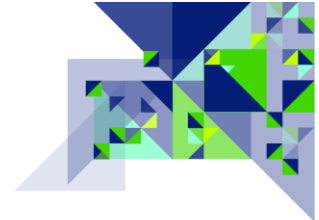# THE Z-WAVE ALLIANCE CERTIFIED INSTALLER TOOLKIT USER'S GUIDE

Version 1.1

Basis: v2.3.5-rc11
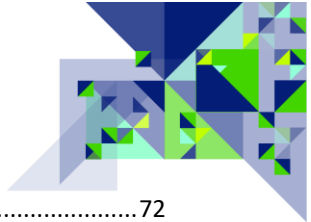
June 28, 2017

47467 FREMONT BLVD.
FREMONT, CA 94538 USA
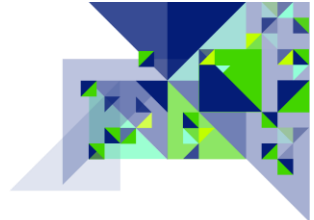**Z-WAVEALLIANCE.ORG**

CONTENTS

Additional Information *76*

Z-Wave Alliance Resources *77*

INTRODUCTION

The Certified Installer Tool (CIT) is a Security Enabled Z-Wave Plus product designed to aid in the installation of new Z-Wave networks and the diagnosis of Z-Wave networks that are experiencing issues. For all uses, except when tracking down a source of noise, the CIT should be physically located in the same place as the customer's own gateway controller. The CIT should then be able to hear and transmit the same Z-Wave signals as the customer's gateway, and it will be able to easily talk to the gateway to get information from it.
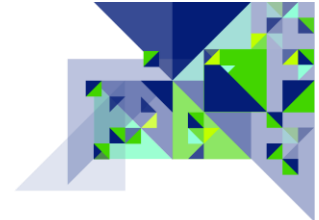
The CIT is used by placing it in the network that you wish to troubleshoot or verify after installation. This allows the CIT to get network information from the primary controller (gateway) as a node in the network. It is important to remember to remove the CIT from the customer's network so that you do not inadvertently create a "bad node" in their network before the CIT is taken off the premises.

KNOWN LIMITATIONS

Z-Wave did not have any installer tools or diagnostic features only a few years ago. The CIT is fully utilizing what is available today and will be updated – along with Z-Wave – and we will continue adding diagnostic features as soon as they are developed by Sigma Designs. As most of the diagnostic features used by the CIT are available to controllers, use the CIT when the manufacturer of your customer's gateway controller does not have diagnostic tools embedded into it, or when the diagnostic tools are a smaller subset of what the CIT offers.

The CIT cannot get information from the nodes of a Z-Wave network where Sigma Designs has not provided a mechanism to do so.

This is an important note because: The CIT will present information such as a neighbor table, but the neighbor table was obtained from the CIT itself; it is not possible to get the *actual* neighbor table from the customer's primary controller because there currently is no mechanism to get this information. If the CIT is placed physically near the customer's primary controller or the node being examined, then the CIT will present a good approximation of what the customer's controller or device should also be experiencing. The CIT will present as much information as it can, but in a network made up of a mix of newer Z-Wave nodes and those from several years ago, features that do not exist in the older nodes may prevent useful information from being able to be retrieved or measured.

USER GUIDE

Please refer to the quick start guide that came with your CIT to get connected to the CIT's user interface (UI). This section discusses getting started using the CIT after you have successfully connected to the user interface.

The first time you access the CIT, you will be prompted to enter information to assign the CIT to your Z-Wave Alliance account. **You must have a Z-Wave Alliance Member Account and that account must be in good standing to use the CIT. You will not be able to register a CIT unit to your account if your membership is within two weeks of expiring.** Let's walk through a few setup items that you should do the first time you start using your CIT:

INITIALIZATION

When the CIT is first accessed, it requires that you initialize it and assign it to the person who will be using it. That person must have a valid Z-Wave Alliance member account. The CIT registration screen appears and looks like this:
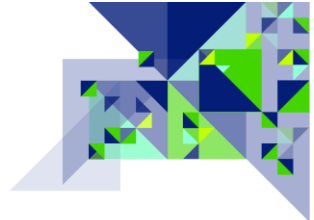

Welcome! Please register your CIT by entering your Z-Wave Alliance authentication.

Login	...

Password	...

CIT Identifier	...

ⓘ *Please enter a unique name to identify your CIT.*

Remote ID: 10020

O Initialize

- In the Login box, please enter your Z-Wave Alliance username.
- In the Password box, please enter your Z-Wave Alliance password.
- Enter a unique/useful identifier in the "CIT Identifier" box. The CIT Identifier is used in the FindCIT service – it is listed along with other CIT units registered to the same Z-Wave Alliance username provided here. If one Z-Wave Alliance username has multiple CITs registered to it, the CIT Identifier allows them to be identified separately.

Complete the registration process by clicking ⭕ Initialize at the bottom of the page. If there are any issues with the registration, a message will be displayed. If you are unable to register/initialize your CIT, please contact the distributor that you received your CIT from for assistance.

LOGIN

If the CIT has already been registered, then connecting to the CIT interface will lead to being prompted for your login credentials. The login screen looks similar to this:
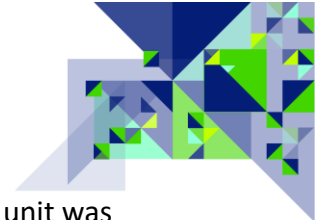
Here at the login screen, the CIT Identifier is displayed at the top. In this example, the CIT unit was registered using a CIT Identifier of "Joe's CIT Unit #4".

- Enter your Z-Wave Alliance Username and Password – the same ones used to register the CIT – to log on to the CIT.

To complete the login, click the Login button.
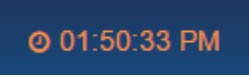
USING THE CIT

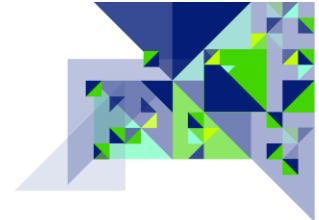As described in the menu section below, the CIT has a menu bar which divides the features of the CIT into functional areas. This section describes each of those functional areas and the capabilities within each area.

MENU
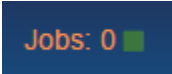
The main menu (shown above) is always visible. The main menu provides direct access to the functional categories and common information about the CIT. The menu features are as follows:

- The **Home icon**, which looks like a house, takes you to the home screen of the CIT where you can access this guide, set the name of the network, add notes about this network or this location, see network information, enter/leave the network, and perform a backup or restore operation.

- The **Device menu** item provides access to device related sub-menus of Status, Type info, Configuration, and Active associations.

- The **Network menu** item provides access to Z-Wave network related sub-menu of Control, Neighbors, Timing Info, Network map, and Link Status.

- The **Analytics menu** item provides access to the analytical sub-menu of Zniffer, Background Noise, Noise Meter, Zniffer History, and Statistics.

- The **Gear (Setup) icon** item provides access to the system setup page and the setup functions which include Language, System settings, Firmware update, Operating frequency, Unregister CIT, and Report Problem.

- The **time** is displayed in the menu according to the display format chosen in the System settings. The time can be set to be set automatically if there is an Internet

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200

connection available, or manually through the System settings when an Internet connection is not available. If the time is set to automatic and no Internet connection is available to the CIT, the time display will not be correct.

- **Jobs: 0** The **Jobs display and link** shows the current number of active jobs in the job queue of the CIT. Clicking on the word Jobs will open a new window in your browser and display the Jobs queue with detailed information about the jobs currently active or jobs waiting to be completed.

- The **Earth icon** indicates whether the CIT has an Internet connection. If the Earth is green, then the CIT has connectivity with the Internet. If the Earth is red, there is no connectivity and functions such as updating the CIT software/firmware cannot be done.

- **Logout** The **Logout command** will immediately log the user out of the CIT. You will have to enter the login credentials of the owner of the CIT to access the system again.
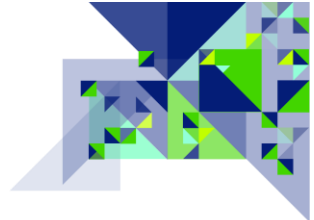
Setup
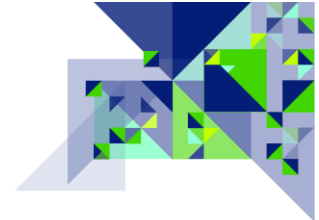
At the top of the UI, to the right of Analytics, click on the gear icon ( ) to access the CIT setup.

Language - Clicking   Language   will take you to the language setting for the user interface of the CIT. The options appear as flags of the home country of the language you desire.
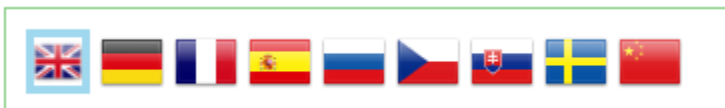
The language you desire may be selected by clicking on the flag for the language you desire – the language options include:

- o   English (en)
- o   German (de)
- o   French (fr)
- o   Spanish (es)
- o   Russian (ru)
- o   Czech (cz)
- o   Slovak (sk)
- o   Swedish (sv)
- o   Chinese (cn)

System Settings – Clicking on ⚙️ System settings will open them up or close them depending upon their current state. When opened, you will see settings as shown here:

⚙️ System settings ⌃

CIT Identifier: Joe's CIT Unit #4 ▦
ℹ️ *Change must be confirmed with login credentials.*

SSID: CIT-demo ▦

WIFI Password: WIFI Password ▦

Date format: yyyy-mm-dd ▾

Time format: 12 Hours ▾

Automatic Time Synchronisation: ON OFF
ℹ️ *En-/disable automatic time synchronisation via NTP (Network Time Protocol). A reboot is necessary.*

Time zone: Automatic (Internet) ▾
ℹ️ *The current time zone is: . You can change the time zone if automatic time synchronisation is disabled or there is an offset difference greater than 30 min. A reboot is necessary.*

Current Server Time: 01:29:45 PM
Date/Time: mm/dd/yyyy --:-- -- ✓
ℹ️ *Configure the server date and time manually if automatic time synchronisation is disabled. A reboot is necessary.*
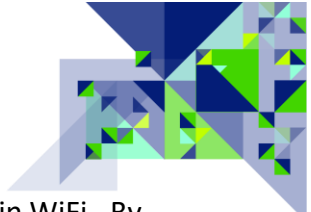
Synchronize Manually: ⟳ Synchronize
ℹ️ *Start manually synchronization of NTP service to get local time and date. Use this if NTP is not synchronized correctly. A reboot is necessary.*

✔ Save

o **CIT Identifier** – This shows the identifier that was entered when the CIT was registered to an owner. The identifier is used to differentiate multiple CITs registered to the same owner at the FindCIT service web page. You may change the CIT Identifier here, but an Internet connection is required for the change to be successful, and the change will be confirmed by being prompted for your CIT Login credentials (Username & Password) when the change is saved.

o **SSID** – The **S**ervice **S**et **ID**entifier is the name that your CIT appears with in WiFi. By default, the SSID is pre-populated with an SSID of "CIT-" followed by a unique 4 digit hexadecimal value. The unique 4 digit code prevents multiple CITs in the same area from having the same SSID. If you wish to change it, you may do so as was done here to make the SSID "CIT-demo". If you connected to the CIT with your client device using a direct WiFi connection to the SSID, changing this value will cause your client to have to re-connect when the settings are saved.

o **WIFI Password** – The WIFI Password comes by default set to installer, but you can (and should) change it here. If you change the WIFI Password, you will be required to re-connect your client to the CIT after the settings are saved.

o **Date format** – Choose the date format that you desire for the date to be shown in the top menu bar of the CIT user interface.

o **Time format** – Choose the time format that you desire for the time to be shown in the top menu bar of the CIT user interface.

o **Automatic Time Synchronization** – Click On or Off to enable or disable time synchronization with an NTP (Network Time Protocol) server from the Internet. Changing this setting will force a restart of the CIT.

o **Time zone** – The time zone setting is only enabled if the Automatic Time Synchronization is turned on. Use this to set the timezone to the desired timezone that the CIT operates in. Changing this setting will force a restart of the CIT.

o **Date/Time** – The CIT current server time is displayed above this setting. When the Automatic Time Synchronization is disabled, set the current date and time here. Changing this setting will force a restart of the CIT.

o **Synchronize Manually** – When Automatic Time Synchronization is enabled, click this button to have the CIT get the current date and time from the NTP server. Changing the date or time will force a restart of the CIT.

Click the [✔ Save] button at the bottom of the System settings when you are done changing the settings. Some setting changes may force a restart of the CIT.

Firmware Update – Access the firmware updater of the CIT and other settings by clicking on

⬆ Firmware update in Settings, then click the [⬆ Open Updater] button that is displayed.
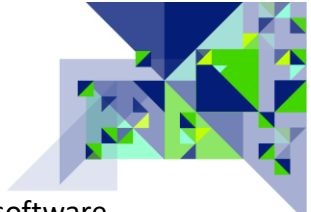
To use the updater, the following criteria must be true:

1. The CIT has Internet access via its Ethernet port.

2. You are not connected to the CIT remotely, via the FindCIT service.

After clicking the Open Updater button and if the above criteria is met, the updater will be displayed:
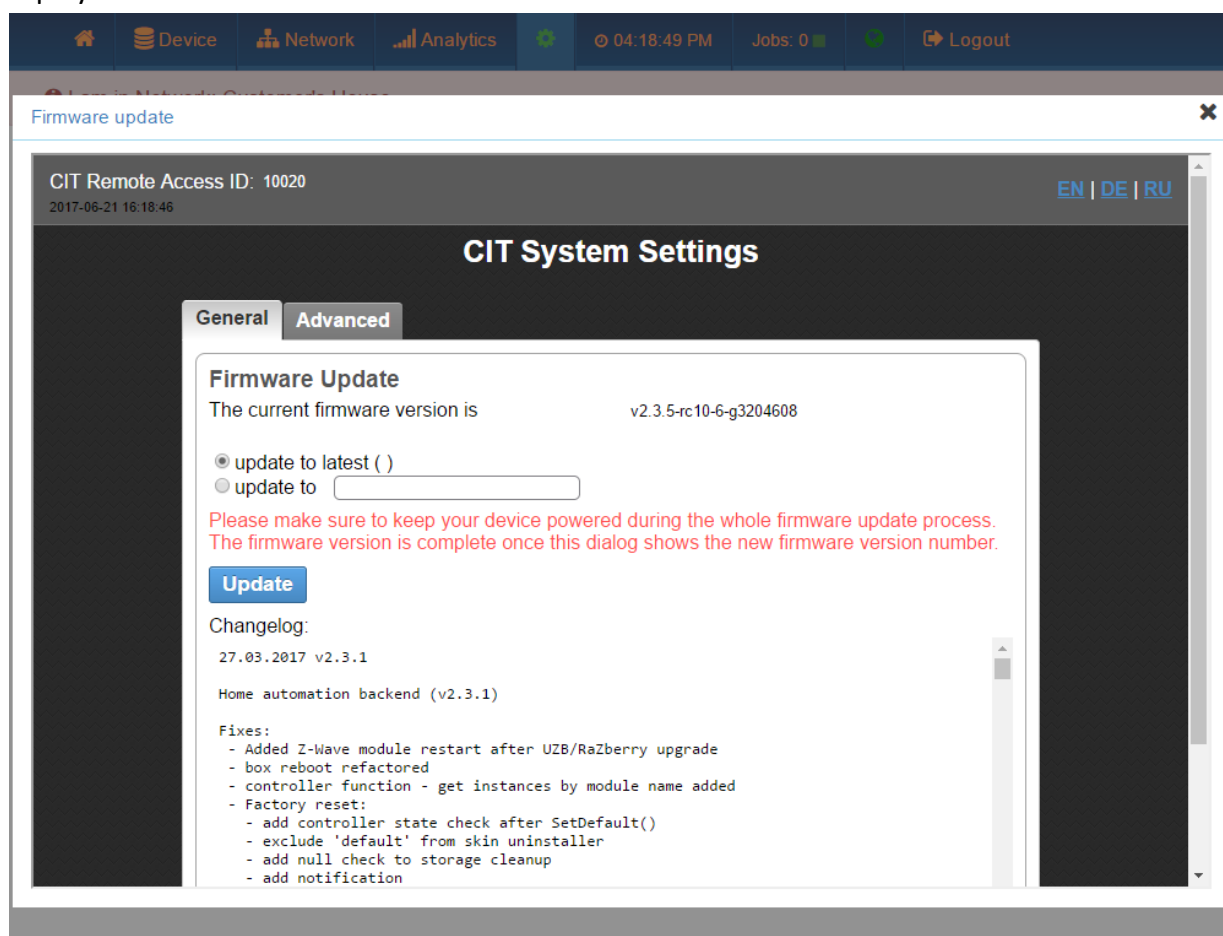
- o   In the upper right corner, you may click on EN, DE, or RU to change the language for the updater to English, German, or Russian.
- o   **General tab** – When you first enter the firmware updater, the General tab is selected automatically. Here are the features of the General tab.
  - ▪   The **Current Firmware Version** file is displayed across from the current version text displayed at the top of the Firmware Update page. This provides more

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA   ●   +1 510.897.0200

detail if requested by support. The base level version of the CIT software – operating system and user interface – is displayed at the bottom of the CIT UI web pages – here is an example:

© 2017 Z-Wave Alliance - UI: 1.3.0 / OS: 2.3.5

- With **update to latest** selected, clicking the [Update] button will cause the CIT to download the latest major release version. If your CIT is version 2.3.4 and version 2.4.0 is available, an update will be downloaded and applied. If your CIT is version 2.3.4 and version 2.3.7 is available, an update will not be downloaded as the major version (2.3) is the same. The update, if applicable, will be downloaded, applied to the CIT, and then the CIT will be automatically restarted when the update is done being applied.

- With **update to** selected, the text box to the right of the words "update to" can be filled in with a specific release identifier. This should be done if instructed to do so by support personnel. After choosing this option and entering the release name, click the [Update] button to have the CIT download the release and apply it. The CIT will be restarted automatically after the update is applied.

  o **Advanced tab** – The Advanced tab does not have any user manageable settings. You should not access this tab unless under instruction from technical support personnel.

Operating Frequency – Set the operating frequency through the setting accessed by clicking on

📍 Operating frequency to open the setting for the CIT's Z-Wave operating frequency. The options available to you will be based upon which version of the CIT you received, but the available settings should include the operating frequency for the country you are working in. Contact the Z-Wave Alliance if you wish to purchase a different model CIT for use in other countries not available to you with the current model. When you open this setting, it will appear similar to what is shown below for the "U" module model of the CIT:
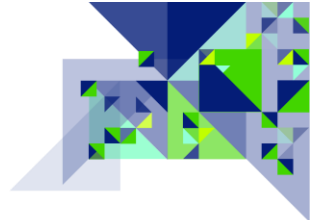
Current frequency: **US**

ⓘ Can be unknown, unsupported or any region (EU/US/RU/....)

US	IL

In this example, the CIT is set to the US frequency group, which handles the US, Canada, Mexico, and several other countries. The other option for this CIT is the IL setting, which is for Israel.

Unregister CIT - Click ⬭ Unregister CIT to access this command. If you are transferring ownership of the CIT to another member of the Z-Wave Alliance, or wish to allow another person in your company to use the CIT without giving them your Z-Wave Alliance login credentials, use this command to remove the registration tying it to your member account. Click on the
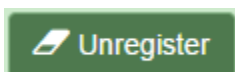
⬭ Unregister button to unregister the CIT. Internet access for the CIT will be required to perform the unregistration, and again to register the CIT to another individual.

Report Problem - Click 🐞 Report Problem to open the problem report submission. This should be used to report a problem that could not be solved by the distributor that you received the CIT from. Problem reports are sent to the manufacturer of the CIT. The problem report submission form looks like this when it is opened:

E-mail: [   ]
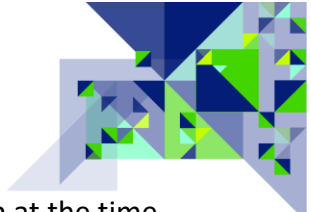
☐ Include log

✔ Submit

To complete a problem report submission:

- o Enter text in the large box that explains the problem, the steps you have taken that led to the problem, and whether you are able to reproduce the problem. If you have

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200
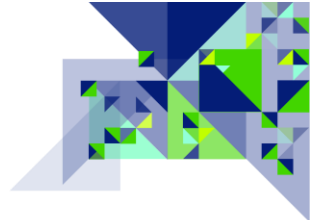
specifics regarding the controllers or devices that you were working with at the time of the problem, please include that information as well. This information is required in order to be able to submit a problem report.

- o Enter your E-mail address in the E-mail box. The Submit button at the bottom will not enable until a valid email address has been entered.
- o Check the "Include log" checkbox by clicking on it, to have a portion of the CIT internal log included with the problem report submission. This log is often the key to allowing the factory to diagnose what went wrong. Z-Wave network keys are not included in the log.

- Click the ✔ Submit button at the bottom right to complete the problem report submission – you must have Internet access for the CIT to submit a problem report.

Home

The house icon represents the home screen, which is where you will get a summary of the network that the CIT is a part of (if it is included into a network) as well as providing a place where you can join or leave a network, assign a name to the network, take notes, or backup/restore the network. Here is what the Home screen looks like for a CIT that has not been included into a Z-Wave network:

Here are the features on this page:

- Clicking on the [User Guide] button will load a PDF version of this **User Guide** into your web browser, and it will be viewed using the default PDF viewer for your client computer.

- Clicking on the [✏] edit button under the **Network Name** heading will allow you to set or change a name for the network you are working with. This is often useful as the network name is displayed in the banner at the top of all of the pages so that you can confirm – if you have several CITs that you work with – which customer the CIT is being used with. To use it, click the button, type the network name in that you want to use, then click the [○ Save] button at the end of the input box.

- Clicking on the [✏] edit button under the **Notes** heading will allow you to set or change notes to be kept along with this network when the CIT is backed up or restored. To add or edit notes, click the edit button, enter the text you wish into the large input box that will be shown, then click the [○ Save] button in the lower right corner under the input box.

- The **Network Information** area tells you about the network when the CIT has been included into a network being examined. When the CIT is the only node and it has not been added to a network, it will only report the 1 node which is the CIT itself. After Network Information in the title, the total number of devices in the network is shown in parenthesis:

  ⓘ Network Information (*147 devices present*)
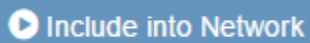
  - The next line shows you how many devices are "mains powered" – a mains powered device is one that always has power that does not come from batteries; mains powered devices are the only devices in a Z-Wave network that participate in routing and can help the mesh network.
  - The next row shows you the number of "battery powered" devices. These are battery powered devices that "go to sleep" which is different from the type described next. Battery devices cannot be communicated with until they "wake up" at programmed intervals or when they wake themselves up to transmit a signal to another device or central controller.
  - The last row under Network Information is the number of FLiRS devices. FLiRS stands for **F**requently **Li**stening **R**outing **S**lave. This type of battery operated device, typically door

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA   ●   +1 510.897.0200
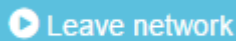
locks for example, gets Z-Wave messages delivered to it from a nearby mains device that holds onto the message until the FLiRS device wakes up its radio to listen for a "beam" signal from the device holding a message for it. As FLiRS devices are battery powered, they still do not participate in routing or help with the mesh network.

- **Enter / Leave different Networks** is shown in the header of the next section of the home page. Under it there is always only one button shown. The button will be blue and says

  ![Include into Network] when the CIT is not currently a part of another controller's network,

  and it will appear as a lighter blue and says ![Leave network] if the CIT is a part of another network. During the process of entering or leaving another network, the button will change to RED and will provide the opportunity for you to cancel an operation. Status information during the operation will be shown along with the red cancel button in this area. Here is a sample of when a CIT is in the process of being included into another network:
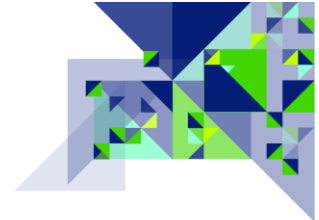
  ⚓ Enter / Leave different Networks

  Start the inclusion or learning mode on the customer's primary controller and click the button below.

  ⟳ (Re-)including myself in network, please wait...

  ⬛ Stop including into Network
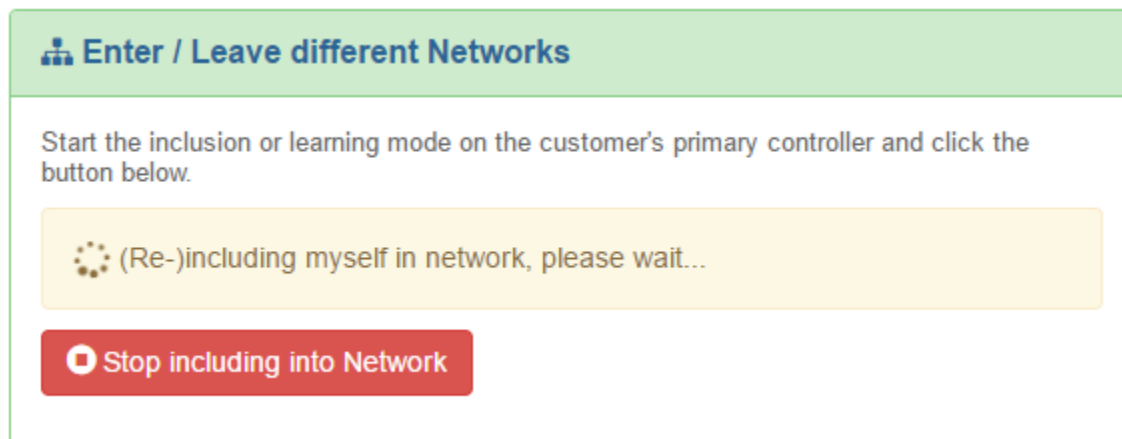
When the inclusion process is completed, the CIT will display a result screen providing three options as shown here:

Include into Network

☺ Controller was (re-)included in network.

C Make restore from a previous backup

Q Detect all nodes (may take some minutes)

→ Just proceed
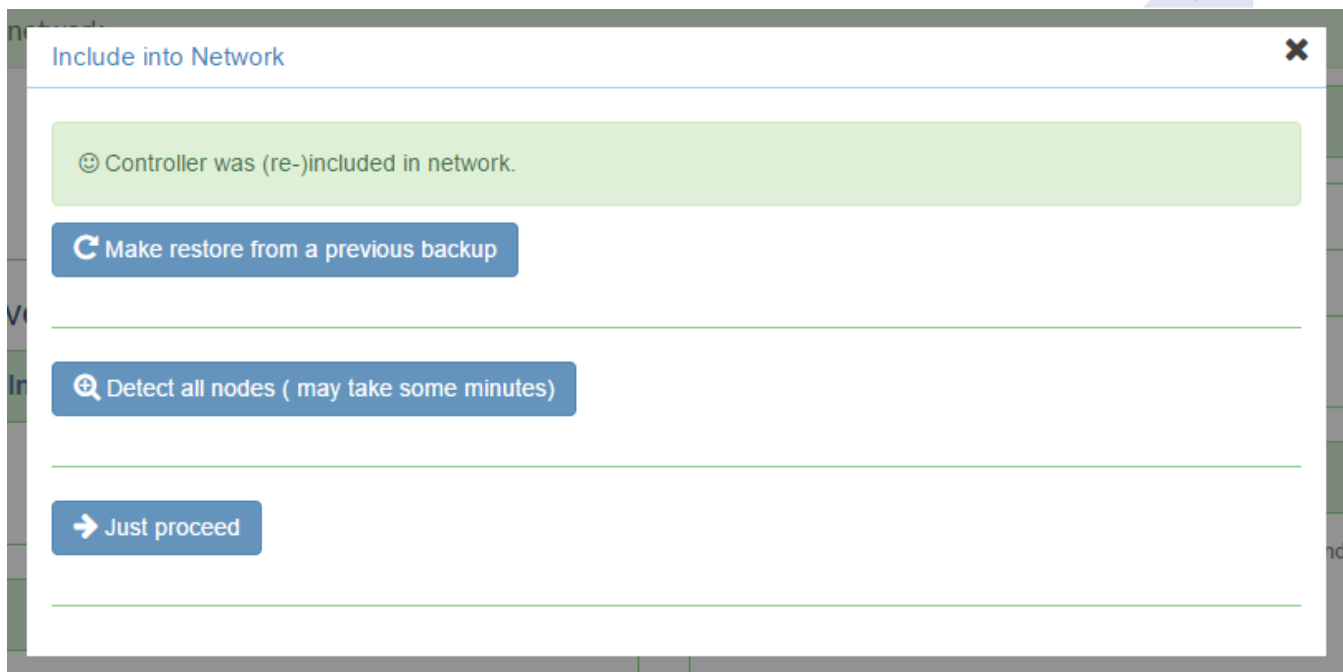
- o *Restore from a previous backup:*
  This option will allow you to restore device names and other device information from a backup file (see Backup and Restore in the next section).
- o *Detect all nodes (may take some minutes):*
  This option will cause the CIT to perform a device interview on all of the nodes in the network. If you have the device information in a backup file, do not choose this option as it does take a long time and will generate a lot of Z-Wave traffic. Do not choose this option if you are diagnosing a network issue as most diagnostic tools can be used without knowing who made the device or what model of device that it is. It is better to resolve network issues first, and then you may initiate an interview on all of the devices if you wish to gather that information.
- o *Just proceed:*
  This is a very simple option and it simply closes the dialog.
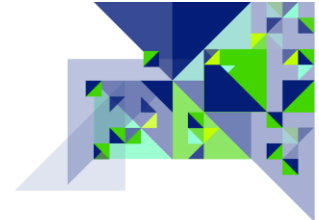
- In the **Backup and Restore** section are two buttons to facilitate you being able to load device names, network name, and notes from a file stored on your client device.

  - o Click on [⬇ Create Backup] to **Create a Backup** and have the CIT download a backup file to your client device. The backup file is named cit-backup-yyyy-MM-dd-hh-mm.zbk

where the letters after cit-backup are replaced with the actual year, month, day, hour, and minute of when the backup was created. Be sure to rename this file to include your customer name or some other information so that you can find it easily when you return to work on the same Z-Wave network.

- o Click on [C Restore] to **Restore** the information created with the backup command to your CIT. The Restore operation does NOT restore Z-Wave node information – it only restores the device names, network name, and notes. You should do a Restore only after you have included the CIT into the network that you are restoring the information for.

Device

The menu items under the device menu allow you to get information about or work with Z-Wave devices in the network. Clicking on Device in the menu does not take you to a function page, but it displays a list of menu options which you may select, and includes (click a box to be taken to the documentation for that menu option):

Status
Type info
Configuration
Active associations

The functions and features of each of these options is provided below:

Status

The status page gives you a quick status of the devices and when it was that the CIT last heard from each device. Here is a sample of the information on the status page:

ℹ️ I am in Network: Customer's House

Status

#	Device name	Type		Date		Check all
1	MainsDevice _1	⚙	✔	09:53 AM	🔍	⭕
2	BatteryDevice _2	🔋	⊘	09:53 AM	🔍	⭕
3	MainsDevice _3	⚡	✔	09:53 AM	🔍	⭕
4	MainsDevice _4	⚡	✔	09:53 AM	🔍	⭕
5	MainsDevice _5	⚡	✔	09:53 AM	🔍	⭕

The columns of information and functions on this page from left to right are:

- **Node number (#)** – this is the Z-Wave node number of this device on the network.
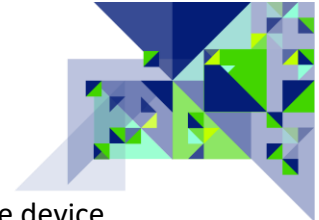
- **Device name** - By default, Z-Wave devices do not contain name information; even if the device supports Z-Wave name and location setting, it must be programmed into the device using Z-Wave before it can be retrieved. The names of the devices are therefore made up of a device characteristic and the device's node number on the network. A MainsDevice is an always-powered device, a BatteryDevice can be a sleeping battery device or a FLiRS device. If the CIT was unable to determine a device type for a device, then the name will be just "Device_" and its node number.

- **Type** – An icon representing the device type will help you to know the device type if you change the device name. Here are the icons and what they represent:
  - ⚙ Indicates a non-portable controller.
  - 🔊 Indicates a portable controller.
  - 🔋 Represents a Battery powered (sleeping) device.
  - 🕯 Represents a FLiRS device.
  - ⚡ Is for Mains (always powered) devices.
  - ⋯ Is for devices whose type could not be determined (Unknown)

- **Communication** – The next column will show one of two symbols representing whether the CIT was able to communicate with the device:
  - ✔ Will be shown if the CIT was able to communicate with the device.
  - 🚫 Will be shown if the CIT could not communicate with the device.

- **Date** – The date column shows the date of the last successful communication with the device.

- **Device Interview** – The presence of the [🔍] button indicates that the device interview is incomplete. The device interview is not required for basic network diagnostics and repairs, but it is needed if you wish to do application layer changes such as Configuration Settings or Associations with the device. Much of the information displayed in the Type info screen is obtained through the device interview process. Clicking on the red symbol will display the device interview status where individual command class interview processes can be attempted again. More information on the device interview process is covered in the Device Configuration section.

- **Communication Check** – Clicking on the [○] symbol will initiate an immediate test by the CIT to see if it can communicate with the device. This is one of the first and easiest tests that can be done to start checking a Z-Wave network.

o   The ⦿ Check all button at the top of the Communication Check column will initiate a check of all devices in the network. You should be able to receive a response from all mains powered devices in the network.

Type info

The type info page goes into more detail regarding the devices in the network, showing you at a glance more information about each device. Here is an example of the Type info screen:

#	Device name	Security	NWI & EF	Z-Wave Plus	Z-Wave Version	Vendor	Product	Device Firmware Version	Device type
1	Primary Controller	🔓	✔	✚	6.51.06			3.00	
54	BatteryDevice _54	🔓			N/A			0.00	Secure Keypad
55	MainsDevice _55	🔓	✔	✚	(4.33)			1.13	Routing Multilevel Switch
58	MainsDevice _58	🔓	✔	✚	(4.34)			1.01	Routing Multilevel Switch
59	MainsDevice _59	🔓	✔	✚	(4.34)			1.01	Routing Multilevel Switch
60	MainsDevice _60	🔓			4.11			2.12	Routing Multilevel Switch
61	MainsDevice _61	🔓			4.22		RF Single Pole Switch	1.10	Binary Power Switch
62	MainsDevice _62	🔓	✔	✚	(4.34)			5.16	Binary Power Switch
63	MainsDevice _63	🔓			4.27		RF Smart Dimmer System Master	1.16	Routing Multilevel Switch
64	MainsDevice _64	🔓			4.22			1.11	Binary Power Switch
65	MainsDevice _65	🔓			4.24			1.13	Routing Multilevel Switch
66	MainsDevice _66	🔓			4.22			2.00	Routing Multilevel Switch

The display can be sorted by each of the columns – to sort by any column, click on the column heading. To reverse the sort order of a column, click on the same column heading again. Here are the columns of information and what you can see or do with them:

- **Node Number (#)** - This is the node number of the device in the network.
- **Device name** – The device name, as mentioned in the Status screen, default to a name based upon the type of device that it is followed by the node number. Clicking on the name here will take you to the configuration screen for that device allowing you to change the name to something more friendly. (Remember to create a backup at the Home Screen so your changes are not lost when you remove the CIT from the customer's network.)
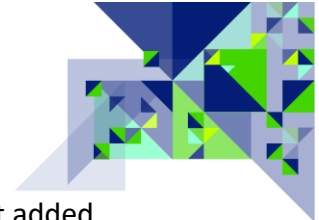
- **Security** – In this column is an image; a red unlocked padlock means the device was not added securely. A green locked padlock means the device is a secure device and was added to the network securely.
- **NWI & EF** – These letters stand for Network Wide Inclusion and Explorer Frame. Although all Z-Wave Plus devices will always have these, there are some Z-Wave devices that had these features before Z-Wave Plus mandated them. Network Wide Inclusion (NWI) allows devices to be added or removed from the network without having to be physically near the primary controller at the time of inclusion or exclusion. (This only works in a network where most or all of the devices support NWI.) The Explorer Frame (EF) is a network "self-healing" capability whereby a node will use a special type of signal to locate a node it wants to communicate with when the normal path is not working. If there is a ✔ (green checkmark) symbol in this column, then the device has these two features.
- **Z-Wave Plus** – If this column has a ✚ (green plus sign) symbol in this column, then the device is a Z-Wave Plus device.
- **Z-Wave Version** – The Z-Wave Library version number is shown in this column if the device interview was able to communicate with the device. If the value here is a number shown in parenthesis, then the library version is the SDK version because it is unknown and could not be decoded into an official Z-Wave Library version.
- **Vendor** – The name of the vendor who created or marketed the device is shown here in this column. This value is obtained through the device interview process.
- **Product** – The CIT has a library of known devices. If the device interview process was able to obtain enough information to find the device in the library of devices, then it will display the device information here.
- **Device Firmware Version** – The manufacturer's firmware version for the device is shown here. If the device supports having its firmware being updated, and that update process takes place using Z-Wave Over-The-Air (OTA) then the firmware update function in the device configuration area will allow you to specify a firmware file to be applied to the device.
- **Device type** – The Z-Wave device type or Z-Wave Plus role type is shown in this column. The type shown here is the base upon which the device's core architecture is based.

Configuration (Device Menu)

Clicking on the device's name in several other pages, such as Device/Type info, will also bring you to this page. This is not a standalone page as it will take you to the device properties of a node, and you can select the other nodes in the network using the list on the left hand side. This page has several functions accessed by clicking on the tabs at the top. The Device/Configuration function tabs are as follows:

💬 Interview	⚙️ Configuration	⋖ Association	📶 Link health	📖 Expert commands	⬆ Firmware update
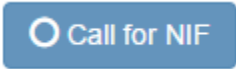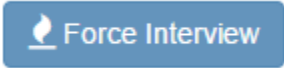
Interview

This tab allows you to view or control the results of the device interview. When the CIT is added to a network, it attempts to contact all of the devices in the network (listening devices) so that it can get detailed information about that device and the command classes that it supports and controls. Information about the device and bar graph showing the interview progress are shown. Here is an example page:
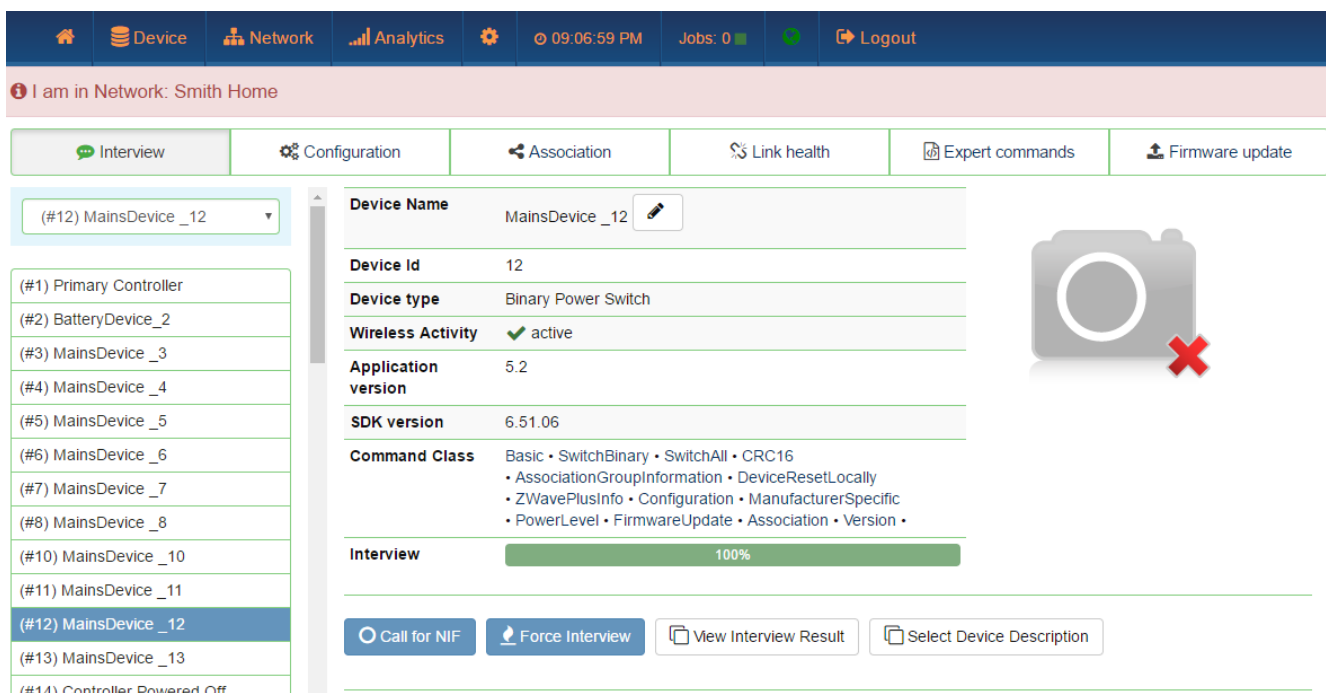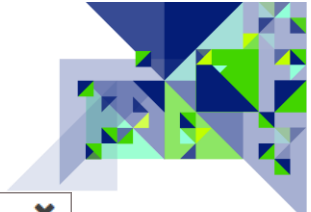
- **Device Name** – Clicking on the (pencil – edit) button will allow you to change the name of the device to something more friendly so you do not have to remember it by its node number. If you change the name of the device, the device will be referred by this name in all of the other screens of the system. Remember to do a Backup before you remove the CIT from

the network so that you can Restore the node names from backup the next time you add the CIT to the same network.

- **Device Id** – This is the device's Node Number in the network.
- **Device type** – This is the device type of the device (See the Type info screen)
- **Wireless Activity** – If the CIT has communicated with the device and the device acknowledged it, or if the CIT heard a communication from this node, then a ✔ active symbol will be shown. If it is a battery operated device and cannot be communicated with, then the ☾ deep sleep symbol will be shown, and if the device type is one that the CIT should be able to communicate with but cannot, then ⊘ Device seems to be dead will be displayed. (Hint: This is a good indicator of a device that may need to be verified as functional.)
- **Application Version** – This is the same as the Device Firmware Version shown on the Type info screen.
- **SDK Version** – This is the same as the Z-Wave Version shown on the Type info screen.
- **Command Classes** – The Command Classes is a list of Z-Wave Application Layer command and response structures that the device uses. Some command classes may be supported by the device, which means it carries out commands given to it by other nodes, and some command classes are controlled, which means it is controlling that command class in another device. The list of command classes is critical to understanding the capabilities of a Z-Wave device. See the Command Classes section for more information.
- **Interview** – This bar graph shows the progress of the interview. If all information has been retrieved from the device, it will show 100% and be entirely green.
- ○ Call for NIF Clicking the **Call for NIF** button will cause the CIT to ask for the device's Node Information Frame (NIF) and it will cause the interview to start all over if the NIF is received.
- ⚡ Force Interview When clicked, the **Force Interview** button will force an interview that previously stopped (perhaps due to too many attempts) to be retried.
- The 🗗 View Interview Result button allows you to see the results of the individual items that the interview process is asking for from that particular device, and you may also force the individual items to be retrieved by clicking on a button to force the CIT to do that interview item immediately. Here is an example:

Interview Results

Interview Results MainsDevice _11
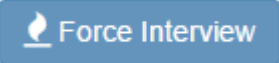
Instance	CommandClass	Result
0	Basic	✔
0	SwitchMultilevel	✔
0	SwitchAll	✔
0	SceneActivation	✔
0	SceneActuatorConf	✔
0	Configuration	✔
0	Alarm	✔
0	ManufacturerSpecific	✔
0	PowerLevel	✔
0	Protection	✔
0	NodeNaming	✔
0	Hail	✔
0	Association	○ Force Interview
0	Version	○ Force Interview
0	Indicator	✔

✖ Cancel
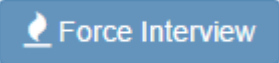
In this example, clicking the **🔥 Force Interview** button for Association or Version would force the CIT to interview those command class capabilities from the device shown at the top of the page.
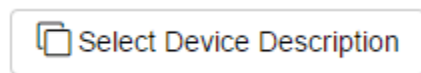
- **📋 Select Device Description** If clicked, will display a dialog allowing you to manually set the make and model of the device – if you are aware of the exact make and model - from a list of devices stored in the CIT. This will short circuit the interview process by bringing in the information for that device that were previously established by somebody else. This is particularly useful for battery devices as their interview may not be easy to complete due to

their sleeping nature. Here is an example of the dialog that would be presented:

Select Device Description   ✖

Manually pick a matching device description

[▾]

ai power QEES Power
Alarm.com Alarm.com Interlogix Simon XT/i Radio Module
Alarm.com Alarm.com Hub
AMC Dimming Switch Module
Andersen VeriLock Translator
Aspire Plug-In Dimming Module
Aspire RF RF 5-Scene Controller
Aspire RF RF Smart Dimmer System Master
Aspire RF Handheld Controller
Aspire RF RF Single Pole Switch
Aspire RF RF Split Control Duplex Receptacle
ASR2-RF Thermoplus ASR2-RF
Athom Homey
AXON™ AXON™ Home Router
BeNext Door/Temperature Sensor
BeNext Plug-in Dimmer
Binary Power Switch HDS
BTSTAR Gateway
BUFFALO HA Adaptor Type1
BUFFALO Smat Tap 100V/15A
Building 36 Intelligent Thermostat Building 36 Intelligent Thermostat
Building 36 Temperature Sensor Building 36 Temperature Sensor
Chromagic Z-Wave Remote Botton (EU) - 300 Series
Chromagic Z-Wave Motion Detector - 300 Series
Chromagic Z-Wave Magnetic Detector - 300 Series
Chromagic Z-Wave In Wall Switch - 300 Series

Configuration

This tab will display a UI to change settings of a configuration nature, such as the Configuration Command Class, Switch All Command Class, Protection Command Class, etc. If the device does not support any of these, the screen is redirected to the Expert commands screen so that any commands that are possible with this device may be shown. Here is an example:

In this example, the Configuration screen is showing the ability to set configuration options for the Configuration Command Class, Switch All Command Class, and Protection Command Class. Not all configuration possibilities are shown here. Some knowledge of the command class may be required in order to be able to use some of these settings.

Association

The Associations tab allows you to work with the device's associations through the Association Command Class (or other association command classes such as Multi Channel Association if present). The screen lists the association groups reported by the device, and any associations that are present in any of those groups. Here is an example:

Here are the options and controls available here:

- The **Update from Device** button will cause the CIT to re-request the association information from the node shown above the button. If the device is a battery operated device that is sleeping, it will be necessary for you to manually wake-up the device so the CIT may communicate with it.

- Click , the plus sign button to **Add an Association** to the association group indicated at the beginning of the line. If the association group already has associations up to the maximum number of nodes supported by the association group, then the button will not appear; it will be necessary for you to remove an existing association to add a new association. When you are able to add an association and click on the button, this dialog will appear:

CommandClass ✖

from MainsDevice _32 to

< Select Device > ▼

(#15) MainsDevice _15
(#16) MainsDevice _16
(#17) BatteryDevice _17
(#18) MainsDevice _18
(#19) MainsDevice _19
(#20) MainsDevice _20
(#21) MainsDevice _21
(#23) MainsDevice _23
(#24) MainsDevice _24
(#25) MainsDevice _25
(#26) MainsDevice _26
(#27) MainsDevice _27
(#28) MainsDevice _28
(#29) MainsDevice _29
(#30) MainsDevice _30
(#33) MainsDevice _33
(#34) MainsDevice _34
(#35) MainsDevice _35
(#36) MainsDevice _36
(#37) MainsDevice _37

✖ Cancel   O Add

The device you wish to be associated with (in this example) Node 32 can be selected from the

list, and then click the O Add button to have the CIT set the association. Click the

✖ Cancel button if you decide you do not want the association.

- In each association group listed, the information at the top of the group shows how many nodes may be added to the association group, along with the date that the association information was last updated from the device.

- If you wish to remove an association, find the device listed under the association group that you want the device association removed from, and click the red X button at the end of the device

which appears like the example to the left.
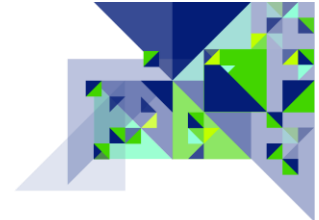
Link health

The Link health tab shows you the strength of the link from the node selected at the top of the page, to each of the other nodes in the network. It is not necessary to know the link health between every node in the network, but this is useful if there is a reason for two nodes to directly communicate (e.g. associations) or if you are trying to track down a failure point in the network and need to examine the link quality between certain nodes. The result shown under the Link quality column will be a circle with a color code indicating at a granular level, the quality of the link between the two nodes. If the link quality has never been measured for the selected node, then there will be no entries under the Link quality column or the Date column. Here is what the link quality page looks like:

- At the bottom of the page, you will find a key to understanding the color coding of the squares in the **Link to node** column:
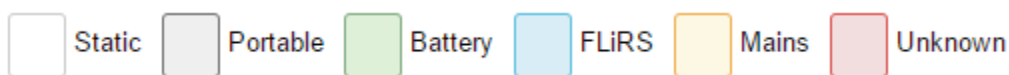
  as this key demonstrates, the color of the square indicates the type of device that it is, allowing for the node number and the device type to be identified together.
- The **Device name** column shows the name of the device.
- The **Device type** column provides another symbol representing the type of device using the icons as explained in the Status page.

- The **Date** column shows the date of the last time the link was tested between the node at the top of the page and the node in the row that the date appears. If there is no date showing, then the test has not been run. If the date is the same as today's date, only the time will be shown. If the date appears in RED, then the date shows the previous date of a test and it indicates that another test has been called for, and the color will return to BLACK once the new test is finished.

- The **Link quality** column shows a circle colored to indicate the quality of the link if it has been tested.

  - ⚫ - Indicates a test that is running on that node or one that did not complete successfully so the link quality is unknown.

  - 🔴 - Indicates a poor link quality or an inability for the CIT to communicate with the device. (Battery operated sleeping devices will return a red circle result if they were not forced awake prior to the test.)

  - 🟢 - Indicates a good quality link between the two nodes.

- The heading for the last column is the **Test all links** button. Clicking this button will cause the CIT to test the link quality from the node selected at the top of the page to each of the other nodes in the network. This will generate considerable Z-Wave traffic and may take several minutes to complete depending upon the size of the network; consider testing individual links instead. Under that button in each row representing the other nodes in the network is a **Test link** button which when clicked, will perform the link test for the link between the node selected at the top of the page and the node shown at the beginning of the row for the Test link button that was clicked.

Expert commands

This page presents a dialog for doing operations on the command classes present in the device selected at the top of the page. As the name implies, use of these should be for experts who have a familiarity with the Z-Wave Application Layer. Some of the functions available here are duplicated from the Configuration and Association tabs. If the Node Information Frame (NIF) has not been
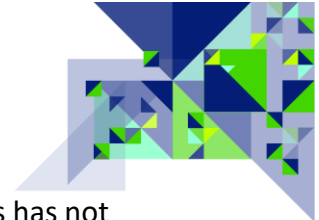
retrieved from the device, no commands will appear on this page. If the interview process has not been completed, only commands for the command classes that have been completed by the interview process will appear. The screen is similar to that of the configuration screen explained earlier – here is a sample:

Using the Switch All command class as an example, you can see the status of the last time the CIT was used to retrieve data for this command class from the device:

Under the heading of the command class (SwitchAll) we see the line with 3 parts to it – in this case the word "mode", the value 255, and the time of 03:03 PM. For this command class, it refers to the Switch All mode having been retrieved at 3:03 PM and at that time had the value 255. In the Mode section shown on the screen, we can see that 255 indicates that the device participates in both Switch All On and Switch All Off commands.

As use of the application layer command classes is mostly beyond the scope of the CIT, no further examples or information is provided here on additional command class expert commands.

Firmware update

If the device chosen at the top of the page supports over-the-air firmware updating, then this tool page can be used to start an update of the firmware on the chosen device. To do an Over-The-Air (OTA) firmware update, you will need the firmware file from the manufacturer to be loaded onto your client device that you are using to connect to the CIT user interface. For best results, all traffic on the Z-Wave network should be reduced as much as possible. If the selected device supports Firmware Updating

OTA, here is what the screen will look like:

The first drop-down box allows you to select whether the firmware update is for the Z-Wave chip, or for an Additional (secondary) chip/SoC in the device. The Z-Wave chip is selected by default as firmware updating of an additional chip is extremely rare. The next drop-down list allows you to select the **firmware update source** – by default a local file will be used; the CIT will look for files with common extensions such as .hex, .bin, or .ota. Click on the **Choose File** button to browse your client computer for the firmware file from the manufacturer. The CIT will look for files with common extensions such as .hex, .bin, or .ota.

In some cases, the manufacturer may choose to host the firmware file on their server and provide to you a URL for the CIT to download the firmware file from and then start the firmware update. To use this feature, the CIT will be required to have Internet connectivity via its Ethernet port. You may change to this mode by clicking on the **firmware update source** drop down list, and choosing the URL option. When the URL option is chosen, the firmware update screen will change and appear in this way:

When in this mode, enter the URL to the location of the firmware update file in the Firmware URL box.

Whether you use File mode or URL mode, click the [Update] button to begin the firmware update process. Depending upon the size of the firmware file and the amount of Z-Wave traffic in the network, the update could take anywhere from a few minutes to 10 minutes or more.

Active associations

The Active associations page provides one place to list all of the associations that have been retrieved from the nodes in the network during the interview process. On this page a comprehensive view of all of the associations can be seen. If all of the associations have been retrieved from the nodes in the network, then this screen is a good diagnostic tool for finding orphaned nodes.

> *Example: Let's say node 51 has an association set up to node 20. At some point, the device at node 20 is upgraded to a newer device that has more features, and the new node number is now 60. Removing a node from the network does not update associations. Therefore, each time the event occurs at node 51 that causes it to send a Z-Wave signal to the nodes in one of its association groups, it will attempt to communicate with node 20 which no longer exists. This communication could cause node 51 to use the Explorer Frame, which has a large network overhead and will cause a significant and noticeable delay before node 51 moves on to the next node in the list and sends the command to that node.*
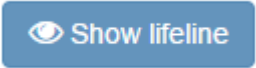
Here is what the Active Associations page looks like:

- The first column (#) and the second column (**Device name**) show the node number and device name respectively.
- The next column, titled "**Assoc group name**" lists the name of the association group if it is a Z-Wave Plus device, or it will list "Association Group" followed by the association group number. If there is more than one node in the first association group (Group 1) then this group will be shown, but normally in this mode, the Lifeline group (Group 1) associations are not shown.

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200
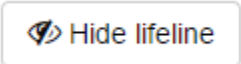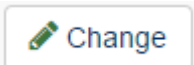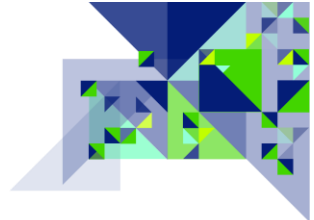
They are filtered out of the screen to make it easier to view OTHER associations because in most cases, a device supporting association will have an association on group 1 to the primary controller. Under the name of the association group is the list of nodes – along with their device name – which are associated to the node shown at the beginning of the row on the indicated association group.

- The last column is headed by the **👁 Show lifeline** Show lifeline button. If this button is clicked, it will toggle the functionality of hiding the Lifeline group associations and it will list all associations. Here is a sample:

As you can see, nodes 3 and 5 which were not previously shown now appear, because the only association they had on their Lifeline (Group 1) association group was with the primary controller at Node 1. To return to filtering out the lifeline associations, click the

👁 Hide lifeline Hide lifeline button which now appears where the Show lifeline button used to be.   Clicking on any of the **✏ Change** Change buttons will lead the UI to the Device Configuration screen for the node, Associations tab, where the associations can be changed.

Network ![Network]

The Network menu option allows you to access information pertaining to the entire network, or items affecting multiple nodes. Here are the menu options under Network:

Control

Neighbors

Timing Info

Network map

Link Status

Control

The Control page provides access to controller functions. The CIT is being fully certified as a gateway controller and as such has the ability to carry out all of the required network commands. For normal diagnostic purposes, the functions on this page are not used. Here are the features of this page – you may click on the areas of the image below to jump to the documentation for that field:
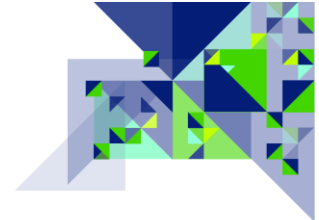
Control

👥 Device Management

Force unsecure inclusion [🔒 Secure] [🔓 Unsecure]

Controller is primary in the network. It is the only that can add and remove devices to/from the network.

Controller is in normal mode

[▶ Start Inclusion] [▶ Start Exclusion]

⚓ Enter / Leave different Networks

Start the exclusion mode on the customer's primary controller and click the button below.

[▶ Leave network]

⚙ Controller Maintenance

This button resets the serial communication between the controller software and the Z-Wave transceiver firmware. Its save to use

[⟳ Reset API]

Handle with extreme care. This function will reset the Certified Installer Toolkit to a factory default state. If the CIT is a part of a customer network, it will transmit a Device Reset Locally command to notify the customer's primary controller that it is leaving the network. Please use the customer's controller to exclude this device from the network under normal circumstances instead of using this command.

[⚠ Controller Factory Default]

🗂 Background zNiffer Collection

[ON] [OFF]

ℹ Controller Info

⚓ Network Maintenance

Pick the failed node from the list and remove it from the network configuration. This will take about one minute to complete.

[▼] [⊖ Remove Failed Node]

Pick a node of a failed device. After hitting the button you can include a new device right with this Node ID.

[▼] [⇄ Replace failed node]

Mains powered nodes are marked as failed automatically. Battery powered device you need to mark yourself in order to remove or replace them. Handle with care.

[▼] [⚑ Mark Battery Device as failed]

This functions run over all existing nodes and asked for a NIF. You can also call a NIF for each individual device using the [configuration tab]

[🔍 Call NIF from all devices]

📢 SUC/SIS management

[◯ Get SUC node Id] [◯ Request network updates from SUC/SIS]

[◯ Assign SUC] [◯ Assign SIS] [◯ Disable SUC/SIS]

on node [168 ▼]

Device Management Section

This section controls how devices are included to a network or excluded from a network by the CIT.

- *Force unsecure inclusion:*
  When a device is included into a Z-Wave network and it supports security through the Security

Command Class (S0) or Security 2 Command Class (S2), the security exchange will normally be done to include the node securely into the network. The Secure/Unsecure buttons can be used to set the next inclusion to not include a node securely, even if it supports security. In situations where Security S0 is available but not required, such as with a lamp module, including the node non-securely can speed up communication with the device. For items which require security to operate like door locks and garage door openers, including them without security will make them inoperable by any device in the network. To set the next inclusion to be done without security, click the Unsecure button. Click the Secure button to set the next inclusion to do security key negotiation to add the node securely to the network.

- *Start Inclusion / Start Exclusion:*
  If the CIT was not added to any network and is a standalone controller, or if the CIT was successfully added to a network with a SIS and was added as a Secondary Inclusion Controller, then these buttons will be enabled allowing the CIT to add or remove nodes to the network. Click the Start Inclusion button to include a new node to the network that the CIT is currently a part of, or click the Start Exclusion button to exclude a node from whatever network it is a part of. (Any controller can be used to exclude a node from a network.)

Enter / Leave different Networks Section

This section allows you to join or remove the CIT from another Z-Wave network such as a customer's Z-Wave network being diagnosed or repaired.

- *Join Network / Leave Network:*
  The functionality here is identical to what is on the Home page. If the CIT is not a part of another network, the button will show "Include into Network", and clicking it when the network primary controller is in inclusion or learn mode will cause the CIT to be added to the other network. When the CIT has already been included into another network, the button will show "Leave network" and clicking it after placing the network primary controller into exclusion mode will cause the CIT to be removed from the other network.

  > *Note: The CIT should always be removed from the customer's network if it is being physically removed from the premises. Leaving the node in the customer's network will cause the customer's primary controller to send network updates to the CIT, which will delay the performance of the customer's network as it attempts to communicate with the CIT.*

Controller Maintenance Section

This section allows you to reset the controller two different ways.

- *Reset API:*

  If the Z-Wave functions by the CIT do not appear to be working, or if advised to do so by support, click the Reset API button to restart the Z-Wave part of the CIT system. This will not cause you to lose any configuration data and the reset will take only several seconds to complete.

- *Controller Factory Default:*

  Clicking the Controller Factory Default button will cause the CIT to prompt for a confirmation before the action is carried out. A factory default will reset the CIT to its factory default state which means that it will lose all nodes, it will no longer be a part of any other network, and all device names will be lost if they were not backed up first.

  > *Note: Controller Factory Default will cause a Device Reset Locally signal to be sent to the primary controller, which under normal circumstances would cause the controller to remove the CIT from the network. However, non Z-Wave Plus nodes, or issues with the network that may prevent the signal from arriving can cause the CIT's node information to remain in the network as described above. Do not rely on Controller Factory Default to remove the CIT from the customer network.*
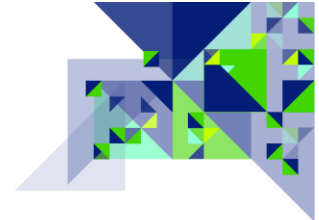
Background zNiffer Collection Section

- *On / Off:*

  The Analytics/Zniffer page only collects and shows Z-Wave frames when you are on the Zniffer page. The Analytics/Zniffer History page, however, is able to show all Z-Wave frames that were heard by the CIT while it was powered up. If you do not wish to have this information recorded, you may click on the "Off" button and background collection of Z-Wave frames will be disabled. Use the "On" button to resume background collection of Z-Wave frames for use on the Zniffer History page.

Controller Info (link)

Clicking on the link in this section will open up the Controller Info page which is described here.

Network Maintenance Section

This section provides access to network maintenance functions for working with troubled nodes in the network.

- *Remove Failed Node:*
  When a powered (normally listening) node fails and you can no longer cause it to send its Node Information Frame (NIF) so that it can be excluded from the network, you can use this selection and the accompanying button to force the removal of the node from the network. The first step is to select the node that needs to be removed from the drop down list to the left of the button. If the node you want to remove is not in this list, it may be that the node is still communicating. You can use any of the test functions of the CIT to attempt communication with the node – if the CIT is unable to communicate with the node, the node will be added to the drop down list so that it may be selected and removed. Once the node has been selected, the "Remove Failed Node" button will enable, and you can then click on it to have the CIT initiate the removal process. Wait for this process to finish before performing other network functions.

- *Replace failed node:*
  When a powered or battery operated node fails, and you can no longer cause it to send its Node Information Frame (NIF) so that it can be excluded from the network, you can use this selection and the accompanying button to facilitate the removal and replacement of the Z-Wave device with a new one, which will be given the same Node ID as the failed node. To do this, you must first make sure that the node you wish to replace can be found in the drop down list to the left of the "Replace failed node" button – if the node ID is not in the list, the device may still be functioning and communicating via Z-Wave. You can use the CIT test functions to attempt to communicate with the failed node – if the CIT is unable to communicate with the node, the node ID will be added to the drop down list. Once the node ID is in the drop down list, go ahead and physically replace the failed device with the new one, but do not include the new device into the network as you normally would – instead, click the "Replace failed node" button, and then activate inclusion on the new device. When the process is completed successfully, the new device will have the node ID of the old device, and the node ID will no longer appear in the drop down list of failed nodes.

- *Mark Battery Device as failed:*
  Since battery devices are not normally listening devices, a lack of a response to a command by a battery operated sleeping device will not cause its node ID to land in the list of failed nodes for

use with the "Remove Failed Node" or "Replace Failed Node" functions. To use this, find the node ID of the battery device you wish to mark as failed from the drop down list of battery node IDs to the left of the button. Select the battery device node ID, then click the "Mark Battery Device as Failed". The node ID you selected will now appear in the failed device list which you can use with Remove Failed Node or Replace Failed Node.

- *Call NIF from all devices:*
  This button will tell the CIT to request the Node Information Frame (NIF) from all devices in the network. If clicked, the process will make the CIT busy for potentially a very long time if the network is large. It is the same as what happens when you include the CIT to a new network and click "Detect all Nodes" because calling for the NIF can cause device interviews which were previously suspended to resume.

SUC/SIS management

Two special functions for a Z-Wave controller are when they are the Static Update Controller (SUC) and SUC ID Server (SIS). When one of the controllers in the network is assigned to be the SUC, it means that other controllers in the network can get updates about network topology (nodes that were added or removed) from the SUC. Normally, updating network information in another controller is done by initiating replication, which is started by "re-including" it into the network. When the SIS functionality is available, it allows other secondary controllers in the network to be able to add and remove nodes from the network – the SUC ID Server talks to the secondary controller to learn about nodes it has removed, or to vend it the Node ID for the next node being added to the network. Most of the time, the network primary controller will also be your SUC/SIS controller. A Z-Wave Plus controller that starts a network (is not included into another network) will always assign itself the SUC/SIS functionality. If a controller has the SIS functionality, it will also have the SUC functionality. These functions deal with these special capabilities.

- *Get SUC node Id:*
  If the Node Id of the SUC in the network changes, which is extremely rare, this button will cause the CIT to send a message requesting the Node Id of the SUC. This is necessary for the next function which is to request a network update. You can see the SUC/SIS Node Id in the Controller Info page.
- *Request network updates from SUC/SIS:*
  After adding or removing nodes from the network, or making any changes to routing and network topology on the primary controller for the network, use this function to have the CIT
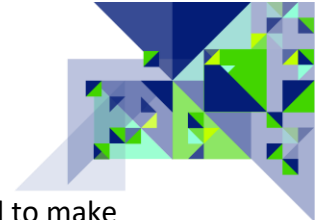
request a network update from the SUC (primary controller). When the CIT is used to make changes to the network, this function can also update the primary controller for the network.

- *Assign SUC:*

    In the unlikely event that you need to force a different node on the network to be the SUC, use this function. Use the Disable SUC/SIS function first. Choose the node you wish to be the new SUC using the "… on node" drop down list, then click the "Assign SUC" button to assign the SUC function to the selected node. This is a very uncommon procedure.

- *Assign SIS:*

    In the unlikely event that you need to force a different node on the network to be the SIS, use this function. Use the Disable SUC/SIS function first. Choose the node you wish to be the new SIS using the "… on node" drop down list, then click the "Assign SIS" button to assign the SIS function to the selected node. This is a very uncommon procedure.

- *Disable SUC/SIS:*

    In the unlikely event that you need to disable the SUC/SIS functionality before assigning a new node to be SUC and/or SIS, use this function. Choose the node you wish to disable the SUC/SIS capability on using the "… on node" drop down list, then click the "Disable SUC/SIS" button to remove those functions from the selected node. This is a very uncommon procedure.
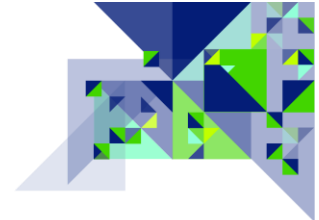
- *… on node:*

    When using the above three SUC/SIS management functions, this drop down list allows you to select the affected node Id. Only controllers in the network capable of being SUC/SIS will be listed.

Controller Info

The controller information page is accessed from the Network / Control area. The controller information page provides another way to get to the controller Job Queue in addition to the one in the main menu, but has no other functions; it is informational only.

Here is a sample of the controller information page:

Controller Info

🔍 View Job Queue	*The inspect queue will open a second window to allow monitoring the commands sent out by this controller.*

Role in Network

Node Id:	168
Home Id:	Other network
Primary Role:	Yes
Primary Capability:	No
SUC/SIS in network:	1 (SIS)

Hardware

Vendor:	Z-Wave Alliance
Vendors Product ID:	0001 / 0001
Z-Wave Chip:	ZW0500

Firmware

Library Type:	Static Controller
SDK Version:	6.71.00
Serial API Version:	05.20

Software Information

Version number:	v2.3.5-rc11-1-gd6ff1d9
Compile-ID:	d6ff1d9d39a164b8d34f7ad988d3141042ae03ff
Compile-Date:	2017-06-23 17:39:03 +0300

UI

UI version	1.3.0-RC-111
Built date	23-06-2017 16:06:50

Operating frequency

Current frequency	US

Of note on this page:

- Role in Network – This will confirm that your CIT has been included into another network (Home Id: Other network), and will list the Node Id of the customer's SUC/SIS in the network if that functionality is provided (SUC/SIS in network: 1 (SIS)). Networks based upon Z-Wave Plus controllers should at least have a SIS in the network.
- Software Information and UI – These sections should be provided to support if requested, as they provide detailed information about your CIT software environment.
- Operating frequency – Use this area to confirm your Z-Wave frequency setting in the event that you work in multiple countries using different settings.

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200
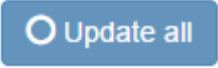
Neighbors

The Neighbors page shows you the relationship of each node in the network to each other node in the network by indicating information about the route that would be used for them to communicate. Here is a sample of this page:
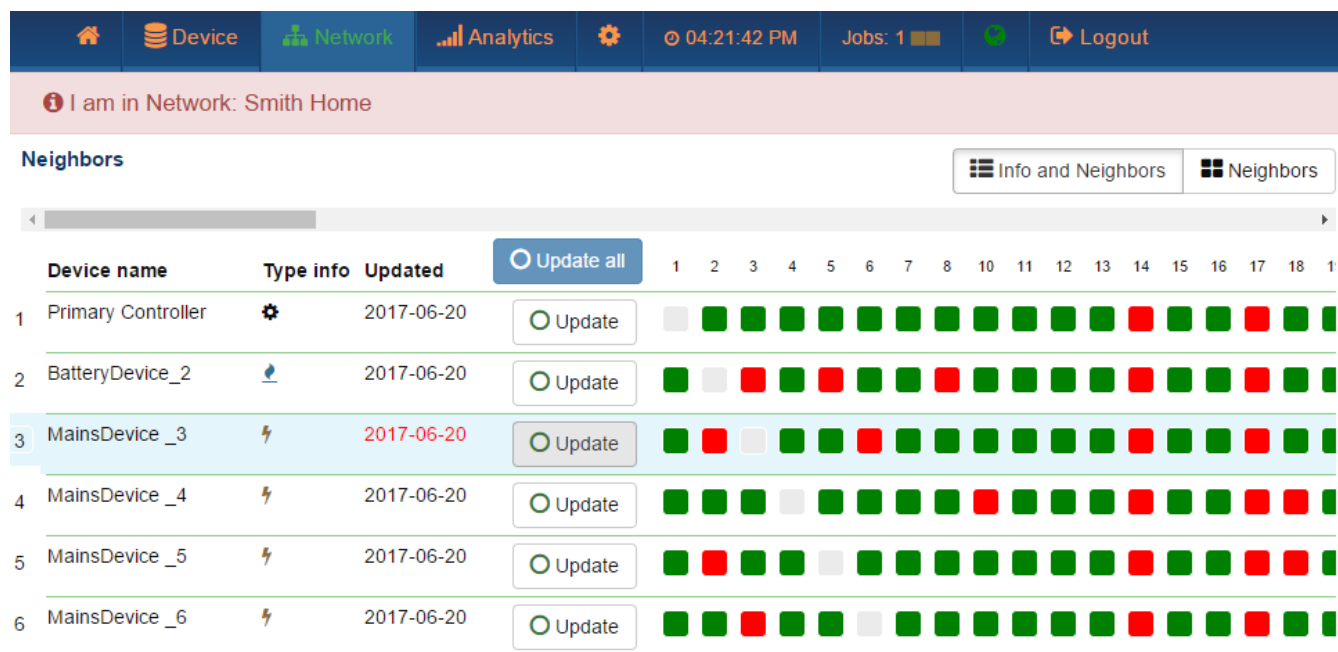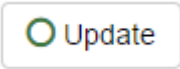
Nodes do not communicate with themselves, and so the series of gray squares running diagonally from top to bottom, left to right represent intersections of the same node number. To read any other neighbor relationship, pick a node along the left hand side of the chart, and then move along that row to your right until you are under the column numbered for the node that you wish to check the neighbor status. The neighbor status is indicated by color using the chart at the bottom of the page. The possible values are ▉ In the Range or ▉ Not in the Range as indicated by green or red. Being "in the range" indicates that the two nodes are within range (distance) for direct communication with each other. Here are the other columns and functions on this page:

- **Device name** – The device name, with the node Id of the device being shown to the left of the device name.
- **Type info** – This is the icon representing the different types of devices as explained here.
- **Updated** – This column shows the last date the neighbor information was retrieved for the node indicated at the beginning of the row. If the time of the last update was within the current day, the time is shown instead. When the time is shown in RED, it indicates that the value is being updated, or that a request to update the value recently has failed.

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200

- The **Update all** button at the top of the page is used to force the CIT to have all nodes in the network do a Node Neighbor Update. The results are then updated in the Network / Neighbors page (a browser page refresh may be needed to get the latest information).

    > *Important Note: Doing a neighbor update causes each node to re-discover the other non-battery powered nodes that are within direct range. The results are used by controllers to determine the routes that will be used for nodes to communicate. The controller being updated with the updated information in this case is the CIT, not the customer's primary controller. Having the nodes re-discover their neighbors is still beneficial after performing work on the nodes to improve the network, but once the neighbor updates have been completed, a Node Neighbor Update (sometimes called "Network Repair" or "Optimize") should be done on the customer's controller so that the latest neighbor information will be uploaded to the controller running the network.*

- To avoid a significant amount of time in updating the neighbor information, especially on a large Z-Wave network, consider using the individual **Update** buttons in each node row on the neighbor page. If a change has been made to one node in the network, performing an update of the nodes around it can save a significant amount of technician time.

- At the top of the Neighbor page, there are two more buttons which act as a toggle against each other:

    The **Info and Neighbors** button causes the default display shown upon entering the page. The **Neighbors** button will eliminate the information and Update buttons to allow for the maximum amount of the neighbor table to be visible. Use the scroll bars at the top or bottom of the page to move the table display right or left as needed.

Timing Info

The timing info page is useful for seeing, at a glance, which nodes are using multiple hops to communicate because their time for a transmission is long. Long transmission times can also indicate

other network problems. Here is a sample of the page:

- Node – This is the node Id of the device.
- Device name – This is the name of the device.
- Type – This is the icon representing the type of device that the node is on the network as explained here.
- Date – This is the date (time if it is within the same day) that the CIT last communicated with the node.
- Total (pkts) – This shows the total number of Z-Wave frames (packets) sent and acknowledged since the CIT was last started or restarted.
- Ok – This shows the percentage of packets acknowledged successfully.
- Last packets (in 10 ms units) – This shows the time that the round trip communication took, from the CIT sending the packet to the time the CIT received an acknowledgement frame back from the node. The unit is 10ms increments, so a value of 33 for example is 330 ms or about 1/3 of a second. Transmission times are shown in one of three different colors according to this legend which is found at the bottom of the page:

Decoding the color values of the response time of the device

🟩 The response time is not beyond the allowable range

⬛ Controller was not able to reach the given node with 3 attempts and tried a different route that finally worked

🟥 The communication finally failed after some re-routing attempts
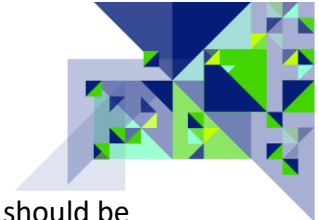
Note: Occasional failures (RED numbers) may be a sign of network congestion, but should be investigated as this means that all other attempts to route the frame to the node have failed. Frequent occurrences of RED values may be an indication of noise, with the source being near the node that frequently experiences failed transmissions. When all of the transmission time values are RED, that is an indication of a failed node, or one that has been orphaned in the network and has no other nodes as neighbors. Battery operated nodes that normally sleep will not have any transmission attempts because the CIT will not try to contact a battery sleeping node unless it knows it is awake.

- The **O Update** Update button in the top right corner of the page can be used to load the latest values without having to refresh the web browser page.

Network Map

The network map page is a graphical representation of the same information on the Neighbors page. It is useful for determining – at a very quick glance – how well the network is meshed for any given node. The nodes are displayed according to the number of connections that they hold when you initially enter the page, so note that the nodes in the same row may appear to only have a connection to one another left and right. Here is a sample:
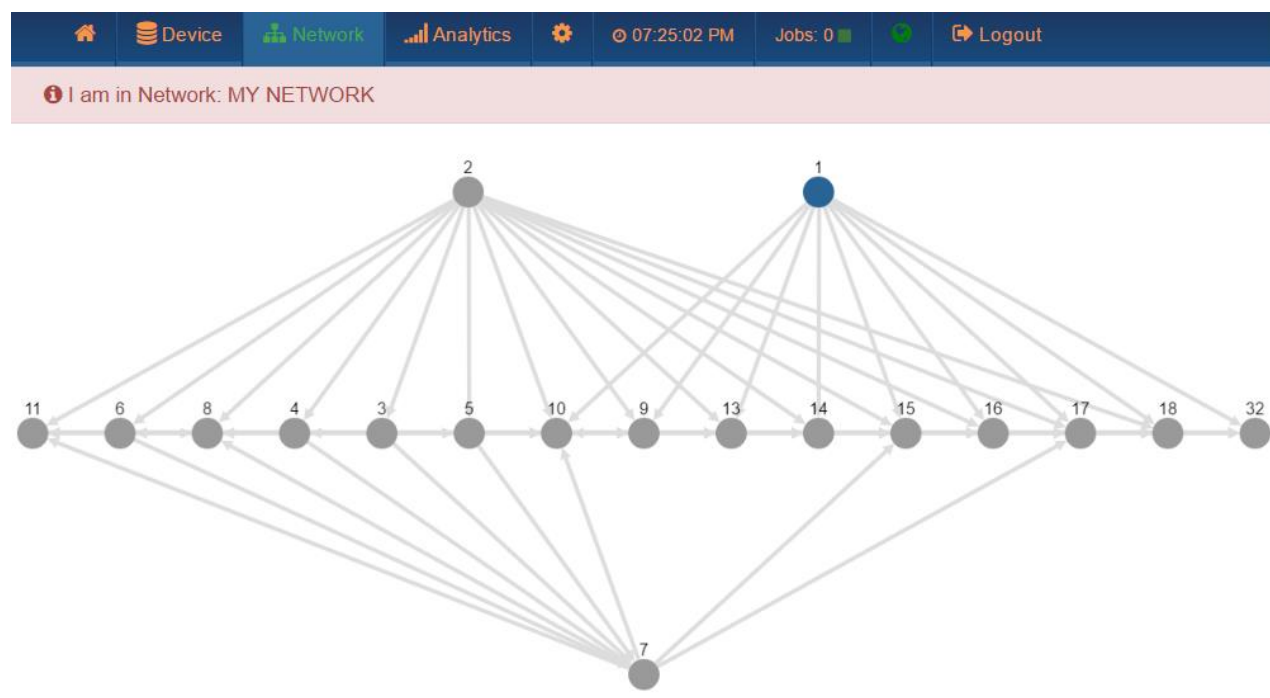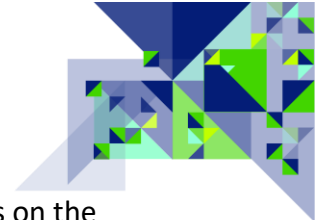
To see a specific node more closely, grab a hold of it and pull it away from the other nodes on the screen – here is how to do this: Using your pointing device, click on a node and hold it while you drag it to another portion of the screen; this will then highlight the true connections that the node has to other nodes in the network. Here is the same network map with Node 4 drawn out to show its links more clearly.
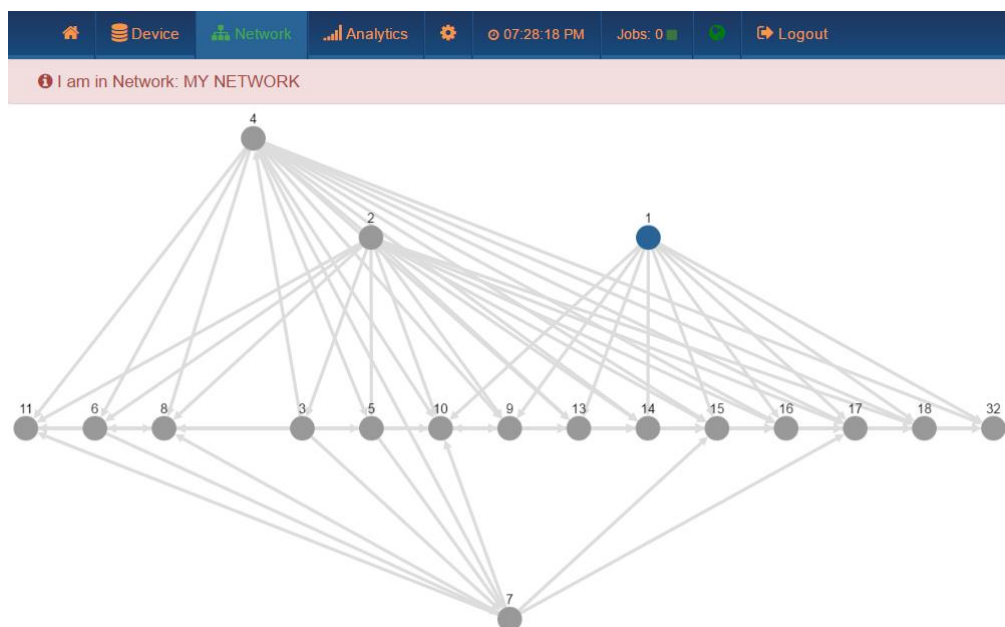
We can now see that node 4 is indeed well connected to other nodes in the network.

You can also use the scroll wheel of your pointing device (if so equipped) to zoom in and out of the network map to examine connections more closely. Here we have zoomed in to Node 4 which we pulled out earlier.
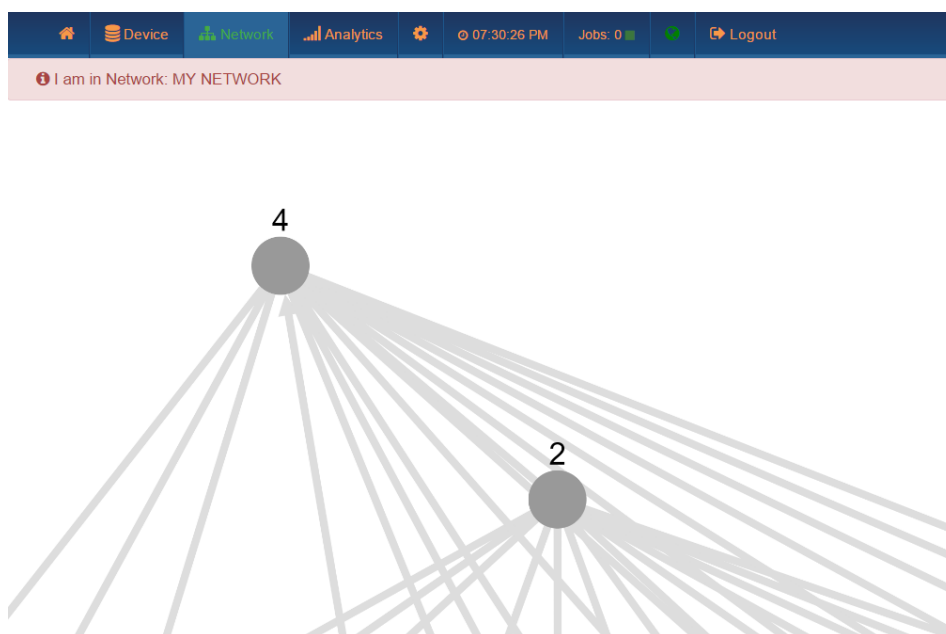
The layout of the nodes on the page is not saved. The network primary controller or SIS is indicated with a blue circle.

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA   ●   +1 510.897.0200

Link Status

The link status page is an indicator and test for the specific quality of the link between two nodes. The link quality is only shown for nodes which are neighbors to each other, the remaining nodes are grayed out. Here is what the screen looks like if no link tests have been performed:

- **Device name** – This is the name of the device, and the corresponding Node Id is displayed to the left of the device name.

- **Device type** – This is the icon representation of the type of node that it is in the network.

- Updated – This is the date, or time if it is within the same day, that the link status information was last updated for the node or if a link status test was never done, it will display the date or time when the neighbor information was last updated.

- The **Test link** button in each row can be used to tell the CIT to perform a link status test on that node. A more comprehensive link status test can be done between two Z-Wave Plus nodes. If a node supports the appropriate command classes to form a test, the Test link button is shown. If the node is an older node or communication has made the CIT unable to determine whether it can do more in-depth tests, then the **NOP** (No Operation) button will be shown instead. NOP will not determine the signal strength and actual quality of

the link, but it will use the round trip timing, and received signal strength, to try to determine the relative quality of the link. After performing link status testing, the display will update and provide you with information on the link status. Just like in the Network / Neighbors page, the node ID in the start of the row on the left can be matched up with node IDs printed along the top and bottom of the display to see the link status between individual nodes. Here is an example:

The legend indicating what the colored squares mean is at the bottom of the page:

Note: A "Poor" link status only needs to be addressed if there is A) a specific reason the two nodes need to communicate, such as an Association that exists between them, or B) if the nodes are used as part of a route for the same reason and there are no other direct links available.

Analytics

The menu items on the analytics tab are used to perform deeper analysis of what is going on in the network in terms of the Z-Wave RF signals, and the Application Layer Frames of data. Here are the menu options under Analytics, click on one of the menu options to jump to that section:

- Zniffer
- Background Noise
- Noise Meter
- Zniffer History
- Statistics
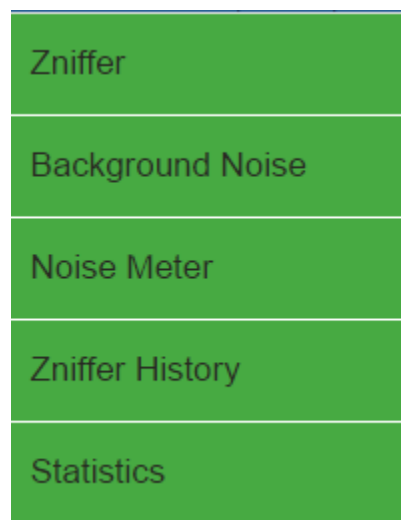
Zniffer

"Zniffer" is the name of a popular Z-Wave Software Development Kit (SDK) diagnostic tool by Sigma Designs; it is a shortened form of Z-Wave Packet Sniffer. Zniffer displays the partially decoded Z-Wave frames so that you can see the actual command class and command that was sent or received. In this version of Zniffer, the CIT is using an eavesdropping mode of the Z-Wave library, which means that it only displays frames heard for its own network, and does not show certain special Z-Wave frames such as the "Beaming" signal that FLiRS devices use and the protocol messages exchanged during network events such as inclusion, exclusion, replication, etc. It is very useful when you have confirmed that the network has a robust health, but perhaps a node is still not reacting to the receipt of a transmission from another node as the customer is expecting. For example, when an association is set up between a dimmer switch and a controller, the dimmer switch – upon being turned on locally – may send a BASIC REPORT command when the receiving controller may have been expecting a SWITCH MULTILEVEL REPORT. These types of signaling issues are normally handled by an integrator with additional knowledge regarding the application layer of Z-Wave. For the installer or integrator, Zniffer is a great tool for determining that nodes are communicating at the application level.

At the top of the zNiffer screen are Play, Pause, and Stop controls:

 When you first enter the zNiffer screen the **Play** control (first button) should be started automatically. zNiffer will not "capture" any new frames for display unless it is in the play mode. To pause the display, use the **Pause** button (the middle button); frames will continue to be captured, but they will not be displayed. Clicking the **Stop** button (the third button) will stop the capture of frames and the display of new frames. Here is what the zNiffer screen looks like after capturing some frames:

- The first column, to the left of the Date column, is an arrow indicating the **direction** of the frame; whether the frame was sent by the CIT (outgoing - arrow pointing left) or was received by the CIT (incoming – arrow pointing right). You can hover your pointing device over the arrow to see whether it is incoming or outgoing as well.
- **Date** – It is here that the date the frame was sent or received is shown.
- **Time** – The time that the frame was sent or received is shown here.
- **SRC & DEST** – These are short forms of SOURCE and DESTINATION, and both of these columns are preceded by a funnel (▼) icon indicating that they are capable of filtering. These columns indicate the Z-Wave node ID that sent the transmission (source) and where the transmission

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA   ●   +1 510.897.0200

was being sent (destination). If you are working with a specific node or nodes, and you only

want to see traffic to/from that node or nodes, click on the funnel icon to configure a filter:

Here, the funnel on the SRC column has been selected. To see only the frames where the source is from nodes 2 or 5, enter "2,5" (without quotes) and click the OK button. If you already have a filter in place, you can click the "**Remove filter**" button to remove the existing filter. This will only show the frames where the sending node (source) is 2 or 5, but it will still display the frames when node 2 is sending to node 7 for example, or 5 is sending to node 10. To isolate zNiffer to only show the traffic between nodes 2 and 5, configure a second filter on the DEST (destination) side using the same node numbers (2 and 5) and the result will be that only traffic between those two nodes will be shown. Here is an example of zNiffer with a filter on source node 13:
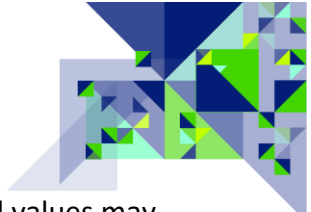
The "**Remove all filters**" button is also shown on the zNiffer screen when a filter is active; click this button to turn off the filters without having to click on the individual funnel icons.

- **Speed** – This indicates the speed that frames sent or received by the CIT were transmitted at; there are currently 3 possible values of 9.6 Kbps, 40 Kbps, and 100 Kbps. If a transmission is being routed through a node that is not capable of higher transmission speeds, a lower speed will be used. If a transmission is not routed, and the node is a newer Z-Wave Plus node capable of 100 Kbps speeds but it is still transmitted at a lower speed, this is an indicator of a possible problem that may be caused by noise or a weak link between the nodes.

- **RSSI** – This is the Received Signal Strength Indicator, a value in dBm (decibel-milliwatts) representing the relative strength (power) that the signal was sent or received with. Starting with the Z-Wave library that the CIT was built upon, Z-Wave is transmitting RSSI information back through routed transmissions as well. As this is a new feature, it will take some time
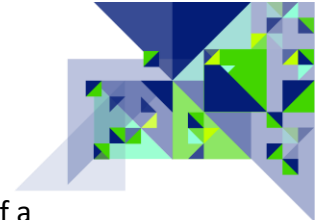
before newer Z-Wave devices are present and the RSSI is available for both parts of a transmission – the send and the acknowledgement – between each hop of a routed transmission. An RSSI value of 0 dBm indicates a perfect transmission with no measurable loss of signal strength. An RSSI value of -70 dBm or lower indicates a weak transmission. A weak transmission can be tolerated if there are no other sources of RF noise or interference in the network (see Background Noise in the next section). Transmissions in the range of -65 dBm and higher are more typical.

- **Hops** – The hops column indicates which nodes a transmission was routed through between the source and destination nodes.

- **Encaps** – Encaps is short for encapsulation. Z-Wave frames which are transmitted securely for example, are first constructed like a normal frame, and then placed inside another type of frame or frame format for transmission. In the case of a secure transmission, the actual frame is encrypted and then placed inside a security frame. The types of encapsulation and how they are indicated are as follows:

  o "I" indicates multichannel (formerly multi-**I**nstance) – Devices which have multiple copies of the same functionality – for example a Z-Wave multiple outlet strip with four outlets controlled by Z-Wave – will use multi-channel frames which include information on the "Endpoint" (which outlet in our example) the transmission is being sent or received for.

  o "M" indicates **M**ulticommand – a multi-command capable device is often a battery operated device, because multi-command allows for multiple Z-Wave frames to be encapsulated into a single transmission to save battery life. By sending multiple frames and waiting for a single ACKnowledgement, battery life can be considerably extended.

  o "S" indicates **S**ecurity – a security encapsulated frame is transmitted no differently than any other Z-Wave frame, but the contents or "payload" of the frame are encrypted.

  o "C" indicates **C**RC16 – a method of encapsulating a frame and including a Cyclical Redundancy Check (CRC) value which, when calculated at the receiving end, would indicate if the contents of the frame may have become damaged in transmission.

- **Application** – The application is the partially decoded Z-Wave Application Layer frame. In a Z-Wave frame, the first couple of pieces of data are the Command Class and the Command (within the given command class). If the Application in zNiffer says "Switch Multilevel Get()", then the command class is Switch Multilevel (a dimming light switch or module) and the command was "Get" which means the source node was asking the destination node for the

Switch Multilevel value that the device is currently set to. In some cases, additional values may be shown in parenthesis – these are the further data points from the frame and may be decoded by reading the Z-Wave Command Class Specifications. The actual application layer part of the frame is an important diagnostic tool. For example, if a controller is expecting either a Basic Report or Switch Multilevel Report when a dimmable light is changed, but the device transmits a Basic Set or Switch Multilevel Set instead, then the zNiffer page can help determine errors such as this. The CIT should be placed physically near the customer's central controller so that it "hears" the same as the customer's controller – in this type of arrangement the CIT can indicate that the frame was received (so it was likely received by the customer's controller as well) and with the information on the type of signal (application layer), technical support time with the controller manufacturer when there is an issue with the controller's response to the frame (or lack of response) is greatly reduced.

Background Noise

Z-Wave devices may select from one of two RF channels to transmit information. If a Z-Wave device is sending at the 9.6Kbps or 40Kbps rates, it is using Channel 1. If the device is sending at the 100Kbps rate, it is using Channel 2. The background noise page shows the effects of RF noise and how it may

affect your Z-Wave network. Here is a sample:

Channel 1

Channel 2
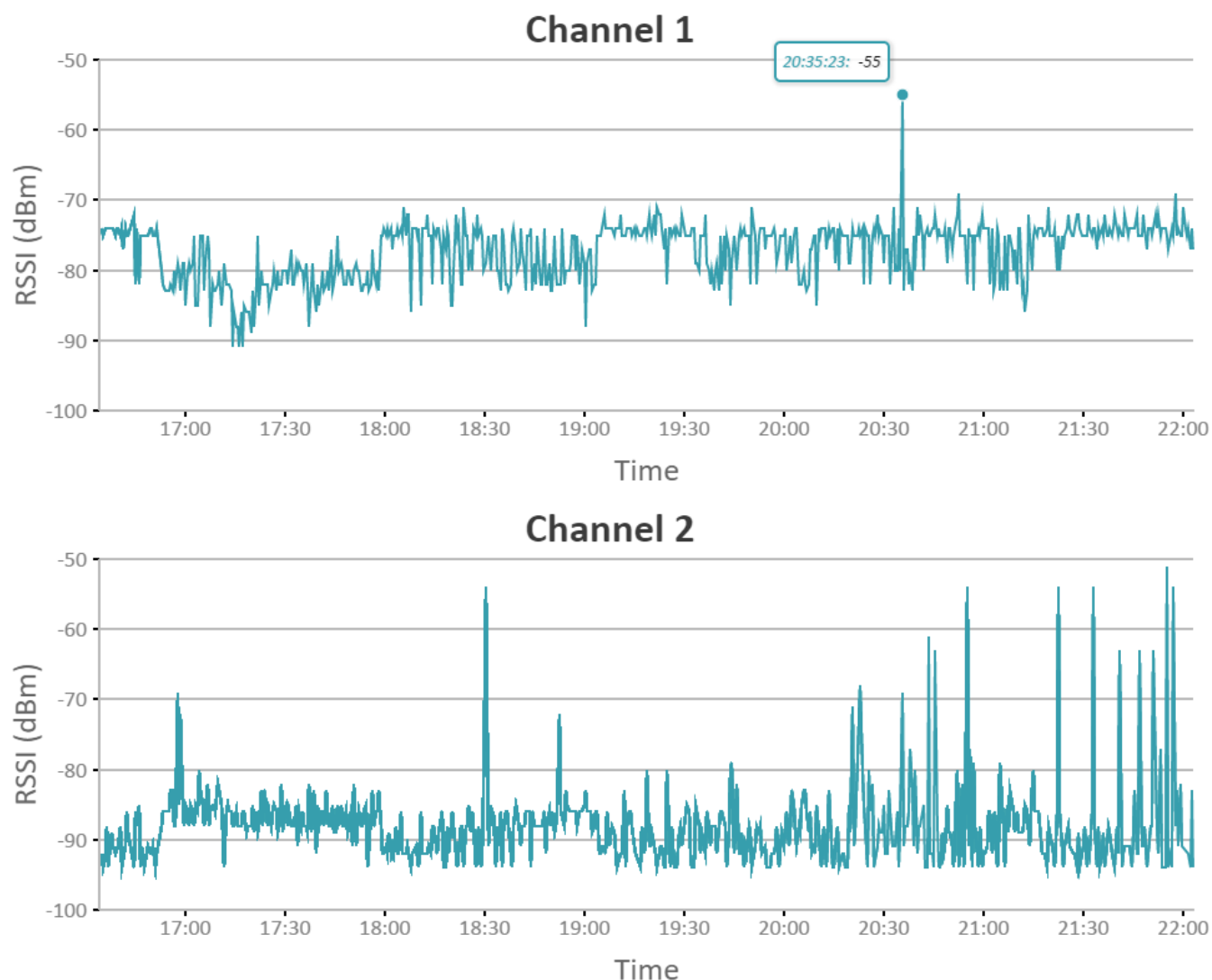
The information to be retrieved from this page is the "Noise Floor", which is the typical level of noise in the location where the CIT has been installed. In the case of the CIT being placed physically near the central controller, the CIT can measure the noise floor at the controller. If you were to draw a line across these two graphs (which will be done for you in a future release) at the point at which it is darkest – eliminating the spikes that go higher – this is your noise floor. In the above example, there is no measurable noise floor as the graph is entirely made up of "spikes" or Z-Wave transmissions. If for example there was a solid mass below the spikes, the level of this solid colored area would be the noise floor. If you have a lot of spikes around this level, indicating a noise floor near your Z-Wave transmission levels, then you have a very noisy RF environment for Z-Wave and steps should be taken to try to reduce the cause of the noise. The noise floor, once established, will help you examine transmissions subject to difficulties because of noise on the Zniffer and Zniffer History pages. On the

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200
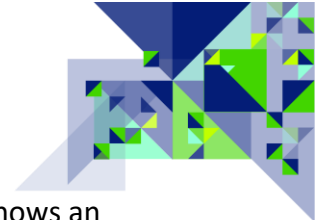
zNiffer pages, if transmissions are being received at -75 dBm, and the Background Noise shows an almost solid line (instead of spikes) at the -75 dBm level, then transmissions at that level are more than likely to fail than to succeed. It is preferred to have a "noise floor" of -80 dBm or lower.

Using your pointing device, you may hover over points along the graph to see the precise measurement and time of any point in the graph. In the example above, the pointer is hovering over a data point showing the time it was measured being at 20:35:23 with a measured value of -55 dBm (a Z-Wave transmission).

Noise Meter

The noise meter examines the RF traffic in the Z-Wave frequency spectrum for each channel that Z-Wave uses. (Channel 1 for 9600bps and 40Kbps, Channel 2 for 100Kbps) Upon first entering the Noise Meter page, the meter will not be active. Using the controls at the top left corner of the page (and shown here) ▶ ‖ click on the Play control (first button) to start the meters "listening". Click the second button (Pause) to suspend the meter's measurements. Here is a sample of the Noise Meters in use measuring the noise:
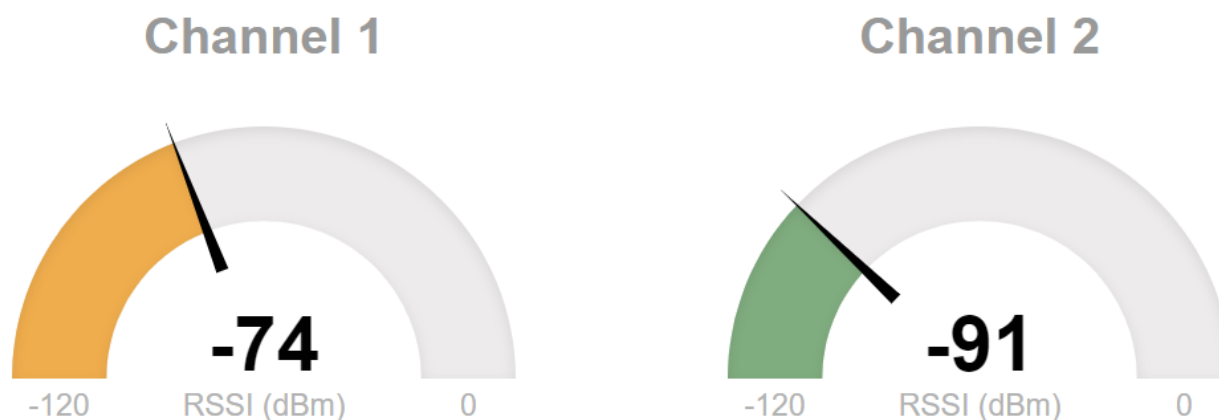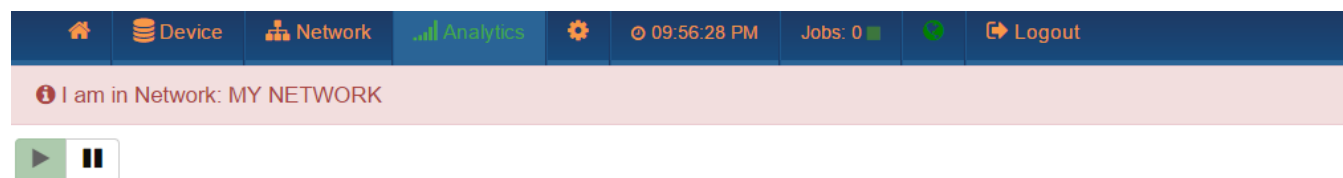
When the noise or activity is sufficiently low, the meter will show green. When there is RF traffic on these channels, the levels may turn yellow-orange or red. It is normal to see the meter go yellow-orange or red for normal Z-Wave transmissions, but long, sustained periods of being yellow or red
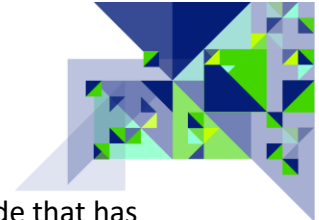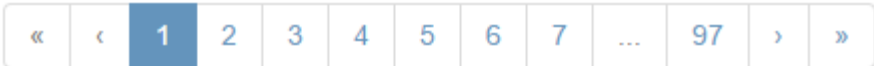
indicate a potential source of noise on that frequency other than Z-Wave, or a Z-Wave node that has gone bad and is transmitting too much.

How to Use the Noise Meters

The noise meters are ineffective when the CIT is placed near the primary controller and the source of noise is elsewhere in the network – noise is frequently strongest nearest its source which may not always be near the primary controller. If the Timing Info screen is providing a clue as to a location where noise may be occurring, go mobile! The CIT uses a micro-USB power adapter, which is the same provided by mobile battery packs for smart phones and tablets. Using one of these, power your CIT and connect to the user interface of the CIT via its built-in WiFi access point. (Consult your Quick Start guide for more help in connecting via WiFi) You may now enable the Noise Meters and move to the area in the dwelling where the devices that experienced noise are located. As you get closer to the source of the noise, the meters will react with a higher noise value and red indicators. Remember that in multi-family buildings such as apartments and condominiums, the source of noise may be in a neighboring unit.

Zniffer History

Zniffer history is the same as the Zniffer page, but the collection of frames never stops unless it is turned off in the Background zNiffer Collection settings of the Network / Control page. All of the frames that have been collected by the CIT are available here. The page will show the most recent frames, and using the navigation buttons at the bottom of the screen, you can navigate through the pages of frames to find what you are looking for. Here is an example of the zNiffer History page navigation menu: « ‹ 1 2 3 4 5 6 7 … 97 › »   In this example, we are on page 1 of 97 pages. The < button will go back one page, the > button will go forward one page, << will go to the first page, and >> will go to the last page.

Statistics

Statistics is a new feature and as such, is being further developed. The Statistics page conveys information about Z-Wave frames transmitted on the network that it is a part of. Here is a sample:
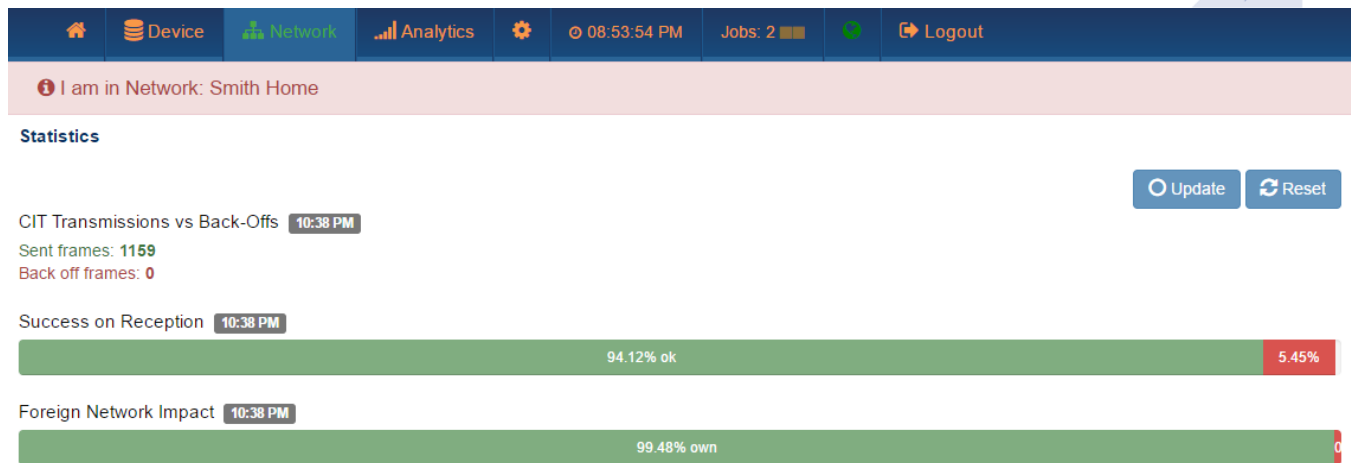
The information displayed is the result of data collected over time by the CIT. Two operational buttons in the upper right corner of the CIT, (Update and Reset) allow you to update the display with the latest information collected (click the Update button) without having to refresh the browser window, and the Reset button will reset all statistics to zero and will begin collecting statistical data again. The information presented on this page includes:

- **CIT Transmissions vs Back-Offs**
  A "Back-Off" is a condition where two or more Z-Wave nodes attempt to transmit at the same time in the same channel. This would result in corrupted frames, so Z-Wave devices detect when this happens and both go into a "back-off" mode; they each wait a random small amount of time and attempt their transmission again. This is very similar to the CSMA/CD method used in an Ethernet network. The presence of a lot of back-offs can indicate that there are too many Z-Wave transmissions occurring, and it could be impacting the performance of the network. If the Z-Wave transmissions are originating from the network in the homeowner's residence, then nodes that do unsolicited transmissions should be checked to see if they are configured to send updates too frequently. However, Z-Wave transmissions among different networks use the same channels, so the source of the transmissions may be from another network (see Foreign Network Impact below). It is common to have some back-offs in a Z-Wave system.

- **Success on Reception**
  This information is represented graphically as a measure of the number of successful transmissions received versus transmissions received with errors. Obviously, it is good to have a low number of failures (the red area) but it is normal to have some amount of errored receptions. If you click on the bar graph itself, it will expand to show the data that underlies the bar itself as in this example:

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA ● +1 510.897.0200

Success on Reception 10:38 PM

94.12% ok | 5.45%

Success on Reception: **3439**
CRC errors: **199**
CRC16 errors: **16**

Here we see that out of 3,654 total receptions, 199 had CRC errors and 16 had CRC16 errors; the error receptions made up 5.45% of the total receptions.

- **Foreign Network Impact**

  If your network is experiencing a high number of back-offs as shown in the first statistic, the source of the additional transmissions may be from a neighbor's Z-Wave network. The Foreign Network Impact statistic can help you figure this out. Because each Z-Wave network has a unique identifier of its primary controller, the CIT can examine this and determine when transmissions are from a different network. This graph shows the percentage of transmissions of the network that the CIT is on against transmissions of any other network. If you click on the bar graph, you can see the data behind the chart as in this example:

Foreign Network Impact 10:38 PM

99.48% own

Own Frames: **3439**
Foreign Frames: **18**

In this case, there were 3,439 transmissions on the CIT's network and 18 from another network.

FIND SERVICE

When the CIT boots up and has an Ethernet connection, it will get its IP address from a DHCP (Dynamic Host Configuration Protocol) Server on the network it is on. The CIT will also use DHCP in itself to create a network on its WiFi interface so that it can be connected to using a client device. In these cases, the IP address that was vended by the customer equipment and the CIT are not known, so it is not easy to connect to it without knowing its IP address. Furthermore, if the CIT has Internet access, connecting to it meant putting an entry in the router for the network that would re-direct requests for the CIT to the IP address that it was vended. The CIT's Find Service which is included with the CIT solves all of these problems!

The Find Service will look on the local network for CIT unit(s) and will present the IP addresses with links so that you can quickly and easily connect to it. If the CIT has internet access, then it also notifies the Find Service server and opens a connection so that you may connect to the CIT remotely without having to configure any routers.
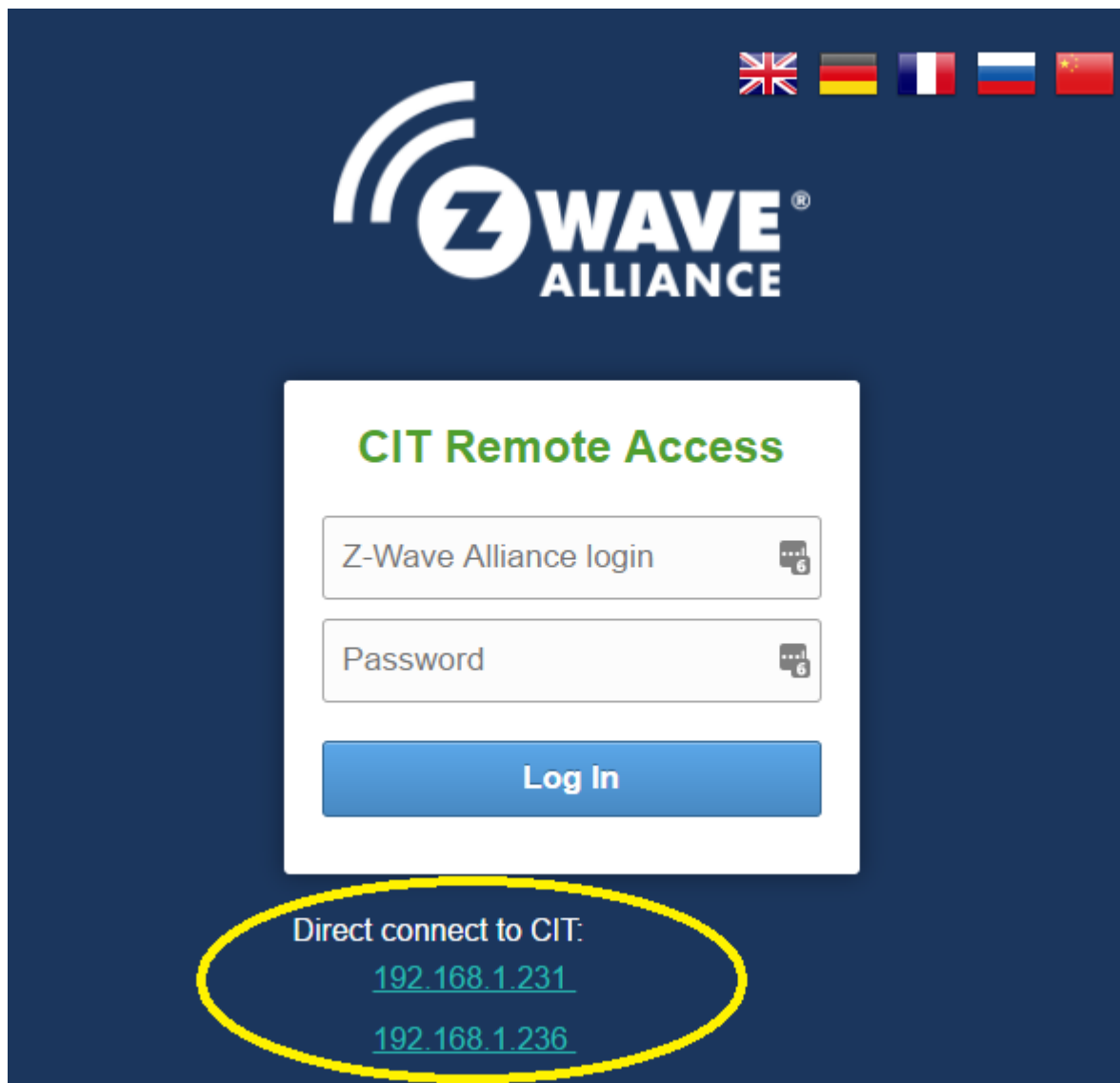
Much of how to use the Find Service is covered in the Getting Started Guide that came with your CIT. This section explains the remote access capabilities.

Connecting Remotely

As explained in the Quick Start Guide, use a computer with a web browser and go to the URL:

https://FindCIT.Z-WaveAlliance.org

Here you will see a screen similar to the one shown below – notice the IP address(es) listed at the bottom of the page:

The address(es) listed here – in this case two of them because there are two CIT units on the local network – are found automatically on the local network without having to log in to the Find Service. Clicking on either one of these CIT units will connect you with the user interface, but it is not possible to tell which CIT unit you will get connected to.

By entering your Z-Wave Alliance login credentials in the username and password fields and clicking on Log In, the CIT units that were registered to you will be found and the CIT identifier you entered will be shown, providing you with a means for identifying which CIT unit you want to connect with. Here is an example after logging in to the service:
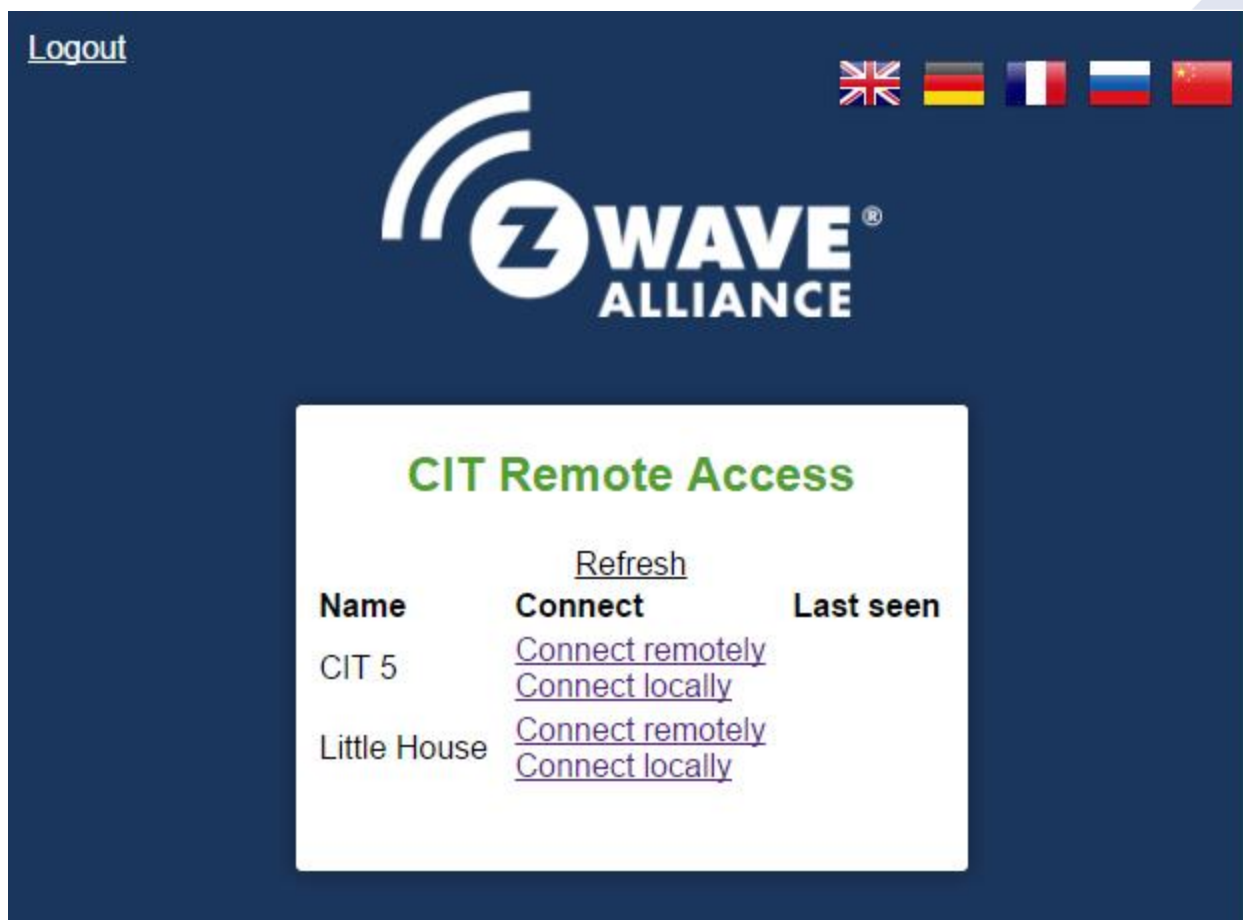
As you can see above, both CIT units were found and are still available on the local network (Connect locally), but they are now identified by their Name which is the CIT Identifier entered when you initialized the CIT.

Using the Find Service from a remote location would result in a slightly different display in that:

- CIT units on the same network, regardless of whether they were initialized/registered or not, would appear on the Find Service page at the bottom by IP address.
- After logging in to the Find Service, CIT units on the same network registered to you (Connect locally & Connect remotely), as well as CIT units registered to you at remote locations with internet access, would be listed. (Connect remotely only)

Remember to Unregister your CIT prior to turning it over to another person to use.
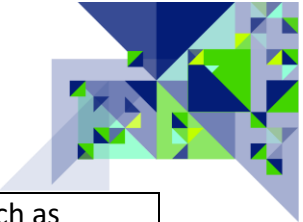
COMMAND CLASSES
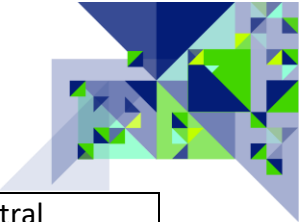
Command Classes are how the features in Z-Wave products are used, or are how the features of a Z-Wave product are communicated and used with other Z-Wave products. Command classes form the structure of communication that all Z-Wave products utilize. Each command class is made up of commands (such as 'set' or 'get') and the expected response (such as 'report'). Since command classes make up the language of Z-Wave, these command classes – how they are interpreted and handled – form the basis of Z-Wave's interoperability rules. When a new feature is added to a command class, the version is incremented. It should be noted, however, that new features are always implemented in such a way as to make it possible for other devices supporting the same level or higher to make use of those features, without breaking the ability for older devices to communicate at a lower version level. This is how a controller that perhaps only supports version 2 of the switch multilevel command class, can still control a dimming light switch that has version 3 of the switch multilevel command class.

Following is a partial list of Z-Wave command classes and what they are used for. This is not the exhaustive list of all command classes available in Z-Wave; these are some of the more common command classes to help you identify features and capabilities that may be frequently found in some Z-Wave devices.
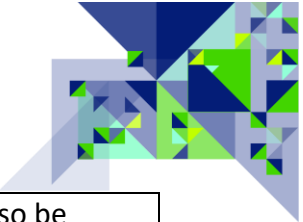
Association & Multi Channel Association	Used to set up a relationship with another node on the network to receive a Z-Wave command class signal when a specific event occurs in a device. The Multi Channel Association command class is used to set up these relationships in devices with multiple copies of the same functionality, such as a Z-Wave outlet strip that has 4 outlets, each controlled separately by Z-Wave.
Association Group Information	This is used to report information about the association capabilities of a device – the events that trigger an associated command to be sent, and what type of command is sent.
Barrier Operator	Barriers to entry such as a garage door or motorized gate are controlled with this command class, and use of this command class requires the device to support security.
Basic	This is a base level command class that all Z-Wave devices support as the lowest possible common command class which can be used for control and status reporting. This command class can be used if no other common command class can be found.
Basic Window Covering	(Replaced with Window Covering)
Battery	This command class is used to report a device's battery level.

Central Scene	This is used to report events that happen on a device, such as button pushes, to a central controller so that the central controller can carry out the commands of a scene defined by the owner of the controller. See also the "Scene" command classes.
Configuration	This command class provides a mechanism to change user changeable settings in a Z-Wave device.
Door Lock (Lock)	Locking mechanisms such as doors and safes are controlled with these command classes, and use of these command classes in a device also requires the Security (or Security 2) command class.
Firmware Update MD	The presence of this command class indicates the potential for the device to support having its firmware be updated via Z-Wave Over-The-Air (OTA).
Indicator	This command class allows for a device's indicators (lights, etc.) to be controlled or set by another device in the network.
Manufacturer Specific	Information regarding the manufacturer, and product identifiers are communicated using this command class.
Meter	This command class reports measured (metered) data for electricity, fluids, and gasses.
Multi Channel (Multi Instance)	Formerly called Multi Instance, this class is used in devices which have multiple copies of the same technology. For example, an outlet strip which has 4 outlets that may be controlled independently by Z-Wave uses this command class to identify each endpoint of duplicated functionality. The first outlet would be endpoint 1, the 2nd outlet would be endpoint 2 and so on.
Multi Cmd a.k.a. Multi Command	To conserve battery life in a battery powered device, it may use this command class as a means of joining together several different Z-Wave command class signals for transmission all at once.
NOP a.k.a. No Operation	This command class has no action associated with it – it is used frequently in a Z-Wave network as a means of determining if another node in the network can be reached. When a Z-Wave command is sent to another node, the receiving node sends an ACK (acknowledgement) of receipt. If this command is sent to another node, the ACK confirms that the node can be reached.
Notification (formerly Alarm, includes Sensor Alarm, & Sensor Binary functions)	Combining the functions of several older command classes, the Notification command class contains many types of notifications used by sensors and other types of devices. This command class is used today to notify of when a door is unlocked, mains power is lost, when there is water present (where it should not be) or when the temperature is too high or too low among many other signals.
Scene Activation, Scene Actuator Conf, Scene Controller Conf	With the Actuator Conf being found in end devices, Controller Conf in controllers or wall controllers, and Scene Activation often in both, this indicates support of the Z-Wave Scene command classes which allow for lighting and control scenes to be configured and

	programmed into devices, eliminating the need for a central controller to activate (invoke) the scene or to turn the scene off. The scene command classes provide for a timeframe for the scene to become active (several seconds to as much as several hours), specific levels for devices, and is implemented in such a way as to usually be able to activate the scene in all devices at the same time, eliminating the "popcorn" effect in many lighting systems.
Schedule, Schedule Entry Lock, Climate Control Schedule	These command classes specify for a day of the week and/or time of day for specific functions in a device to take place.
Security, Security 2	High levels of data encryption and protection are provided by these command classes.
Sensor Multilevel	This command class is used to report varying levels of information reported by a sensor in a device. Temperature, Humidity, and Light level are common examples of information reported by this command class.
Switch All	This command class allows for devices that have the feature enabled and the appropriate setting, to all be switched ON or OFF together.
Switch Binary	Devices which turn something on or off, open or closed, up or down will use this command class. This class is used frequently in light switches and plug-in modules that cannot be dimmed.
Switch Multilevel, Switch Color	Devices such as dimming light switches, dimming modules, or motors which can have their level raised or lowered use this command class. Devices supporting multiple colors will have the Switch Color command class combined with it; Switch Multilevel is used to control the on/off and device level, while Switch Color is used to specify the color value.
Thermostat Fan Mode / Fan State / Heating / Mode / Operating State / Setback / Setpoint	Thermostats use different combinations of these command classes depending upon the features they provide. Often, Sensor Multilevel is present in a thermostat to report the temperature as well.
User Code	This is used to program and report codes for users in door locks, security panels, and other devices controlling locks or barriers.
Version	Version information for Z-Wave and the device itself are reported through this command class.
Wake Up	Battery operated devices that go into long periods of sleep – when their Z-Wave radio is turned off – use this command class to be told how often to wake up and check for commands, as well as to notify a central controller when they have awakened and can be delivered their commands from their mailbox.
Window Covering	As the name implies, different types of window coverings (shades, blinds, curtains, etc.) are controlled through this command class. In

	some cases, the Switch Multilevel command class may also be used.
Z-WavePlus Info	This command class is used by a Z-Wave device or controller to report that it is a Z-Wave Plus capable device or controller, and which role type and node type it is in the network.

Z-WAVE TROUBLESHOOTING

Now that you are familiar with the CIT, let's take a look at how you can diagnose specific things about the Z-Wave network being examined.

Missing communication, delayed execution of commands or nodes that appear in the failed node list indicates problems in Z-Wave networks. For trouble shooting it is helpful if the problem nodes are already identified however sometimes the whole network seems to be infected.

To find the root causes of the problem follow the steps below:

Defect and/or nonconforming electrical gear causing noise (baby monitor, old cordless phones, wireless speakers, motors …)

Check Noise Floor. The noise floor is the middle line of the viewgraph. If < 80 dBm you are fine, if its > -60 dBm it can cause severe problems. You can move the CIT to find the direction of the noise source. Use instant noise floor testing for this. The Noise Meter provides instantaneous measurements of the noise floor – look for prolonged periods of the meter(s) being red.

Other Z-Wave Networks nearby

If you see too many spikes above noise floor this is an indicator that other Z-Wave networks may be interfering with your network, or that devices on your network are configured to send unsolicited reports too frequently. You can verify this with network statistics and compare the portion of foreign Z-Wave frames to the total amount of received frames. Please keep in mind that Z-Wave devices have to comply with the 1% duty cycle rule.

Faulty behavior of devices in own network (e.g. endless loop)

Check the Zniffer!

Weak mesh of devices

It is the best if you already know the trouble making devices. You can test their connection to the controller and to the devices they have association connections to. If the device in trouble does not have a stable direct link to the controller or the associated device, you need to dig in and fix the routing. Look at the network map to see problems with routing.

Weak signal of devices
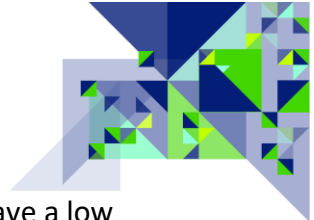
Use Zniffer to look at the traffic between nodes and the RSSI to determine the links that have a low (e.g. < -60 dBm) connection strength between two devices that are communicating. If the device has a low number of routes, it is advisable to add a node in between as two strong hops are better than one weak one.

Wrong configuration - Polling

Check the Zniffer – devices should be getting polled, or sending unsolicited frames, more often than the 1% duty cycle of the network. Polling is done by the controller (change the setting for anything polling too often) and unsolicited frames are usually caused by bad configuration settings in the device.

Dead Associations

Check the Active associations! See "Occasional Delays" below for further details.

No Battery Levels / Reports

Battery level can only be obtained by the CIT if it "eavesdrops" on the battery level being sent to the primary controller at a wake-up event; it is very rare. However, a lack of accurate battery level and updates on the primary controller indicates either A) that the wake-up interval needs to be set/reset, or that B) the battery device does not have a route back to the controller. After making sure that there are valid path(s) between the battery device and the controller, remove and re-add the association using the CIT or – preferably – the primary controller.   When a battery device wakes up, it sends an "I'm awake" signal to the controller so the controller can send it any commands from its mailbox for that node. In many cases, the battery device will also send its battery level, but not always! In some cases, the battery level has to be requested as it is not sent automatically. In these cases, be sure to set up a poll of the battery level on a regular basis that is at a lower interval than the wake-up interval for the device.

Here are some **further scenarios** and ways you can detect and repair:

- **Communication to the nodes** – The first two device screens should give you an indication of any nodes that cannot be reached, excluding the sleeping battery devices. For any nodes that you should be able to reach but cannot, use the neighbor table and the network map to see if there are obvious gaps in the mesh network that can be easily fixed by adding a repeater device. If this is an older network where the Explorer Frame is not always available, then you may try using Node Neighbor Update or "Repair Network" as some gateways call it to cause the

nodes in the network to re-discover their neighbors. Remember, at the end of inclusion of a node (let's say node 10 for example), its neighbor information is transmitted to the controller. If more nodes are added which are neighbors to node 10, the controller may record nodes that are neighbors to 10, but will not know that 10 is a neighbor to them unless the neighbor information is updated. You may think that if two nodes are neighbors that it works both ways, but not always! Another way to force the update of the neighbor information is to repeat the inclusion procedure. Re-including a node that is already a part of the network will not cause it to get a new node number, but it will cause the examination of its neighbors to take place again.

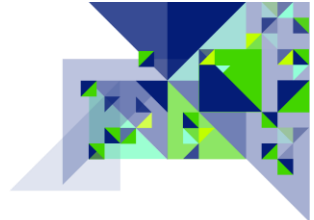- **Occasional Delays** – There can be a few causes of this including noise, but one situation that you definitely want to resolve are nodes which have associations to nodes that no longer exist. When a node is replaced, it is possible that another node that had an association to it was never updated to use the new node ID. The customer may not notice this because it is an infrequently used device, or perhaps the association is to keep an indicator up to date and the customer never noticed that it was inaccurate. The attempts to reach a node that no longer exists are no different than if the destination node failed – Z-Wave will make several attempts to reach it including use of the Explorer Frame, which will make multiple seconds to complete on even a medium sized network. Make sure – using the Device/Active Associations page, that you do not have any associations in place to old node numbers.

- **Occasional Delays** – Another cause of this could be other Z-Wave networks, in the situation where the customer is in a multi-family dwelling. A quick check of the Foreign Network bar on the Analytics/Statistics page will tell you if many of the transmissions of your customer's Z-Wave network are hearing (and thus having to wait for) another network's transmissions. This is usually OK and is a logical reason for occasional delays, but if the RSSI of the neighboring network is strong enough that it is blocking communication to some of your nodes, then it may be time to add nodes to the mesh network so that each hop is stronger than the background noise of the other network.

- **Transmission failures, Signals not being received, Occasional delays** – this can be indicative of weak links between nodes, which are then being blocked or delayed by some of the previously mentioned reasons. On the Analytics/Statistics page, frequent Frequency Backoff or a high number of CRC frames being corrupted are sure signs of either strong noise, or weak transmissions that are being affected by noise that would otherwise have not caused a problem. If there is a specific node experiencing this problem more than others, go to the Link status page for that device and update the link quality measurement, then take steps to

Z-Wave Alliance, 47467 Fremont Blvd., Fremont, CA 94538 USA   ●   +1 510.897.0200
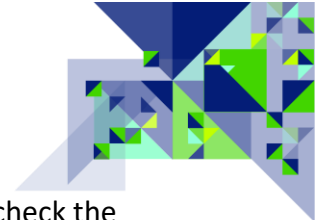
improve the mesh in areas where there are weak links. If the links appear strong, check the Analytics/Background noise page for a potentially high noise floor. You can physically move the CIT closer to a node experiencing an issue with noise so that you may more accurately measure the noise near the affected node. If a plug-in power source is not available, the CIT can be powered using a commercially available cell phone portable battery source for a period of time. Remember once you have moved the CIT to allow for adequate time for the measurement of noise at the new location to take place.

- **Controller Not Updating** – when you know the network is robust and a node sends a status update to the controller, but the controller is not updating, it may be that the controller was not expecting the type of signal it received. When a controller requests the status from a node, it may use a specific command class supported by the node, but when the node is sending an unsolicited update, it may be sending a different type of command class. A great example of this is when a controller requests the level from a dimmer using SWITCH_MULTILEVEL command class, but status updates sent by the dimmer unsolicited use BASIC command class. Use the Zniffer screen to capture what is sent unsolicited, as well as when the controller requests the status (this means having to use the customer's controller to request the status). Take this information to the controller manufacturer along with the information about the product used in the sending node, and you may find the controller manufacturer receptive to addressing the situation.

ADDITIONAL INFORMATION

- As a controller in a Z-Wave network, the CIT may receive signals from other nodes in the network. If the CIT receives a BASIC command from another node in the network, it will be acknowledged but not displayed to the end user. The UI of the CIT does not include a way to render a status UI for devices in the network.

- Within this guide, the Z-Wave terms Inclusion, Exclusion, and Replication are synonymous with the corresponding terms Add, Remove, and Copy and may be used interchangeably with one another.

- Z-Wave networks comprised of certified Z-Wave devices will operate together and communicate easily – they are known to be "Interoperable" with one another – regardless of who manufactured the device. This level of interoperability is guaranteed through the Z-Wave Certification program which is required for all Z-Wave devices sold commercially in the world. Interoperability is different from compatibility however, in that manufacturer's partnerships with other manufacturers may result in a reduced level of functionality at the User Interface (UI) level.

- No nodes in a Z-Wave network which are battery powered may act as a repeater or assist with the routing of Z-Wave frames from a source to a destination. Conversely, all "mains" or permanently powered Z-Wave devices are configured to transparently assist with the routing of information around a Z-Wave network.

- The CIT supports 1 Association group at Group 1 – the Z-Wave "Lifeline" group. It can have 3 nodes in that group. The CIT will send a Device Reset Locally notification to the node(s) in this group if the CIT is factory default reset.
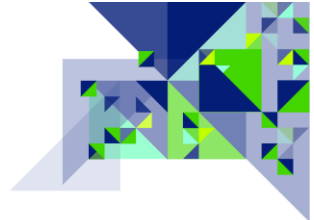
Z-WAVE ALLIANCE RESOURCES

- For support of your Certified Installer Toolkit, please contact your CIT Distributor.
- Training to go along with your CIT is provided as part of your membership with the Z-Wave Alliance. Complete the training course to have your company listed as certified on our public website: http://z-wavealliance.org/find-an-installer   (Companies with a Certified Installer are listed before other companies.)

  Access the training by logging in to the Z-Wave Alliance Member Website at http://Members.Z-WaveAlliance.org, then click Quick Links on the menu, and then Training & Education. Browse the catalog and click **Launch** on the Z-Wave Certified Installer course.
- Find Integrator specific groups, Installer forums, other integrators, installers, and manufacturers at the Z-Wave Alliance Member Website.
- To provide feedback on this User's Guide or the Getting Started Guide, please contact the Z-Wave Alliance at CITFeedback@Z-WaveAlliance.org