF output power during the inclusion process, which can cause range problems because it is static, i.e., located in a fixed position. It is, therefore, recommended that one use a portable controller as primary for adding new nodes to the Z-Wave network.

To include Long Range devices, use Smart Start inclusion only, described in 4.16. For Long Range included devices, the PC Controller uses Long Range Network Keys for Security Schemes Access and Authenticated.

The Default Inclusion process in Add Node command combines inside protocol inclusion part, auto setup SIS in a network according to Role Type specifications, security bootstrap, and setup default lifeline (route, association and wakeup if supported by joining node). To manage the inclusion process, use: Add Node Custom.

Note: For the correct behavior of Z/IP Gateway as SIS in network and for support of the Inclusion controller command class, set up unsolicited destination. For more information, see Section 3.2.4.

Controller is waiting for the node information. Press shortly the pushbutton on the node to be included in the network.
14:36:13.686 'Add Node' Started

Abort
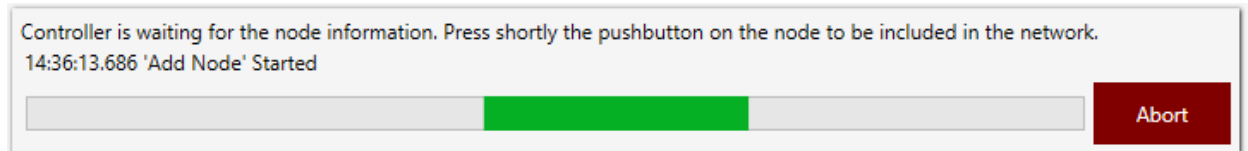
Figure 57. Popup Message After Pressing 'Add' Button

A secure S2 node asks for network keys during inclusion. The PC Controller application shows the following dialog:

The device may control these classes
☑ S0
☑ S2_UNAUTHENTICATED
☑ S2_AUTHENTICATED
☑ S2_ACCESS
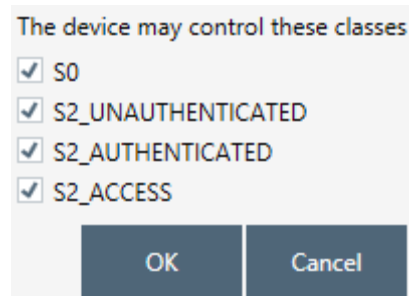
OK   Cancel

Figure 58. Network Keys Request

The secure inclusion flow will be cancelled if the user presses the Cancel button. As a result, the node will be included non-securely.

The Device-Specific Key (DSK) may be required during a secure S2 node inclusion. The PC Controller application shows the next dialog where the user may input text as decimal or hex value using check box or scan it from a QR Code – button "QR Code":

Enter first five digits and verify all other numbers
☐ Hex input
00000
41043-
20863-
47628-
30995-
11652-
62353-
43561

QR Code   OK   Cancel
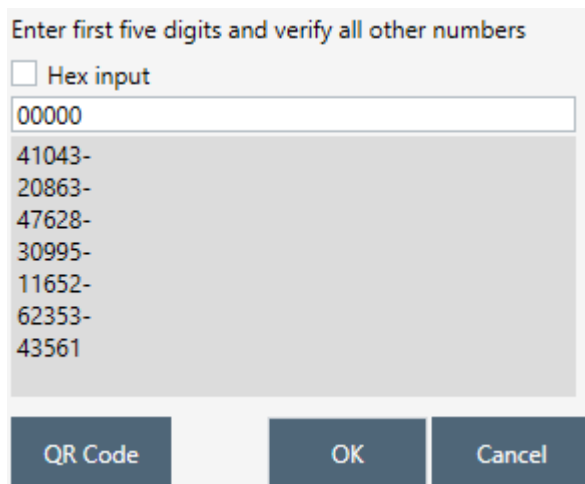
Figure 59. Enter DSK Dialog

The secure inclusion flow will be cancelled if the user presses the Cancel button. As a result, the node will be included non-securely.

PC-based Controller is Secondary

It is not possible to add nodes to the Z-Wave network.

4.2.2   How to Add Multichannel Node with EndPoints

The process of inclusion a Multichannel node is the same as for other nodes. When adding the node with supported command class, Multi Channel PC Controller will additionally ask End Points to list and indicate the capability for each.

<div align="center">

2   [S2] Switch Binary
2.1   --- Switch Binary
2.2   --- Switch Multilevel

</div>

<div align="center">

Figure 60. Multi Channel Node with End Points View

</div>

4.2.3   How to Remove a Node

PC-based SC is Primary / Inclusion / SIS

To remove a node from the Z-Wave network, select the node in the node list and activate the button 'Remove'. After activating the button, the Status popup message will display 'Press shortly the pushbutton on the node to be excluded from the network'. If this operation was completed successfully, the node and its information will be removed from the node list. The PC-based Controller reduces the RF output power during the exclusion process, which can cause range problems because it is static, i.e., located in a fixed position. It is, therefore, recommended one use a portable controller as primary to remove a node when having range problems.

Controller is waiting for the node information. Press shortly the pushbutton on the node to be excluded from the network.
14:57:24.744 'Remove Node' Started

Abort

<div align="center">
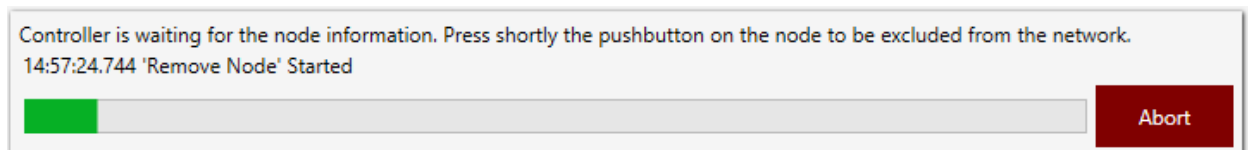
Figure 61. Popup Message After Pressing 'Remove' Button

</div>

PC-based Controller is Secondary

It is not possible to remove nodes from the Z-Wave network.

4.2.4   Network Wide Inclusion

The NWI button on the PC Controller results in the PC Controller calling AddNodeToNetwork and, after a successful inclusion, the AddNodeToNetwork is called again.

To start mass inclusion of nodes, press the Network Wide Inclusion button. The dialog will appear with the text: "Controller is waiting for the node information… Press shortly the pushbutton on the node to be included in the network."

Once all nodes have been included, press the 'Abort Operation' button to stop the NWI.

4.2.5   Network Wide Exclusion

Pressing the NWE button on the PC Controller calls RemoveNodeFormNetwork and, after a successful exclusion, the RemoveNodeFormNetwork is called again.

To start the Network Wide Exclusion nodes from the controller, press the NWE button and press the pushbutton on each node to exclude it.

4.2.6   Send NOP

This button is used to send a NOP frame to a selected node. Enter the Node ID of the target node in the text box and press the 'NOP' button.

4.2.7   How to Send a Failure Signal to a Node

If a node is corrupt and does not respond to commands, it can be marked as failed, and either replaced or removed.

Push "Is Failed" button for the selected node. The node will be marked in the list as failed (in red font).

4.2.8   How to Replace a Failed Node

PC-based SC is Primary / Inclusion / SIS

A non-responding node can be replaced by another node from the node list in the Z-Wave network by activating the button 'Replace Failed'. The following message will appear: "Replacing the non-responding node… Press shortly the pushbutton on the replacement node to be used instead of the failed one". If the operation was successful, the failed node is removed, and the other node will take the node ID of the failed node. Association setup in the failed node will be lost and must be reprogrammed.

PC-based SC is Secondary

It is not possible to replace a failing node.

4.2.9   How to Remove a Failing Node

PC-based SC is Primary / Inclusion / SIS

A non-responding node can be removed from the Z-Wave network by activating the button 'Remove Failed'. If the operation was successful, the node and its information will be removed from the node list. Responding nodes cannot be removed.

PC-based SC is Secondary

It is not possible to remove a failed node.

4.2.10　Set SIS

It is possible to assign a SIS network role to the selected controller by sending the CmdZWaveSetSucNodeId to it. To perform this operation, press on 'Set as SIS' button on the 'Network Management View'.

It is possible to set only one SIS in the network. If trying to set more than one SIS, the PC Controller will show the following warning.
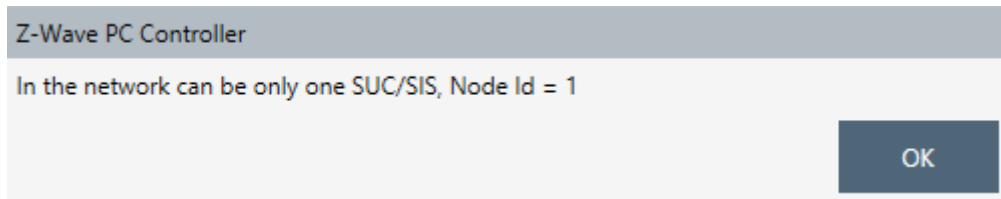
Figure 62. Set SIS Warning Message

4.2.11　Request Node Neighbors Update

It is possible to send the Find Nodes in Range command to the selected node.

4.2.12　Node Info

When the Node Info button is pressed, the PC Controller application sends a REQUEST NODE INFO command to the selected node.

For Multichannel nodes, the application will update End Points list and capability for each.

4.2.13　Version Get

Send Version Get command to the selected node(s).

4.2.14　Switching a Node or a Subset of Nodes on and off

Basic Set On

Activate the button 'On' to send the 'On' command to the selected node(s).

Basic Set Off

Activate the button 'Off' to send the 'Off' command to the selected node(s).

4.2.15　Set Wake-Up Interval

It is possible to set the wake-up interval for a non-listening node. Enter the desired wake up interval (in minutes) into the textbox and press the 'Set Wake Up Interval' button. The WAKE_UP_INTERVAL_SET command will be queued in the application memory and sent to the non-listening node the next time it wakes up.

4.2.16　'Switch All On' Command

To send an 'All on' command to all nodes in the Z-Wave network, press the button 'Switch All On'.

4.2.17　'Switch All Off' Command

To send an 'All off' command to all nodes in the Z-Wave network, press the button 'Switch All Off'.

4.2.18　'Identify' Command

To send an "Indicator Set" command to selected node if it supports this command class.

4.2.19　Start/Stop Basic Test

This option is for stress test purposes. When the 'Start Basic Test' button is pressed, the PC Controller sends a BASIC GET command to the selected node(s). After a BASIC REPORT is received from the node in the queue, the next BASIC GET command is sent either to the same node (if it is the only node selected for operation), or to the next node in the list. If the node does not respond, the controller sends the next command or moves to the next node after a timeout of 10 seconds.

Node settings contains following actions with Security:

4.2.20　Reset SPAN

To clear Singlecast Pre-Agreed Nonce table for selected node.

4.2.21　Next SPAN

To roll Singlecast Pre-Agreed Nonce entry for selected node.

4.2.22　Security Scheme

The controller can change the security scheme for communication with a selected node.
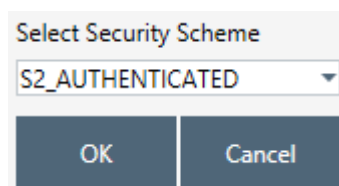
Figure 63. Select Security Scheme Dialog

4.3   Controller View

When including a PC-based SC to a network, activate the 'Add' button on the primary controller, then activate the 'Learn Mode' button on the second PC-based SC (the sequence of these two steps is not vital). This will include the SC into the Z-Wave network and transfer the complete network topology. Furthermore, it is possible to update the network topology in an existing secondary controller.

If the replication went successfully, the second PC-based SC's functionality depends on the selected option button:

If 'SIS' is chosen, and one does not already exist in the network, the SC will become the SIS in the network. If a SIS is already present, the SC will become an Inclusion controller.

If 'None' is chosen, then SC will become a secondary or inclusion controller.

PC-based SC is Inclusion / SIS / Secondary

It is not possible to shift the primary role from the PC-based SC.

Serial API End Device

The PC Controller can manage End Device Learn Mode by activating Classic Learn mode or set specific learn mode from "Select Learn Mode". To exclude LR Smart Start included device is required select "Smart Start" node. DSK won't be shown in the dialog during S2 Learn Mode but available in the Controller information section. Set of S2 Security Schemes for joining device is not implemented and controlled by inclusion device.

4.3.1   Reset Controller

To reset the PC-based SC, activate the 'Reset' button. See also paragraph 4.2.3 to learn how to exclude nodes from the network.

4.3.2   Send Node Info

Send the broadcast node information from the controller.

4.3.3   Controller Shift

PC-based SC is Primary

To shift the primary role from the PC-based SC to another controller in the network, activate the 'Learn Mode' button within the controller to be made primary, and the 'Shift' button within the second controller interface. The second PC-based SC will now become Secondary and the first one will become Primary.

4.3.4   Request Update of PC-based SC

PC-based SC is Primary / SIS / Secondary

It is not possible to request the network topology update from another controller.

PC-based SC is Inclusion

The PC-based SC can request network topology updates from a SIS by pressing the 'Update' button.

4.4   Command Class View

Open the 'Command Class ' view to send specific command classes to nodes.

Select the node ID to receive the command from the node list.

To select a command class and command, click on the button 'Select'. 'Select Command' view will only contain those commands that are supported by the selected nodes; however, it is possible to show all command classes by enabling of 'All Command Classes' checkbox. Some commands require setting a value, e.g., Value. In this case, additional value fields will appear below with their names. All selected and entered values will be shown in HEX string in the Send Data text block. This text block allows changing manually Send data to send.

Finally, send the frame by activating the button 'Send'.

4.5   Association View

Open the 'Associations' view to configure associations between nodes.

Add any nodes that support the Association command class, e.g., Binary sensor.

To view the current association groups of a selected node, press the button 'Get Groups Info'. To get all nodes in the selected group, press 'Get Nodes' button.

4.5.1   Create Association

Select a node from Nodes List to associate with the node that supports the Association command class in Association tree, Select Group, and click the 'Create' button. The node ID will appear in the appropriate group.

4.5.2   Remove Association

Select the node to be removed from the association in the Groups list and press 'Remove'.

4.6   Setup Route View

Open the 'Setup Route' view to assign return routes between the two nodes in the network.

4.6.1   Assign a Route

The PC-based SC supports assigning a route between, e.g., a Binary Sensor, and any other node. Assigning a route specifies how the binary sensor can communicate with the node. To assign a route,

select first a source and a destination node. The source node can be any node based on the routing end device library while destination node can be any node that is always in listening mode. Activate 'Assign' button to generate a route between the two nodes. For a binary battery sensor, the route assignment will be executed next time it wakes up. Until then, the request is queued in the PC-based Controller.

4.6.2   Delete a Route

To delete routes in a node, press the 'Delete' button. All routes assigned to the source node will be deleted. The new routing can be built either automatically or manually.

For a binary battery sensor, the route deletion will be executed next time it wakes up. Until then, the request is queued in the PC-based Controller.

4.7   Security Test Schema View

In Z-Wave Security PC Controller, Security Test Schema functionality is available to test secure networks for failures in case of device malfunctioning with using Security or Security version 2 Command Classes.

With this feature, it is possible to simulate different malfunctions of a Security PC Controller. This is needed to test the proper functioning of other devices in the network.

To use this feature, the "Enable Security Test Schema" checkbox must be checked.

'Use Permanent Network Key' checkbox allows overriding generated by the controller Network Key. It will use a specified Network Key for all operations after pressing "OK" or "Apply" button.

The testing Controller in Security version 0 can be configured either as the Including Controller or as the Included Node. The corresponding options for an Including Controller or Included Node are present dependent on the selection. All changes will be applied after pressing "OK" or "Apply" button.

The testing Controller in Security version 2 can be configured by using security parameters, messages, and extensions overrides. All changes will be applied after pressing "OK" or "Apply" button.

Save Security Keys to Storage is used to generate file with network keys to load it from Zniffer Application.

4.7.1   Test S2 Parameters Overrides

The "Test Span S2" field is used to encrypt S2 Message Encapsulation with a specific SPAN. It will ignore Receivers Entropy input that is sent with the S2 Nonce Report.

The "Test Sender Entropy Input S2" field is used to substitute the SPAN extension value in the S2 Message Encapsulation in response to the S2 Nonce Report.

"Test Secret Key S2" – replaces current secret key of the S2 keypair. The DSK value will be calculated based on the secret key.

The "Test Sequence Number S2" is used to override the S2 Message Encapsulation's Sequence Number property with a specific value.

The "Test Reserved field S2" is used to override the S2 Message Encapsulation's Reserved property with a specific value.

4.7.2 Test S2 Messages Overrides

The "Test Frame" list contains all frames that are normally sent during the S2 inclusion. Therefore, the user is allowed to interfere with the inclusion process with custom frames. Click the corresponding checkbox to activate the parameter override and specify a new value. If the parameter override is not active, the PC Controller will use a valid specific frame parameter value.

"Command" field is used to substitute the selected "Test Frame" with any command that is entered.

When enabled, the "Delay" field will postpone sending the selected "Test Frame" for a specified amount of time.

"Is Multicast" field allows sending the "Test Frame" as multicast or singlecast.

"Is Broadcast" field allows sending the "Test Frame" as broadcast or singlecast.

"Is Encrypted" checkbox allows force sending the frame encrypted or force sending the message unencrypted.

"Network Key" field is used to encrypt the selected "Test Frame" with specified bytes. It will only be used if the 'Is Encrypted' checkbox is enabled and set.

"Is Temp Network Key" field is used to encrypt the selected "Test Frame" using a temporary expansion algorithm. It will only be used if the 'Is Encrypted' checkbox is enabled and set. It will also use the "Network Key" value as a security key to obtain the temporary key.

Example 1: The user wants to substitute the KEX Report (Echo) with the KEX Report frame that is unencrypted, delayed for 2 seconds and with Echo flag set to 0.
KEX Report (Echo) test frame should be configured on the *including* controller. The following screenshot shows all necessary properties that should be set.

Figure 64. Test Frame Configuration for Example 1

Example 2: The user wants to substitute the "Network Key Verify S2 Unauthenticated" frame which will not be delayed, command will be used default but should be encrypted with the custom temporary key. The Network Key Verify test frame should be configured on the *joining* controller. The following screenshot shows all necessary properties that should be set.

Figure 65. Test Frame Configuration for Example 2

4.7.3 Test S2 Message Encapsulation Extensions Overrides

"Clean up existing extensions first" checkbox is used to delete all default extensions that should be added in a normal flow. Note that this will take effect even if no test extension is specified deleting all extensions of S2 messages.

Message type allows filtering which extensions will be changed within the S2 message encapsulation frame:
- Type "Singlecast All" means all S2 message encapsulation singlecast frames.
- Type "Singlecast with SPAN" means all S2 message encapsulation singlecast frames containing SPAN extension.
- Type "Singlecast with MPAN" means all S2 message encapsulation singlecast frames containing MPAN extension.
- Type "Singlecast with MPAN Group" means all S2 message encapsulation singlecast frames containing MGRP extension.
- Type "Singlecast with MOS" means all S2 message encapsulation singlecast frames containing MOS extension.
- Type "Multicast All" means all S2 message encapsulation multicast frames.

Extension type allows selecting a specific extension to add to the filtered S2 message encapsulation frame:
- SPAN
- MPAN
- MGRP (MPAN Group)
- Test (value=FF)

Applied Action value enables applying a set test extension to the next message encapsulation and contains next:
- "Add" add predefined extension, even if extension was not added by application.
- "Add or Modify" remove extension filtered by extension type if it was added by the application, add predefined extension.
- "Modify If Exists" replaces extension filtered by extension type with predefined only if it was added by application.

- "Delete" remove extensions which are matches to filter item if it was added by application.

Extension length is an auto-calculated field.

Extension value allows specifying the extension data.

Click the corresponding checkbox to activate a parameter override and specify a new value. If the parameter override is not active, the PC Controller will use valid specific extension parameter value.

Extension parameters

- "Is Encrypted" option allows overriding the selected extension encryption.
- "More to follow" option allows changing "more to follow" parameter of the selected extension if activated.
- "Is Critical" option allows changing the "Critical" parameter of the selected extension if activated.
- "Number of usages" option allows limiting number of filtered S2 message encapsulation frames. After adding the extension with several usages, the active counter will be "0 of N". To reset the counter, select the frame and click the button "Set". Remember to click "OK" or "Apply" to make the new test settings active.

Examples:
1. Filter the message with a SPAN extension by message type <Singlecast with SPAN>:
   a. Put override <Add>, < SPAN > extension type, <NEWSPAN> value – Resulting message with SPAN and <NEWSPAN>.
   b. Put override <Add Or Modify>, <SPAN> extension type, <NEWSPAN> value – Resulting message with <NEWSPAN>.
   c. Put override <Modify If Exists>, < SPAN> extension type, <NEWSPAN> value – Resulting message with <NEWSPAN>, if needed SPAN synchronization.
   d. Put override <Delete>, < SPAN> extension type – Resulting message without any <SPAN> extension, extension added by the application can exist.

2. Filter message with MPAN by message type <Singlecast with MPAN> and that message doesn't have SPAN:
   a. Put override <Add>, < MPAN > extension type, <NEWMPAN> value – Resulting message with MPAN and <NEWSPAN>.
   b. Put override <Add Or Modify>, <MPAN> extension type, <NEWMPAN> value – Resulting message with MPAN and <NEWSPAN>.
   c. Put override <Modify If Exists>, < MPAN> extension type, <NEWMPAN> value – Resulting message with NEWMPAN.
   d. Put override <Delete>, < SPAN> extension type – Resulting message without any MPAN extension, extension added by the application can exist.

4.8   ERTT View

The ERTT (Enhanced Reliability Test Tool) is used to test the reliability of an RF link by sending a defined number of frames and performing a simple count on how many frames were not received correctly. A DUT node must be included in the network first. Then select the DUT in the node list of the PC Controller and configure the ERTT.

The following controls are available:

Test Iterations – enter the required number of iterations.

Run forever – check this box for the test to run until stopped.

Test Mode – select the data format to be used in the test (Basic Set, value 0; Basic Set, value 255; Basic Set, value 0/255).

Stop on error – check this box for the test to stop on an error.

Low Power – check this box to use low power RF transmission.

TX Control – an optional group of controls which is active only if SerialAPI reports support for (#define FUNC_ID_SERIAL_API_TEST 0x95):

- **TX is Controlled by the module** – If ticked, ZW_Test is used instead of SendData, and the module is informed to send the specified command the defined amount of times. If checked, the following fields must become available:
    - **TX Delay Field:** Define delay between each transmitted frame
    - **Payload length** field

Retransmission - if not ticked, send data will be called with TRANSMIT_OPTION_NO_RETRANSMIT = 0x40.

Packets sent shows the numbers of sent packets.

Packets received: shows the number of reply packets received from the node.

UART Errors: shows the number of UART errors. These errors are logged when the Serial API returns transmit completion status TRANSMIT_COMPLETE_FAIL (0x06).

The UART error is a count of packages not sent to the other Z-Wave device on air traffic. Z-Wave does listen before talking to avoid interference with an ongoing communication. So, if the Z-Wave protocol "is listening" to Z-Wave air traffic, it will not send the package. Normally the Z-Wave protocol will automatically do a random back off and re-try communication. But the ERTT is a special version and will not do the random back-off. The ERTT will therefore have a higher count of non-transmitted packages.

When calculating the Frame Error Rate (FER), the UART error must be subtracted from the Packets sent to obtain the number of Packets transmitted:

Packets transmitted = Packets sent – UART Errors

FER = (Errors/Packets transmitted) * 100 (%)

Node list grid displays information about the nodes which ERTT communicates with:

- **Node ID**

- **Device type**

- **Status** – current transmit completion status for the node. 0 stands for TRANSMIT_COMPLETE_OK.

- **Errors** – the total number of errors (all transmit completion statuses different from TRANSMIT_COMPLETE_OK).

4.9   Polling View

Polling is an infinite process for sending Basic Get command to each node in the list with the interval 'Poll Time, sec' after the last polling command was sent and 'Report Time, sec' before Ack received and before sending to the next node. To perform Polling the 'Poll Time, sec' should be set for the needed nodes and the button 'Start' should be pressed to start. To stop the process, press the button 'Stop'.

'Requests' column shows the number of iterations for a specific node.

'Failure' shows the number of failed transmits.

'Missing Report' shows the number of requests without reports.

'Max Command Time [ms] shows the maximum delay in sending the Basic Get command and receiving a callback.

4.10   Topology Map View

The small squares on the sides of the graphic map use the color codes shown in the Node type Colors area.

The larger squares indicate the state of link between two units. Blue squares indicate that the link between two nodes exists, red squares indicate that the link does not exist, and white squares indicate that no link can exist. Note that the table is always symmetrical around the white line.

The *"Reload"* button loads the Topology map from the Z-Wave module. This is not done during startup because of the time it takes when the Z-Wave module holds a large network setup.

4.11   IMA Network View

Open the 'IMA Network' view to perform analysis of the network health. Add any listening node to start executing the algorithm.

The selection works as follows:

If no node selected:

1)   Nodes range = all nodes except non-listening and controller itself.
2)   If nodes range is empty, do nothing.

If one or many nodes selected:

1)   Nodes range = selected nodes except non-listening and controller itself.
2)   If nodes range is empty, range = all nodes except non-listening and controller itself.
3)   If nodes range is empty, do nothing.

For Non-listening nodes, it is possible to set "Queue overridden" check mark in the node list view, which indicates that the node is a listening node.

4.11.1 Network Health

Starts network health algorithm. This is a time-consuming process and can be aborted. After the process is finished, the Last Working Route for each node will be shown and Network Health Status will be displayed on each node. The iteration information is shown on the right side of the view.

4.11.2 Power Level Test

To perform the test, make sure that the selected nodes, marked as Source (Src) and Destination (Dest), support the power level command class. The test will be started from -9 dB reduction and continue to lower reduction until the report is received with an OK status.

4.12 Security Encrypt/Decrypt

In case of Security (tab S0), enter External Nonce, Internal Nonce, and Security Key. Then, put the encrypted message and click the "Decrypt" button or enter the decrypted message and press the Encrypt button. The outcome will be presented in the corresponding field.

For Security version 2 (tab S2), fill all fields including the network key entered manually. Select the key extract algorithm. Then, enter a message in the corresponding field and click 'Decrypt' or 'Encrypt'.

Example of the S2 encapsulated message decryption using the temporary key:

After including node PC Controller displays last used temporary key at the Security Settings view:

Network Key S0	5C 5C 5E 2C 59 72 DE 8E 05 21 22 BC F5 87 C8 D0
Unauthenticated	8C EE 5E 6C 52 B5 0C 92 40 CE 42 27 83 51 AC 0F
Authenticated	16 9B 94 60 59 F9 32 D3 D2 87 03 16 F9 99 14 D3
Access	84 06 A3 6E 4C 6A 13 73 96 3E BC E8 48 FE 72 8F
LR Authenticated	5D 77 74 99 B1 F8 BB 69 9E 2B B0 F2 41 DA 6A E8
LR Access	A9 BD BF B3 F3 78 5D A3 A4 2A F6 B7 42 AF 52 E3
Last used Temp	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 66. Last Used Temp Key

Choose S2 Message encapsulation frame from the Z-Wave PC Zniffer:

004	001	EC 2E CF D0	Singlecast	Public Key Report	EC 2E CF D0 04 41 0B
001	004	EC 2E CF D0	Ack		EC 2E CF D0 01 03 0B
001	004	EC 2E CF D0	Singlecast	Public Key Report	EC 2E CF D0 01 41 0D
004	001	EC 2E CF D0	Ack		EC 2E CF D0 04 03 0D
004	001	EC 2E CF D0	Singlecast	S2 Nonce Get	EC 2E CF D0 04 41 0C
001	004	EC 2E CF D0	Ack		EC 2E CF D0 01 03 0C
001	004	EC 2E CF D0	Singlecast	S2 Nonce Report	EC 2E CF D0 01 41 0E
004	001	EC 2E CF D0	Ack		EC 2E CF D0 04 03 0E
004	001	EC 2E CF D0	Singlecast	S2 Message Encapsulation	EC 2E CF D0 04 41 0D

Figure 67. S2 Message Encapsulation Frame

Fill all fields in the S2 Encrypt/Decrypt tab

- Home ID = EC 2E CF D0.
- Sender ID = 04.
- Receiver ID = 01.
- Sequence Number = 6D (look in the frame details of the selected S2 Message Encapsulation frame).
- Generations = 1 (first frame after S2 synchronization, you may specify range 1...N).
- Receiver Nonce = 45 D7 23 53 64 1E 5D 76 76 92 29 AF F4 65 B0 CD (look Nonce Report frame from receiver to source which was used for S2 synchronization).
- Sender Nonce = 73 35 2F 2C 32 B0 3E 93 84 EC 37 C7 85 1C 02 40 (look in the frame details of the first S2 Message Encapsulation frame after synchronization with SPAN extension, this is the selected frame in this example).
- Security Key - 08 7A B4 94 18 E3 B9 2C 69 67 3A 33 D0 9C 92 8F (last used temporary key after node inclusion).
- Key Extract algorithm – Temporary.
- Encrypted message - 9F 03 6D 01 12 41 73 35 2F 2C 32 B0 3E 93 84 EC 37 C7 85 1C 02 40 9B B4 52 12 38 43 76 3F A4 13 0B 68 DD 9E (look in the hex data of the selected frame, starting from 9F 03 to end of frame without checksum bytes. Selected frame has 2 bytes checksum).

EC 2E CF D0 04 41 0D 2F 01 9F 03 6D 01 12 41 73 35 2F 2C 32 B0 3E 93 84 EC 37 C7 85 1C 02 40 9B B4 52 12 38 43 76 3F A4 13 0B 68 DD 9E 9C C8

Figure 68. S2 Message Encapsulation Frame Hex Data

Then, enter a message to the corresponding field and click 'Decrypt'.

Original message command - 9F 06 01 02 01 81

Figure 69. S2 Message Encapsulation Frame Decrypt

4.13 Firmware Update

If the device supports the Firmware Update Meta Data command class, it is possible to use this feature to update its firmware over the air.

Current firmware ID and manufacturer ID of the device can be checked. Press the 'Get' button to send Firmware MD Get command to the device.

New firmware file can be uploaded through selecting the file and pressing the 'Update' button.

If the update needs to be delayed, the 'Activation' checkbox should be checked before pressing the 'Update' button. After the process is finished, the 'Activate' button should be pressed to send Firmware Update Activation Set command and start the local update process on the device. This functionality is available only for Firmware Update MD Command Class Version 4.

Option 'Stop transmitting bulk reports on missing acknowledge' stops transmitting reports when acknowledge is not received for one or multiple packets of bulk transmission. For example, if node requested 7 reports and acknowledge for 3rd report is not received then discard transmission of 4th-7th reports and wait next request from the device.

4.14 NVM Backup/Restore

This functionality saves and uploads the non-volatile memory content of the device.

Buttons with the label '…' are used to create or select a hex-file for the device data.

Press 'Backup' to copy the content of device non-volatile memory to a selected file. The file will be auto generated if it does not exist. The backup file can be either saved in the '*.zip' format or '*.hex' format. The compressed '*.zip' file contains additional information from PC Controller, such as Security keys.

 'Restore' will write data from file to device.

Note: When restoring from backup file, which is '*.hex' format, it will only restore device's memory. To back up Security keys and other additional information including all non-listening nodes (for example Sensor PIR) Wake Up interval settings, use the '*.zip' format file.

4.15   Configuration Parameters

The Devices Configurations view realizes the Configuration Command Class which allows product-specific configuration parameters to be changed. One example could be the default dimming rate of a light dimmer.

Configuration parameters MUST be specified in the product documentation. Configuration parameters accessed via this command class MUST NOT replace similar commands provided by other existing Command Classes.

A device MUST be able to operate with default factory configuration parameter values.

4.16   Smart Start

The PC Controller provides the Z-Wave Smart Start functionality which ensures that the S2 network keys are not handed out to an attacker. In the 'Smart Start' view, it is possible to add a new or view an existing DSK to allow inclusion of devices with Security S2 without the user's participation.

Smart Start contains a Device-Specific Key (DSK) list – the Provisioning List. Besides the DSK each item in the Provisioning List has 'Grant Schemes' and 'Node Options' attributes.

-   Grant Schemes: Select which security schemes to be granted if requested
-   Node Options: Select which node options to be used during smart start inclusion process. Only Long-range or only normal smart start requests will be accepted depending on the 'Long Range' node option.

During inclusion with Security S2, the PC Controller selects the required key. In case of successful security inclusion, the used item from the list will be marked with an included Node ID and never used again until the device is reset or removed from the network. Items can be removed from the list, but if the selected DSK corresponds to the added node, the user will be notified that device will stay in the network and needs to be removed manually by the next popup:
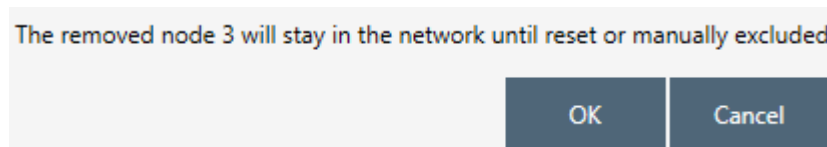
Figure 70. Provisioning List Item Delete Popup

The PC Controller reacts on the device reset event, removes the node from nodes list, and drops the link with the current DSK in the provisioning list. Users may choose whether to delete the item from the list or not:
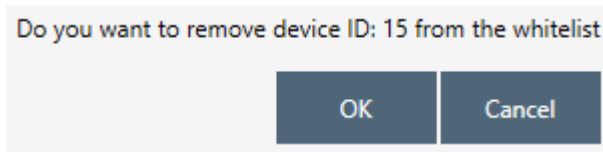
Figure 71. Smart Start Added Device Locally Reset Popup

4.17 Set Controller Node Information

The PC Controller makes it possible to generate the Node Information frame and save information about node capabilities by settings Application Node Info and changing Z-Wave Plus Info Report.

Lists of supported and securely supported classes will be applied automatically according with security settings. Apply settings possible only connected device doesn't included in any network.
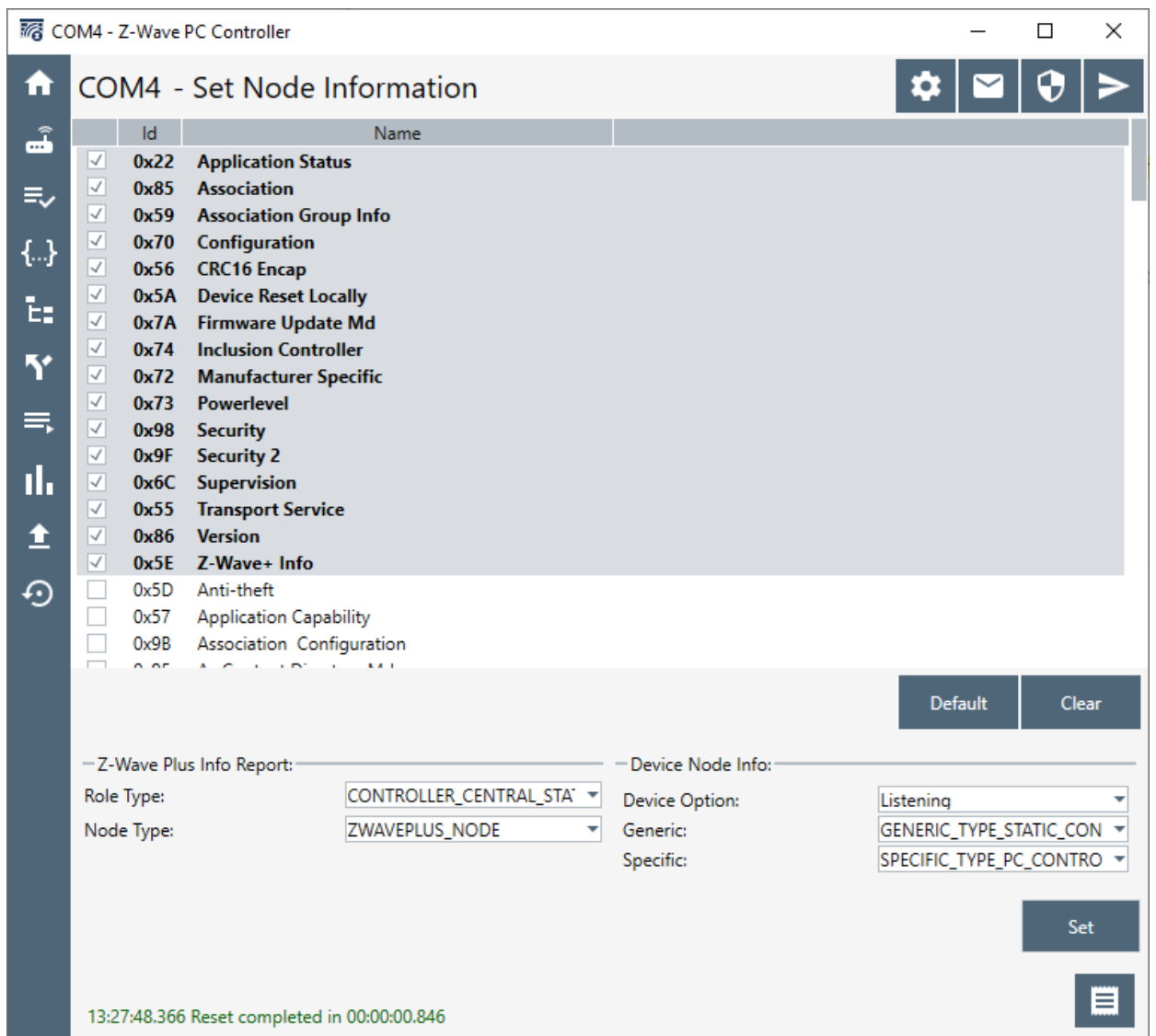
Figure 72. Set Node Information view

Application Node Info contains lists of command classes and Device Node Info fields which can be selected from appropriate drop-down lists:
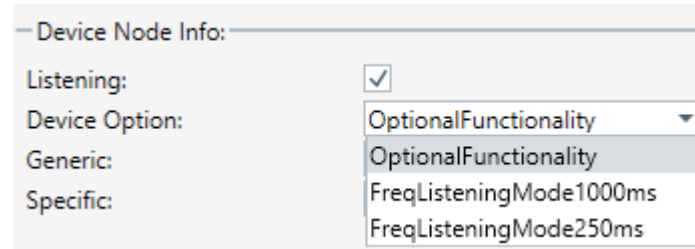
Figure 73. Device options
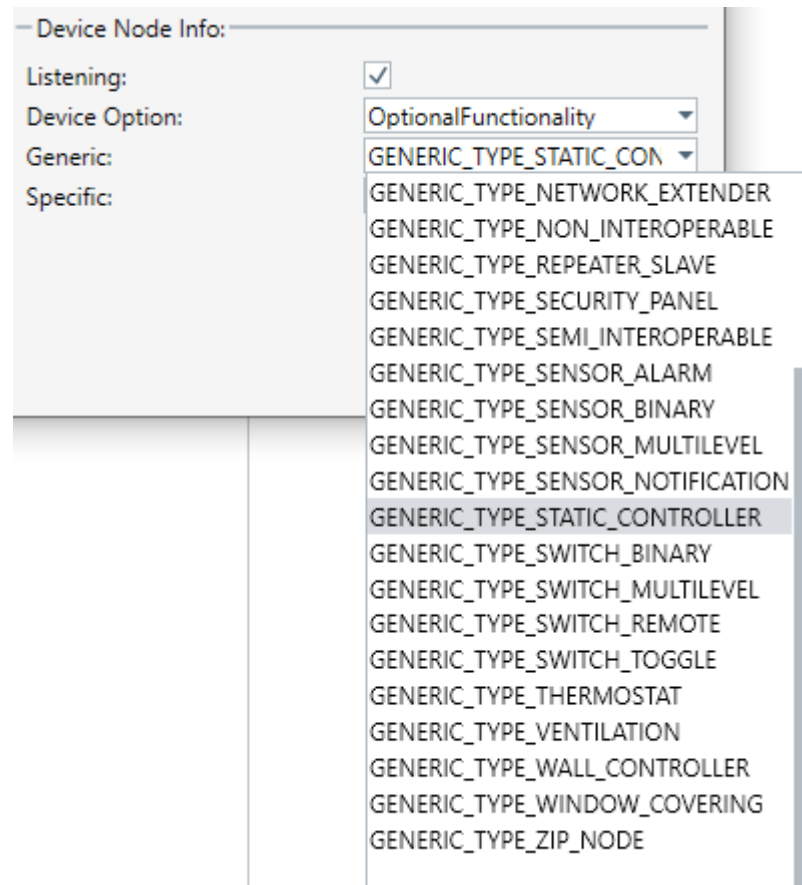
Figure 74. Generic options
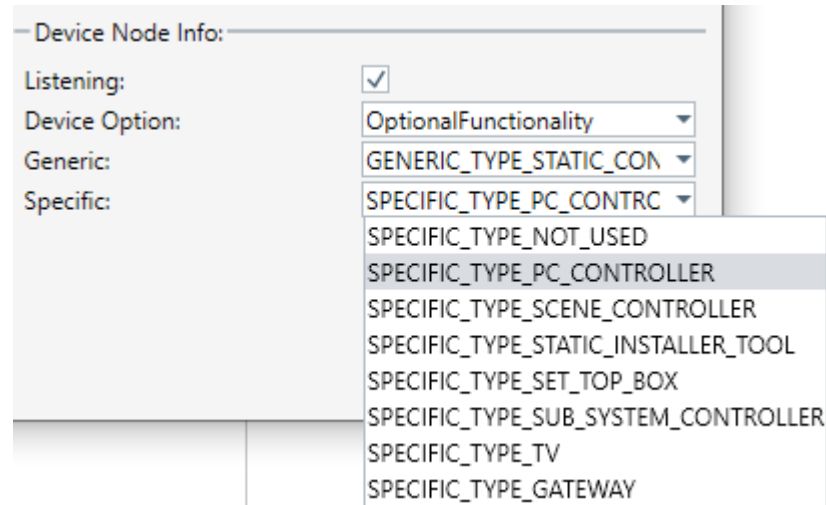
Figure 75. Specific options

The Z-wave Plus Info Report section allows setup reports for Z-wave Plus Info Command Class requests which are used to differentiate between Z-wave Plus, Z-Wave for P and Z-wave devices.
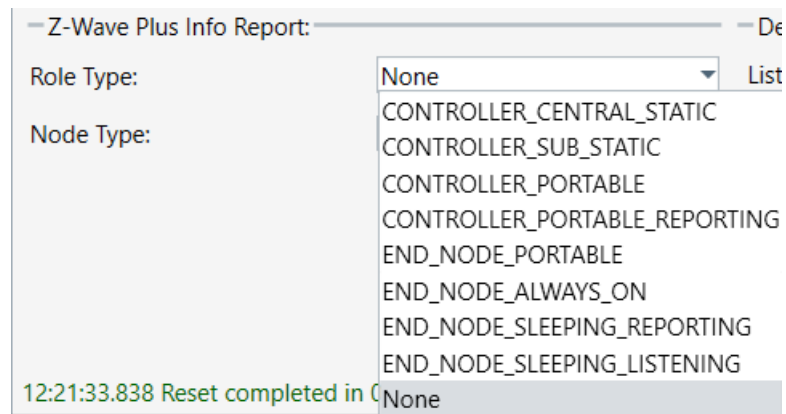
Figure 76. Role Types
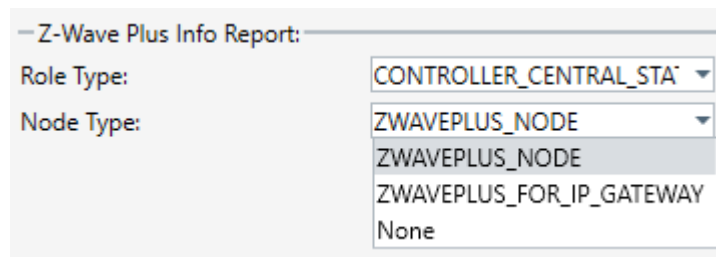
Figure 77. Node Types

4.18   Transmit Settings

The Transmit power and RF Region settings can be configured through Serial API by using PC Controller Transmit Settings View. These fields are filled from a device on connection automatically.

Normal (dBm) - The power level used when transmitting frames at normal power. The power level is in deci dBm, for example 1 dBm output power will be 10 in NormalTxPower and -2 dBm will be -20 in NormalTxPower.

Measured (dBm) - The output power measured from the antenna when NormalTxPower is set to 0 dBm. The power level is in deci dBm, for example 1 dBm output power will be 10 in Measured0dBmPower and -2 dBm will be -20 in Measured0dBmPower.

Figure 78. Transmit Settings Tx Power Level

Since an application can be included both as a Z-Wave node and a Z-Wave LR node, the max power setting must be available for both ZW and ZW LR:

Figure 79. **Select Max LR Tx Power**

The RF Region setting can be configured through select Region from list box:

Figure 80. **Select RF Region setting**

For 'US_LR' set region is possible to change Channels:

Figure 81. **Select LR Channel**

DCDC Configuration automatically detects on the application start and can be changed to one of the next values:

Figure 82. **Select DCDC Mode**

Enable PTI Zniffer functionality is possible using 'Set Radio PTI', checkbox is displaying current support mode (on/off). Works since Z-Wave version 7.15 for the 700/800 SoC as Serial API Controller and Zniffer in one time.

4.19 Network Statistics

The button 'Get' in Network Stats section retrieves the current Network Statistics as collected by the Z-Wave protocol. The Z-Wave protocol will continuo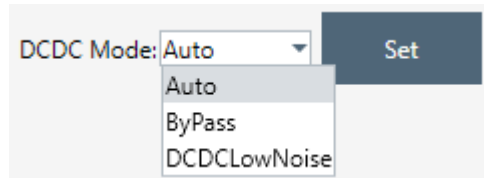usly update any Network Statistics counter until it reaches 65535, which then indicates that the specific counter has reached 65535 or more occurrences. The Network Statistics counters are cleared either on module startup or by calling 'Clear'.

Data description:

- Tx Frames – Transmitted frames including retries and ACKs
- Rx Frames – Received frames (no errors)
- Tx LBT Back Offs – Receiving Z-Wave frame or RSSI detected to be too high for starting transmission.
- RX LRC Errors – Received Checksum Errors (2-channel only)
- Rx CRC16 Errors – Received CRC16 errors
- Rx Foreign Home Id – Received Foreign Home Id

The button 'Get' in Tx Timers section gets the protocols internal Tx timer for the specified channel. The returned value is in milliseconds from the last call to 'Clear'. The Tx timers are updated by the protocol every time a frame is send.

4.20 Z-Wave PC Controller Log

Allows showing an application action log in the single view. The log contains all received and requested messages in the controller in a user readable form. Also, the log writes information about application work, e.g., successful connection or errors in settings. To clear the log window, press the button Clear, and auto scroll to enable scrolling of the log items list.

4.21   Settings Trace Capturing

It is possible to enable capturing of communication trace in the settings view. This functionality allows saving sent and received messages of the device to file in the capture folder. The path to the folder can be changed by users, but the name of file will be auto generated by the app and consists of ZWaveControllerDump, com port name and '*.zwlf' extension, e.g., ZWaveControllerDump_COM1.zwlf.

The Auto split possibility will separate the capture file on parts by size or/and duration. The name of these will be the same as the main file of trace plus date time of saving. Keep the last files controls count of temp files (parts) in a system. All separated parts are saved in the capture folder.

4.21.1   Open Saved Capture Trace File

The saved capture trace file can be converted to a readable format using any external script.

Example of PowerShell script:

```
##################################################
#
# Script for reading zwlf trace capture file
#
##################################################

#take trace file from arguments
$FILENAME=$args
$pos=0

function ReadHeader([IO.BinaryReader] $bReader)
{
  $header = $bReader.ReadBytes(2048)
  $i = 0
  While ($i -lt 64)
  {
      $j = 0
    $outStr = ""
      While ($j -lt 32)
      {
        $outStr += "{0:X2} " -f $header[$i * 32 + $j]
        $j ++
      }
      $i ++
      $outStr
  }
}

function ReadDataChunk([IO.BinaryReader] $bReader)
{
  $outStr = ""
  $tmpBuffer = $bReader.ReadBytes(8);
  $TimeStamp = [DateTime]::FromBinary([BitConverter]::ToInt64($tmpBuffer, 0));
  $outStr += "{0:HH:mm:ss.fff}" -f $TimeStamp
  $tmpBuffer = $bReader.ReadBytes(1);
  $IsOutcome = $tmpBuffer[0] -ge 0x80
  if($IsOutcome)
  {
    $outStr += " >> "
  }
  else
  {
    $outStr += " << "
  }
  $SessionId = $tmpBuffer[0] -band 0x7F
  $outStr += "[{0:00}" -f $SessionId
  $tmpBuffer = $bReader.ReadBytes(4)
  $DataBufferLength = [BitConverter]::ToInt32($tmpBuffer, 0);
  $Data = $bReader.ReadBytes($DataBufferLength);
  $tmpBuffer = $bReader.ReadBytes(1);
  $outStr += ":{0:X2}] " -f $tmpBuffer[0]
  foreach ($i in $Data)
  {
    $outStr += "{0:X2} " -f $i
  }

  $outStr
}

$scriptPath = split-path -parent $MyInvocation.MyCommand.Definition
if(Test-Path ($FILENAME))
{
      $FILENAME = (Get-Item $FILENAME).FullName
}
else
```

```
{
        $FILENAME = Join-Path($scriptPath,$FILENAME)
}

"Opening "+$FILENAME

$stream = New-Object -TypeName IO.FileStream -ArgumentList $FILENAME, Open, Read, ReadWrite
"Stream opened"
$binStream =  New-Object -TypeName IO.BinaryReader -ArgumentList $stream
"Binany wrapper set"
$done = $false
"HEADER:"
""
ReadHeader $binStream
""
"CONTENT:"
""

while (!($done))
{
    if($binStream.BaseStream.Position -lt $binStream.BaseStream.Length)
        {
          ReadDataChunk $binStream
        }
        else
        {
          $done=$true
        }
}

$binStream.Close()
$stream.Close()
```

5   REFERENCES

[1]   Silicon Labs, INS10236, Instruction, Development Controller User Guide.

[2]   Silicon Labs, INS10244, Instruction, Z-Wave Node Type Overview and Network Installation Guide.

[3]   Silicon Labs, INS13113, Instruction, Z-Wave DLL v5 User Guide.

[4]   Silicon Labs, SDS11274, Specification, Security 2 Command Class.

Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

IoT Portfolio
www.silabs.com/IoT

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support & Community
www.silabs.com/community

Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice to the product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Without prior notification, Silicon Labs may update product firmware during the manufacturing process for security or reliability reasons. Such changes will not alter the specifications or the performance of the product. Silicon Labs shall have no liability for the consequences of use of the information supplied in this document. This document does not imply or expressly grant any license to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any FDA Class III devices, applications for which FDA premarket approval is required or Life Support Systems without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons. Silicon Labs disclaims all express and implied warranties and shall not be responsible or liable for any injuries or damages related to use of a Silicon Labs product in such unauthorized applications. **Note: This content may contain offensive terminology that is now obsolete. Silicon Labs is replacing these terms with inclusive language wherever possible. For more information, visit www.silabs.com/about-us/inclusive-lexicon-project**

Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Redpine Signals®, WiSeConnect , n-Link, ThreadArch®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, Gecko OS, Gecko OS Studio, Precision32®, Simplicity Studio®, Telegesis, the Telegesis Logo®, USBXpress® , Zentri, the Zentri logo and Zentri DMS, Z-Wave®, and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. Wi-Fi is a registered trademark of the Wi-Fi Alliance. All other products or brand names mentioned herein are trademarks of their respective holders.

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

www.silabs.com