Z-Wave

Technical Basics

Version 01.06.2011

1 Introduction

Z-Wave is an international standard for wireless home automation. Home automation allows to interconnect all functions dealing with electricity such as light, heating, cooking, cooling, security etc with each other and to apply automation of these functions. This results in more security and more convenience in homes and offices. Home automation also helps to save energy and other resources.

The interconnection of all these functions can be accomplished using wires or a wireless technology. Particularly for wired home automation the so-called European Installation bus or KNX is very popular and the defacto standard.
Wired solutions are very reliable but require proper planning of wires and devices during the construction of the home and the installation of all the utilities.

For retrofitting or partial solutions a wired home automation system is not applicable. Here wireless solutions come into play. Unfortunately there is no clear standard for wireless home automation protocol in the market yet.

1.1 Requirements of a wireless system for home control

To identify a good wireless technology for house automation a list of requirements must be considered. These are:

1. Reliability of the communication: Important functions such as window blind or even security installations are to be controlled via wireless signal. Hence it is essential that all messages will reach its destination and will be confirmed by the received device back to the transmitter. Not all wireless protocols comply with this requirement.

2. Security of communication: It must be guaranteed that an unauthorized third party cannot – on purpose or accidently – intercept or interfere the communication of the wireless system. Typically encoding technologies and handshake mechanisms ensures this.
3. Low radio emission: Wireless technology for home automation is used on living rooms; hence issues like electromagnetic emission need to be taken into account.
4. Simple usage: Home automation shall make the life of the user easier and not more complicated.
5. Adequate price:
6. Protection of investment: Home automation solutions are typically installed during the construction of new buildings or renovation and need to comply with typical product life cycles of home installation equipment. It is important to make sure, that the user can replace devices or extends their systems even after years and do not run into compatibility issues.
7. Interoperability: Home automation functions such as heating, lighting or window control are implemented with products of different vendors with expertise in their respective area. It is not acceptable to be forced to stick with one vendor and buy - as an example - heating technology from a vendor with core competence in lighting just to enable interoperability. Each installed wireless technology has to be used independent from several manufacturers.

1.2 Alternatives for wireless home control

On the market there are various wireless technologies, which comply more or less with the requirements just outlined.

1.2.1 Analogue Control using 27 MHz or 433 MHz frequency band

Analogue wireless systems, which are available from no-name vendors, have a remarkably low price. The strong focus on the price will result in low manufacturing quality and very poor security. Because a frequency is used which is shared with baby sitter radio or CB transceivers malfunctions are typical and the behaviour of this equipment becomes unpredictable. Analogue products are there not widely used for more serious installations in homes.

1. Reliability of communication: no
2. Security of communication: no
3. Low radio emission: yes
4. Simple usage: yes
5. Low price: yes
6. Protection of investment: no
7. Interoperability: no

1.2.2 Proprietary Protocols of different vendors

Multiple manufacturers have developed their own proprietary solution for wireless control and some of them offer a variety of different products. Some names from this category are Intertechno, Free Control (Kopp), Homeeasy, FS 20, Homematic (both ELV) or Xcomfort (Eaton). Most of these protocols use the frequency of 868 MHz and communicate digitally.
Some protocols have implemented a two-way communication.
The by far biggest disadvantage of these solutions is the limitation of few or even one single vendor. While this may be attractive for the installation “out of one hand” it bears a great risk for long-term availability of components and stability of the protocol. Several vendors have already proven their willingness to change protocols and make the former products obsolete.

1. Reliability of communication: partly
2. Security of communication: partly
3. Low radio emission: yes
4. Simple usage: yes
5. Low price: yes
6. Protection of investment: no

7. Interoperability: no

1.2.3 Power line

The so-called power line communication uses the 230 V mains lines as communication medium. This is not a wireless technology but it competes with wireless automation technologies.

The first and still important technology for power line communication is called X10. It was introduced almost 20 years ago in the US and still has plenty of users both in US and Europe. X10 has reached its end of life since the bandwidth is very limited and the protocol has problems with the modern switched power supplies of PCs injecting a lot of electrical noise into the power network.

Modern power line communication technology uses digital signal coding and is more robust against noise. Unfortunately multiple different “standards” exists which are not compatible with each other. Furthermore the compatibility to the CE regulation on cable emission is questionable.

Another initiative based on power line is called Digitalstrom. This is a development from the University of Zurich and has gained some awareness in the press. As of today the technology hasn’t yet proven its stability in real environments beyond prototype installations.

1. Reliability of communication: questionable
2. Security of communication: questionable
3. Low radio emission: yes
4. Simple usage: yes
5. Low price: yes
6. Protection of investment: yes
7. Interoperability: yes

1.2.4 Zigbee

„ZigBee“ is quite a new player on the block, with the first products on the market in the beginning of 2005.
„ZigBee“ is an open wireless networking protocol which works similarly, but better than Bluetooth. Whereas Bluetooth will pair up with a mere seven devices, „ZigBee“ can pair with many hundred!
A part of the functionality is based on the IEEE specification IEEE 802.15.4, which enables to connect household appliances, sensors, etc. on short distances (10 to 100 metres).
The downside is ZigBee devices from different manufacturers are not compatible with each other because Zigbee standardises only the lower protocol layers (radio layer), whereas different manufacturers have defined their own higher software layers.

1. Reliability of communication: usually yes
2. Security of communication: yes
3. Low radio emission: yes
4. Simple usage: -
5. Low price: not yet
6. Protection of investment: -
7. Interoperability: no

1.2.5 En-Ocean

EnOcean GmbH is a spin-off company from the German company, Siemens AG, founded in 2001. EnOcean actors and sensors work without battery using energy harvesting techniques.
In the meantime, more than 100 manufacturers, primarily from Europe, adopt EnOcean. Pricewise Enocean tries to align with the higher pricing level of KNX.

1. Reliability of communication: no
2. Security of communication: no
3. Low radio emission: yes
4. Simple usage: yes
5. Low price: no
6. Protection of investment: yes
7. Interoperability: yes

1.2.6 Z-Wave

Z-Wave technology is the key to having complete control over your home security and energy solutions, with the minimum of fuss. With a Z-Wave home automation system, you can program all major electrical elements of the home, such as light, heating, cooking, cooling and even your home security.

The benefits don‘t end there, although its a sophisticated system, it is simple to use, and works out to be an energy efficient and cost effective option.

The system works via a remote control, and uses low-powered radio waves. Its mesh network covers all areas of the home, as the radio waves travel easily through walls, floors and furniture, making connectivity 100% reliable.

This freedom of connectivity means that you can easily start with a basic package, and build it up over time with additional components, personalising your home energy and security system, unique to your home and at your convenience. Each Z-Wave module can act as an RF repeater and commands can route through a maximum of four devices. This gives the system a maximum range of 400 ft and routing is managed automatically. Components include sockets, switches, remote controls, and the Z-Wave Internet Gateway VERA where you can create scenes, events and timer settings to personalise your electrical appliances as you would your home. In terms of pricing Z-Wave products ranges above proprietary solutions of some manufacturers but are clearly lower than comparable solutions by

Zigbee or Enocean.

1. Reliability of communication: yes
2. Security of communication: yes
3. Low radio emission: yes
4. Simple usage: yes
5. Low price: not yet
6. Protection of investment: yes
7. Interoperability: yes

1.3 History and Characteristics of Z-Wave

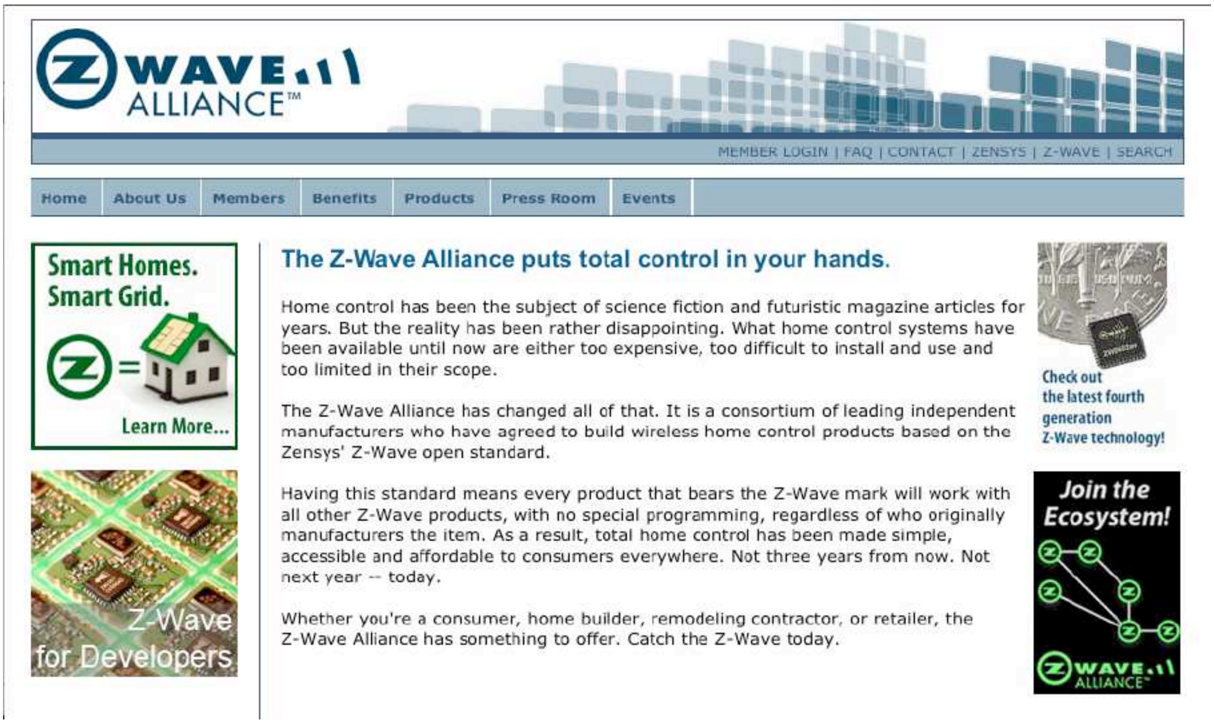
Z-Wave is a development of the Danish company of Zen-Sys. Two Danish engineers founded Zen-Sys at the end of the nineties of the last century. From the initial idea of developing their own home automation solution the company soon evolved into becoming a chip provider selling a home automation ASIC together with own firmware to other manufacturers. This formed an ecosystem of manufacturers with compatible products.

Figure 1.1: 3rd Generation Zen-Sys Chip

The first generation of Zensys hardware was sold from 2003 - at that time still as a combination of a standard microcontroller (Atmel) and a radio transceiver. This hardware platform was extended during the following years with the chip generations 100 (2003), 200 (2005), 300 (2007) and last 400 (2009).

Zen-Sys found the first big customers in the USA where - thanks to X10 – a relevant market and market awareness already existed for home automation.

The first larger Z-Wave device manufacturer in Europe was the German switch manufacturer Merten (now a part of Schneider Electric), which publicly introduced the Z-Wave based lighting system CONNECT in the end of 2007. Since beginning of 2009 the market dynamics has strongly increased in Europe and Z-Wave also gets more and more adopters in Asia. This is also fostered by the takeover of Zen-Sys by the Asian-influenced chip manufacturer Sigma Designs. Sigma bought the venture capital funded Zen-Sys – among other funded by Intel Ventures - in December 2008.



The Z-Wave Alliance puts total control in your hands.

Home control has been the subject of science fiction and futuristic magazine articles for years. But the reality has been rather disappointing. What home control systems have been available until now are either too expensive, too difficult to install and use and too limited in their scope.

The Z-Wave Alliance has changed all of that. It is a consortium of leading independent manufacturers who have agreed to build wireless home control products based on the Zensys' Z-Wave open standard.

Having this standard means every product that bears the Z-Wave mark will work with all other Z-Wave products, with no special programming, regardless of who originally manufacturers the item. As a result, total home control has been made simple, accessible and affordable to consumers everywhere. Not three years from now. Not next year -- today.

Whether you're a consumer, home builder, remodeling contractor, or retailer, the Z-Wave Alliance has something to offer. Catch the Z-Wave today.

Figure 1.2: Z-Wave Alliance Website (as of 2009)

One other landmark of the Z-Wave development was the foundation of the Z-Wave Alliance in 2005. In this industrial alliance the manufacturers of Z-Wave compatible products are gathered. The alliance had more than 200 manufacturers in the end of 2009. The Z-

Wave alliance enhances the standard and also takes care of central marketing events such trade shows. Another central duty of the Z-Wave alliance is the maintenance of the interoperability of the devices on the basis of the Z Wave protocol. This is guaranteed by a certification program, which results in a logo on the device guaranteeing the compliance to the Z-Wave protocol.

Figure 1.3: Z-Wave Compatibility Program

While all manufacturers base their products on the hardware of Zen-Sys, they have some freedom to implement application.
Zen-Sys defines the radio level with the line encodings and also defines the functions to organize the network itself. Precompiled firmware libraries accomplish this. The manufacturers cannot change them. Z-Wave also defines application specific functions (e.g. switch A is switched when button B is pressed) but the manufacturers are responsible to implement this. Most manufacturers optimize and enhance functions on application layer.

Hence, the certification tests concentrate to make sure that the application layer functions of the device comply with the standard to allow and guarantee interoperability across functionality and manufacturers boundaries.

1.4 General Layer Model of wireless communication

Wireless systems are complex and consist of a huge number of functions. As you have already read, there are numerous routes to choose from, but importantly, whatever you choose, has to be

compatible with the products you are using. To help manage the huge number of functions, its useful to split them into different layers.
The lowest layer is always used for communication media. In the case of a wireless protocol, this is the air. The highest layer is always the user, in this case, a human being. In case of Z-Wave a three-layer structure has turned out to be useful.

1. **Radio Layer:** This layer defines the way; a signal is exchanged between a transmitter and a receiver. This includes issues like frequency, encoding, hardware access, etc.
2. **Network Layer:** This layer defines how real control data are exchanged between two communication partners. This includes issues like addressing, network organization, routing, etc.
3. **Application Layer:** This layer defines which messages need to be exchanged to specific applications such as switching a light or increasing the temperature of a heating device.

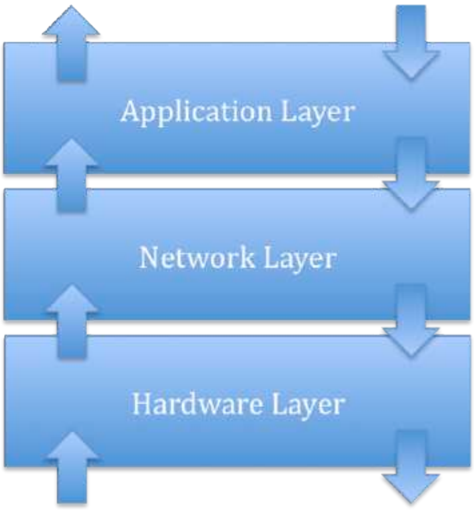


Figure 1.4: General model of an communication architecture

The following chapters describe the architecture and the necessary user's knowledge of the three communication layers radio, network and application.

2 Radio Layer

2.1 Wireless Basics

Z-Wave uses radio waves, and in comparison to other similar systems, proves to be stronger and more reliable.
In an ideal situation, radio waves spread out steadily like light waves in all directions, generating a spherical field. For technical applications the wavelength and the frequency are related to each other with the formula:

$$\lambda = c / f$$

In contrast to infrared light, or light waves in general, radio waves can penetrate in ceilings, walls, pieces, of furniture and other objects. Such obstacles however weaken the radio signal and reduce the range.

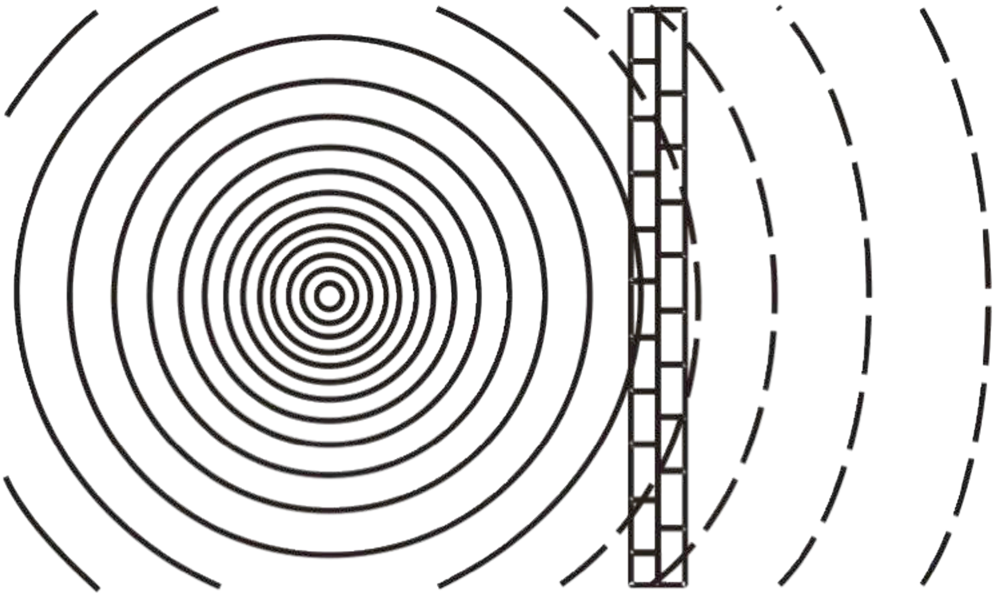


Figure 2.1: Attenuation of radio signals on a wall

Ideally, if you are going to install wireless components, the less obstacles there are the more effective it will be. In practise, this means that wireless components should not be installed in random places.

Z-Wave uses the so-called ISM Band in Europe (Industrial-Scientific-Medical) that is open for various industrial and scientific applications. The frequency is 868.42 MHz that results in a wavelength of about 34cm.

Devices can use this band free of further certification and permits; however the maximum transmitting power and transmission time is limited. The transmission time is in Milli Watts and transmitters have to strictly regulate the maximum airtime to minimise interferences. Sending a permanent carrier signal is strictly forbidden.

Transceivers using the ISM band are permitted in most European Countries that have signed the CEPT agreement. Countries like UK, Germany, Netherlands, and even the Middle East have adopted the CEPT regulations into their national wireless band control scheme.

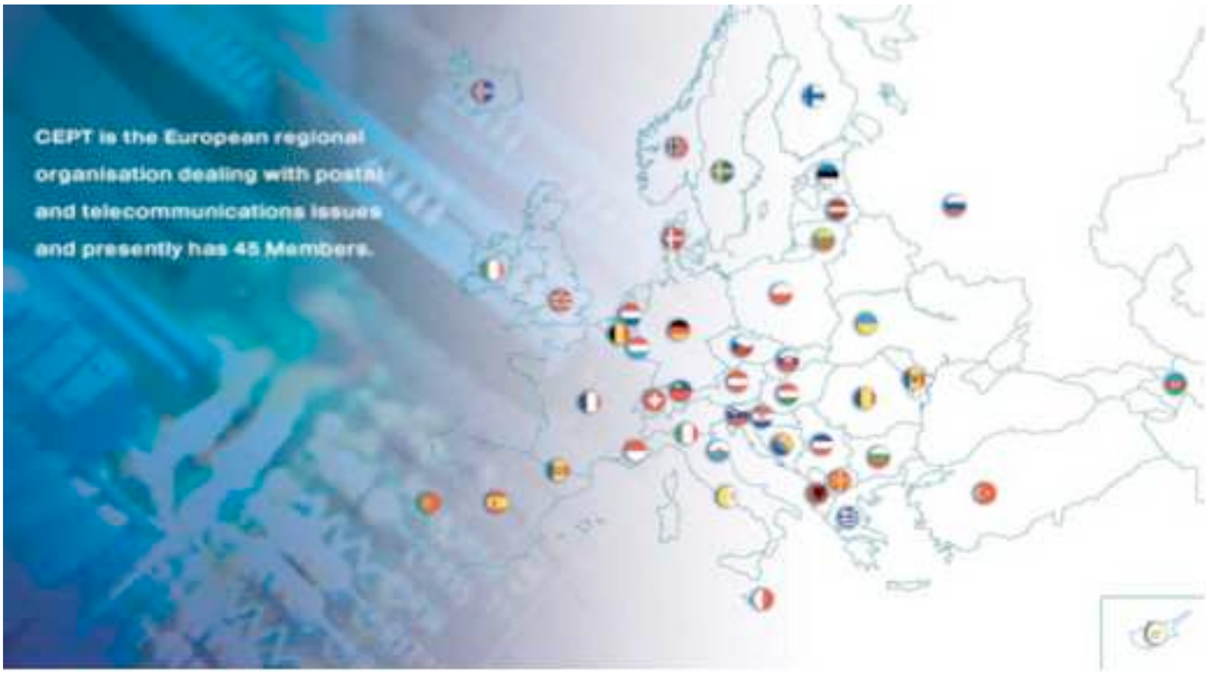

CEPT is the European regional organisation dealing with postal and telecommunications issues and presently has 45 Members.

Figure 2.2: Members of the CEPT-Accord in Europe

2.1.1 Wireless Distance Estimations

When planning your wireless network, there are various aspects you need to consider. As with most installations, it’s all in the planning. The fitting is relatively easy after that.

The general basics to consider are as follows:

- Distance to disturbance sources;
- Effective wall thicknesses;
- Pay attention to shielding materials;
- Attenuation by building materials and furnishings;
  with a negative calculation result if necessary to check whether the radio transmission will function thanks to reflexions.

ATTENUATION

The main thing to consider is the wireless distance between the transmitter and receiver. This distance needs to be shorter than the maximum distance of the technical device’ s parameter (50m or 100m). Then every possible obstacle is determined between the transmitter and the receiver.
The table overleaf can determine the total attenuation of the radio signal.

Here are some aspects explained...

Obstacle	**Former distance**	**Type**	**Attenuation**	**New distance**
No 1	30 m	Concrete	30%	21 m
<< Take new value to next step <<				
No 2	21 m	Glass	10 %	18,90 m
<< Take new value to next step <<				
No 3	18,9 m	Plaster wall	10 %	17 m
<< Take new value to next step <<				
…	17 m	…	…	…

Figure 2.3: Work Sheet to determine the max wireless distance

If the radio signal penetrates the obstacle at a different angle (more than 90 degrees), then the attenuation effect will be increased. If the range resulting in the end is bigger than the measured distance between transmitter and receiver, the components should function well.

Pieces of furniture, installation of radio components, metal coatings, plantings and high air humidity should all be considered when planning the best route for your wireless system. Because these attenuations are approximate, a test is recommended before the fixed installation is made.

Nr.	Material	Thickness	Attenuation
1	Wood	< 30 cm	10 %
2	Plaster	< 10 cm	10 %
3	Glass (without metal coating)	< 5 cm	10 %
4	Stone	< 30 cm	30 %
5	Pumice	< 30 cm	10 %
6	Aerated concrete stone	< 30 cm	20 %
7	Red brick	< 30 cm	35 %
8	Iron-reinforced concrete	< 30 cm	30 ...90 %
9	... Ceiling	< 30 cm	70 %
10	... Outer wall	< 30 cm	60 %
11	... Inner wall	< 30 cm	40 %
12	Metal grid	< 1 mm	90 %
13	Aluminium coating	< 1 mm	100 %

Table 2.1: Attenuation by building materials

2.1.2 Distances to other wireless signal sources

Radio receivers should be attached in a distance of minimum 50 cm from other radio sources. Examples of radio sources are:

- Computers;
- Microwave devices;

- Electronic transformers;
- Audio equipments and video equipment;
- Pre-coupling devices for fluorescent lamps.

The distance to other wireless transmitters like cordless phones or audio radio transmissions should be least 3 metres. As well as this, the following radio sources should be taken into account:

- Disturbances by switch of electric motors;
- Interferences by defective electrical appliances;
- Disturbances by HF welding apparatuses;
- Medical treatment devices.

2.1.3 Effective thickness of walls

The locations of transmitter and receiver should be selected in such a way that the direct connecting line only runs on a very short distance through material, which causes attenuation.

Metallic parts of the building or pieces of furniture shield the electromagnetic waves. Behind a structure like this, there may be a so-called radio shadow, where no direct reception is possible.

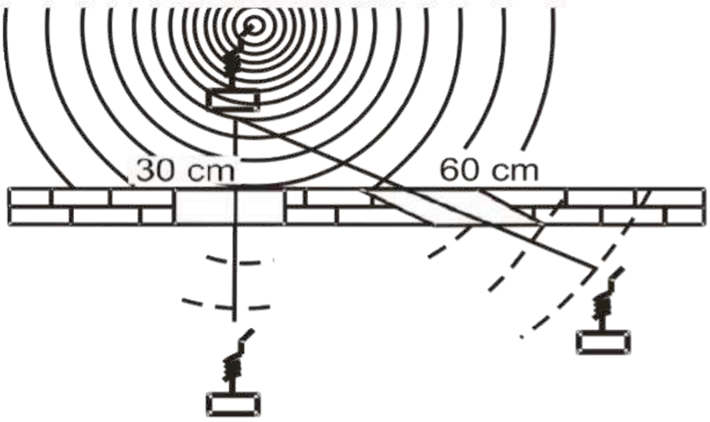


Figure 2.4: Effective wall thickness

2.1.4 Wireless Shadows

Metallic parts of the building or pieces of furniture shield the electromagnetic waves. Behind a structure like this, there may be a so-called radio shadow, where no direct reception is possible.

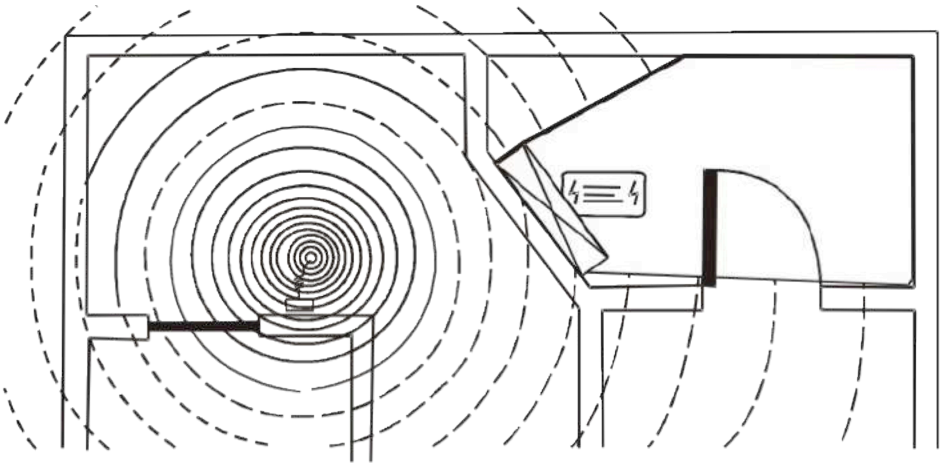


Figure 2.5: Radio shadow by metallic structures

Despite radio shadow, it is possible for wireless signals to be reflected by metal structures and still reach the final destination. Reflections are unpredictable and it is recommended that you test your systems until you create a more permanent fixing.

2.1.5 Reflexions

Reflexions are used by amateur radio connections to bridge big distances (several thousand kilometres with relatively low power) in the short wave band. On this occasion, the reflective property of the ionosphere is used.

Within buildings reflections may cause disturbances or attenuation if the original and the reflected way are received together.

2.1.6 Interferences

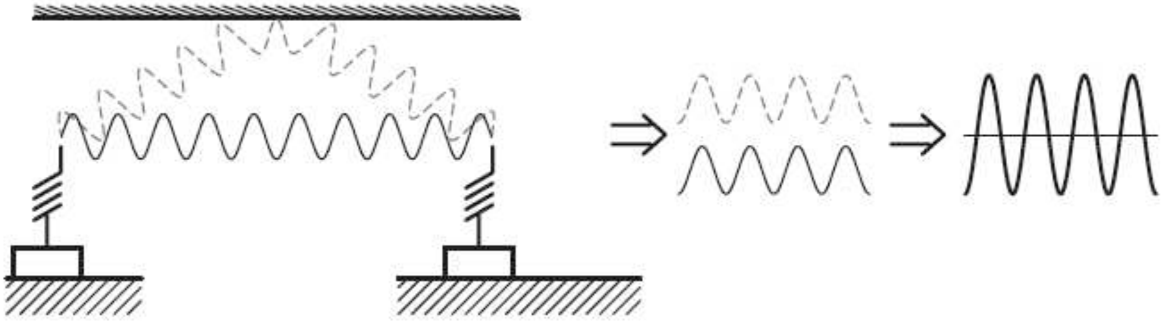


Figure 2.6: Signal gain by interference

Interference can occur in different phase situations that are caused by different run times and by the way the radio waves are increased or attenuated.

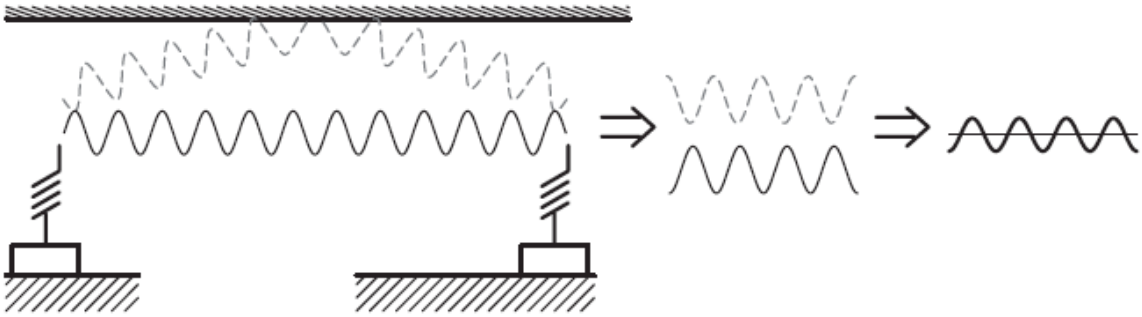


Figure 2.7: Signal assuagement by interference

Interference can be resolved by changing the positions of the transmitter or receiver slightly. Even a couple of centimetres may work. It really is a process of trial and error to see what works for you in your home. 2.1.7 Relevance of Mounting heights

If motion detectors are mounted outside the house, the assembly height is critical. If the motion detector is mounted next to a floor or ceiling level, then the radio signal has to penetrate the concrete of the floor/ceiling. This will be ineffective as this will result in very high attenuation of the signal.

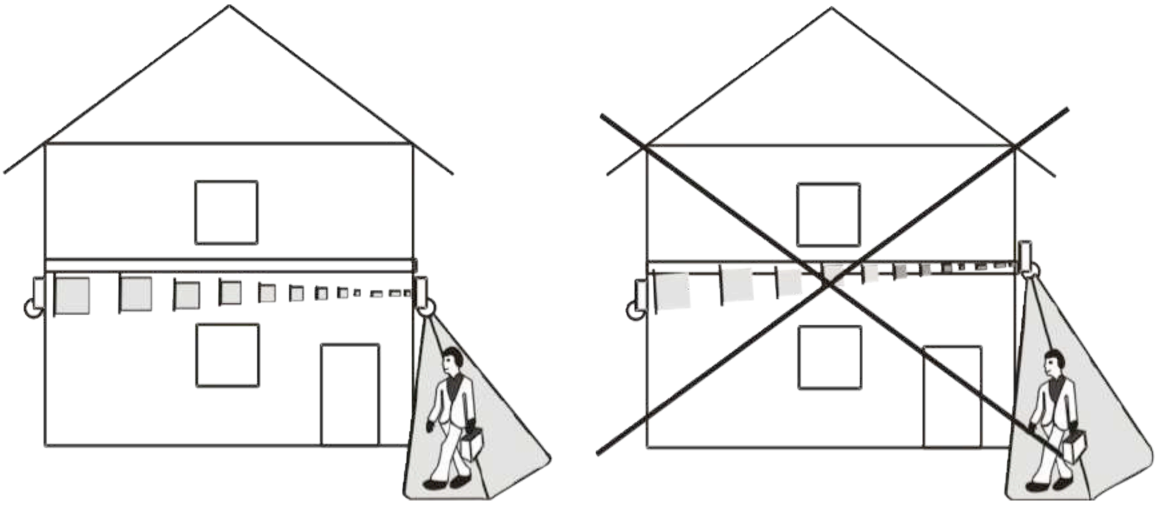


Figure 2.8: Challenge of mounting height

2.1.8 General Basics of Installation

The following basic rules should be considered in every planning of a wireless control system:

- Distance to disturbance sources,
- Effective wall thicknesses,
- Pay attention to shielding materials,
- Attenuation by building materials and furnishings,
- With a negative calculation result if necessary to check whether the radio transmission will function thanks to reflexions.

2.1.9 EME and Biology

From infrared, to Bluetooth, to Z-Wave, there are numerous wireless messages flying through the air. Its bound to be a concern whether it can affect users health.

Radiation power from radio transmitters is a critical factor. As most of us use mobile phones, a comparison can be drawn.

Mobile phones transmit a constant radio signal with a peak capacity of 2000 mW into the brain. Without any other protection and mostly it’s operated next to your ear, a human will consume about 100 mW into their head. This exposure continues throughout the whole telephone call!

Z-Wave is nowhere near as much of a threat, as mobile phones. The system works with peak transmission power, of a maximum of 10mW at a short time. This corresponds to an average radiation power of only 1mW. This is because neither a radio remote control, radio switch nor a radio transmitter from a motion detector operates directly in or close to the body.

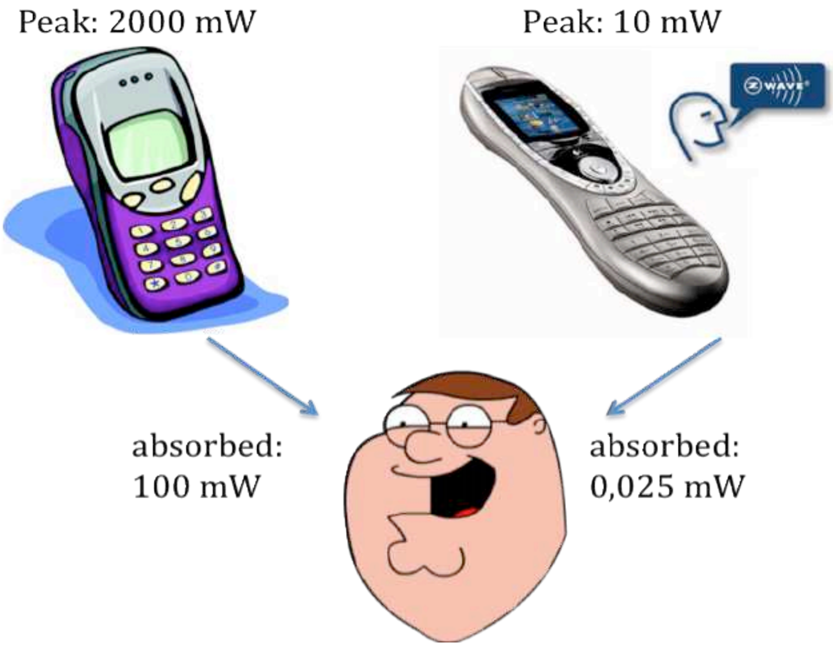


Figure 2.9: Transmitting power of Z-Wave compared to cell phone

The signal attenuation that is generated in a distance of only 1 m causes another reduction of the radiation power around the factor of 40. The human body is only hit by a radiation power of 0.025 mW. This is about 1: 4000 lower than the emission of a mobile phone.
Taking further into account that the radio signal will only be transmitted during a short period of time when a button is pressed or a sensor signal is transmitted, the electromagnetically emission of a Z-Wave network does not contribute to the general electromagnetic pollution in a home and does not have any negative effect to human beings.

2.2 Z-Wave encoding

Z-Wave uses the ISM frequency band in Europe which is fixed at 868.42 and uses a very robust frequency key modulation (Gaussian Frequency Shift Keying), which allows transmitting data with up to 40 KB/s. Older devices still use 9.6 kb/s so that (for backward compatibility reasons), all devices also understand a line encoding based on 9.6 KB/s.
The new hardware family Z400, which was introduced in 2009, offers an additional radio, using the frequency of 2.4 GHz

A good antenna for 868 MHz will allow a bridging distance of up to 200 m outdoors. However, inside buildings the maximum distance is limited to 30 m or even below, depending on the structures and the levels of attenuation in the building.
Generally though, all devices use compatible hardware so therefore the details of modulation and line encoding is not of interest to the end user.

3 Network Layer

The network layer is divided into three sub layers:

- Media Access Layer: The MAC layer controls the usage of the wireless hardware. Its functions are invisible for the end user and hence only of little relevance to him.
- Transport Layer: This function makes sure, that a message can be exchanged free of error between two wireless nodes. The end user cannot influence functions of this layer but the results of this layer are visible.
- Routing Layer: This layer makes sure, that – by utilizing other nodes if needed – a message is passed between the original sender and the desired receiver. The functions of the routing layer are visible to the end users and can be optimized by him.

3.1 Media Access Layer and Transport Layer

In many wireless communication networks a communication between a sender and a receiver is accomplished by simply sending a message over the air.
In case the message gets lost (due to interference or positioning of the receive too far away from the sender), the sender does not get any feedback, if the message was received and the receiver was able to execute the command properly. This may result in stability problems and frustrate the user of such a network.
In Z-Wave the receiver will acknowledge every command sent by the transmitter. This gives an indication whether the communication was successful or not.

This approach can be compared to the delivery of a letter by traditional mail service. Not having acknowledged messages is like sending a normal standard letter to a destination. In most of the cases this letter will be delivered correctly and the receiver will be able to read the letter. However there is no guarantee and some uncertainty remains.

Important messages are therefore to send as “registered letter with return receipt”

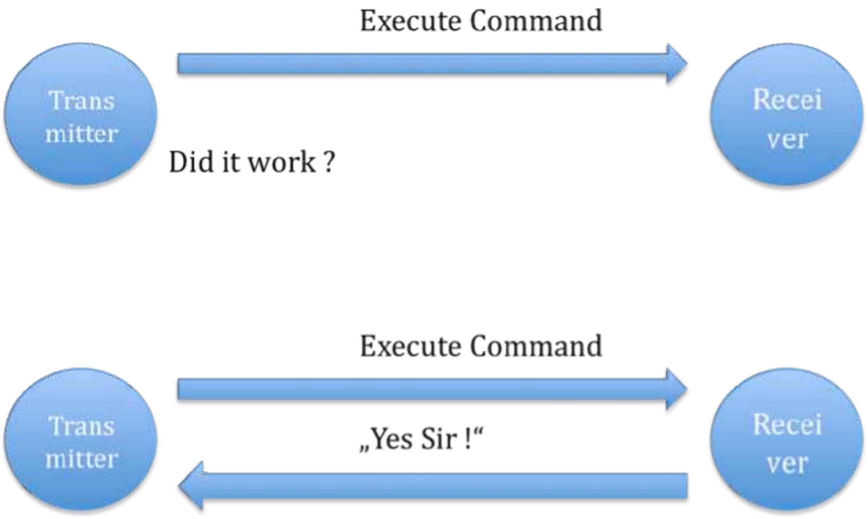


Figure 3.1: Communication with and without acknowledgement

Now the sender has a written proof that his letter was delivered correctly and handed over to the receiver.

Even a “registered letter with return receipt” does not guarantee that the letter will always be delivered correctly. However, the sender will get an indication when a receiver has for instance moved out of town and can do other actions to make sure the letter will finally reach its destination.

The return receipt is called Acknowledge (ACK). A Z-Wave transceiver will try up to three times to send a message while waiting for an ACK. After three unsuccessful attempts the Z-Wave transceiver will give up and report a failure message to the user. The number of unsuccessful transmission attempts can be served as an indicator of the quality of wireless connection.

3.2 Z-Wave Network Basics – Inclusion of Nodes

A network consists of at least two nodes that communicate with each other. To be able to communicate with each other, these nodes need to have access to a common media or need to have “something in common”. In most cases this is a physical communication media like a cable. The communication media for radio is the air that is used by all kind of different users. Hence the communication protocol needs to define an identification that allows the different nodes of one network to identify each other and to exclude received messages from unknown or other radio sources.

Furthermore every node in a network must have an individual identification to distinguish him from other nodes within the network.

The Z-Wave protocol defines two identifications for the organisation of the network:

- The **Home ID** is the common identification of all nodes belonging to one logical Z-Wave network. It has a length of 4 bytes = 32 bits and is less of interest for the final user.
- The **Node ID** is the address of the single node in the network. The Node ID has a length of 1 byte = 8 bits.

As nodes with different Home ID’s can not communicate with each other (this is like they are connected to different cables), they may have a similar Node ID. Within one network, defined by one common home-id it’s not allowed and not possible to have two nodes with identical Node ID.

Z-Wave distinguishes two basic types from devices:

- **Controllers** are Z-Wave devices that can control other Z-Wave devices,
- **Slaves** are Z-Wave devices that are controlled by other Z-Wave devices.

Controllers already have their own individual Home ID at factory default. Slaves do not have a Home ID.

Because controllers have already an own Home ID, they can hand over this Home ID to other Z-Wave devices and add them to their own Z-Wave network.

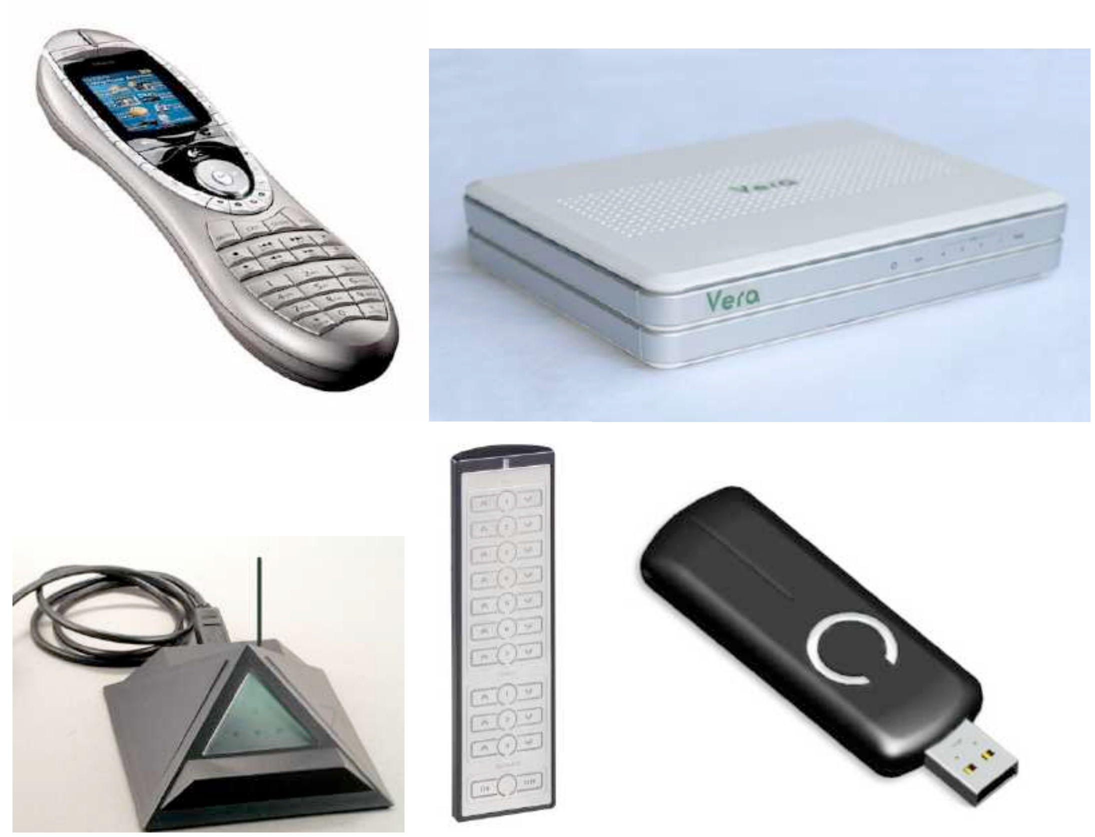


Figure 3.2: Different types of Z-Wave Nodes

Z-Wave controllers exist in different forms: as a remote control, as PC software in conjunction with a Z-Wave transceiver connected in the PC (typically via USB), as a gateway or as a wall switch with special controller function.

The Home ID of a controller cannot be changed by the user and becomes the common Home ID of all devices, which were included by this controller.

Modern Controllers create a random Home ID at every factory reset to avoid problems with re included slave nodes (see chapter 5.4.4 for details)

The controller who begins to build up a network transfers its Home ID to other devices becomes the designated primary controller of this network. In a bigger network several controllers can work together, but there is always only one controller with the privilege to include other controller - the primary controller.

The primary controller includes other nodes into the network by assigning them his own Home ID. If a node accepts the Home ID of the primary controller this node becomes part of the network. Together with assigning the Home ID the primary controller also assigns an individual Node ID to the new device, which is included. This process is referred to as **Inclusion**.

	Definition	In the Controller	In the Slave
Home ID	The Home ID is the common identification of a Z-Wave network	The Home ID is already available at factory default.	No Home ID at factory default
Node ID	The Node ID is the individual identification (address) of a node within a common network	Controller has its own Node ID predefined (mostly 0x01)	Is assigned by the primary controller

Table 3.1: Home ID versus Node ID

The following figure clarifies the process:

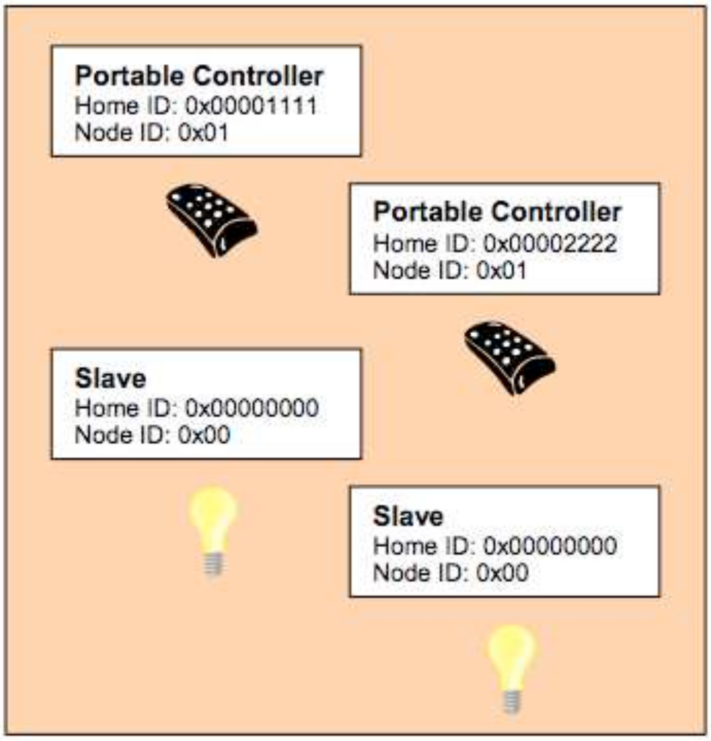


Figure 3.3: Z-Wave devices before inclusion in a network

In Figure 3.3 four devices are available in factory default state. There are two controllers with a preset Home ID. Two other devices cannot operate as a controller (Slave) and, hence, have no own Home ID.

Depending on which of the controllers is used to build up a Z-Wave network, the network Home ID in this example will be either 0x00001111 or 0x00002222.

Both controllers have the same Node ID #1. The slave devices do not have any Node ID assigned. In theory this picture shows two networks with one node in each of them.

Because none of the node in the figure has any common Home ID, no communication can take place.

One of the two controllers is now selected as being the primary controller of the network. This controller assigns his Home ID to all the other devices (includes them) and also assigns them individual Node ID.

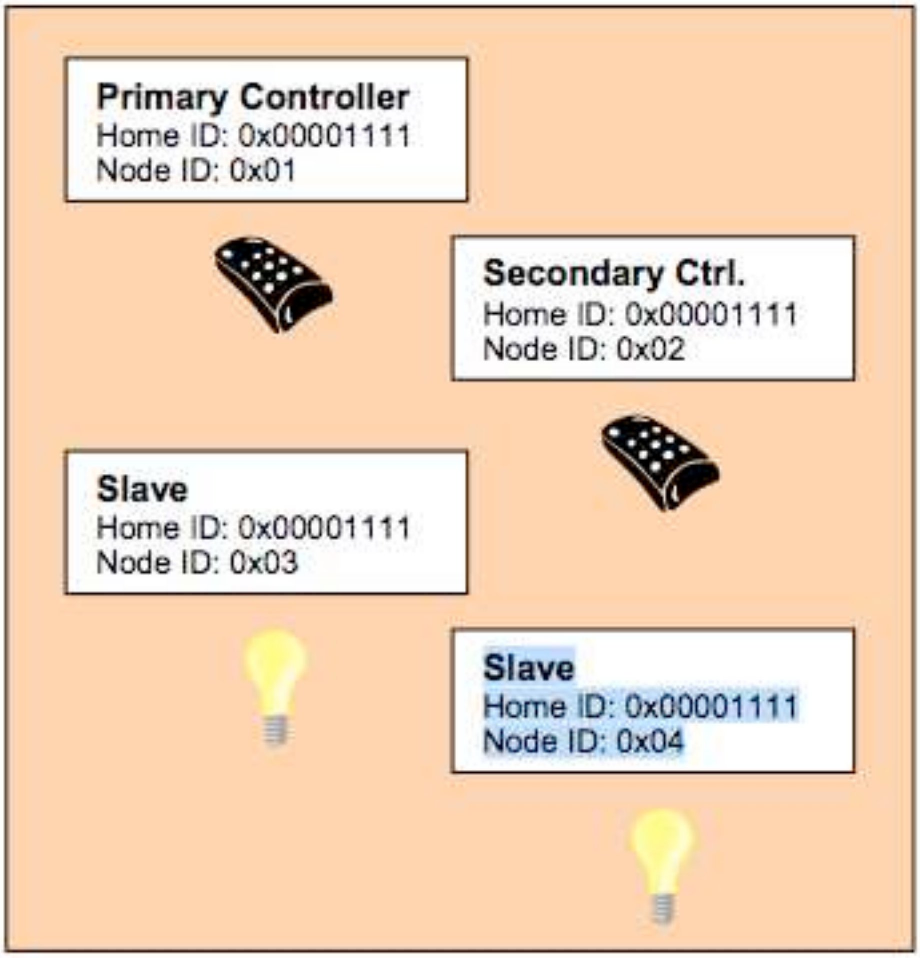


Figure 3.4: Network after successful Inclusion.

After successful Inclusion all nodes have the same Home ID, i.e. they are connected in a network with each other. At the same time every node has a different individual Node ID. Only with this individual Node ID's they can be distinguished from each other and can communicate with each other. In a Z-Wave network several nodes having a common Home ID must not have the same Node ID ever.

In the network shown as an example there are two controllers. That controller whose Home ID became the Home ID of all devices is the primary controller. All other controllers become so called secondary controllers.

A secondary controller is also a controller from the technical point of view and does not differ from the primary controller. However, only the controller with the privilege being the primary controller can include further devices.

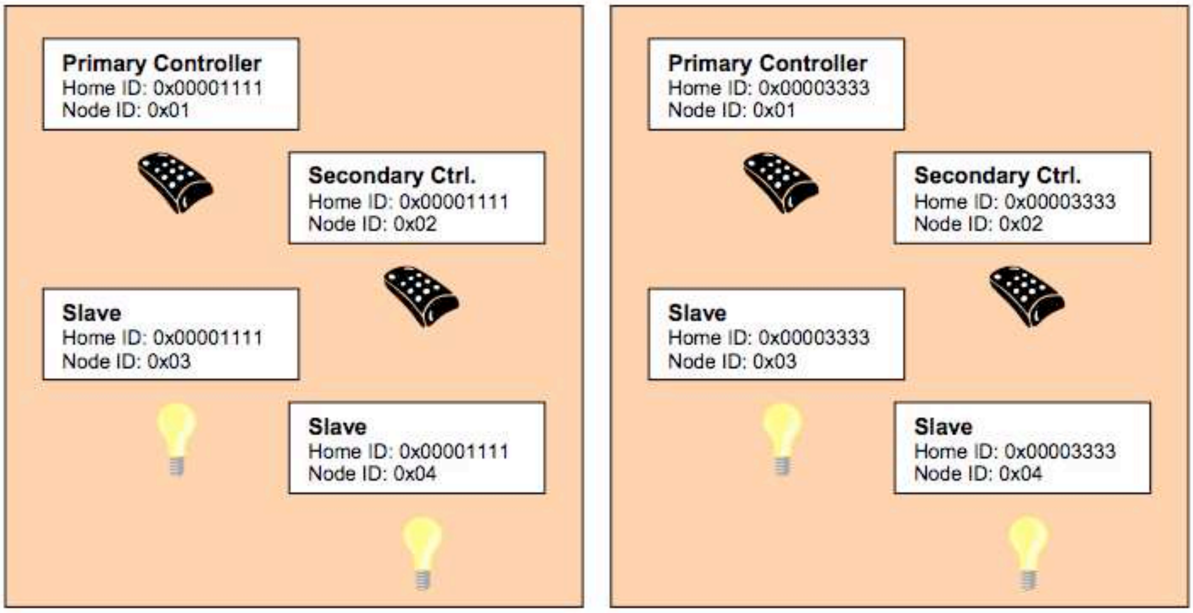


Figure 3.5: Two Z-Wave-Network with different Home IDs coexist

Because the nodes of different networks can’t communicate with each other due to the different Home ID, they can coexist and does not even “see” each other.

The 32 bit long Home ID allows to distinguish up to 4 billion (2^32) different Z-Wave to networks with a maximum number of 2^8 = 256 different nodes.

It is not possible that one single node has two different Home IDs or Node IDs. There are devices (so called bridge controllers) that allow bridging two different networks but they consist of two independent Z-Wave nodes with an interconnection of a higher layer. With their individual Z-Wave networks they still appear as a simple node.

Because some addresses of the network are allocated for the internal communication and special functions, maximum 232 different nodes can communicate in a network.

If Z-Wave nodes are deleted from a network, this is called **Exclusion** in the Z-Wave terminology. During the Exclusion process the Home ID and the Node ID are deleted in the device. The device is moved back in the factory default state (controllers have their own Home ID and slaves do not have any Home ID).

3.3 Meshing and Routing

In a typical wireless network the central controller has a direct wireless connection to all of the other networking nodes. This always requires a direct radio link. In case of disturbances the controller does not have any backup route to reach the nodes.

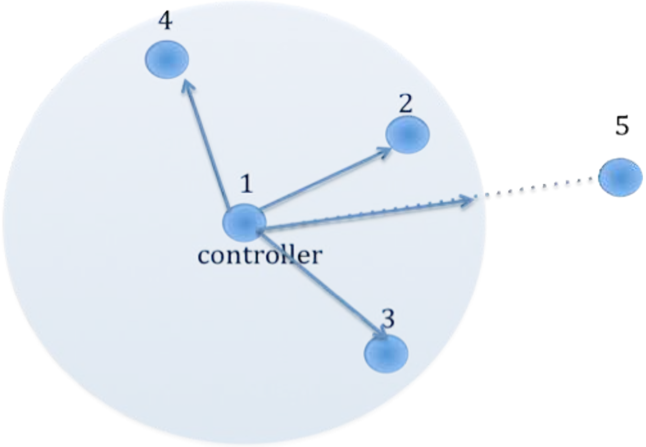


Figure 3.6: Network without routing

The radio network illustrated above is a non-routed network.
Nodes two, three and four lie within the radio ranges of the controller that is labelled number 1. Node 5 lies beyond the radio range and cannot be reached from the controller.
However, Z-Wave is a wireless system that offers a very powerful

mechanism to overcome this limitation. Z-Wave nodes can forward and repeat messages that are not in direct range of the controller. This gives greater flexibility as Z-Wave allows communication, even though there is no direct wireless connection or if a connection is temporarily not available, due to some change in the room or building.

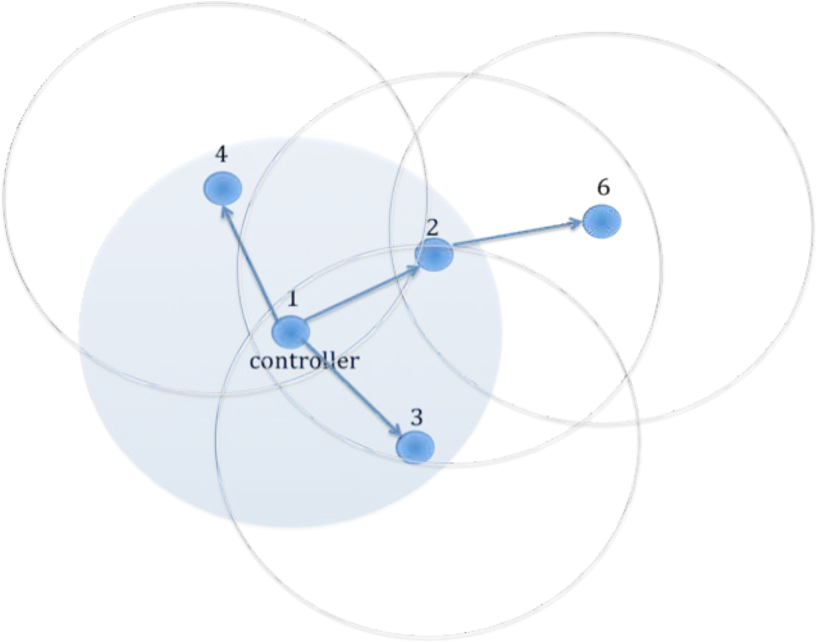


Figure 3.7: Z-Wave-Net with routing

Figure 3.7 shows the controller with „Node ID 1" can communicate directly to the nodes 2, 3 and node 4. Node 6 lies outside its radio range, however, it is within the radio range of node 2. Therefore the controller can communicate to node 6 via node 2. This way from the controller via node 2 to node 6 is called a "route".

Figure 3.7 illustrates another side effect of the routing. In case the direct communication between Node 1 and Node 2 is blocked, but there is still another option to communicate to node 6 via node 2, by using node 3 as another repeater of the signal. It is evident, that more nodes result in more different routing options for the controller and therefore in a more stable network.

Z-Wave is able to route messages via up to four repeating nodes. This is a compromise between the network size and stability, and the maximum time a message is allowed to travel in the network.

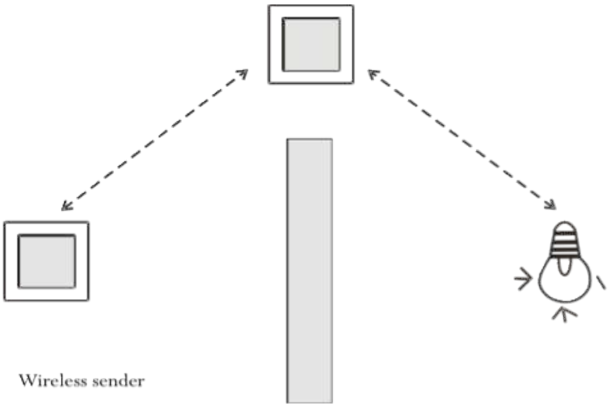


Figure 3.8: Z-Wave communicates „across the corner“

How are these routes built in a Z-Wave network?

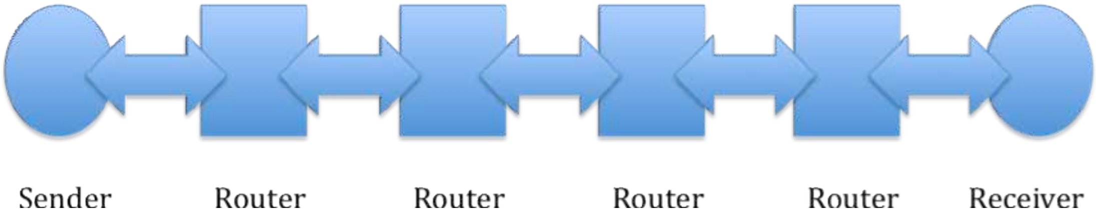


Figure 3.9: Maximum distance between two nodes via 4 repeaters

Every node is able to determine which nodes are in its direct wireless range. These nodes are called neighbours. During inclusion and later on request, the node is able to inform the controller about its list of neighbours. Using this information, the controller is able to build a table that has all information about possible communication routes in a network. The user can access the routing table. There are several software solutions, typically called **installer tools**, which visualise the routing table to optimize the network setup.

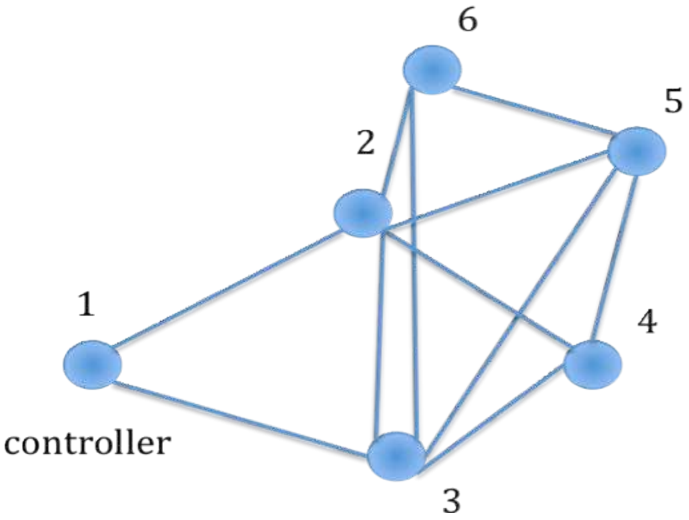
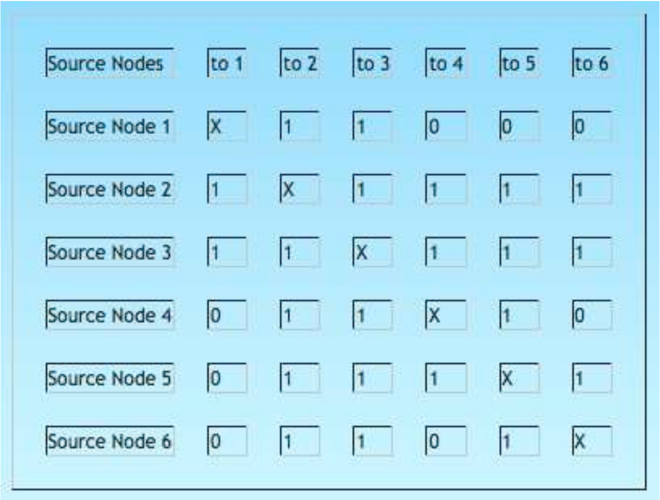


Figure 3.10: Example of a meshed network

Figure 3.10 shows an example of a Z-Wave meshed network, with one controller and five other nodes. The controller and is the primary controller with Node ID 1.It can communicate directly with node 2 and 3. There is no direct connection to node 4, 5 and 6. Communication to node 4 works either via node 2 or via node 3.

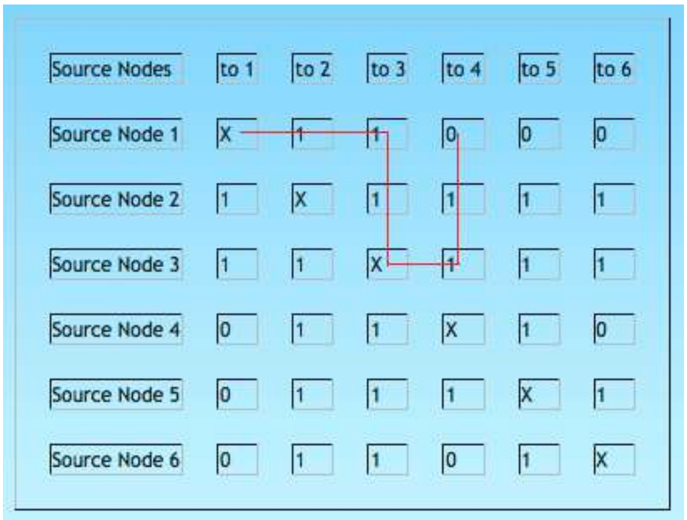
Figure 3.11 shows the routing table of such a network:



Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	1
Source Node 3	1	1	X	1	1	1
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	1	1	0	1	X

Figure 3.11: Routing table for the example network

The rows of the table contain the source nodes and the columns contain the destination nodes. A “1” is a cell which indicates that the two nodes are direct neighbours.



Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	1
Source Node 3	1	1	X	1	1	1
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	1	1	0	1	X

Figure 3.12: Routing from Node 1 via Node 3 to Node 4

The example shows the connection between Source Node 1 and destination Node 4. The cell between Node 1 and 4 is marked “0“. This means the nodes are not neighbours and cannot communicate directly. The route goes via Node 3 that is in direct range both from Node 1 and Node 4.

In the example below Node 6 can only communicate with the rest of the network using Node 5 as repeater. Since the controller does not have a direct connection to Node 5, the controller need to use one of the following routes: 1 -> 3 -> 4 -> 5 -> 6 or 1 -> 2 -> 5 ->6.

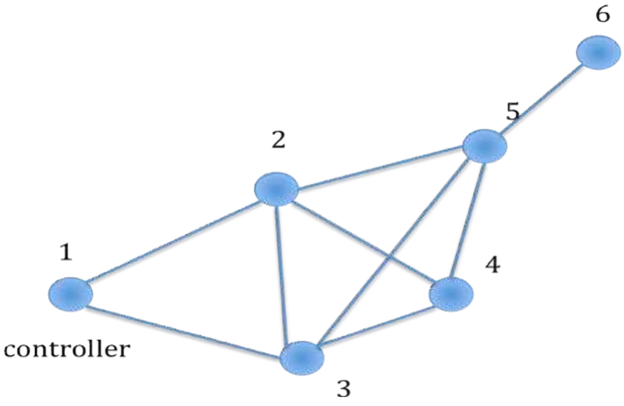
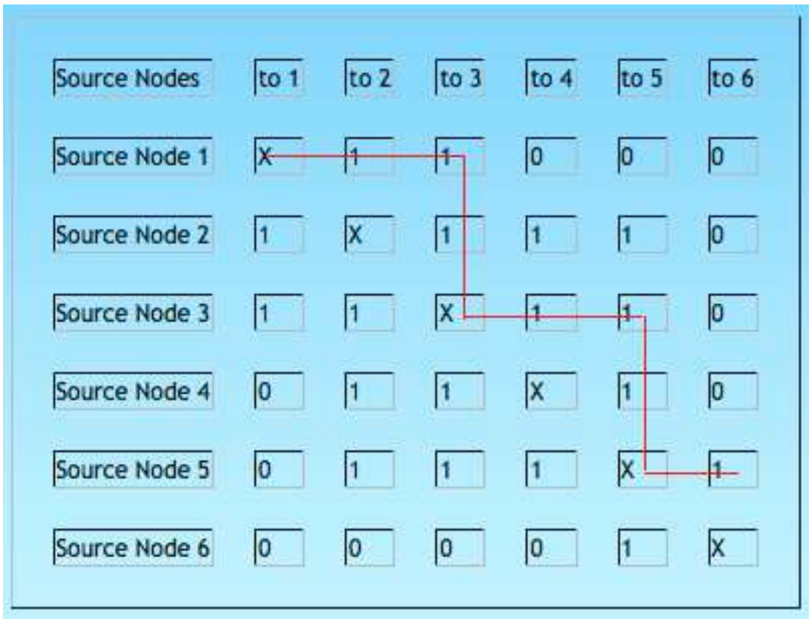


Figure 3.13: Routing using multiple repeater



Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	0
Source Node 3	1	1	X	1	1	0
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	0	0	0	1	X

Figure 3.14: Routing table example of a meshed network

A controller will always try first to transmit its message directly to the destination. If this is not possible it will use its routing table to find the next best way to the destination. The controller can select up to three alternative routes and will try to send the message via these routes. Only if all three routes fail (the controller does not receive an acknowledgement from the destination) the controller will report a failure.

3.4 Types of Network Nodes

It was already mentioned that a Z-Wave network consists of two different node types:

- Controller and
- Slaves.

A routing slave is a slave with some advanced functions regarding routing capabilities. Slaves are categorized further into standard slaves and routing slaves.

The three different node types have three main capabilities. The main difference between the three node types is their knowledge about the network routing table and subsequently their ability to send messages to the network:

	Neighbours	Route	Possible functions
Controller	Knows all neighbours	Has access to the complete routing table	Can communicate with every device in the network, if a route exists.
Slave	Knows all neighbours	Has no information about the routing table	Can only reply to the node that he has received the message from. Hence, can not send unsolicited messages
Routing Slave	Knows all his neighbours	Has partial knowledge about the routing table	Can reply to the node that he has received the message from and can send unsolicited messages to a number of predefined nodes he has a route to.

Table 3.2: Properties of the Z-Wave device models

From this comparison a number of basic rules arise:

- Every Z-Wave device can receive and acknowledge messages

- Controllers can send messages to all node in the network, solicited and unsolicited (“The master can talk whenever he wants and to whom he wants”)
- Slaves can not send unsolicited messages but only answer to requests (“The slave shall only speak is he is asked”)
- Routing Slaves can answer requests and they are allowed to send unsolicited messages to certain nodes the controller has predefined (“The sensor slave is still a slave but - on permission – he may speak up”)

Since the functionality of standard slaves is quite limited, this type of node is only used for dimmers and switches that are installed in a fixed location. Every kind of sensor or any device that can be used on multiple locations must be a routing slave or even a controller.

Typical applications for slaves are:

Slave	Fixed installed mains powered devices like wall switches, wall dimmers or Venetian blind controllers
Routing Slave	Battery-operated devices and mobile applicable devices as for example sensors with battery operation, wall plugs for Schuko and plug types, Thermostats and heaters with battery operation and all other slave applications

Table 3.3 Typical applications for slaves

Establishing, Changing and Destroying a Z-Wave Network

If a device is added to a Z-Wave network (Inclusion), the controller always requests an updated list of neighbouring nodes from these nodes and updates his routing table.
In case another – secondary - controller is included into the network, the including (primary) controller hands over an actual snapshot of his

routing table to the included controller. Right at this moment both controllers have the very same routing table. If more nodes are included later, the routing table of the primary controller gets updated while the routing table of any secondary controller may still show the old status. These secondary controllers need to be updated manually in such a case.
If nodes are excluded from the network, the corresponding entries in the routing table are deleted. If a secondary controller is excluded from the network this secondary controller will not only delete its old Home ID but also the old routing table which is not longer relevant to him once he left the network.

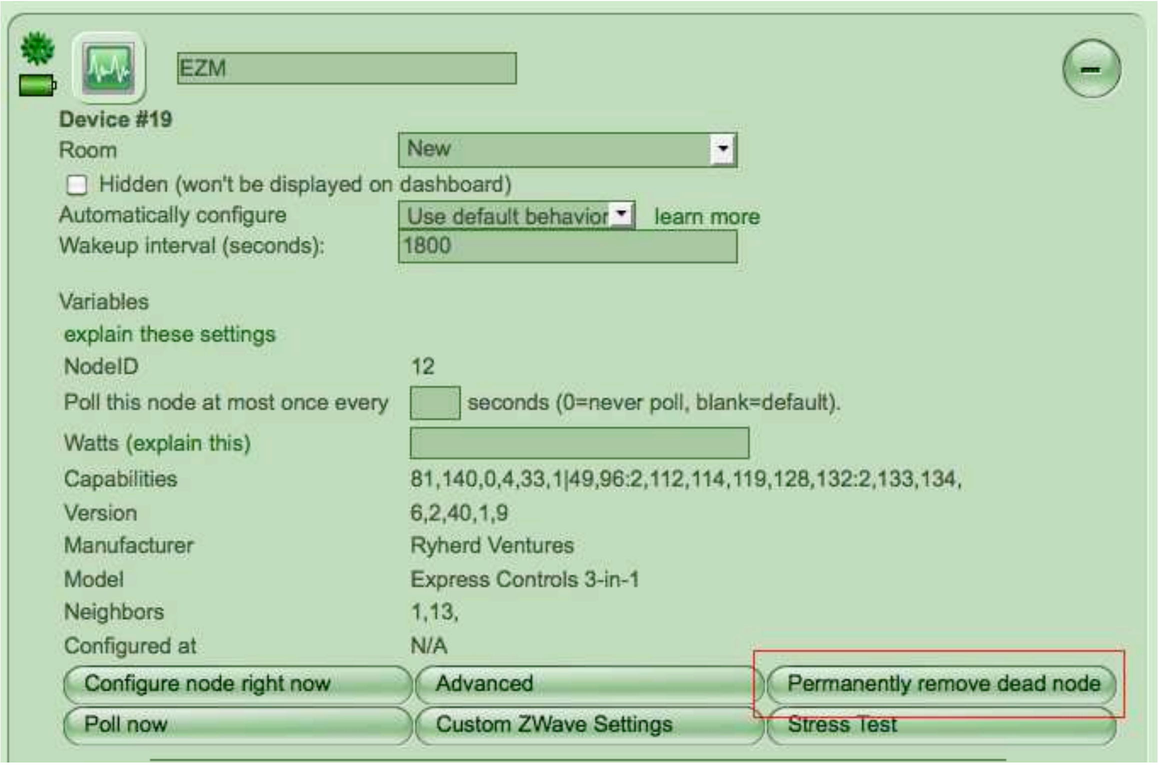
The routing table in the primary controller always shows the actual status of the network after inclusion of the devices. During normal operation a node can however

- go out of operation (damaged) or
- can be moved to a different location.

In both cases the routing table is not longer valid and communication to the moved or damaged node may fail (if the node is just moved its possible that it was moved luckily in direct range of the controller or into a place where his old neighbours still can reach him).

Any failed communication to a node results in an error message. In parallel the controller will mark this node as failed node by putting him into a so called “failed node list”. The failed node list contains nodes with a failed communication. Being in the failed node list does not necessarily mean that node is permanent damaged. Any working communication will move the node back into the original routing table.

If no successful communication happens, the node will stay in the failed node list and can be removed from the network. This will not be done automatically but on user request. Figure 3.15 shows a user dialog to enable to remove a failed node from the network.



EZM

Device #19

Room New

□ Hidden (won't be displayed on dashboard)

Automatically configure Use default behavior learn more

Wakeup interval (seconds): 1800

Variables

explain these settings

NodeID 12

Poll this node at most once every seconds (0=never poll, blank=default).

Watts (explain this)

Capabilities 81,140,0,4,33,1|49,96:2,112,114,119,128,132:2,133,134,

Version 6,2,40,1,9

Manufacturer Ryherd Ventures

Model Express Controls 3-in-1

Neighbors 1,13,

Configured at N/A

Figure 3.15: Screenshot of a Z-Wave Controller with a button to exclude a failed node

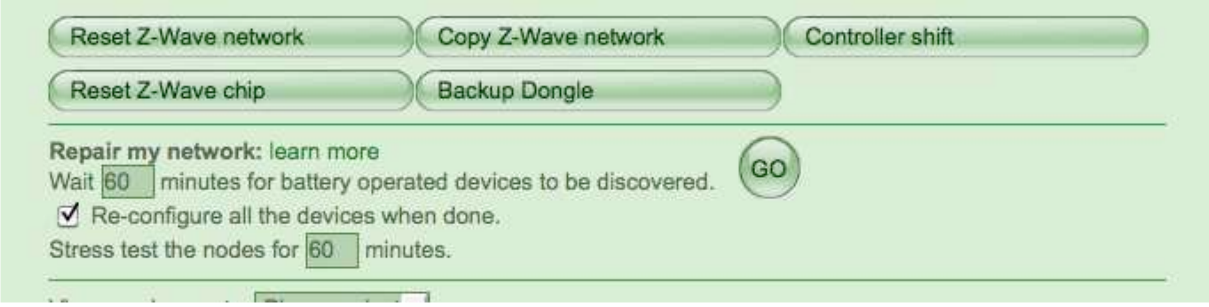
The Z-Wave network is furthermore able to determine movements of devices and update the routing table automatically, however certain conditions need to apply for this. Refer to chapter 3.7 for more details.

Slaves:

If a slave is moved into a different location its neighbours are not longer able to reach him for communication. A message from the controller to this slave will therefore fail. The controller can’t determine if the slave was just moved or is permanently removed or dead. The controller will always treat these nodes as failed and move them to the failed-node-list.

To find a moved node in the network the controller can scan the whole network and ask every known node to update its neighbouring list. If the moved node is still in range of at least one node, this operation will locate the moved node and the controller is able to update its routing table and remove the moved node from the failed-node-list.

Such a network rebuilt will generate a lot of data traffic that is the reason why this is not done automatically through failed node detection.
User can trigger such a network scan on the controller, either by pressing special keys on mobile primary controllers or by using a special dialogs on PC controllers (repair my network).



Repair my network: learn more
Wait 60 minutes for battery operated devices to be discovered.
☑ Re-configure all the devices when done.
Stress test the nodes for 60 minutes.

Figure 3.16: Network Reorganization

The controller will test all connections to its direct neighbours first and scan its neighbourhood for lost devices. In a next step he will ask all known nodes to do the same scan and report back the result.

Figure 3.16 also shows that battery powered devices need a special treatment. Battery powered devices are mostly in an energy savings mode and will only wakeup occasionally. The dialog on Figure 3.16 sets a maximum timeout to wait for any life signal from the battery-operated device during the network scan.

Controller:
Controllers know the whole network topology and can therefore always find a valid route to a communication partner (assuming that the routing table is correct and updated).

Controllers are distinguished into static or portable controllers. A static controller is supposed to be located on a fixed position in the network and shall not be moved. A static controller is mains powered and can route messages.

A portable controller is supposed to be moved around and is therefore typically battery powered. As a battery powered device the portable controller will sleep most of the time and is therefore not able to route message from other nodes.

If a static controller is moved, a network reorganisation or network scan is required. A portable controller will always try to reach nodes in wireless range. If this fails the controller will try to generate a temporary routing table to find a routed way to the destination device.

3.5 Challenges in typical network configurations

As a result of the routing functionality there are some typical network configurations with their individual challenges and requirements.

3.5.1 Z-Wave Network with one portable controller

Z-Wave works by starting with a very small network and extending this network later on as and when you need. A very typical small network consists of a remote control and a couple of switches or dimmers. The remote control acts as primary controller and includes and controls the switches and dimmers.
During inclusion the dimmers and switches should be installed at their final location already, to make sure that a correct list of neighbours will be recognised and reported.

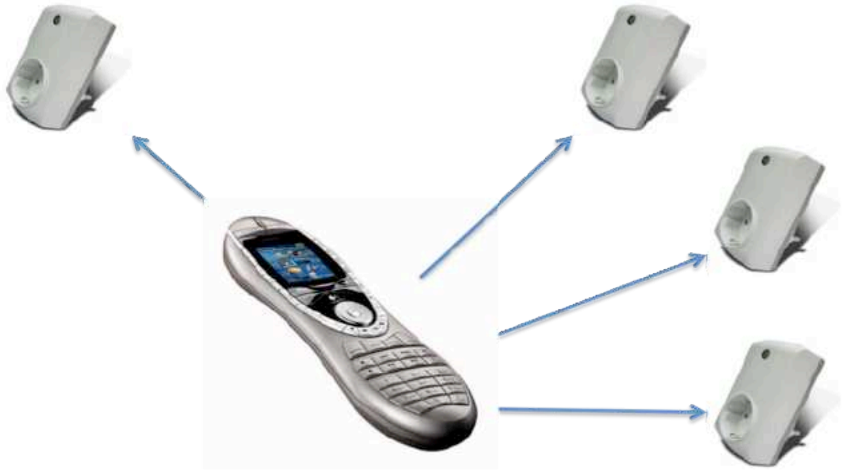


Figure 3.17: Z-Wave Network with one portable controller

A network configuration like this works well as long as the remote control can reach all switches and dimmers directly (the node which is to be controlled is “in range”). In case the controlled node not in range, the user may experience delays, because the remote control needs to detect the network structure first before controlling the device.

In case a device was included and moved afterwards to a new position, this particular device can only be controlled by the remote control if it is in direct range. Otherwise the communication will fail, because the routing table entry for this particular device is wrong and the remote control is not able to do a network scan at the moment of operation.

3.5.2 Z-Wave Network with one static controller

Another typical network consists of a static controller - mostly PC software plus Z-Wave transceiver as a USB dongle or an IP gateway IP as well as a number of switches and dimmers.

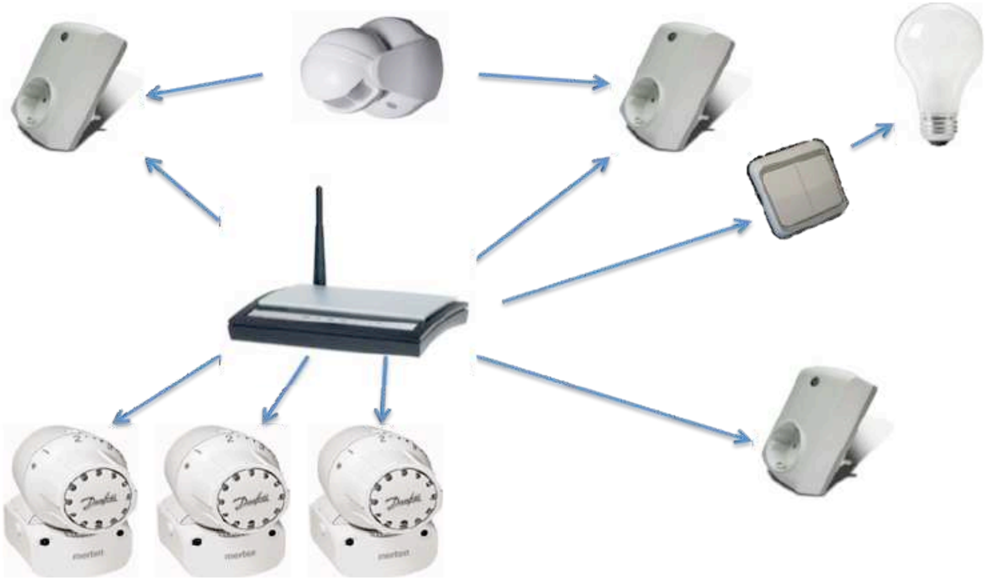


Figure 3.18: Example of a network with one static controller

The static controller is the primary controller, and includes all other devices.

Because a static controller is bound to a certain location, the other Z-Wave devices must be included while being in direct range with the static controller. They will typically be installed at their final location after inclusion.

3.5.3 Networks with multiple controllers

In a larger network several controllers will work together. A static controller – e.g. a PC – is used for the configuration and management of the system and one or several remote controls carry out certain functions in different places.

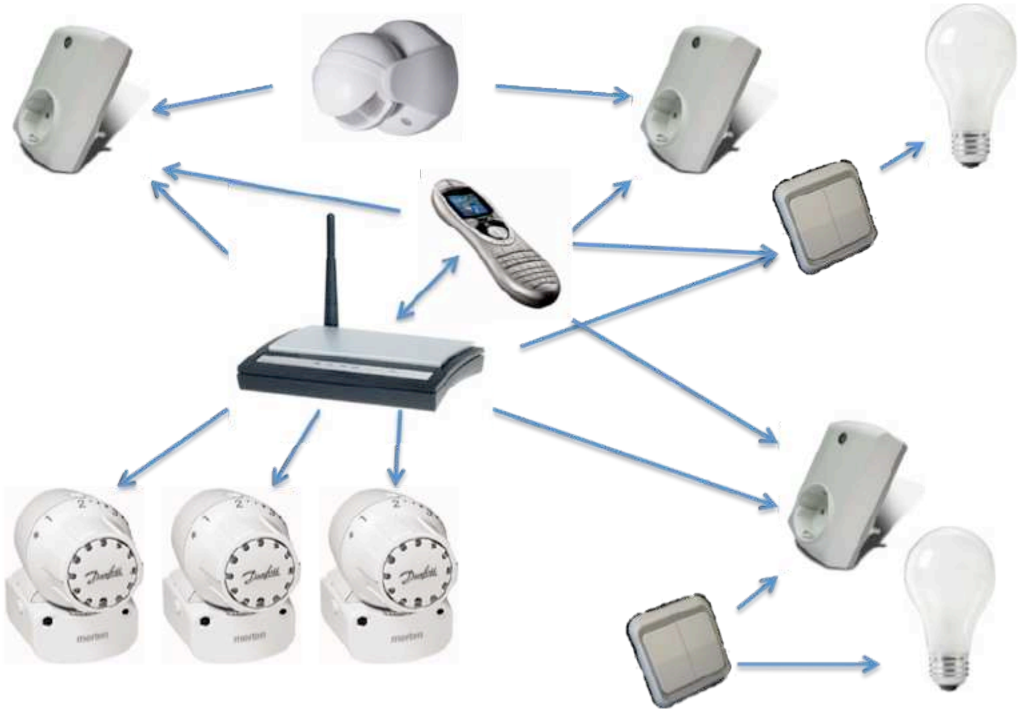


Figure 3.19: Z-Wave Network with multiple controllers

If a network has multiple controllers, the user needs to determine which of the controllers will be the primary controller.
Inclusion of a static controller is a challenge, if the devices need to be moved to their final location afterwards. A network re-organisation needs to be performed.

Static controllers are usually more reliable and cannot get lost easily. They typically offer backup functions to replace the hardware in case of severe damages.

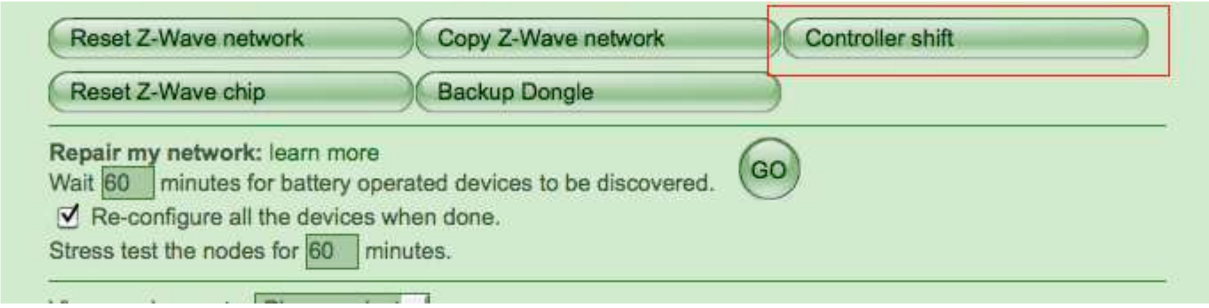
Network with static controller as a primary controller:

Inclusion on a static controller is a challenge if the devices need to be moved to their final location afterwards – a network reorganisation need to be performed.

Static controllers are usually more reliable and cannot get lost so fast. They typically offer backup functions to replace the hardware in case of severe damages.

Network with portable controller as a primary controller:

Remote controls are more vulnerable to damage and loss. Usually remote controls do not offer a backup function. If the primary controller was damaged or lost, a complete re-inclusion of the whole network would need to be performed. However, devices can be included after they were installed, which results in a much more stable network, and no need for network re-organisation.
The choice of the primary controller - static or portable - depends more on the personal preference of the user than on technical necessity.



Repair my network: learn more
Wait 60 minutes for battery operated devices to be discovered.
☑ Re-configure all the devices when done.
Stress test the nodes for 60 minutes.

Figure 3.20: Example of a Controller-Shift

Nevertheless, a basic problem in networks with several controllers is the synchronization of the routing tables of the different controllers. The primary controller passes a snapshot of the routing table to every included secondary controller at the moment of inclusion. At this moment and only at this moment the two routing tables are equal.
Any inclusion or exclusion of further devices will results in different routing tables of the secondary and the primary controller. These results in a failure if the secondary controller will communicate with a device that is not longer included in the network. Furthermore the secondary controllers with outdated routing tables can't communicate with the device included after they were included in the network.

There are two approaches to minimize this problem.

1. Secondary controllers are always integrated into the network last. They will then receive a more or less correct routing table.
2. After inclusion of new devices all secondary controllers will be reincluded to update the routing table. This is a lot of work and not user friendly.

If several portable controllers exist in a network, it is practically nearly impossible to keep an updated routing table in all controllers.
A solution to this problem is offered in additional functionality of static controllers in the network – SUC and SIS.

3.6 Static Update Controller (SUC) and SUC ID Server (SIS)

If there is one primary controller in the network, it will hand over its routing table, to every secondary controller included. After the next inclusion or exclusion of a device, by the primary controller the routing tables of all secondary controllers become invalid. To make sure that there is at least one updated and valid routing table only, the primary controller shall have the privilege to include/exclude devices. For a secondary controller it is always possible to request an update of his routing table.

The requirement for a user friendly and stable network is, that:

- Every battery operated mobile controller shall be able to include devices.
- The routing tables of all controllers in the network are kept consistent and an update shall allow every controller to control every device in the network.

This goal is accomplished by activating a SUC /SIS controller in the network.

3.6.1 Static Update-Controller (SUC)

The Static update controller (SUC) is a special function of a static controller. Most static controllers (a controller with fixed location and powered by mains) can perform as an SUC. However, the function typically needs to be activated first.

The SUC receives the updated routing table from the primary controller and offers this routing table to all other controllers in the network. Because the SUC is a static controller and therefore always active in the network, any other controller can frequently request an updated routing table from the SUC.

To make sure that all other nodes and particularly other controllers are aware of the presence of a SUC in the network, the Node ID of an activated SUC is communicated within the network periodically.

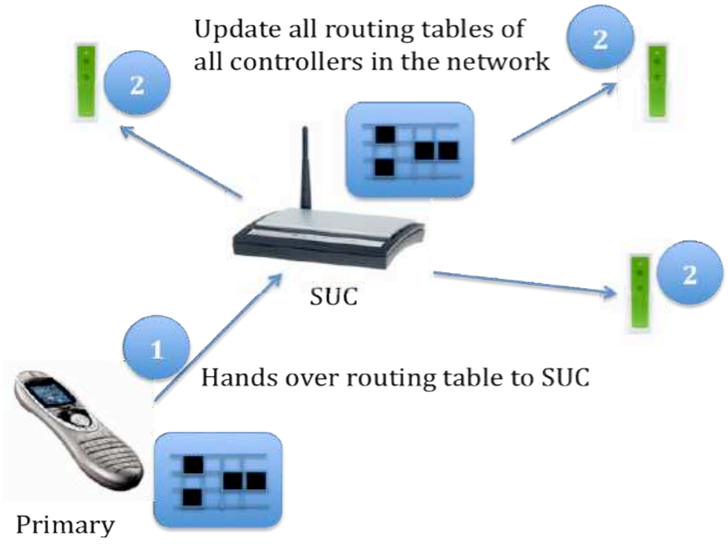

Update all routing tables of all controllers in the network
2
2
2
SUC
1
Hands over routing table to SUC
Primary

Figure 3.21: SUC in a Z-Wave Network

Having an active SUC in the network allows you to keep the primary controller role on a portable controller. Every change of the network caused by inclusion or exclusion of a node by the primary controller will be reported to the SUC and is then available to all other controllers, even if the primary controller is not active.

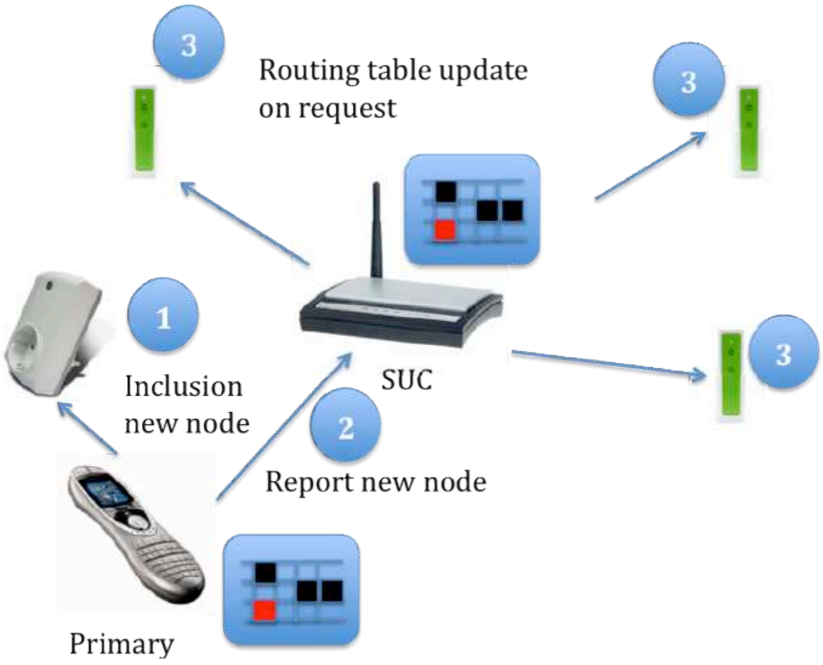


Figure 3.22: Update of the Routing table in a SUC

Since most of the controllers are battery operated and therefore not active all the time, these controllers have to request an updated routing table periodically or at least when woken up, by pressing a

button. To perform this task the mobile battery operated controllers need to be informed about the presence of a SUC in the network.
If the original – mobile – battery operated primary controller is lost or damaged, the SUC can assign the primary privilege to a new mobile controller, protecting the user from re-establishing the whole network with a brand new primary controller, and having a different Home ID.

3.6.2 Static ID Server (SIS)

Even a SUC in the system does not solve the problem that only one controller has the primary privilege and can include new device. This limitation is overcome by enhancing the SUC functionality by another function called SIS = Static ID Server.

The SIS acts as depot for new Node IDs which can be assigned by mobile controllers. Having an SIS present in the network allows every controller in the network to include a further device. The controller will just request a new node ID from the SIS and assign this new Node ID to the server. With the SIS it is made sure that no two nodes get as signed the same node ID. The only requirement is a mobile controller needs to fulfil in order to include new devices, is that it has a network connection to the SIS server to request a node ID.

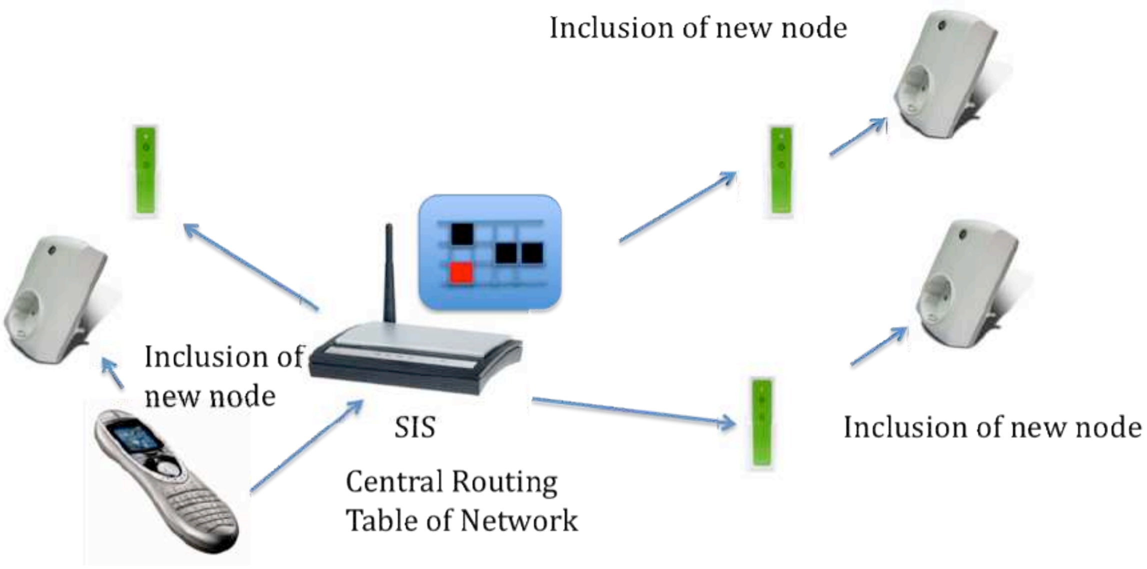


Figure 3.23: SIS Server in a Z-Wave-Network

This kind of configuration with server SIS has the following advantages and disadvantages:

Advantages:

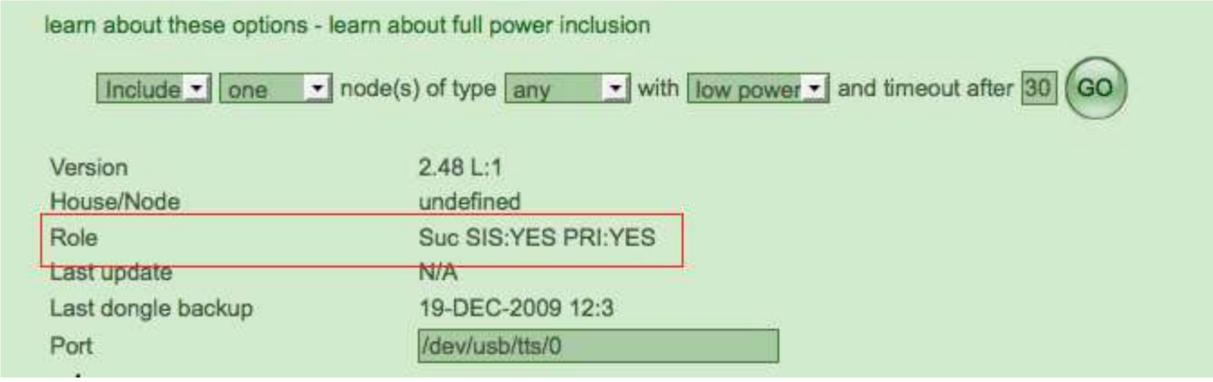
- The actual network topology and the information about all nodes are saved in a static controller and are therefore better protected than within a mobile battery powered device.
- All controllers in a network can integrate new devices.
- The network configuration and handling becomes very flexible.

Disadvantages:

- Function is available only from the firmware version 3.40. It is possible that there are some devices in the network with older firmware that do not support this configuration.
- Inclusion controller can integrate only devices if it has a wireless connection to the SIS.
- With the SIS there exists a "Single Point of Failure". A damaged SIS result in a complete new network setup.

Since the SUC/SIS functionality is already included in the firmware of most modern static controller, or a USB dongle, most Z-Wave networks can take advantage of these functions if a static controller is present. However, this function needs to be activated.

A static controller can also be a primary controller, as well as have SUC/SIS functionality. This configuration is typical in real networks.



learn about these options - learn about full power inclusion

Include ▾ one ▾ node(s) of type any ▾ with low power ▾ and timeout after 30 GO

Version	2.48 L:1
House/Node	undefined
Role	Suc SIS:YES PRI:YES
Last update	N/A
Last dongle backup	19-DEC-2009 12:3
Port	/dev/usb/tts/0

Figure 3.24: Controller rules shown in a Gateway User Interface

3.7 Networks with portable slaves

It was already described how a Z Wave network can handle a changing position of controllers or slaves. If slaves or static controllers are changed in their physical position, a new organisation of the whole network must be performed afterwards.

Get Lost

If an SUC controller is present in the network it is able to determine a new position of a slave and update the networks routing table accordingly. The procedure to achieve this is called in Z-Wave terms "Get Lost –Algorithm" and only works for routing slaves.
A normal slave is not allowed to send unsolicited messages and can therefore never determine any change of its position in the network, since no unsolicited message can fail. Routing slaves however have this ability.
If the sending of an unsolicited message from a routing slave fails, this routing slave will conclude that its routing table is not longer valid.

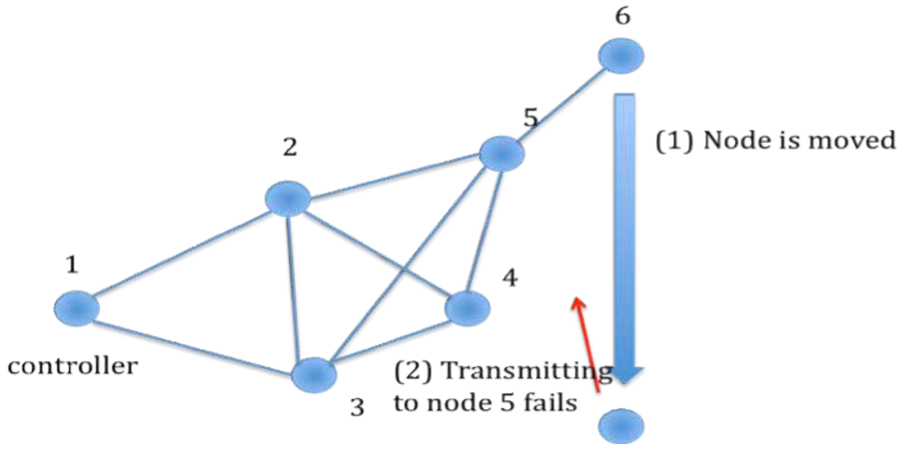


Figure 3.25: Routing-Slave realizes movement

As a first step this node will send out a broadcasting message to anybody with a "cry for help" message. A node that received an unsolicited "cry of help" message knows that the sender of this message has found itself in a new location. This node, however, is not possible to help the crying node with an updated routing table. If this node is also a routing slave and does have routing information about how to reach the SUC in the network, it will forward the "cry for help" message to the SUC.

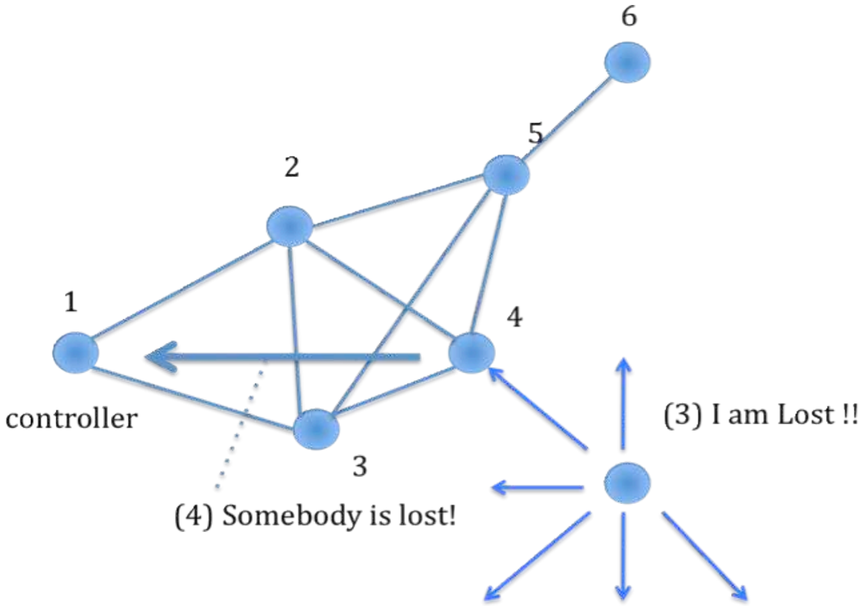


Figure 3.26: Routing-Slave cries for help

The SUC can update its own routing table and assign new routes to the crying node by performing the same steps he would do when including the device. The “cry for help” message is able to auto-heal a network in case a node has been moved.

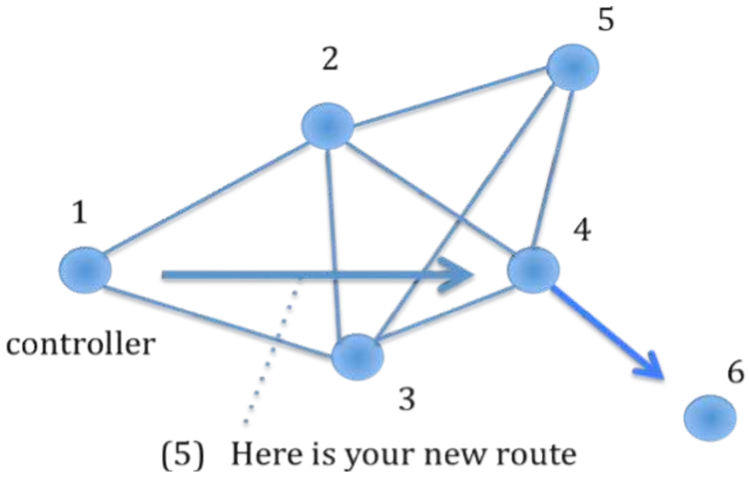


Figure 3.27: New Route for the moved Routing Slave.

In order to have a working auto-healing function within the network, the following requirements need to be fulfilled:

1. A SUC need to be present in the network
2. The moved nodes must be a routing slave not a standard slave.
3. In the new position there must be at least one routing slave in range.
4. The moved node must detect that he was moved. This is only possible if this node sends out an unsolicited message.

3.8 Inclusion and Exclusion in practise

This section describes how inclusion and exclusion of nodes works in practical terms.

3.8.1 Inclusion and Exclusion of Slaves

(1) Inclusion of nodes is always started by the primary controller (or any controller in case a SIS controller is present). The including controller must be turned into a so-called inclusion mode. This is done either by pressing a special key or a special key sequence or by turning a Z-Wave USB stick into the inclusion mode using control software on a PC.

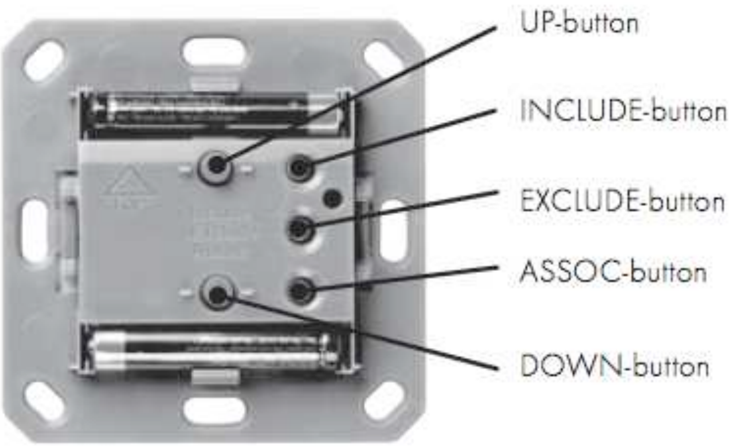


Figure 3.28: Wall Controller with special button for inclusion

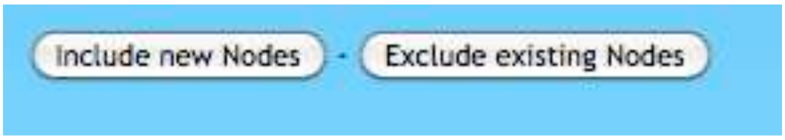


Figure 3.29: Example of Inclusion Function in PC software

(2) Once the controller is in the inclusion mode each node to be included need to confirm inclusion by performing a local action, typically pressing a button. All Z-Wave devices will have at least one button to confirm the inclusion. This may be a function button of the device, a dedicated inclusion button or simply an anti-tampering switch.

(3) The number of times the button needs to be pressed depends on the product and the vendor. Vendors either choose a single click or a triple click as confirmation sequence. To unify the user experience it is meanwhile recommended to use the triple press action for confirmation. Since the triple press always also performs a single press and two more single presses does not harm, it is recommended **to always do a triple press**.
The single or triple press of a button causes the node to issue an information packet, in Z-Wave terminology called **node information frame,** with its current Node ID and Home ID.

(4) If a controller in the inclusion-mode receives a node information frame it will check this frame. If there is no Home ID given, this frame will be included into the network by assigning a Node ID and the Home ID of the controller. This action is typically confirmed with a LED blinking or other useful form of user feedback. Otherwise the Information frame will be simply ignored.

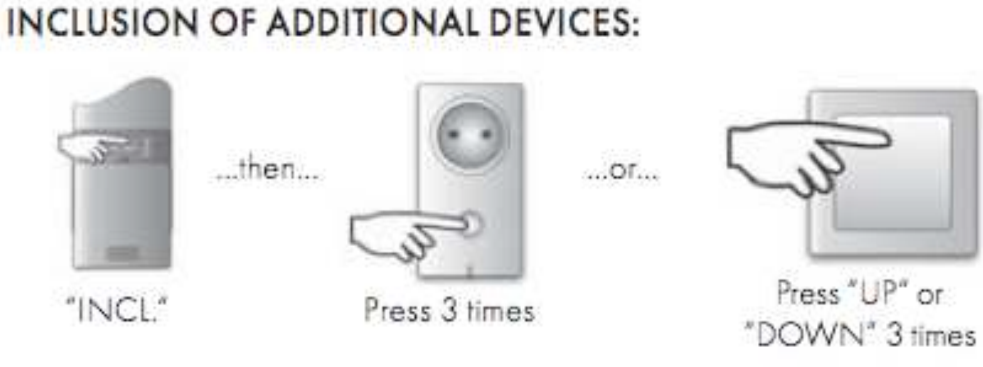

INCLUSION OF ADDITIONAL DEVICES:
...then...
...or...
"INCL."
Press 3 times
Press "UP" or "DOWN" 3 times

Figure 3.30: Example of a manual describing of the inclusion process

Figure 3.30 shows the manual section of a manufacturer about his Z-Wave products and the inclusion process. By pressing "INCL" on the controller here at an schematically displayed remote control – this device is moved into the Inclusion mode. The triple press on a button of a Z-Wave device gives a confirmation for the inclusion.

This process leads to the following conclusions:

(1) Only a controller can include new devices
(2) Its only possible to include a node which was not already included into a different network
(3) There is always a physical interaction needed at the device that is to include. This makes sure that no device is included against the will of the physical owner of the device. Having physical access to the device is defined an ownership in this regard.

In case a node shall be integrated into a new network that was already included in a different network this nodes must be detached from the previous network first. This process is called "**Exclusion**" and is performed the same way as the inclusion.

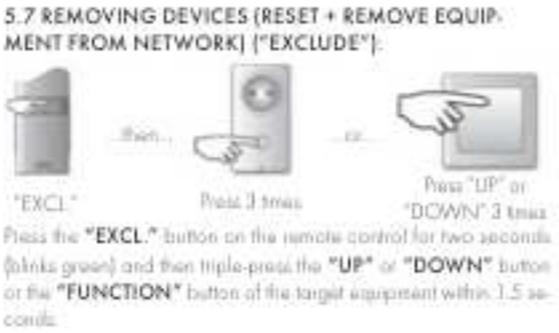
(1) The excluding controller must be turned into an exclusion mode. This is done either by pressing a special key or a special key sequence or by turning a Z-Wave USB stick into the exclusion mode using a control software on a PC.

(2) The node to be excluded has to send out a node information frame. Either single or triple press of a button on the device triggers this.

(3) If the excluding controller receives a node information frame from a node which contains a valid Home ID the controller will send this node a reset message to delete the Home ID and turn the node back into factory default status. If no valid Home ID is received which means that the sending nodes is not part of a network the process is terminated without any further action.

(4) Its possible to exclude multiple devices after another. As long as the controller is in the exclusion mode devices can be excluded. A special key sequence or pressing the exclusion key again typically terminates the exclusion mode.

Any Z-Wave controller regardless of its inclusion in the same network can perform the exclusion of a device. This is required to make sure that nodes from a network with damaged controllers can still be reused in a different network. However, a local interaction like pressing a button is required to proof the ownership of the node.



5.7 REMOVING DEVICES (RESET + REMOVE EQUIPMENT FROM NETWORK) ("EXCLUDE"):

then...
or
"EXCL."
Press 3 times
Press "UP" or "DOWN" 3 times

Press the **"EXCL."** button on the remote control for two seconds (blinks green) and then triple-press the **"UP"** or **"DOWN"** button or the **"FUNCTION"** button of the target equipment within 1.5 seconds.

Figure 3.31: Example from a user's manual describing the exclusion process

Within a Z-Wave device the exclusion leads to a full reset of all functions and settings back to factory default

3.8.2 Inclusion of Controllers

From the primary controller users point of view including a controller is similar to including a normal slave device. The only difference occurs behind the scene. After inclusion the primary controller will pass his routing table to the new secondary controller if he recognize that the new device is a controller as well. The process of including a secondary controller and handing over the routing table is referred to as **replication.**
While the primary controller is turned into inclusion mode, the secondary controller needs to be turned into a special mode as well which is referred to as Learn mode.
Only in Lean Mode a controller is able to replace his own Home ID by a new Home ID. Typically there is a special button or a sequence of keystrokes to turn a controller into the learn mode. Additionally the learn mode will time out quickly to protect the controller from unintentionally loosing his own Home ID and becoming part of a different network.

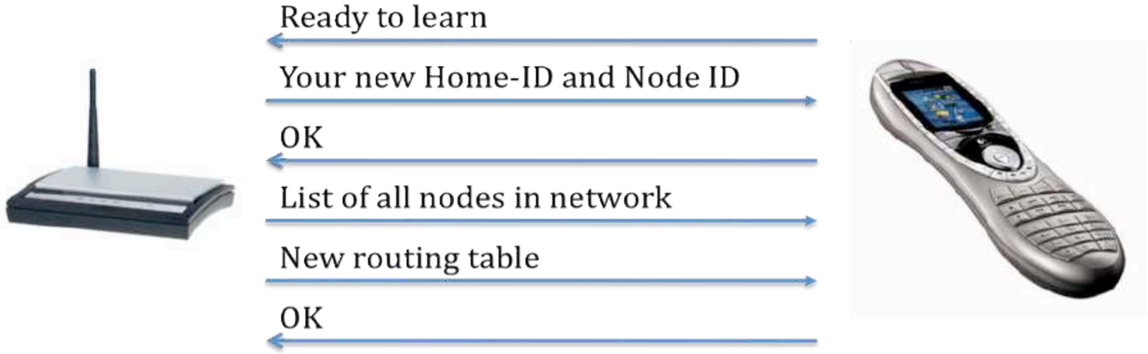


Figure 3.32: Controller-Replication

In case the secondary controller already had included other devices when he was a primary controller, but not yet included into a different network, these relationships will get lost when this controller receives a new Home ID and becomes a secondary controller. It's therefore recommended to only include controllers into a secondary network that had not acted as primary controller before and are in factory default state.

Figure 3.33: Example of Controller Inclusion in PC software

3.8.3 Inclusion of battery operated devices

Battery operated devices are in a sleep state on default. In order to send and receive messages these devices need to be activated.
To save battery power, battery operated devices will limit the active time of inclusion mode or exclusion mode even further.

It's possible that the root cause of a failed inclusion of a battery operated device is the simple fact, that the device has been turned back into sleeping state already too quickly.

It is therefore recommended to include battery-powered devices right after inserting battery without loosing any time.

4 Application Layer

So far we only looked at how different nodes can communicate with each other. The application layer of the Z-Wave product now defines and specifies **what and why** two nodes communicate with each other.

4.1 Types of Z-Wave Devices

In theory every controllable or controlling device in a home or office can be equipped with Z-Wave technology. Hence one should expect a broad variety of different devices and functions. However there are some basic functionality patterns that allow categorizing different devices.
Each device will either control other devices or being controlled by other devices. In the Z-Wave terminology controlling devices are called controllers, reporting devices are called sensors and controlled devices are called actuators. It is also possible to combine a logical sensor controller or actor function within one physical device.
Actors switch either digital (on / off for a electrical switch) or analogue signals (0 %. 100 % for a dimmer or venetian blind control). Sensors deliver either a digital signal (door, glass breaking, motion detector, window button on the wall) or an analogue signal (temperature, humidity, power).

In today's market of Z-Wave device there is a surprisingly short list of different product categories. Nearly all Z-Wave devices on the market can be categorized into one of the following function groups:

1. Electrical switches are designed either as plug in modules for wall outlets or as replacement for traditional wall switches (digital actors). It's also possible to have these actors already built into certain electrical appliances such as electrical stoves or heaters.

2. Electrical dimmers, either as plug in modules for wall outlets or as replacement for traditional wall switches (analogue actors)
3. Motor control, usually to open or close a door, a window, a window sun blind or a venetian blind (analogue or digital actors)
4. Electrical Display or other kind of signal emission such as siren, Led panel, etc (digital actors)
5. Sensors of different kind to measure parameters like temperature, humidity, gas concentration (e.g. carbon dioxide or carbon monoxide) (analogue or digital sensors)
6. Thermostat controls: either as a one knob control or using a temperature display (analogue sensors)
7. Thermostats controls such as TRVs (Thermostat Radiator Valves) or floor heating controls (analogue or digital actors)
8. Remote Controls either as universal remote control with IR support or as dedicated Z-Wave Remote Control with special keys for network functions, group and/or scene control
9. USB sticks and IP gateways to allow PC software to access Z-Wave networks. Using IP communication these interfaces also allow remote access over the internet

The following images give an idea about the variety of products based on the Z-Wave standard.

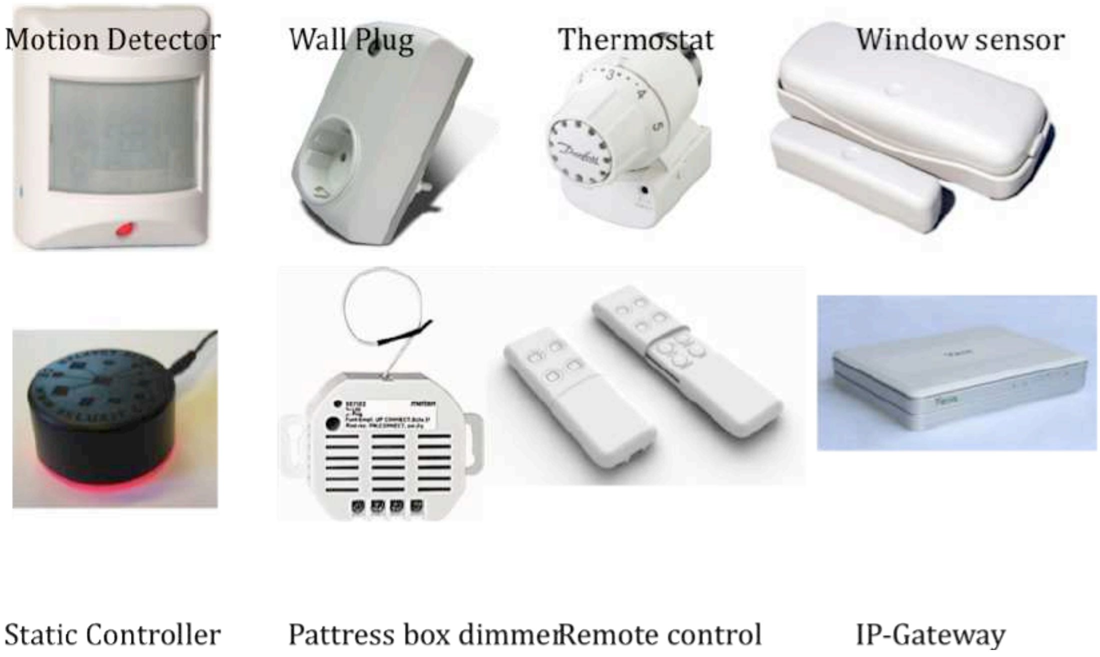


Figure 4.1: Different Z-Wave Devices

4.1.1 Command Classes

All communication within the Z-Wave network is organised in Command Classes. Command Classes are a group or commands and responses related to a certain function of a device.

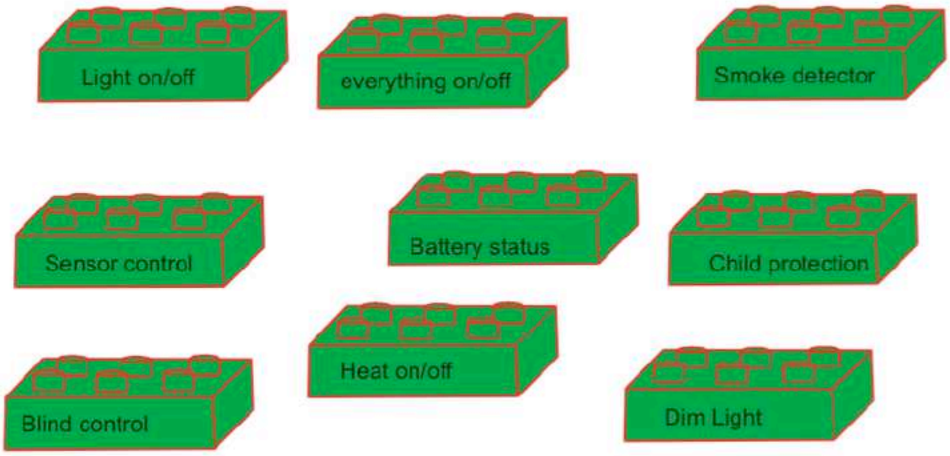


Figure 4.2: Examples of different command classes

A normal on/off switch is referred to as a binary switch. The basic function of a binary switch is to be switched on and off. With a Z-Wave system it is also possible to know the status of the switch, hence a status request function and a status report function is required too.

The Command Class for a binary switch consists of three different function responses, commands or reports.

- Binary Switch – Set: is sent from a controller to the switch to turn the switch on or off
- Binary Switch - Get: Is sent from the controller to the switch to request a report about the switching state.
- Binary Switch – Report: is sent from the switch back to the controller as a response to the Binary Switch Get Command.

These three commands and responses are grouped and referred to as command class „Binary Switch‟. If a certain Z-Wave device supports the command class binary switch it is supposed to be able to deal with all these commands:

- The switch need to understand the set command and set the switch accordingly
- The switch is able to receive a get command and is able to response with a report command in the proper format.

Annex A gives an overview of the different command classes defined in the Z-Wave protocol.

4.1.2 The command class „Basic“

Command Classes represent the functions of a certain Z-Wave device. Switches will support different command classes rather than thermostats.

To make sure Z-Wave devices can communicate with each other even without further knowledge about their specific function, there is one special command class called “basic”.

The basic command class consists of two commands and one response:
- SET: set a value between 0 and 255 (0x00 …0xff);
- GET: ask the device to report a value;
- REPORT: response to the Get command. Reports a value between 0 and 255 (0x00 … 0xff);

The specialty of the basic command class is that every device will interpret the basic commands dependent of its specific functionality.

- A binary switch will switch on when receiving a value 255 and switch off when receiving a value of 0;
- A thermostat may turn into a convenience temperature mode when receiving value = 0 and may turn into a energy saving mode when receiving a higher value;

- A temperature sensor will issue a basic report and send a integer temperature value;
- A door sensor will either send out a value = 0 in case the door is closed or a 0xff when the door is opened.

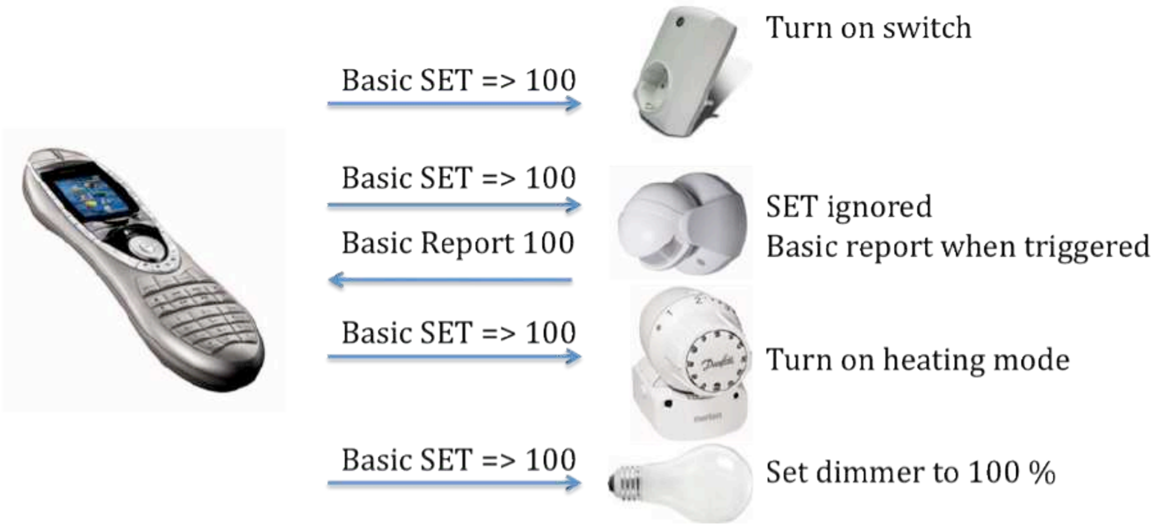


Figure 4.3: Basic Command Class

The basic command class is the smallest common denominator of all Z-Wave devices. Every Z-Wave device must support the Basic command class.

4.1.3 Device Classes

To allow inter-operability between different Z-Wave devices from different manufacturers, certain Z-Wave device must have certain well-defined functions above and beyond the basic command class. The structure behind these requirements is called device class. A device class refers to a typical device and defines which command classes are mandatory to support.

Device classes are organised as a hierarchy with three layers:

- Every device must belong to a basic device class;
- Devices can be further specified by assigning them to a generic device class;

- Further functionality can be defined as assigning the device to a specific device class.

Basic Device Class

The BASIC device class makes a distinction merely whether the device is a controller, a Slave or a Routing-Slave. Therefore every device belongs to one basic device class.

Generic Device Class

The generic device class defines the basic function as device is supposed to offer as a controller or slave. Current generic device classes are:

- General controller (GENERIC_CONTROLLER)
- Static controller (STATIC_CONTROLLER)
- Binary switch (BINARY_SWITCH)
- Multi level switch (MULTI_LEVEL_SWITCH)
- Binary sensor (BINARY_SENSOR)
- Multilevel-Sensor (MULTILEVEL_SENSOR)
- Meter (METER)
- Input controller (ENTRY_CONTROL)
- Thermostat (THERMOSTAT)
- Window Venetian blind controller (WINDOW_COVERING)

Specific Device Class

Assigning a specific device class to a Z-Wave device allows it to specify the functionality of the device further. Each generic device class refers to a number of specific device classes. Assigning a specific device class is voluntary and only makes sense, if the device really supports all specific functions of a specific device class. Special device classes are, for example:

- Setback Thermostat (SETBACK_THERMOSTAT) is a specific device class of the generic device class “Thermostat“;
- Multi-level Power Switch (MULTILEVEL_POWER_SWITCH) is a specific device class of the generic device class Multilevel Switch;

In case the Z-Wave device is assigned to a specific device class, it is required to support a set of command classes as functions of this specific device class.

These required command classes are called **mandatory command classes** and they are individual of certain generic and specific device classes.

Above and beyond the mandatory device classes, Z-Wave devices can support further optional command classes. They may be very useful but the standard does not enforce the implementation of these classes.

A Z-Wave manufacturer is allowed to implement an unlimited number of optional device classes, however if these device classes are implemented, the standard defines how these commands and functions are to be supported.

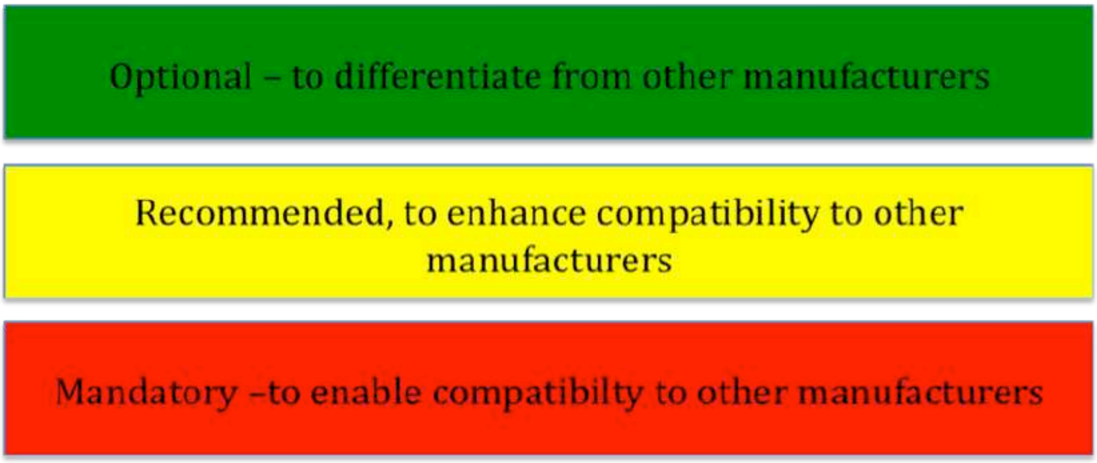

Optional – to differentiate from other manufacturers
Recommended, to enhance compatibility to other manufacturers
Mandatory –to enable compatibilty to other manufacturers

Figure 4.4: Optionally, recommended and mandatory Command Classes within a device class

The basic device class, the generic and, if available, the specific device class is announced by the device during inclusion, using a Node Information Frame.

As well as the device classes, the Node information frame also announces all optional command classes of the device included. With this announcement, a controller can control and use an included Z-Wave device according to its functionality.

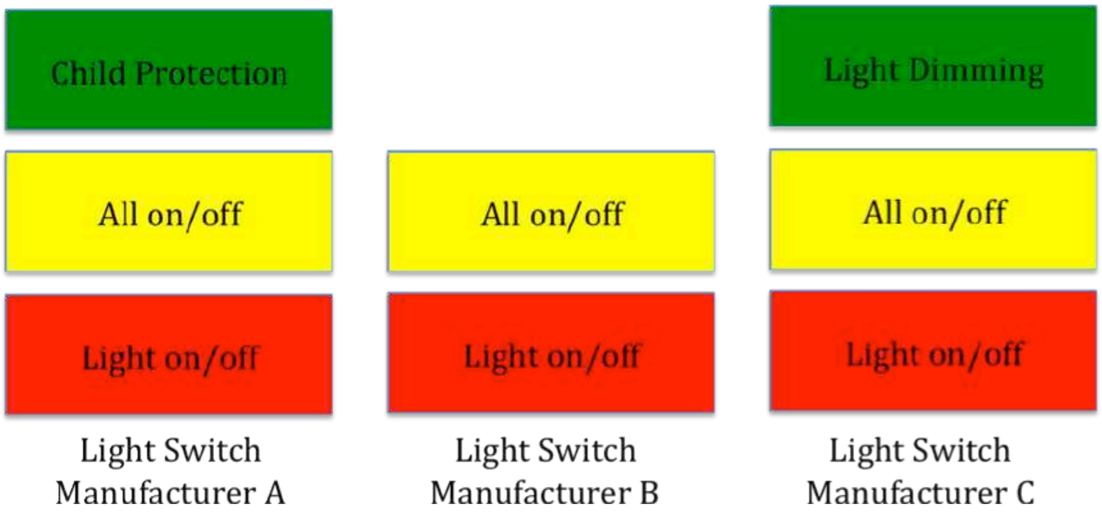


Figure 4.5: Different Implementation of a Device Class „Binary Power Switch" by different vendors

A Z-Wave device works according to the Z-Wave standard if

- It belongs to a basic device class and a generic device class, and is able to report these classes on request using a Node Information Frame.
- It supports all mandatory command classes of the basic and generic command class by sending commands and reports as well as accepting and executing commands according specification of the command class;
- In case a specific device class is defined the mandatory command classes of this specific device class, needs to be supported as well and the specific device class needs to be reported on request;
- In case optional command classes are implemented, these command classes need to be announced in the Node Information Frame on request and need to be supported according to the Z-Wave command class specifications. Frame on request and need to be supported according to the Z-Wave command class specifications.

Z-Wave defines a broad variety of command classes covering almost every aspect of home automation and control. Nevertheless it's possible that manufacturers want to implement further functionality not already defined in a command class specification.

The command class “proprietary function” is defined to cover these needs. A proprietary function would allow a manufacturer to implement specific functions that can then be used only by other devices supporting this proprietary function as well.

The use of a proprietary function is subject to approval by the Z-Wave alliance certification authority and is required to be documented extensively. So far only very few device make use of this function. Typically new requirement result sooner or later in an amendment to the existing standard, which makes this function part of the official standard and any proprietary extension becomes obsolete.

One example shall illustrate the use of device classes and command classes:

Figure 4.6: Schuko Wall Plug

A manufacturer wants to offer an Schuko Plug-in Switch as shown in Figure 4.6. The basic function of this switch is switching the mains on and off.
Since such a device can be used at multiple locations the basic device class “routing slave” is used.
As a binary switch the device belongs into the generic device class “BINARY SWITCH”. It is allowed and in this case even recommended to use a specific device class Binary Power switch since this Schuko plug switch will always switch power lines.

- Basis class: Routing-Slave
- Generic class: Binary switch
- Special class: Binary switch for power

1. The binary switch device class requires the implementation of the mandatory command class “binary switch” and of course the implementation of the basic command class.
2. As binary power switch the device is furthermore requested to implement the so-called “switch all” command class. This is a command class a controller may send to all devices in the network to an “all off” function. The “switch all” device class also implements ways to configure the device under which circumstances it should react to this “switch all” command issued by a controller. A generic switch is not required to implement such a command class, since an “all off” command may not mean something useful to a generic switch. In case of a power switch an “all of” command is clearly defined and therefore a mandatory command class.

   If would be allowed by the standard not to implement the “switch all” command class but in this case the device is not allowed to announce a specific device class “binary power switch”. A switching device without “Switch All support” which just announces a generic device class “Binary switch” would still be a valid Z-Wave compliant device.
3. The manufacturer wants to offer more a competitive product and adds further functionality to the switching device. One may be the so called “child protection”. A Child protection function on a binary switch means the ability to turn off all local control capability and only allow switching the device wirelessly.
4. If the manufacturer decides to implement such function the standard defines in the “protection” command class how to do this. Also the optional command class “child protection” needs to be announced in the Node Information Frame.
5. The manufacturer may decide to further enhance the switch by offering a special function, which randomly switches the device

on and off. In conjunction with a lamp this function may be used as anti theft device in the home.

At the moment there is no command class defining such a capability. The manufacturer could now ask for approval to implement this function and still be certified as Z-Wave compliant device. Depending on the approval the function would be realized as “proprietary function”.

4.2 Configuration

The Z-Wave standard defines that every device shall be functional on factory defaults. Nevertheless there are device, which may require further user and application specific setups such as

- Sensitivity of a motion detector
- Behaviour of control LED lights
- Switching delay of an alarm sensor
- Specific behaviour under error conditions

The configuration of a device is performed using the optional command class “configuration”. The configuration command class allows the setting of up to 255 parameters with one value each. A configuration is device specific and all parameters and possible values need to be described in the manufacturers manual.

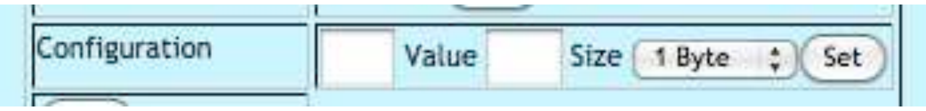


Figure 4.7: Example of a Configuration Interface in PC Software

In order to do a configuration the user needs to know the configuration parameter number and the desired value.

Example: Configuration of a status LED on a device.

Parameter # 2: switches the Led on the device on, off or blinking according to status of the device

Value = 0:	*Always off*
Value = 1:	*Blinks when active*
Value = 2:	*Always on*

Configurations are usually done using static controllers, either as PC software or an IP gateway. This allows giving a nice graphical interface for setting up the configurations. Modern Software solutions use a verbal translation of the configuration parameter number by using databases that give further information about the configuration parameters and possible values.

4.3 Battery operated devices

Battery-operated devices are a special challenge within a Z Wave network, because they are mostly in a sleeping state for current savings reasons and cannot be reached from a controller in this state.

Battery operated device know two states:

- They are awake and can communicate with other devices of the network
- They are sleeping and do not communicate at all. For other controllers they may appear as non existing to damaged

In order to allow communication with battery operated devices a mains powered and therefore always active static controller needs to maintain a waiting queue, where all commands are stored which are to be sent to a sleeping device. When the battery operated device wakes up it will inform this controller and “empty the mailbox”.

At the moment a battery operated device wakes up it sends a so-called WAEKUP_NOTIFICATION to the controller and stays awake. The WAKEUP_NOTIFICATION indicates to the controller that the battery device is now listening to commands. If all commands are sent the controller will send a final command "NO_MORE_INFO" to indicate to the battery device that it can't go back to sleeping mode.
If the battery operated device does not receive a "NO_MORE_INFO" if will go back to sleeping mode after a defined time.

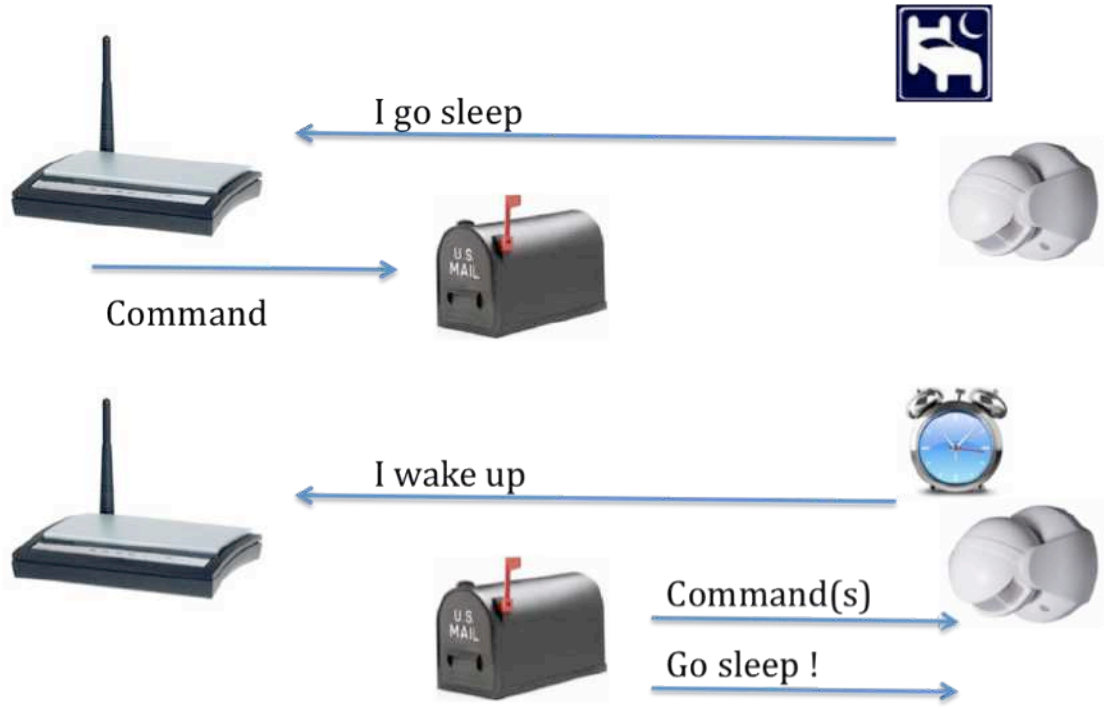
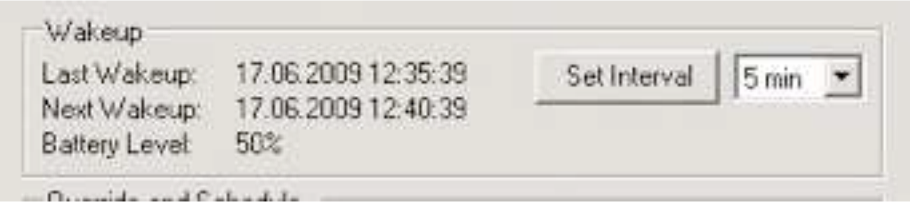


Figure 4.8: Sleeping and wakeup

The operation of battery-operated devices requires at least one static and mains powered controller in the network to store commands for sleeping battery devices.
If a local action on a battery operated device is performed such as pressing a button the battery device is usually woken up immediately to issue a command according to this action. Each battery device needs to have a defined local action for wake up such as pressing a certain button.



Wakeup

Last Wakeup: 17.06.2009 12:35:39

Next Wakeup: 17.06.2009 12:40:39

Battery Level: 50%

Figure 4.9: Example of a wakeup time dialog

Most battery-operated devices will have an internal timer, which wakes up the device regularly to check for queued commands. This maximal sleeping time can be configured. A typical sleeping interval is between 30 seconds and days and can usually be configured on a user interface of the controller. Any change of the wakeup time will, like any other command sent to the battery device, become effective after the next wakeup.

Certain devices will limit the wakeup interval to a maximum and minimum value. Unfortunately it is not defined how the device shall react if a forbidden interval value is configured.

Therefore the wakeup command class was extended to allow manufacturers to announce a minimum and maximal wakeup time during configuration. If these new command classes are used a misconfiguration is impossible. Nevertheless its worth to refer to the manufacturers manual for further information.

To allow an initial configuration of a device after inclusion every battery device shall stay awake for a defined time, which may vary between 20 seconds and some minutes.

Table 4.1 summarized again the different states of a battery operated device and the conditions to change the status,

Situation	**Awake**	**Sleeping**
Inclusion	Right after inclusion	Turns into sleeping mode after a couple of minutes without any

		further user action.
Regularly	Wakes up after a defined interval and sends a notification to static controller. Typical Wakeup intervals are between minutes and hours and can be configured by the user within certain boundaries	Controller can turn back the battery-operated device by sending a command. Otherwise the battery device turns back into sleeping mode after a defined time (usually a minute)
Local operation of the device	Wakes up on every local operation and communicates status if needed (e.g. button pressed)	Immediately after finishing action

Table 4.1: Conditions to change state for battery operated devices

This wakeup/sleep behaviour may cause a couple of failures or unclear conditions.

4.3.1 Typical Failure during Inclusion into a Network

It’s a common approach to include multiple devices one after each other. However it can happen that a battery powered device may be sleeping already when the controller wants to include it. The controller will not “see” the device and may conclude that the device does not exist or is dead.

The battery-operated device will usually wake up after a defined time interval but this may happen after multiple hours or days.

Therefore its recommended to configure the battery-operated device right after inclusion or make manually wakeup the device later on for configuration. In case of manually wakeup it may happen that the device goes back into sleeping mode right after wakeup if no further information is available from the static controller.

It’s possible that a battery-operated device wakes up but does not know where so send the wakeup information to. This happens if the device was not configured after inclusion to know the Node ID of the static controller who holds his command waiting queue.
Therefore it’s highly recommended to configure a battery operated device right after inclusion and to have the static controller included first. Only then the static controller is able to configure the battery-operated device correctly.

Certain devices will stay awake after first power up only and go right into sleep state after first inclusion. This is not longer accepted by the standard but older model may behave like this. If the device is powered up using the batteries and is included into the network much later it may result again in an error since the battery device will not stay awake long enough after inclusion to allow correct configuration.

Therefore it is recommended to follow the following guideline when including battery devices into a Z-Wave network:

1. Include every battery-operated device right after inserting the batteries the first time. Make sure to configure a reasonable wakeup time before the device goes into sleeping state for the first time.
2. In case there is further configuration work to do configure a low wakeup time first but make sure that you configure a longer battery saving wakeup time when all configuration is finished.
3. Do not batch include and configure afterwards and don’t loose any time after inclusion to configure the device.
4. A reasonable wakeup time is a trade-off between two goals:
    a. A very long wakeup interval will save battery capacity but may create problems in case of network reorganization. The static controller may not hear anything from the battery device during the reorganization and then threat the device as not functioning.
    b. A very short wakeup time helps the controller to keep track of the device but costs battery lifetime.

5. The wakeup interval must be configured between the allowed boundaries. Refer to the manual of the manufacturer has set any boundaries.

4.3.2 Maximization of battery life time

The battery lifetime is the critical measure of battery-operated devices. Therefore some estimates should be given and taken into account.

- A typical Alkaline-Microcell (AAA) has an energy capacity of approx. 1000 mAh. A typical battery-operated sensor has 2 such batteries.
- A Z-Wave module of the class 300 consumes 2.5 myA in the hibernation state and 21 mA in the wakeup mode. During transmission of packets about 36 mA are required. Table 4.2 shows the current need of the single chip generations in their respective working conditions.
- Additional battery power can be used for the devices functionality such as operating an infrared sensor or moving a thermostat valve. This power consumption varies from device to device and is usually only a fraction of the power used for the electronics. For the following estimate this portion of the power usage should be neglected

Chip Generation	Hibernation (mA)	Transmitting (mA)	Listening (mA)

100	31	25	21
200 (since 2005)	2.5	36	21
300 (since 2007)	2.5	36	21
400 (since 2009)	1	23	21

Table 4.2 Power consumptions of different chip generations

If a sensor is in the active reception mode constantly, his battery is empty after 1000 mAh / 21 mA = 47 hours = 2 days!

It is therefore mandatory to move a battery-operated device into the sleeping state. The maximum battery lifetime in the permanent sleeping state for the accepted configuration is 1000 mAh / 0.0025 mA = 400,000 hours = 16.666 days = 45 years. In this time even alkaline batteries will have become empty by self-unloading.

If a battery device is not turned back into sleeping mode right after wake up and exchange of queued commands from the mailbox the device will stay in listening mode for about one minute A transmitting time of 1% of the reception time is assumed corresponding with the regulation of the Z-Wave radio standard. The programmed wakeup interval determines, how long the battery will last.

Wakeup interval	Battery life time
120 Seconds	4 days
1800 Seconds = 30 Minutes (typical)	118 days
24 hours	2439 days

Table 4.3: Battery Lifetime as function of wakeup time

A battery lifetime of 118 days (under disregard of all local operations like blinking of a LED, moving of a motor etc.) is still unacceptable. Hence, it is necessary to operate a static controller in the network to manage battery-operated devices and shorten the wakeup time.

If a static controller is programmed in a way that he will send every device back into sleep mode right after wakeup and cleaning the mailbox the battery live time is extended dramatically.

Assuming typical wakeup intervals and assuming that 50 % of the wakeup time is used for transmitting signals from the battery operated device to the controller with a total communication time of 50ms. Table 4.4 shows the resulting battery lifetime.

Wakeup interval	Battery lifetime
120 seconds	59 days
1800 seconds = 30 minutes (typical)	850 days
24 hours	12400 days

Table 4.4: battery lifetime depends on wakeup interval

These numbers are only valid under the assumption that no additional power is used for the functionality of the battery-operated device, e.g. turning a valve of a heat of measuring some environmental data. Assuming a factor of 50 % of the total power consumption for these functions the resulting battery lifetime is in the neighbourhood of 1 year that confirms values given on vendor data sheets for typical battery operated devices.

However to reach these value the presence of static controller is mandatory managing the battery operated devices. In a network with only portable controllers the lifetime of battery powered devices will be shortened. The values of table 4.3 should apply in this case.

These estimate are only applicable for battery operated slave devices. Portable controllers, which are battery-operated devices as well, will always sleep unless pressing a button wakes them up. Hence, the battery life time of these device totally depends on the self discharging effect of batteries and the usage pattern and will typically reach 2...3 years.

4.4 Groups, Scenes and Associations

With Z-Wave, you can not only operate individual actions with appliances such as lights, heating and window blinds, but also create “Scenes” like “Leave for Work”, and select what you want to happen in your home, when you leave for the day.

Also you can create **“Events”** which react when something happens – so for example, when a motion detector is tripped, a light can come on for 5 minutes.

And if that wasn’t enough, there is a **“Timer”** setting where you can set the lights or the thermostat to go on or off at a certain time.

If you are at work, its good to be reassured that lights are going off when they should for example. The VERA Gateway is great for this, as VERA can reassure you with an optional text message alert to tell you everything is ok! Through the FREE optimized iPhone application, VERA offers additional support to help you manage all your Z-Wave devices.

VERA is focused on simplicity. It does “complicated” things but in a really simplistic way. It’s centred on usability and practicality, making managing your home energy consumption a joy rather than a chore.

Literally, just plug in the VERA Gateway and setup is quick and automatic. It even doubles up as a pre-configured Wi-Fi access point, Firewall, gateway and router, giving you a secure wireless home network.

Z-Wave technology is really effective when setting up a home security management system. You can control your alarms remotely using Z-Waves, as well as set your doors, windows and motion sensors to high alert. With the aid of Z-Waves, the components can be managed by a central home hub - Gateway VERA, so if a detector senses an intruder, then a signal to VERA will set off lights, alarms and even a text message to alert you at work.

The uses of more complex usage patterns are best managed using Association, Groups and Scenes.

4.4.1 Associations

In a typical Z-Wave network, the controller communicates with slaves in two typical ways. They send out commands to change the status of slaves, e.g. switch them on or off – and they receive status information from sensors, e.g. movement info from a motion detector (only from routing slaves). Meaningful function in a network may include dependencies and interaction between two slaves as well. Example: One Z-Wave device is a motion detector, a second device shall be a power switch controlled by a remote control. It' s the desire that the switch shall switch on, if a motion is detected.

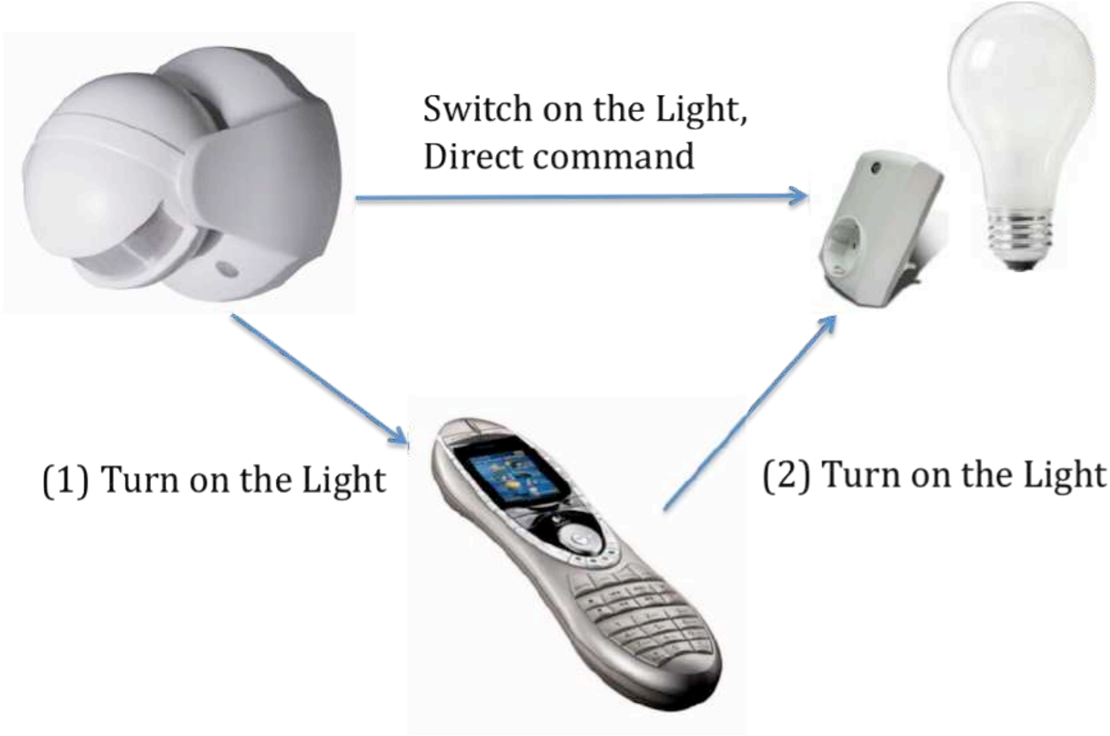


Figure 4.10: Small Z-Wave Network with Association

One setup would be that the motion detector sends a signal to the controller and as a second step the controller sends the switch command to the power switch. However this means that:

- The controller is added as additional source of failure;
- The communication takes much longer then necessary;
- The controller needs to be in the listening mode, which means it needs to be a static controller;

An association allows that the motion detector sends its signal directly to the power switch without involving the controller. This allows using sensor even in a network without a static controller. This saves time, reduces the complexity of the communication and the amount of airtime, which directly translate into allocation of the wireless communication channel and the electromagnetic emission.

To be able to use an association, the sending node (in the example the motion detector) must have the knowledge of a valid route to the destination (in the example the power switch). Therefore only a routing slave or a controller can use associations. A normal slave does not have any information about routes and only send signals as answer to received commands.

In order to set an association the sender needs to learn about the node id (s) of the receiving node (s).

There are two different ways to accomplish an association scenario:

Direct Association:

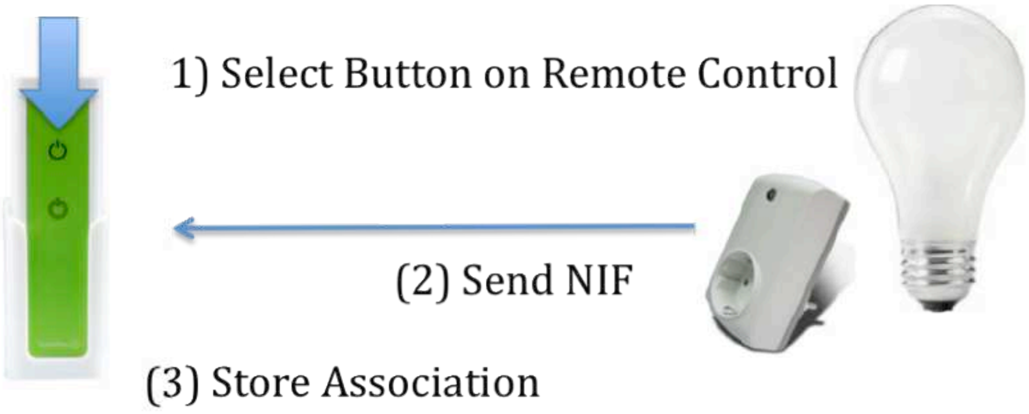


Figure 4.11: Direct Association

The source node of the association will be turned into an “association set mode” waiting to receive a node information frame from the device to associate. The receiving node needs to send out node information usually accomplished by just pressing a button. The node information frame received contains the Node ID of the association partner and allows the source node to set the association.

Because the node information frame is always sending out as a broadcast to all nodes “in range” direct association only works if both sender and receiver as “in range” which means they have a direct not routed wireless connection established.

Assigned Association

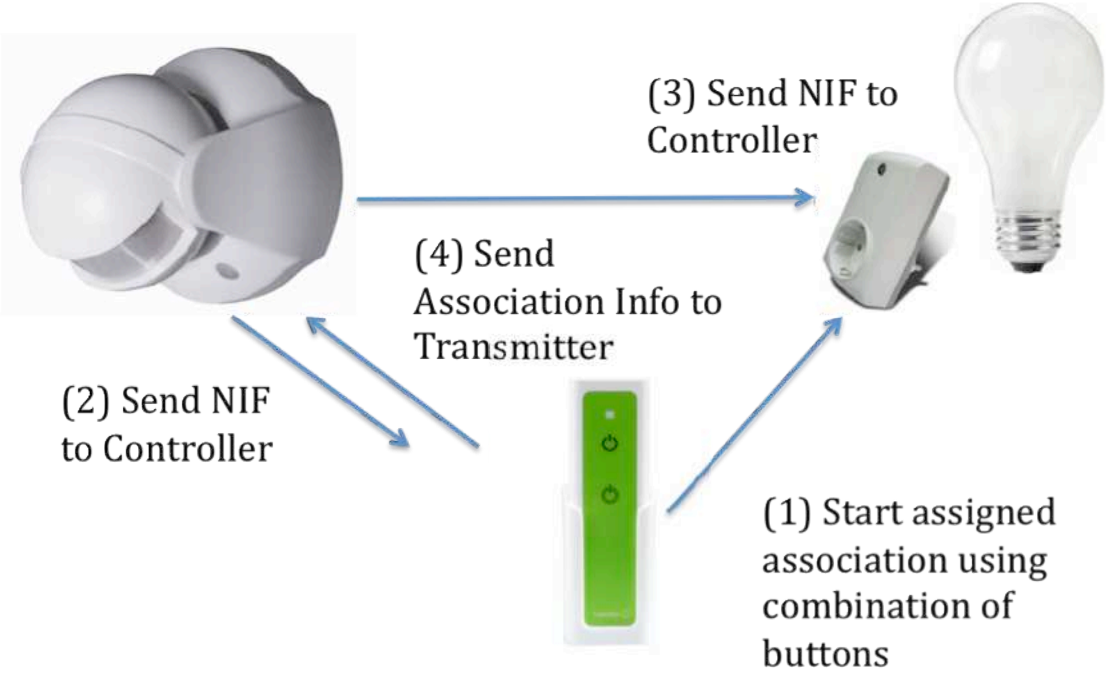

(3) Send NIF to Controller
(4) Send Association Info to Transmitter
(2) Send NIF to Controller
(1) Start assigned association using combination of buttons

Figure 4.12: Assigned Association

Assigned associations allow connecting two Z-Wave devices, which are not in range. To do this the help of a third node –a controller with knowledge of the complete network and its routes is needed.

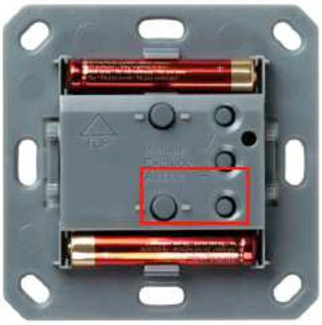


Figure 4.13: Wall controller with dedicated button for Association

The connecting controller needs to be turned into a association mode by either pressing dedicated buttons or selecting a function on a PC software controlling a USB connected Z-Wave transceiver.
The controller now expects (1) a node information frame from the desired source and in a second step (2) a node information frame from the desired target node. Again the Node Information frame can only be received by nodes in range, hence the controller need to be brought in direct wireless range of the two nodes, but not at the same time.
First the controller is near the source node receiving its Node information frame and in the second step it needs to be places near the target node to receive its node information frame as well.
In a last step the controller will communicate with the source node and set the association by informing this node about the association target and the route to reach this target. The user accomplishes this without further interaction. Since the controller knows the route to the target node its not required to bring the controller back in range to the target to perform the final configuration.

A node needs to announce its capability to accept an assigned association configuration in his node information frame.
It„s possible to have multiple target nodes assigned to one single source node. All these target nodes will receive the same command at the moment when the event takes place triggering the event, which was configured by association.
It is possible that there are multiple different events, which may cause to send commands to different nodes. The number of target node that can be associated to this given node for the given event are called association groups.
The number of different association groups (i.e. different event which can cause to send out a command to associated nodes) and the maximal number of nodes, which can be associated to a given group, are a performance indicator for Z-Wave devices.

An example of a Z-Wave device with association is a wall switch with two switching paddles.

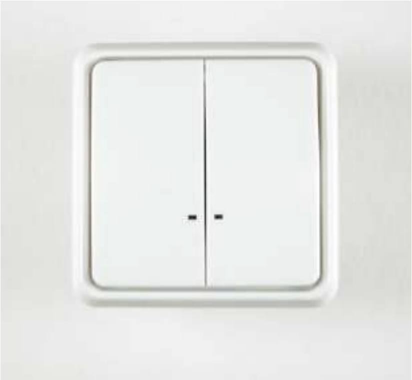


Figure 4.14: Wall controller with two switching paddles

For this particular product there should be at least two association groups, one for the left and one of the right paddle. A lot of vendors of wall switches offer even more groups, which get activated when doing a double press or press both paddles at the same time.

The number of receiving nodes per groups is typically limited to five devices. This limitation is caused by the limited memory space of the device, hence it’ s possible that certain device without memory constrains offer many more possible target nodes.

If nodes are assigned to one of the association groups of a device this device will send a signal to all the target devices every time this groups gets activated – typically by pressing a button, a combination of buttons or when a sensor value reached a certain level.

To make sure a maximum number of different target devices can be controlled, most devices with association functions will use the BASIC command class to control target devices. However there are devices on the market offering to configure which command class to be used to control target devices. With this feature it„s possible to execute very special functions on the target device.

The inclusion function of a device includes the device into a network and makes sure that the device is able to communicate with other devices in the network. The association function describes a specific action between a specific sending and a specific receiving node. The action is triggered by a certain condition at the sending node (e.g. button pressed) and will cause a certain action at the receiving node. Associations are also used to assign certain remote control buttons to certain devices in a Z-Wave network.

4.4.2 Groups

It is possible and usual to connect multiple devices from one single button on a remote control. These controllers, joins certain devices into a group and control them, as if they are one device. This means that all devices are switched simultaneously when the button is pressed. Since all devices in a group receive the very same switching commands, it‘s useful to only group similar devices into one group. If different devices are mixed, the result can be surprising and confusing.

Similar to associations, most remote controls only use the BASIC command class to control groups. This allows mixing different devices but only to a certain extent. Mixing a dimmer and a switch will result in the dimmer acting as a switch.

Most remote controls describe the switching of groups but don’t refer to the switching of a single device. In order to switch a single device it’s possible to just place this single device into a group and switch the group. It„s also possible to assign one device into different groups.

4.4.3 Scenes

The definition and the usage of scenes is a very powerful tool to control Z-Wave networks. Like a group, a scene groups together multiple Z-Wave devices. While groups tread all devices similarly, scenes cause a controller to send different commands to different devices. This results in endless possibilities such as: “turn switch off and open the window B” or “dim all lamps to 50 % and turn on the TV”. Scenes are very flexible and much more powerful than groups, but take a lot of memory to store the different commands. Hence in a remote control the number of scenes is typically much smaller than the number of groups. Static controllers such as IP gateway or PC software typically allow an almost unlimited amount of scenes.

4.4.4 Comparison of groups, scenes and associations

Groups, Scenes and Associations are different ways to realize functions and interactions within the z-wave network.

	Used in	**Function**
Associations	Slaves	Sends control signals to one of more target devices (Slaves or controller)
Groups	Slaves and controllers	Grouping of multiple devices receiving the same control message - typically via association (from Slaves or controllers)
Scenes	To controllers	Activation of a scenes leads to switching different devices using different control messages

4.5 Usage of IP-Gateways

IP gateways allow a very user-friendly configuration and usage of a Z-Wave network. Different functions and sensor values can be access using a convenient web interface or even a mobile phone like the iPhone.

The user friendly and usually self-explaining web interface allows performing all relevant functions of a Z-Wave network in a convenient way.

These gateways offer user interfaces for user management and special interfaces for mobile access.

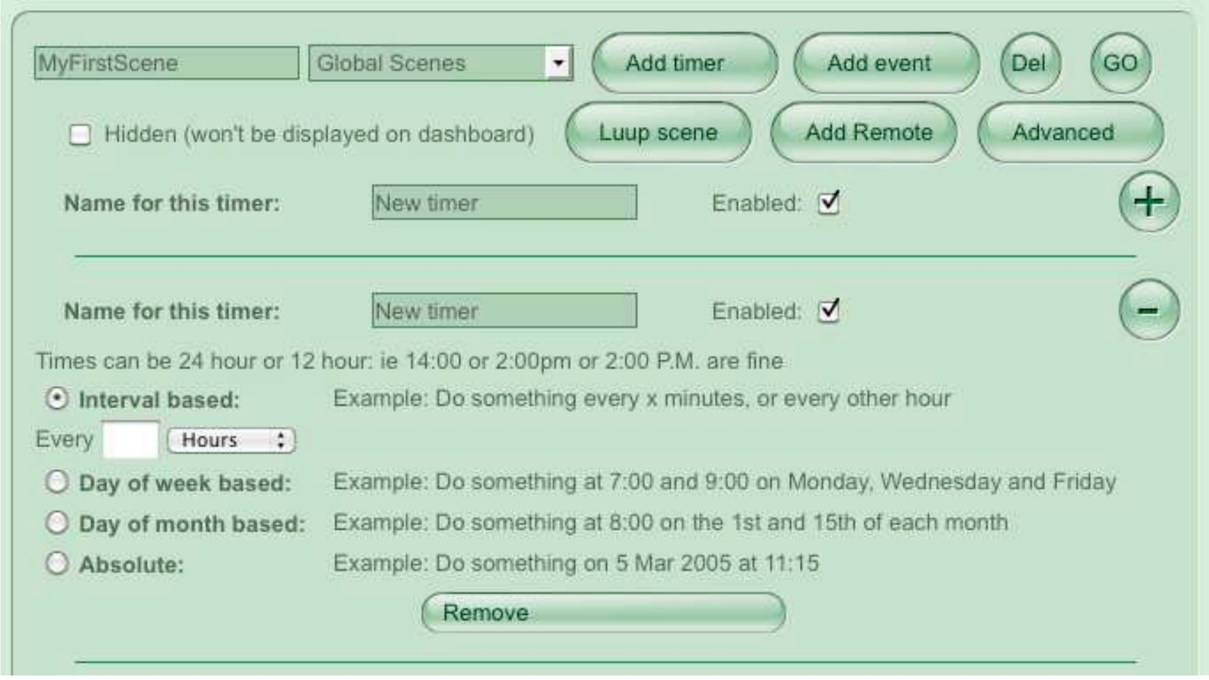
In order to increase usability, devices can be assigned to different rooms or zones of the home. Some gateways offer an upload opportunity for floor plans.

The central function of an IP gateway is the definition and activation of scenes. Scenes define a certain switching state for different devices; e.g. switch is switched off, window is closed, dimmer is at 50 %, window blind is 90 % open. Scenes can be defined for the whole home or for different parts of the home, such as different rooms.

Defined Scenes can be activated depending on certain conditions, e.g.:

- A certain sensor values (Activate open window scene with open windows, and heat turned down when CO2 sensor reached 100 ppm);
- A certain button is pressed (Turn off al electrical devices and turn down all light when the “all off” button near the front door is pressed);
- A certain time is reached (Turn down all window blinds 30 minutes after sun set);
- A Boolean logic determines the event (Turn on all outside lights when time is between 18.00 and 0600 AND all off button is pressed);

It‟s typically possible to run multiple scenes in parallel. In this case the user need to make sure no contradicting commands and settings are defined.



MyFirstScene | Global Scenes

□ Hidden (won't be displayed on dashboard)

Name for this timer: New timer Enabled: ☑

Name for this timer: New timer Enabled: ☑

Times can be 24 hour or 12 hour: ie 14:00 or 2:00pm or 2:00 P.M. are fine

● **Interval based:** Example: Do something every x minutes, or every other hour

Every Hours

○ **Day of week based:** Example: Do something at 7:00 and 9:00 on Monday, Wednesday and Friday

○ **Day of month based:** Example: Do something at 8:00 on the 1st and 15th of each month

○ **Absolute:** Example: Do something on 5 Mar 2005 at 11:15

Figure 4.15: Scene Setup Dialog

Besides switching devices the activation of a scene may trigger more functions such as sending of an email or an SMS or calling a predefined phone number.

During configuration and usage of an IP gateway there are three challenges worth to be discussed:

- Reporting of status changes of devices cause by local usage rather than initiated via the wireless network;
- Associations configured directly on the devices rather than set by the user GUI of the IP Gateway;
- Scene activation using Z-Wave remote controls or other wall controllers.

4.5.1 Display of Switching Status Information

Users want to see the status of their electrical devices on their mobile phone or PC screen. The gateway is able to poll the states of each devices but the poll interval is way too long to ensure a real-time update of the status. In case the status is changed from the gateway using a phone or the PC interface, the gateway is initiating the status change and is able to request the new status right after executing the switching command.

However, certain devices offer to switch the state locally by pressing a button (e.g. a wall plug switch of a simple wall switch). In this case the gateway does not get any update information from this particular switch.

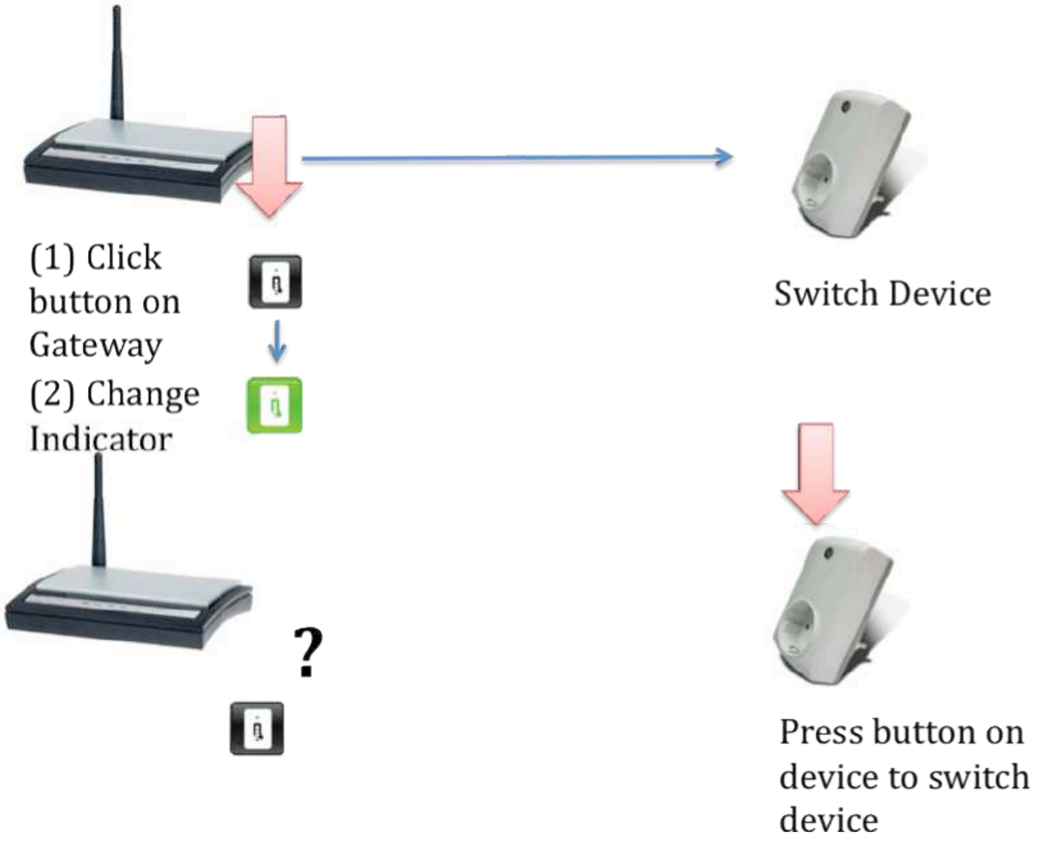

(1) Click button on Gateway
(2) Change Indicator
Switch Device
?
Press button on device to switch device

Figure 4.16: Missing status message

Activating a scene from a wall controller or a remote control is a desirable function of a Z-Wave network. In order to activate the scene,

the IP gateway must receive information, if and which button of a remote control or a wall controller is pressed.
So whether it‟s by Groups, Associations, Scenes or all three, you can personalise your Z-Wave wireless system to the way you want it.

The Lutron-Patent

The US company Lutron has filed the patent 5.905.422 in the mid nineties describing the wireless control of lights from wall switches. The patent relates specifically to wireless networks with mesh routing functions. That’s why a lot of the simpler wireless technologies on the market do not infringe the patent but Z-Wave would do.
The key patent claim #1 describes:

1. Apparatus for controlling at least one electrical device by remote control comprising:

> *at least one control device coupled to the electrical device by a wire connection for providing power to the electrical device, the control device having a controllably conductive device for adjusting the status of said electrical device**, the control device further having a manual actuator for adjusting the status of the electrical device**, the control device further having a radio frequency transmitter/receiver and antenna coupled thereto for adjusting the status of the electrical device in response to control information in a radio frequency signal, the transmitter/receiver being coupled to the antenna of the control device for receiving the radio frequency signal and for transmitting **a status radio frequency signal having status information therein regarding the status of the electrical device as affected by the control information and the manual actuator;***
>
> *a master control unit having at least one actuator and status indicator thereon, the master unit comprising a transmitter/receiver for transmitting a radio frequency signal having the control information therein to control the status of said at least one electrical device and for receiving the status information from the control device**, the status indicator indicating the status of the electrical device in response to the status informatio**n; and*
>
> *a repeater transmitter/receiver for receiving the radio frequency signal from the master unit and transmitting the control information to the control device and for receiving the status information from the*

> *control device and transmitting the status information to the master unit.*

Every sending of a status signal as result of a status change of a wireless device in a routed network infringes the patent. This is the reason why manufacturers of Z-Wave device intentionally did not implement a status report function as a result of local status change.

As a result the gateway does not recognize a local status chance of the device and will remain showing a wrong status of this particular device.

Meanwhile people found – as almost always – a way to solve the problem without infringing the Lutron Patent. Devices such as wall switches, wall dimmers or Outlet plug switches and dimmers with a local button to operate offer an association group. Using the local button is not only switching the local state but is causing to send a switching command to an association group. The main difference to the patent-protected scenario is that there is no longer a status report (protected by patent) but a switching command (allowed by the patent). Beside other switches, which can be switched simultaneously with the particular button on one switch the Gateway itself may also be a target device. In this case the gateway must emulate the behaviour of a standard switch to be able to receive switching commands. Receiving a switching command from a wall switch will not cause the gateway to switch on a lamp but to immediately check the status of this particular switch and, subsequently, update the switch state on the gateways GUI.

Unfortunately not all wall switches and dimmer already support this association function yet,

4.5.2 Using controllers to switch scenes

Activating a scene from a wall controller or a remote control is a desirable function of a Z-Wave network. In order to activate the scene

the IP gateway must receive an information if and which button of a remote control or a wall controller is pressed.
To realize this function Z-Wave offers multiple ways:

Associations

An association means to send a switching command from a Z-Wave device to another Z-Wave device. This command is initiated by a local condition such as a sensor value or a button pressed.
To activate a scene in an IP gateway using an association the controller must set an association to the IP gateway and the IP gateway must refer the switching command from a particular device to the activation process of a specific scene.

A very typical command setup for such a relation would be the activation of a (I am back home) scene by a motion detector (on the main front door). The motion detector recognizes a movement and sends a switching command to the association group related to the motion detection (Most motion detectors just have one single association group which gets activated when the motion detector gets triggered)

Using associations for scene switching is a common setup in a Z-Wave network but bears two major challenges:

1. Typically the association is set from the IP gateway using the “assigned association” function. This works fine for mains powered devices that are always active. Setting up a battery-operated device will work fine as well. However the user either need to wakeup the battery operated device for configuration or need to wait until the next interval wakeup with cause the IP gateway to send all queued commands. Certain Z-Wave controllers may not support assigned associations but direct associations only; In this case the IP gateway is not able to set the proper association function in this device. The annex B gives some overview of current remote controls and their support for

assigned associations.

2. Association commands are typically BASIC commands just sending 0 or 1. As long a there is only one association group in a device – means one basic function such as one button or one sensor- this does not cause any problems. Remote controls or wall switches with more than one paddle typically offer more than one association group to support the different functions of the device. If more than one groups will send basic commands to the IP gateway for scene switching the gateway is not able to distinguish the different groups. Hence it’s not possible to switch more than one scene from one specific device. All groups – in case of a remote control all buttons – create the very same switching command, which is received from the very same device.
   Hence associations are only suitable for scene switching, if only one button on a device is available or only one sensor of a device is present.

Scene Configuration

There are remote controls available which were developed particularly to allow scene switching in an IP gateway. These remote controls support a special command class for scene switching (SCENE_CONTROLLER_CONF).

IP Gateway recognizes this command class and can perfectly activate scenes based on these commands. Each button of a remote control will send a different scene activation value to the gateway allowing activating different scenes based on these values.

Scene Replication

Some Remote Controls are able to handle scenes by themselves. They offer scene-switching buttons and can store the whole scene (certain commands to certain devices to a scene) in their own memory.

It is possible to load scenes from the IP Gateway into the remote control. The remote control will then activate the scene by sending all the commands directly to the target nodes instead informing the IP gateway to send out these commands.

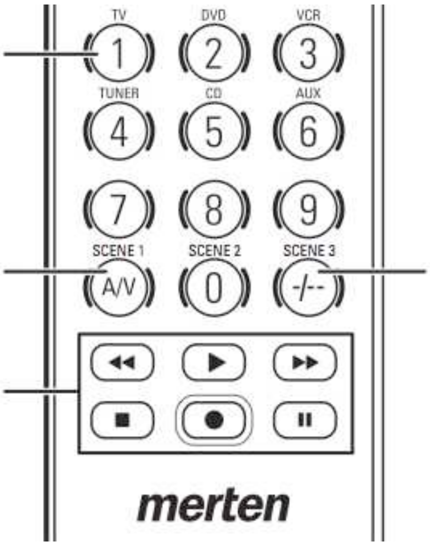


Figure 4.17: Dedicated buttons to control scenes on a universal remote

Scene replication – the ability to store whole scenes from a different controller into a remote control – are only available on few remote controls and not even then they are implemented in a very powerful und flexible way. Hence they are only used rarely.

Double Inclusion

The configuration of scene activation from a battery-operated device such as a remote control causes a hen-egg problem.

The configuration dialog of the scene switching will only offer the scene switching once the remote control is included in the network and the Node ID is known. After inclusion the battery operated remote control will go into sleep mode.
After inclusion the gateway is able to use the node ID and other device specific information to offer a scene activation dialog. Every

configuration done in this dialog however is only stored in the gateway and not yet known in the Z-Wave device.
To configure a battery operated device such as a remote control, the user must give the IP gateway the opportunity to configure this remote control. This is typically done during inclusion process. Therefore a remote control used for scene switching needs to be included twice into the Z-Wave network: first time before scene activation configuration and another time right after the scene activation configuration.

For scene activation by Z-Wave devices the following rules apply:

1. The best way is to directly set scene activation in a gateway using the scene activation command class. However not all remote controls offer this capability.
2. Replicating a complete scene into the remote control is the second best option, but only very few remote control support this and even then the implementation is limited in functionality
3. Associations are a good way to activate scenes, but only as long as there is only one single button or one single sensor in one physical device. Otherwise the Gateway is not able to distinguish different scene activation from the very same device.
4. Associations need to be set from the controller using "assigned association". Not all controllers allow assigned associations.

IP gateway will always try to automatically find the best way to use other Z-Wave controllers and devices for scene activation. Different options and some unclear implementation in older devices may still cause problems. Regardless of the option used a double inclusion of a battery-operated device is typically required in order to load a configuration back into this device.

Annex B shows a list of known European Remote Controls and their scene switching capabilities.

4.5.3 Configuration of Devices by the gateway

- During inclusion the IP Gateway will recognize the device and read all interesting device parameters.
- All manufacturer specific information such as vendor, vendors product ID and product type
- All firmware and Z-Wave version information
- All switching and reporting capabilities including current switching states and sensor values.
- Number and maximum size of association groups
- Configuration values if known

The Gateways will then do some initial setup:

- If needed a certain predefined wakeup interval is set for battery operated devices
- If available and requested certain standard defaults behaviours are configured in the device
- If association groups are available the gateway will always put its own Node ID into these association groups in order to be informed about status changes and to be prepared for using associations for scene switching

The user can change all values. However it needs to be clear that particularly removing the gateways Node ID from the association groups may cause malfunctions of the gateway.

5 Z-Wave Practice

This chapter will give some practical guidance for setting up and operating a Z-Wave network.

5.1 General approach to setup a Z-Wave Network – „A Quick Start Guide“

The setup of a Z-Wave network always needs the following four steps:

(1) Select all devices that are needed and install them on the final location. Every network consists of controllers (or senders) and slaves (or receivers) Even if these products are already powered up they will not be able to communicate with each other and perform any meaningful functions.

(2) All devices need to be setup to speak the same language. This process is called inclusion. After inclusion of all devices in the network all devices speak the same „language“ but still may not perform any meaningful function. One controller always initiates the inclusion by turning him into the inclusion mode. All slaves are announced to the controller by triple press of a button or a different useful way describes in the manual.

(3) The third step assigned certain meaningful functions and relationships to the network. This is called association. Association means to setup relationships in the way of „Press button A to Switch Device B“. Associations are initiated by the controller and confirmed by the receiving devices. The manual of the controller will give further advice.

4. Ready!

After inclusion of the devices and doing associations the network is ready to be used. It is always possible to include further devices and chance the association relationships. Just repeat steps 1 to 3.

5.2 Selection of Devices

5.2.1 Controller

The selection of devices is always based on the desired function of the network. A network always consists either of a central remote control or a central static (fixed location) gateway on a dedicated device (e.g. IP gateway or set top box) or as software on a PC.
Controlling a Z-Wave network only from a remote control is only recommended if:
There are only few devices to be controlled (less than ten is a good measure);

- No battery operated devices are in the network;
- No time dependent functions like shutting down the window blinds at a certain time of the day are required.

Otherwise it’ s highly recommended to use a static controller as IP gateway or PC software. To use PC software an additional USB adapter, typically a USB stick is needed.

5.2.2 Slaves

Portable dimmers and switch, also called “smart plugs” or “wall outlet plugs” are easy to choose. It’s only recommended to check the maximum switching capability (in W or A). Design issues may play a role as well.
For wall switches the design or the plates play an important role. Switches shall have the same industry design as wall outlets and other wall installations such as antenna and phone jacks or Ethernet outlets. Its possible to turn existing legacy switches into Z-Wave switches by using special insert, which are placed behind the legacy switch. However the depth of the pattress box needs to support this.

5.3 General recommendation for installation of Z-Wave networks

For the installation of Z-Wave devices the following recommendation apply:

- Try to avoid metal pattress boxes. They may shield the radio signal.
- Check the maximum wireless range. Z-Wave typically allows to cover all distances within a home either direct or using the routing capabilities. However reflections and interference may cause problems.
- The fact that a Z-Wave network worked perfectly during installation is no guarantee that it will stay the same forever. Even slight changes in the house layout like moving furniture may cause changes in reflections and interferences. This is rare but not impossible.

- • Networks installed by remote controls may not have proper routing. This may reduce the range of the network.
- • If a static gateway is used for inclusion it's always recommended to do network reorganization after installation.
- • Certain remote controls combine the association function with the inclusion function. The user only does the association of a certain device into a certain group of the remote control and the remote control automatically performs the inclusion as well.
- • In case multiple controllers are used and one static controller is present it's recommended to run the static controller as SUC/SIS.
- • Portable remote controls have an updated routing table only at the moment of inclusion. It's recommended to include remote controls after including all other slave devices.
- • In a network with a static IP gateway it is recommended to prefer scene switching instead of setting and maintaining direct associations between devices.

- There are multiple ways to use Z-Wave controller to activate scenes in an IP gateway. Check the manual or the Annex whether the device is able and how it is able to switch scenes.
- In case the device needs further configuration work consult the manual for description of the various configuration parameters.
- Z-Wave devices which are moved with only automatically heal the routing table if
    - the moved device is a routing slave,
    - There is another routing slave in range of the moved devices,
    - a SUC/SIC controller is present in the network.

For battery-operated devices the following recommendations apply:

- There must be a static controller in the network.
- Every battery-operated device shall be included in the network right after putting the batteries into the device.
- In case there are tests or further configuration needed, the wakeup interval of the battery operated device should be set to a short value. After this work is done the wakeup interval needs to be set to a longer value (> 5 min) in order to preserve battery live time.
- Each battery-powered device should be included and configured right after inclusion. Try to avoid inclusion of multiple battery-operated devices at once with configuration afterwards. The battery-operated device may already be in the sleeping state.
- The wakeup time of a battery operated device needs to be within the allowed boundaries. Modern devices report these boundaries, but older devices may still accept forbidden wakeup intervals. The behaviour of the device may be unpredictable in this case. Consult the manual for further information.

5.4 Typical difficulties using Z-Wave

5.4.1 Lack of knowledge

Z-Waves aim is to enable non-technicians to install and maintain the network. This goal is certainly achieved in smaller networks with one remote control or with one gateway. Larger and more complex networks with multiple controllers and battery-operated devices however do need more then basic knowledge about the technology. The knowledge described in chapter 3 to 5 will allow all users to install and operate all kind of Z-Wave networks.

5.4.2 Unclear and confusing language

Z-Wave has unified basic terms for network operations such as inclusion, exclusion or association. Unfortunately these definitions only apply in English language. Vendors have to use these terms in their English manuals but they are free to use their own creation of terms in their local languages like French or German. The result may be confusing to end users, since different vendors may refer to the same process with different terms.

Part of the certification process is however to check the manual which requires to translate the local terms into English. Referring to the manual can solve uncertainly and confusion in regard to Z-Wave terminology

5.4.3 Different usage of similar devices

The Z-Wave standard well defines the interaction between different devices but does not provide the same level of detail for the human – machine – interface. This allows - again – vendors to do their own ways and implement their own ideas in regard to usability. Here are some examples:

(1) Inclusion

To perform the inclusion of a device into a Z-Wave network, a local operation of the device is required to ensure the right ownership of the device and to protect the device against highjacking from other networks.

Some vendors require a single click on a universal button, some vendors offer a dedicated button for inclusion and some vendors require a triple press of a button. Please consult the manual for further information about the inclusion process.

(2) Automatic Inclusion at association with remote controls

5.4.4 Multiple Nodes with similar IDs

Every wireless network such as Z-Wave only works if there is a unique identification for each node in the network. In Z-Wave the Node ID serves this purpose.
During inclusion every device receives a unique Node ID for a given Home ID. The controllers will make sure that each Node ID is only assigned once to one single device.
In case the controller is reset, all network information will be erased. The controller will then start again assigning Node IDs to devices included to this particular controller starting form Node ID 2.

Assuming there was an other device from the previous network (before the controller was reset) and this device was not reset properly this device may still have the same – old- Home ID and its old Node-ID which may conflict with newly assigned Node IDs. This will certainly result in an unstable network and unpredictable conditions.

Before a controller is reset the user need to make sure that all devices previously included by this controller are excluded or set back to factory default.

Most recent implementations of controllers randomly change their Home-ID at every reset to avoid this type of confusion and malfunction. However the better part of Z-Wave controllers in the market do not support this function yet.

5.4.5 Compatibility Problems

The main value proposition of Z-Wave is that devices from different manufacturers can work together. The Z-Wave alliance has put a lot of effort behind a process to make sure this compatibility is achieved and maintained.

Despite its success there are some limitations to the compatibility, which are worth to be mentioned:

1. **Limited and wrong implementation of Z-Wave in PC-Controller-Software:** By far the most problems with Z-Wave are caused by wrong or insufficient implementation of Z-Wave by PC software solutions. In a lot of cases the support for Z-Wave was added later to already existing software and certain compromises were done to squeeze Z-Wave in already existing architectures and structures. Typically these software solutions are not Z-Wave certified but they are still perceived as Z-Wave compatible products. Z-Wave control software or IP gateways that are Z-Wave certified will not face this problem.
2. **Sins from the past**: The initial certification process was not as precise as required. As a result certain products were certified which would not longer pass the current more detailed certification process. However the revocation of a Certification is not possible, hence older devices may have compatibility problems. This problem is very rare and only happens with devices certified before 2008.

6 Some Recommendations for Installers

This book does not have the ambition to be used as a handbook for installers. However there are two problems related to Z-Wave, which is worth to be covered.

- Selection of dimmers
- Switching Series

6.1 Dimmers

Dimmers are electrical devices, which allow to continuously dimming a light according to the users requirement. There are multiple types of electrical lights and unfortunately there is no dimmer, which is able to dim all lights.

Lamps can be

- The classical incandescent light invented by Thomas Edison
- Halogen lamps operated by 230 V AC (High Voltage Halogen)
- Halogen lamps operated by 24 V (Low Voltage Halogen). The conversion from 230 V down to 24 V is done in two different ways: (a) using a simple transformer or (b) using an electronic switching power supply.
- Fluorescent Light in general, and compact fluorescent light (CFL) in particular. They are also called energy saving lamps.
- Lamps based on Light Emitting Diodes, calls LED lights

6.1.1 Leading-edge phase control

Conventional lamps are dimmed using a so-called leading edge phase control. This means that a changing portion of the sine wave is cut off. The resulting energy is reduced and the light is dimmed. Figure 6.1 shows a sine wave for full load and for 50% where the sine wave is cut right at 50 %

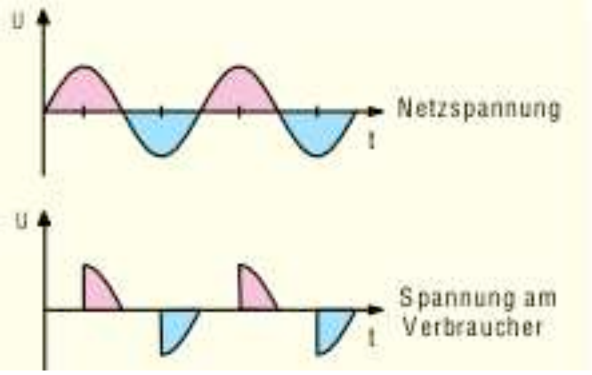


Figure 6.1: Voltage at **leading-edge phase control dimmer**

At leading edge dimmers the Voltage remains 0 after the wave crossed the zero line. After the defined time a Triac (is ignited. This brings the full voltage of the sine wave to the lamp. The characteristic of a Triac is to block the current again when the sine wave crosses the zero line. Hence, the Triac needs to be ignited at every current wave again.

Leading Edge Dimmers work well with incandescent lights and HV Halogen light but fail to dim low voltage Halogen, Fluorescent lamps and LED lamp. Even worse, they may even destroy these lamps.

6.1.2 Leading Edge Phase Control for inductive loads

Transformers used in Low Voltage Halogen Lamps realize an inductive load. A load that is called predominantly inductive if the alternating load current lags behind the alternating voltage of the load. Such a load is also known as lagging load. This means that the voltage is already at zero while the current is not zero yet.

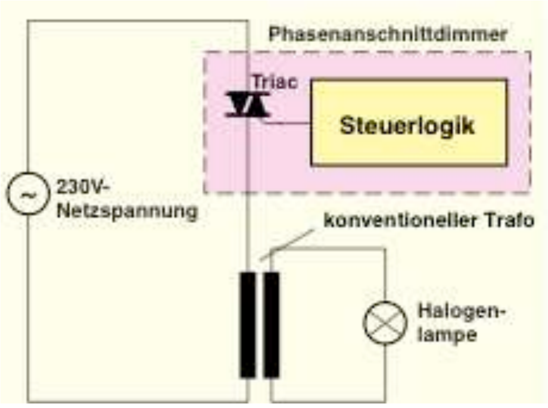


Figure 6.2: Schematics of a leading edge phase control dimmer

This creates a huge problem for traditional cutting edge dimmers using a Triac. The Triac closes when the current is zero, not when the voltage is zero. An ignition pulse for the Triac may be received “too early” at a moment, when the current is not zero, hence the Triac not closed yet. The ignition pulse is then ignored and the Triac will stay open for the next half wave.
Only the subsequent ignition pulse will again trigger the Triac in a correct way.

The result of this “missing” ignition is a misbalanced wave, which results in destroying transformers and other inductive loads.

To dim halogen lamps with conventional transformers a special electronics is needed to make sure that the Triac switches at the right time.

Figure 6.2 shows the schematics of such a leading edge dimmer with inductive load compensation. These dimmers can still dim all conventional - resistive - loads

6.1.3 Trailing Edge Phase Control Dimmer

Electronic Power supplies typically represent a conductive load. In a conductive load the capacitive reactance exceeds the inductive reactance. Hence the load draws a leading current. To dim these loads a trailing edge phase control dimmer is needed.

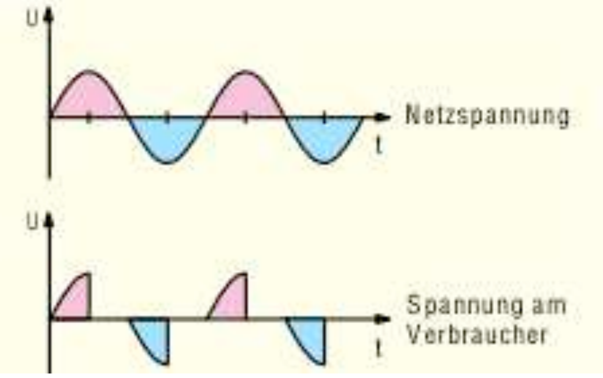


Figure 6.3: Voltage at a trailing edge phase control dimmer

The trailing edge dimmer cuts off the trailing part of the sine wave like shown in Figure 6.3. Such behaviour cannot be achieved using a Triac component. High Voltage MOSFET components are used instead.

Figure 6.4 shows the schematics of such a dimmer.

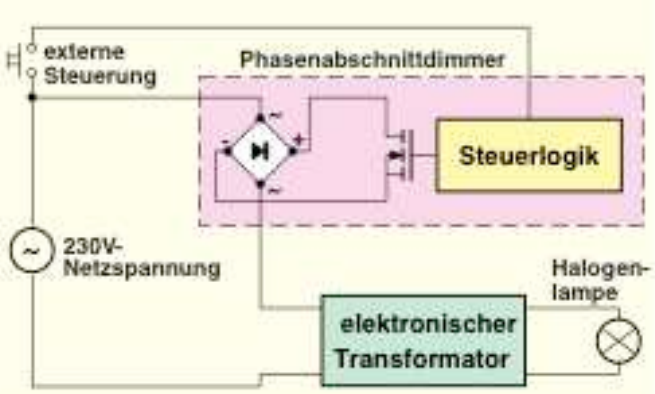


Figure 6.4: Schematics of a trailing edge phase control dimmer

6.1.4 Universal Dimmers

The dilemma of edge phase control dimmers is that - in case of leading edge – either inductive loads or - in case of reactive loads-capacitive loads can be dimmed. The dimmer may even destroy the load not supported.

The solution is so called universal dimmer.

Universal dimmers detect initially if the load has inductive or reactive characteristics and change between leading and trailing edge.
To make sure the detection delivers the correct result, the user need to make sure that only one load is connected to the dimmer during power on. Also changing the load later on may result in problems.

6.1.5 Fluorescent Lamps

Conventional Fluorescent Lights are not dimmable. However there are special transformer devices, which allow dimming of these devices. For CFLs these transformers are already integrated in the lamp socket. CFLs with this unit are called dimmable CFLs and usually have a much higher price.

CFL are typically dimmed either by a trailing edge dimmer or a universal dimmer. Manufacturers of modern CFLs have done a good job in compensation the reactive load, so that even normal leading edge dimmers can dim such a lamp.

6.1.6 LED Lamps

LED lamps can be dimmed very well but neither with leading nor with training edge dimmers. There are dimmed using a so-called PWM (pulse wide modulation). Hence LED s lights need a special dimmer only applicable for LED lights.

6.1.7 Dimmer Summary

The following table gives a summary overview of the different types of dimmers and the types of lamps dimmable

Phases	Leading edge	Leading edge with inductive support	Trailing edge	Universal
Electric light bulb	Yes	Yes	Yes	Yes
HV Halogen	Yes	Yes	Yes	Yes
Low Voltage Halogen (conv. Transformer)	No	Yes	No	Yes
Low Voltage Halogen (Switched power supply)	No	No	Yes	Yes
Dimmable Fluorescent lamp	No	Yes	No	Yes
LED lamp	No	No	No	No

6.2 Product Families

Some manufacturers offer whole portfolios of Z-Wave products, which are marketed under a common manufacturer specific trade name. Usually references are made in the documentations of these products to other products of the same product family. Also the documentation typically stresses the fact that the products of this particular family work very well together. While this is certainly true these products remain certified Z-Wave products and therefore they are able to work together with all other Z-Wave compliant products form different vendors.

6.2.1 ACT HomePro

The HomePro series of the US-American manufacturer Advanced Control Solutions was the first product series of a manufacturer based on Z-Wave.
Homepro offers a series of wall switches with one or two buttons which realize either a dimmer or a switch. If two buttons exist, the left button always switches the locally available switch or dimmer, while the second button can be used as a controller for other switches and dimmers.
ACT Homepro products are always shipped completely with mounting frame and switching paddles and they are all 230 V main powered.
The industrial design corresponds well with the switch series CD 500 from Jung.

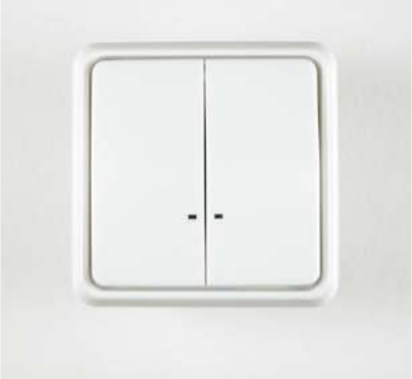


Figure 6.6: ACT HomePro Wall Switch Design

Beside the wall switches ACT complete the series with a motion detector and a remote control usable for setting up, configuring and operating the network.

With the Homepro remote control switches and dimmers of other manufacturers can be controlled. Controllers of other manufacturers can control the wall switches from ACT without problems.

6.2.2 Merten Connect

The German manufacturer Merten, part of the Schneider Electric group, offers a lighting control system MERTEN CONNECT that is based on the Z-Wave protocol. It is targeted to professional installers.

The product series has three basic types of product:

- Battery-operated wall controllers to control other devices such as switches, dimmers or Venetian blind controls. These controllers are available with one or two switching paddles
- Dimmers, switches and Venetian blind controls are offered either equipped with or without local operation capabilities. All these products are powered my 230 V mains.
  The switch products with local operation capabilities consist of a switching (or dimming) base, which is completed by a Z-Wave enabled switching paddle. The bases are shared with other Merten Control series, namely the wire based KNX system. Merten offers a variety of different mounting frames and switching paddles so that the installer has to always choose the base and the switching paddle and mounting frame in the design and colour of choice.
- For the central control of the Z-Wave network multiple options exists. It is possible to select one of the wall controls as Primary Controller, however a universal remote and a LCD equipped wireless control centre give more functionally during setup and operation.

For the initial setup and configuration as well as for the setup of the associations between the wall controllers and the switches or dimmer of the network Merten suggests the use of special installation software. This software is free of charge but requires a special USB interface to operate.
The Merten CONNECT wireless control centre also acts as IP gateway allowing a remote access to the switching system using a web browser or a mobile phone.

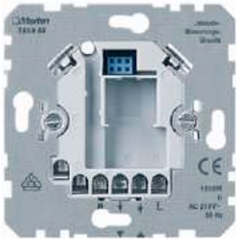


Figure 6.7: Merten – Wall Insert, to be completed by Z-Wave equipped switching paddles

Merten devices can be controlled well by controllers from other manufacturers and the Merten-radio remote controllers are also able to control products of other manufacturers. However the support of third party devices within the Merten installer software is very limited. The installer software is therefore perfect only in pure Merten CONNECT environments.

6.2.3 Duwi Z-Wave (former Interact)

The switch system of Duwi is optimised for the needs of the "do it yourself" home user. The base unit consist of an insert and a mounting frame that allows completing the insert – if desired - by a switching paddle for local operation. This means that the very same product can be used with or without local switching paddle.

Duwi offers multiple switching designs for the completion of the inserts in multiple colours.

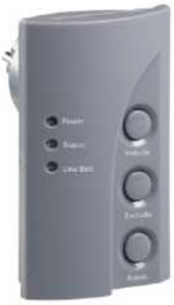


Figure 6.8: Duwi – Wireless Controller to administrate larger Z-Wave networks

The switches, dimmers and window blind inserts are controlled by either a remote control or a battery powered wall controller, which is available for the different switching series designs as well.

To allow bigger installations of Z-Wave network Duwi completes the Z-Wave system by a radio control centre, which works as static controller with SUC/SIS functionality.

Duwi products work well together with other Z-Wave compliant products of different vendors.

Annex A: Z-Wave Command Classes

COMMAND_CLASS_NO_OPERATION

COMMAND_CLASS_ALARM

COMMAND_CLASS_BASIC

COMMAND_CLASS_CONTROLLER_REPLICATION

COMMAND_CLASS_APPLICATION_STATUS

COMMAND_CLASS_SWITCH_BINARY

COMMAND_CLASS_SWITCH_MULTILEVEL

COMMAND_CLASS_SWITCH_ALL

COMMAND_CLASS_SWITCH_TOGGLE_BINARY

COMMAND_CLASS_SWITCH_TOGGLE_MULTILEVEL

COMMAND_CLASS_CHIMNEY_FAN

COMMAND_CLASS_SCENE_ACTIVATION

COMMAND_CLASS_SCENE_ACTUATOR_CONF

COMMAND_CLASS_SCENE_CONTROLLER_CONF

COMMAND_CLASS_SENSOR_BINARY

COMMAND_CLASS_SENSOR_MULTILEVEL

COMMAND_CLASS_METER

COMMAND_CLASS_METER_PULSE

COMMAND_CLASS_THERMOSTAT_HEATING

COMMAND_CLASS_THERMOSTAT_MODE

COMMAND_CLASS_THERMOSTAT_OPERATING_STATE

COMMAND_CLASS_THERMOSTAT_SETPOINT

COMMAND_CLASS_THERMOSTAT_FAN_MODE

COMMAND_CLASS_THERMOSTAT_FAN_STATE

COMMAND_CLASS_CLIMATE_CONTROL_SCHEDULE

COMMAND_CLASS_THERMOSTAT_SETBACK

COMMAND_CLASS_BASIC_WINDOW_COVERING

COMMAND_CLASS_MTP_WINDOW_COVERING

COMMAND_CLASS_MULTI_INSTANCE

COMMAND_CLASS_DOOR_LOCK

COMMAND_CLASS_USER_CODE

COMMAND_CLASS_CONFIGURATION

COMMAND_CLASS_MANUFACTURER_SPECIFIC

COMMAND_CLASS_POWERLEVEL
COMMAND_CLASS_PROTECTION
COMMAND_CLASS_PROTECTION_V2
COMMAND_CLASS_LOCK
COMMAND_CLASS_NODE_NAMING
COMMAND_CLASS_FIRMWARE_UPDATE_MD
COMMAND_CLASS_GROUPING_NAME
COMMAND_CLASS_REMOTE_ASSOCIATION_ACTIVATE
COMMAND_CLASS_REMOTE_ASSOCIATION
COMMAND_CLASS_BATTERY
COMMAND_CLASS_CLOCK
COMMAND_CLASS_HAIL
COMMAND_CLASS_WAKE_UP
COMMAND_CLASS_ASSOCIATION
COMMAND_CLASS_VERSION
COMMAND_CLASS_INDICATOR
COMMAND_CLASS_PROPRIETARY
COMMAND_CLASS_LANGUAGE
COMMAND_CLASS_TIME
COMMAND_CLASS_TIME_PARAMETERS
COMMAND_CLASS_GEOGRAPHIC_LOCATION
COMMAND_CLASS_COMPOSITE
COMMAND_CLASS_MULTI_INSTANCE_ASSOCIATION
COMMAND_CLASS_MULTI_CMD
COMMAND_CLASS_ENERGY_PRODUCTION
COMMAND_CLASS_MANUFACTURER_PROPRIETARY
COMMAND_CLASS_SCREEN_MD
COMMAND_CLASS_SCREEN_ATTRIBUTES
COMMAND_CLASS_SIMPLE_AV_CONTROL
COMMAND_CLASS_AV_CONTENT_DIRECTORY_MD
COMMAND_CLASS_AV_RENDERER_STATUS
COMMAND_CLASS_AV_CONTENT_SEARCH_MD
COMMAND_CLASS_SECURITY
COMMAND_CLASS_AV_TAGGING_MD
COMMAND_CLASS_IP_CONFIGURATION
COMMAND_CLASS_ASSOCIATION_COMMAND_CONFIGURATION

COMMAND_CLASS_SENSOR_ALARM

COMMAND_CLASS_SILENCE_ALARM

COMMAND_CLASS_SENSOR_CONFIGURATION

COMMAND_CLASS_MARK

COMMAND_CLASS_NON_INTEROPERABLE

Annex B: Generic Device Classes

Alarm Sensor Generic Device Class

- No Specific Device Class defined
- Basic Routing Alarm Sensor Specific Device Class
- Routing Alarm Sensor Specific Device Class
- Basic Zensor Net Alarm Sensor Specific Device Class
- Zensor Net Alarm Sensor Specific Device Class
- Advanced Zensor Net Alarm Sensor Specific Device Class
- Basic Routing Smoke Sensor Specific Device Class
- Routing Smoke Sensor Specific Device Class
- Basic Zensor Net Smoke Sensor Specific Device Class
- Zensor Net Smoke Sensor Specific Device Class
- Advanced Zensor Net Smoke Sensor Specific Device Class.

Binary Switch Generic Device Class

- No Specific Device Class defined
- Binary Power Switch Specific Device Class
- Binary Scene Switch Specific Device Class

Remote Controller Generic Device Class

- Portable Remote Controller Specific Device Class
- Portable Scene Controller Specific Device Class
- Portable Installer Tool Specific Device Class

Static Controller Generic Device Class

- PC Controller Specific Device Class
- Scene Controller Specific Device Class
- Static Installer Tool Specific Device Class

Repeater Slave Generic Device Class Basic

- Repeater Slave Specific Device

Multilevel Switch Generic Device Class

- No Specific Device Class defined
- Multilevel Power Switch Specific Device Class
- Multilevel Scene Switch Specific Device Class

- Multiposition Motor Specific Device Class (Not recommended)
- Motor Control Class A Specific Device Class
- Motor Control Class B Specific Device Class
- Motor Control Class C Specific Device Class

Remote Switch Generic Device Class

- Binary Remote Switch Specific Device Class
- Multilevel Remote Switch Specific Device Class

Binary Sensor Generic Device Class

- Routing Binary Sensor Specific Device Class

Multilevel Sensor Generic Device Class

- Routing Multilevel Sensor Specific Device Class

Pulse Meter Generic Device Class

Display Generic Device Class

- No Specific Device Class defined
- Simple Display Specific Device Class

Entry Control Generic Device Class

- Specific Device Class Not Used
- Door Lock Specific Device Class
- Advanced Door Lock Specific Device Class
- Secure Keypad Door Lock Specific Device Class

Semi Interoperable Generic Device Class

- Energy Production Specific Device Class

Thermostat Generic Device Class

- Thermostat General V2 Specific Device Class
- Setback Schedule Thermostat Specific Device Class
- Setback Thermostat Specific Device
- Setpoint Thermostat Specific Device Class

AV Control Point Generic Device Class

- No Specific Device Class defined

- Satellite Receiver V2 Specific Device Class
- Doorbell Specific Device Class

Meter Generic Device Class

- No Specific Device Class defined
- Simple Meter Specific Device Class

Ventilation Generic Device Class

- No Specific Device Class defined
- Residential Heat Recovery Ventilation Specific Device Class

Z/IP Gateway Generic Device Class

- Z/IP Tunneling Gateway Specific Device Class
- Advanced Z/IP Gateway Specific Device Class

Z/IP Node Generic Device Class

- Z/IP Tunneling Node Specific Device
- Advanced Z/IP Node Specific Device Class

Annex C: Z-Wave Controllers for Scene Switching in IP Gateways

Controller	**Works for scene switching**	**Scene Configuration**	**Accepts assigned association**
Tricklestar	No		
Düwi Wall Controller	Somewhat		Yes
QEES Key Ring	**Yes**	Yes	Yes
QEES Wall Controller	**Yes**	Yes	Yes
Aeon Labs	**Yes**	Yes	
Merten Wall Controllers	Somewhat		Yes
Merten Universal	Somewhat		Yes
Duwi Remote Control	Somewhat		Yes
Remotek ZURC 500	Yes	Yes	Yes

-