

# WaveNet

---

## Manual

25.09.2024

## Contents

1.	General safety instructions .....	4
2.	Product-specific safety instructions .....	6
3.	Meaning of the text formatting .....	8
4.	Further documentation.....	9
5.	WaveNet system.....	10
5.1	Transmission paths.....	13
5.2	Item numbers .....	14
5.2.1	RouterNodes .....	14
5.2.2	LockNodes.....	15
5.2.3	Accessories .....	17
5.3	Devices.....	19
5.3.1	Computer .....	19
5.3.2	RouterNodes .....	20
5.3.3	LockNodes.....	20
5.4	Radio network.....	21
5.4.1	Segments.....	22
5.4.2	Signal quality.....	23
5.4.3	Challenges in wireless networks.....	24
5.5	Safety and alarms.....	27
5.5.1	Encryption (WaveNet) .....	27
5.5.2	Monitoring the devices in the network.....	28
5.5.3	Alarms.....	29
5.6	WaveNet and LSM.....	30
5.7	Firmware.....	30
5.7.1	Reading out firmware .....	30
5.7.2	Updating firmware .....	32
6.	WaveNet Manager.....	35
6.1	System requirements .....	35
6.2	Unpacking, updating and starting the software.....	35
6.2.1	Unpacking.....	35
6.2.2	Update.....	36
6.2.3	Start.....	37
6.2.4	Password .....	39
6.3	Firmware information.....	39
6.4	Management .....	41
6.4.1	Basic principles.....	41
6.4.2	Auto-configuration.....	44

6.4.3	Finding and adding devices.....	48
6.4.4	I/O configuration and protection functions.....	69
6.4.5	RingCast.....	95
6.4.6	Device-specific settings.....	148
6.5	Fault rectification.....	152
6.5.1	Improving signal quality.....	152
6.5.2	Device restart.....	159
6.5.3	Reprogram or replace the device.....	163
6.5.4	Delete netcfg.xml.....	167
6.5.5	Resetting/Deleting.....	168
6.6	Maintenance.....	177
6.6.1	Overview.....	178
6.6.2	Check signal quality.....	180
6.6.3	Testing accessibility (WaveNet).....	183
6.6.4	Test reachability (LSM).....	186
6.6.5	Device function test.....	187
6.6.6	IO Status and LockNode responsiveness.....	188
<b>7.</b>	<b>Battery management.....</b>	<b>193</b>
7.1	LockNodes.....	193
7.1.1	Battery change with integrated LockNodes.....	199
7.1.2	Battery change for external LockNodes.....	199
7.2	Locking devices.....	200
<b>8.</b>	<b>Signalling the operating status.....</b>	<b>201</b>
8.1	In LSM.....	209
<b>9.</b>	<b>Technical specifications.....</b>	<b>212</b>
9.1	WaveNet in general.....	212
9.2	RouterNodes.....	214
9.3	LockNodes.....	216
<b>10.</b>	<b>Help and other information.....</b>	<b>218</b>

## 1. General safety instructions

### Signal word: Possible immediate effects of non-compliance

WARNING: Death or serious injury (possible, but unlikely)

IMPORTANT: Property damage or malfunction

NOTE: Low or none



#### WARNING

##### Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

##### Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- ❑ Modify the product only when needed and only in the manner described in the documentation.

#### IMPORTANT

##### Operational malfunction due to radio interference

This product may be affected by electromagnetic or magnetic interference.

- ❑ Do not mount or place the product directly next to devices that could cause electromagnetic or magnetic interference (switching power supplies!).

##### Communication interference due to metallic surfaces

This product communicates wirelessly. Metallic surfaces can greatly reduce the range of the product.

- ❑ Do not mount or place the product on or near metallic surfaces.



#### NOTE

##### Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- ❑ Do not use SimonsVoss products for any other purposes.

##### Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to  $\pm 15$  minutes per year.

- ❑ Regularly reprogram time-critical locking devices.

### Qualifications required

The installation and commissioning requires specialized knowledge.

- ❖ Only trained personnel may install and commission the product.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

---

## 2. Product-specific safety instructions



### WARNING

#### Personal injury or damage to property due to non-redundant safety concept

The protective functions of your WaveNet system are only one element of an entire safety concept. They are not suitable as the only protection against hazards such as fire, burglary or similar.

1. Make use of redundant systems to protect against your individual risks (burglar alarms, fire alarms and the like).
2. Have a technical risk manager (Certified Security Manager or the like) create and evaluate a security concept.
3. Please pay particular attention to relevant regulations on escape and rescue routes.

#### Impairment or failure of protective functions due to changed conditions

The activation of the protection functions in RingCast is based on wireless connections and Ethernet connections. Wireless connections in particular can be affected by changing environmental conditions (see *Radio network* [▶ 21] und *Challenges in wireless networks* [▶ 24]). This also influences the activation of the protective functions in the RingCast and can jeopardise the safety of persons and property that are additionally protected by the protective functions in the RingCast, for example.

1. Test the protective functions at least once a month (see *RingCast function test* [▶ 143]).
2. If necessary, also observe other guidelines or regulations that are relevant for your locking system (especially for escape and rescue routes and fire protection. You are solely responsible for ensuring compliance with these guidelines and regulations).

#### Change in the sequence of emergency functions due to malfunctions

SimonsVoss and "Made in Germany" stand for maximum safety and reliability. In individual cases, however, malfunctions of your devices cannot be ruled out. This may pose a risk to the safety of persons and property, which are additionally protected by the protective functions in the RingCast.

1. You should test your devices at least once a month (see *Device function test* [▶ 187] Shorter intervals may also be required according to other regulations concerning your overall system).
2. Test the protective functions at least once a month (see *RingCast function test* [▶ 143]).

**NOTE****Redundant protection of the network infrastructure**

In addition to SimonsVoss security measures, the network infrastructure in which you use WaveNet must also comply with current security standards.

1. You can meet these security standards by, for example using virtual networks or active network monitoring (the list does not claim to be complete).
2. talking to your IT infrastructure specialist.

**Exclusion of liability for the consequences of changed environmental conditions**

Ambient conditions can change and, despite regular testing, can interfere with the RingCast and its protective functions (see *Radio network* [▶ 21] und *Challenges in wireless networks* [▶ 24]). Neither SimonsVoss Technologies GmbH nor the product itself has influence on changing environmental conditions. The stability of the ambient conditions is a functional prerequisite. Therefore, the failure of protective functions can result in personal injury and damage to property. SimonsVoss Technologies GmbH shall not assume any liability for personal injury and material damage due to changing environmental conditions.

1. Record the current ambient conditions and the current signal quality during the project planning to be carried out (see *Signal quality* [▶ 23] und *Check signal quality* [▶ 180], see snapshot).
2. Ensure by continuous monitoring that the ambient conditions do not change unexpectedly.
3. Record the current ambient conditions and the current signal quality during the acceptance test to be performed (final snapshot).

### 3. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

<b>Example</b>	button
<input checked="" type="checkbox"/> Example <input type="checkbox"/> Example	checkbox
<input checked="" type="radio"/> Example	Option
[Example]	Tab
"Example"	Name of a displayed window
Example	Upper programme bar
<b>Example</b>	Entry in the expanded upper programme bar
<b>Example</b>	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
<i>Example</i>	Field
<i>Example</i>	Name of a (Windows) service
<i>Example</i>	Commands (e.g. Windows CMD commands)
<b>Example</b>	Database entry
[Example]	MobileKey type selection



## 4. Further documentation

Your WaveNet connects the Locking System Management (LSM) software and your locking devices. Further information can be found in the download area of the SimonsVoss website <https://www.simons-voss.com/>.

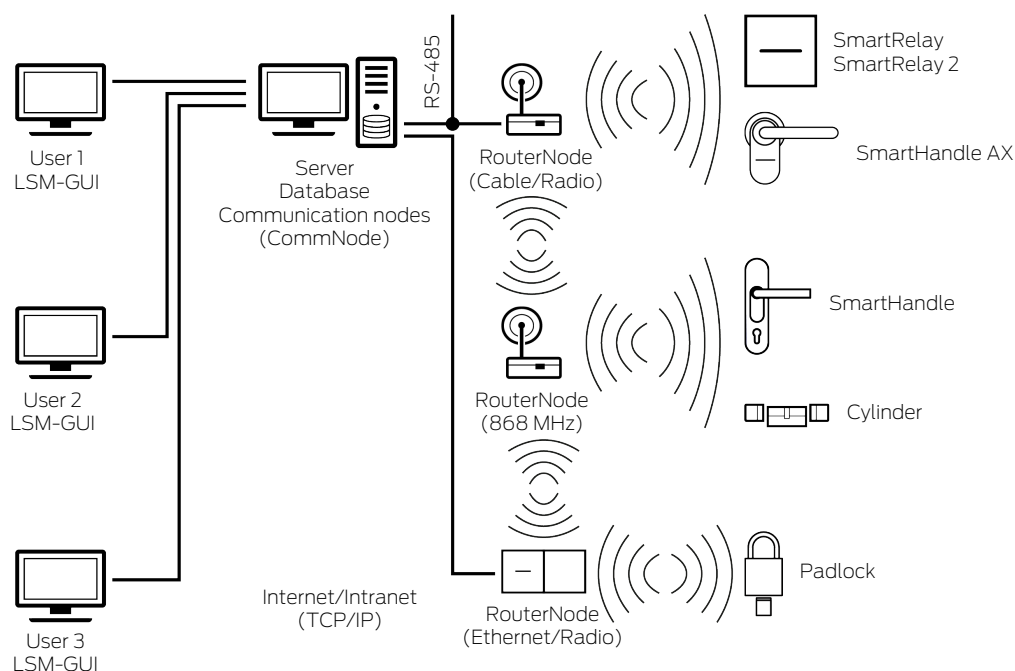
- Detailed information on LSM can be found in the LSM manual, in particular Performing standard WaveNet-based tasks in LSM.
- Detailed information on the locking devices can be found in the respective manuals and brief instructions.

## 5. WaveNet system

You can network SimonsVoss locks (locking cylinders, SmartHandles and SmartRelays) in a number of different ways and thus manage them centrally. WaveNet is the most advanced and convenient way to manage and monitor larger locking systems with many locks.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Functional principle	Data transmission with networked WaveNet devices (see <i>Transmission paths</i> [▶ 13] and <i>Devices</i> [▶ 19]).	Data transmission with identification media (except programming data).	Data transmission with programming devices.
Extension	WaveNet devices are connected via various transmission media. All types of data are transmitted using these transmission media.	In a virtual network, certain data is transferred to the identification media using a gateway (entries in the blacklist). If you operate this identification media on a virtually networked locking device, the data is transferred to the locking device.	Locking devices that are not networked can only exchange data with the programming device. You must go to the locking devices with the programming device.
Programming effort	Low.	Low.	Effort depends on the size of the locking system. <ul style="list-style-type: none"> <li>■ Small locking system: Low effort.</li> <li>■ Medium locking system: Medium effort.</li> <li>■ Large locking system: Extensive effort.</li> </ul>
Transmission speed of the data exchange	Immediately. Data exchange with different transmission media.	Speed between gateway and locking devices highly dependent on the intensity of use of the locking devices. Identification media are transmission media - no data transmission without identification.	Slow.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Central activation/deactivation of locking devices	Possible.	Not possible.	Not possible.
Activation/deactivation centrally traceable	Possible.	Not possible.	Not possible.
Remote opening	Possible.	Not possible.	Not possible.
Remote monitoring (Door-Monitoring)	Possible.	Not possible.	Not possible.
Event management	Possible.	Not possible.	Not possible.
Access lists centrally retrievable	Possible.	Not possible (except SREL 3).	Not possible.
Software/server independent protective functions	Possible.	Not possible.	Not possible.
Immediate locking device system-wide response to critical situations (availability of protective functions, see <i>I/O configuration and protection functions</i> [ <a href="#">▶ 69</a> ] and <i>RingCast</i> [ <a href="#">▶ 95</a> ])	Possible.	Not possible.	Not possible.



WaveNet is a dedicated network that you can install and use in building automation with just a few cables. If you want to retrofit WaveNet, you can also use existing building networks such as a LAN. This is why WaveNet is not only suitable for equipping new buildings with a locking system (e.g. for flexibly used room units). WaveNet is also particularly suitable if you want to manage and control your existing SimonsVoss 3060 locking system online in existing buildings.

Networking types can be freely combined with one another as an alternative to full networking. For instance, you can virtually network the doors of the outer shell (= building envelope) and particularly critical locks (for example on server room doors) with your WaveNet and all other locking devices.

You can choose from various devices and transmission media depending on your specific situation (see *Transmission paths* [▶ 13]). Data transmission in WaveNet largely depends on the transmission medium.

With your WaveNet and the IO functions (see *I/O configuration and protection functions* [▶ 69]), you can optimise security or the precautions against danger levels far beyond the level of a mechanical locking system.



## NOTE

### WaveNet training and planning

WaveNet is a comprehensive solution that can be very well tailored to your requirements. If you want to fully exploit the potential of your WaveNet, you can attend a SimonsVoss Technologies GmbH WaveNet training course. You can also plan your WaveNet project together with a SimonsVoss technician and benefit from their many years of experience.

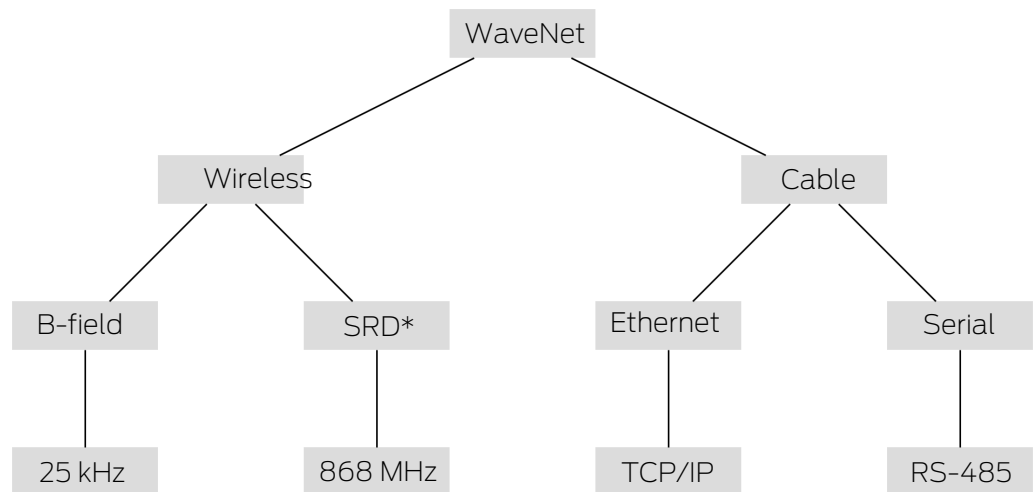
Further information on the devices, locks and LSM software can be found in the relevant manuals and quick guides on the SimonsVoss website (<https://www.simons-voss.com/>) in the download area under Documents.

### 5.1 Transmission paths

The WaveNet transfers data from the locking devices to a central administration, including:

- Authorisations
- Status changes
- protective functions

You can transmit this data using various transmission paths (availability of devices for certain transmission media may vary).



\*SRD=Short Range Device

25 kHz	B field for communication between: <ul style="list-style-type: none"> <li>■ Transponders and locking devices</li> <li>■ External LockNodes and locking devices</li> </ul>
868 MHz	SRD field for communication between: <ul style="list-style-type: none"> <li>■ RouterNodes and LockNodes</li> <li>■ RouterNodes and RouterNodes</li> </ul>
Ethernet	Ethernet cabling for communication between: <ul style="list-style-type: none"> <li>■ Computer and RouterNodes</li> </ul>

RS-485	Bus cabling for connection to the network: <ul style="list-style-type: none"> <li>■ RouterNodes</li> <li>■ Wired LockNodes</li> </ul>
--------	--

## 5.2 Item numbers

The WaveNet consists of different devices. You can configure your WaveNet according to your needs.

### 5.2.1 RouterNodes

The item codes of the RouterNodes are made up of modules (which change depending on the product characteristics).

WNM	.RN2	.E	R	.IO
<ul style="list-style-type: none"> <li>■ WNM (WaveNet-Manager → Addressing automatically)</li> <li>■ WN (WaveNet → Addressing fixed)</li> </ul>	Type of node: <ul style="list-style-type: none"> <li>■ .RN2 (RouterNode 2)</li> <li>■ .RN (RouterNode)</li> <li>■ .RP (RepeaterNode)</li> <li>■ .CN (CentralNode)</li> </ul>	Supported transmission medium (input segment: connection to network): <ul style="list-style-type: none"> <li>■ .E (Ethernet → TCP/IP)</li> <li>■ .R (Radio → 868 MHz)</li> <li>■ .C (Cable → RS-485)</li> <li>■ .W (WLAN → TCP/IP)</li> <li>■ .U (USB → USB)</li> <li>■ .S (Serial → RS-232)</li> </ul>	Optional supported second transmission medium (output segment: connection to LockNodes): <ul style="list-style-type: none"> <li>■ R (Radio → 868 MHz)</li> <li>■ C (Cable → RS-485)</li> </ul>	Optionally supported protective function. <ul style="list-style-type: none"> <li>■ .IO (protective router)</li> </ul>

### RouterNode portfolio

The table shows which RouterNodes support which transmission media.

	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WNM.RN2.ER.IO	✓			✓		
WNM.RN.R.IO	✓					
WNM.RN.CC.IO						✓
WNM.RN.CR.IO	✓					✓
WNM.RN.EC.IO				✓		✓
WN.RN.R (EOL)	✓					
WN.RN.CR (EOL)	✓					✓
WN.RN.CC (EOL)						✓
WN.RN.ER (EOL)	✓			✓		
WN.RN.WR (EOL)	✓	✓				
WN.RN.EC (EOL)				✓		✓
WN.CN.UC (EOL)			✓			✓
WN.CN.UR (EOL)	✓		✓			
WN.RP.CC (EOL)						✓
WN.RN.WC (EOL)		✓				✓
WN.CN.SC (EOL)					✓	✓
WN.CN.SR (EOL)	✓				✓	

### 5.2.2 LockNodes

The item codes of the LockNodes are composed of building blocks (which change according to product characteristics).

WNM	.LN	.I	.(product specific)
WNM (WaveNetManager → Same for all LockNodes)	.LN (LockNode → Same for all LockNodes)	<ul style="list-style-type: none"> <li>■ .I (Inside → LockNode can be integrated into the locking device)</li> <li>■ .R (Radio → LockNode external, communicates with the lock via 25 kHz)</li> <li>■ .C (Cable → LockNode external, communicates via cable with the network and via 25 kHz with the locking device)</li> </ul>	<p>Registration of various abbreviations for closure-specific properties, for example:</p> <ul style="list-style-type: none"> <li>■ .WP (weatherproof version for weatherproof locking devices)</li> <li>■ .MS (brass-coloured version for brass-coloured locking devices)</li> </ul> <p>This list is not exhaustive, other product-specific properties are possible that require a special LockNode. The properties of this column can also be combined with each other.</p>

### LockNode portfolio

The table shows which LockNodes support which transmission media.

	25 kHz	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WNM.LN.I		✓					
WNM.LN.I.MP		✓					
WNM.LN.I.S2		✓					
WNM.LN.I.SH		✓					
WNM.LN.I.SREL2.G2		✓					
WNM.LN.I.SREL.G2		✓					
CompactReader-LockNode (cannot be retrofit)	✓	✓					
WNM.LN.R	✓	✓					
WNM.LN.C	✓						✓





### 5.2.3 Accessories


Accessories are available for your WaveNet.


Power supply	Item order code	Image
<p>External power supply for RouterNode 2</p> <ul style="list-style-type: none"> <li>■ 12 V<sub>DC</sub>, 500 mA</li> <li>■ Connector Ø5.5/2.5 mm</li> </ul>	POWER.SUPPLY.2	
<p>External power supply for SmartRelay, CentralNode, RouterNode, RepeaterNode and BAMO</p> <ul style="list-style-type: none"> <li>■ 12 V<sub>DC</sub>, 500 mA</li> <li>■ Reverse polarity protected plug connector (RM 5.08)</li> </ul>	WN.POWER.SUPPLY.PPP	
<p>External plug-in power supply for LockNode with RS-485 interface</p> <ul style="list-style-type: none"> <li>■ 12 V<sub>DC</sub>, 500 mA</li> <li>■ Open ends with wire end ferrules mm</li> </ul>	WN.POWER.SUPPLY.LNC	
Battery set for WaveNet LockNode (10 pieces)	WN.BAT.SET	
Cable	Item order code	Image
<p>Sensor cable for connection to LockNodes (WN.LN.R/ WN.LN.C) for door monitoring (5m)</p>	WN.LN.SENSOR.CABLE	
<p>Connection cable to connect the SmartRelay to a LockNode (WNM.LN.R/C)</p>	WN.WIRED.BF.G2	

Cable	Item order code	Image
Connection cable for WNM-IO-Router type RN	WNM.CABLE.IO	

Antenna	Item order code	Image
External antenna for LockNodes: <ul style="list-style-type: none"> <li>■ WN(M).LN.R</li> <li>■ WN(M).LN.C</li> </ul>	WN.LN.ANTV	
External additional antenna for WNM.RN2.ER.IO (cable length 2.5 m)	ANTENNA.EXT.868	

Holder	Item order code	Image
Bracket for RN housing (not suitable for Router-Node 2)	WN.RN.BOX	

Measurement	Item order code	Image
Test set for illumination of the WaveNet radio network at 868 MHz: <ul style="list-style-type: none"> <li>■ Base station</li> <li>■ Mobile station</li> </ul> Prerequisite: Two hours telephone instruction (included in the price)	WN.TESTER.BAMO.EU	
Base station of the test set	WN.TESTER.BASIS.EU	

Measurement	Item order code	Image
Mobile station of the test set	WN.TESTER.MOBILE.EU	

### 5.3 Devices

Devices that can be used as network components in WaveNet basically have two independent interfaces (first and second letter according to router type, *RouterNodes* [[▶ 14](#)] and *LockNodes* [[▶ 15](#)]). You are therefore able to connect two network segments with different transmission media.

RouterNodes connect two network segments with (different) transmission media (see <i>Transmission paths</i> [ <a href="#">▶ 13</a> ]) with each other.	LockNodes connect a lock to a network segment. Depending on the version, the LockNode is connected to the lock either wirelessly (LN.R and LN.C) or physically (LockNode Inside).
--	---

With the exception of the computer, each WaveNet device is assigned its own address and a network ID that is the same for all devices. The assignment of the network ID makes your WaveNet unique and distinguishable from other devices that may be within range.

#### 5.3.1 Computer

Computers play two roles in WaveNet:

- As a server with an LSM database
- As a client with LSM interface

If the server and the clients are connected via an existing network, then you can access the WaveNet components from both the server as well as the client. This allows you to span your WaveNet over long distances, including various buildings, despite physical separation. Special software for the communication nodes must be installed on the server (CommNode). The communication nodes are the connection for the WaveNet devices.

You can use different interfaces on your computer:

- Ethernet
- Serial (RS-485, EOL)

- Serial (USB, EOL)

### 5.3.2 RouterNodes

RouterNodes are the backbone of your network. RouterNodes allow you to transmit data in WaveNet right up to the LockNodes. The LockNodes then take over further communication for locking.

The new generation of RouterNodes (=RN2) is a further development of the previous generation of RouterNodes (=RN) and offers the following advantages:

- Easy firmware updates (40.1 and higher) with OAM tool (see [Updating firmware \[▶ 32\]](#))
- IO interfaces directly on the terminal block
- Extended selection of cables (use of own cables is possible)
- Extended power supply options

#### RN2.ER.IO

This RouterNode supports Ethernet and Radio (=868 MHz).

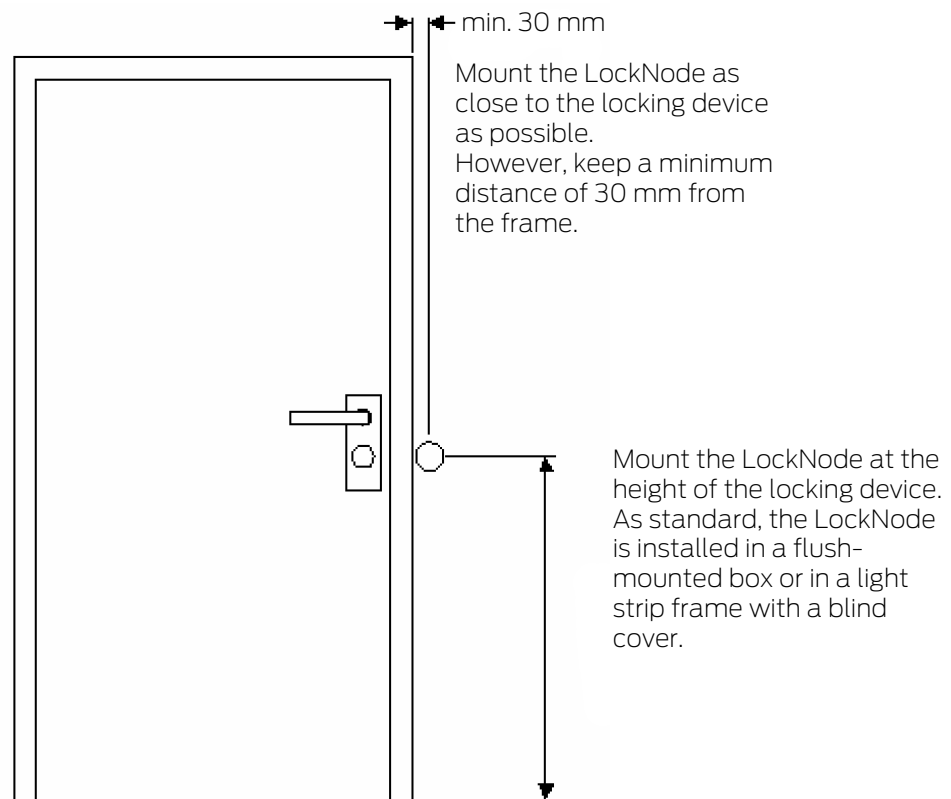
### 5.3.3 LockNodes

LockNodes allow you to connect your locking devices to your WaveNet. LockNodes are available as inside versions for many locking devices (see [LockNodes \[▶ 20\]](#)). These LockNodes are installed inside the existing locking device and are invisible from the outside. Alternatively, you can use external LockNodes and install them visible or concealed (for example in a flush-mounted box) near the locking device.

#### Installing internal LockNodes ("Inside")

Information on the installation of the internal LockNodes can be found in the short instructions for the respective LockNodes.

### Installing external LockNodes



## 5.4 Radio network

You can use WaveNet to wirelessly transfer authorisations, status changes, protection functions and other data.

WaveNet's state-of-the-art wireless technologies have to meet different expectations than standard wireless networks.

Since 2000, a special SRD band (short range device) in the 868 MHz range has been available for this area. This SRD band is divided into several sub-bands (you can select the sub-band, see [Adding a Radio channel \[▶ 43\]](#) and [Add RouterNode to WaveNet \[▶ 53\]](#)).

Separate frequency ranges are reserved for safety applications. In addition, WaveNet devices transmit on the basis of the "listen before talk" principle, which means that a check is performed before transmission to see whether communication is currently in progress on the channel set. If communication is in progress, the WaveNet devices will not transmit until communication is complete.

WaveNet therefore offers you a secure transmission path in the 868 MHz range.

Like all wireless networks, WaveNet is influenced by device and environmental characteristics:

- ❑ Transmitting capacity
- ❑ Antennas (size, orientation)
- ❑ (Unauthorised) modification of the WaveNet devices
- ❑ Receiver sensitivity
- ❑ Transmission frequency
- ❑ Environmental influences (humidity, temperature, electromagnetic interference sources)
- ❑ Structural conditions (walls, ceilings, etc. See table)
- ❑ Installation site (change in environmental conditions, see also *Product-specific safety instructions* [[▶ 6](#)])
- ❑ Network utilisation by co-users of the radio frequencies
- ❑ Random or deliberate interference
  - ❑ Unauthorised use of spectrum by other devices
  - ❑ Electromagnetic fields (for example from switching power supplies)
  - ❑ Jammers

These influences can interfere or hinder the transmission. You recognise this by:

- ❑ poor RSSI (Received Signal Strength) values
- ❑ slow or failed data transmission
- ❑ reduced range

The WaveNet is also influenced by:

- ❑ power failure in a (sub) range
- ❑ Failure of a transmission path in an external network (e.g. Ethernet connection)

#### 5.4.1 Segments

Each RouterNode can reach LockNodes within a range. These areas can also overlap - a LockNode can therefore be located in several areas at the same time and could be addressed by several RouterNodes simultaneously. You therefore assign the LockNodes to a segment in the WaveNet Manager (see *Adding Lock Nodes to WaveNet* [[▶ 59](#)]).

Network segments are identified by:

- ❑ Transmission medium (see *Transmission paths* [[▶ 13](#)])
  - ❑ Ethernet (TCP/IP)
  - ❑ 868 MHz

- WLAN (TCP/IP)
- USB
- RS-485 cable
- RS-232 cable
- Input-side segment address and output-side segment address
  - GID=Group-ID → Slave or master address

### Input and output segment

Each RouterNode has an input segment and an output segment, whereas each LockNode has only one input segment.

If in WaveNet, a RouterNode is to communicate with a LockNode (or another RouterNode), then the input segment of the LockNode (or the other RouterNode) must match the output segment of the RouterNode. You can read the segments from the WaveNet overview (see [Overview \[▶ 178\]](#)), taking the network mask into account (see [Addressing \[▶ 42\]](#)).

#### 5.4.2 Signal quality

Your WaveNet transmits data wirelessly between networked RouterNodes and LockNodes. In order for the data to be transmitted, the radio signal must have a certain signal strength so that it can be distinguished from interference and received (also see [Challenges in wireless networks \[▶ 24\]](#)).

### IMPORTANT

#### Recommended signal strength

The signal strength in the WaveNet Manager should be between 0 dBm and -70 dBm.

If the signal strength is insufficient, the connection and communication between devices can become slow or interrupted, and there will also be higher power consumption.

- If the signal strength is between -75 dBm and -90 dBm, there may be limited functionality. Improve the signal quality (see [Improving signal quality \[▶ 152\]](#)).

#### Unit of signal strength

The WaveNet Manager displays the signal strength as an RSSI value (Received Signal Strength) in dBm. This value is:

- Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.

- ❑ Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm (i.e. the smaller the amount), the better the reception.

### Influences on signal strength

Signal strength is influenced by various factors, but most significantly by the environment and the materials used in its construction.

Material	Permeability
<ul style="list-style-type: none"> <li>❑ Wood</li> <li>❑ Plaster</li> <li>❑ Gypsum plasterboard</li> </ul>	90%-100%
<ul style="list-style-type: none"> <li>❑ Brick</li> <li>❑ Particle board</li> </ul>	65%-95%
<ul style="list-style-type: none"> <li>❑ Reinforced concrete (transmitter on metal)</li> </ul>	10%-70%
<ul style="list-style-type: none"> <li>❑ Metal</li> <li>❑ Metal grid</li> <li>❑ Aluminium cladding</li> </ul>	0%-10%

#### 5.4.3 Challenges in wireless networks

Radio waves propagate in all directions. Unlike cables, they are not bound to a transmission medium (cable). This results in some radio-specific characteristics.

Three decisive influences determine whether a radio signal is transmitted successfully:

- ❑ Signal strength
- ❑ Signal-to-noise ratio
- ❑ Frequency utilisation



## Explanation of the influences

Signal strength	Signal-to-noise ratio	Frequency utilisation
<p>The signal strength is the amplitude of the radio wave. The stronger the signal, the more clearly the receiver can receive the transmitted data. The signal strength decreases with increasing distance or due to unfavourable transmission media.</p> <p>The more sensitive a receiver is (the better the antennas are), the less signal strength it needs.</p>	<p>The signal-to-noise ratio (SNR) indicates how strong the noise is compared to the wanted signal. Radio waves do not "end". Theoretically the range is unlimited, practically only the signal strength decreases. This means that radio waves penetrate other radio networks and no longer produce a useful signal, but (disturbing) static noise. If the noise is too strong (i.e. the signal-to-noise ratio is very poor), the receiver can no longer distinguish the wanted signal from the noise.</p>	<p>The utilization of the frequency is the ratio of free transmission time to occupied transmission time. A receiver can only receive one radio signal at a time. WaveNet devices operate according to the "listen-before-talk" principle. No WaveNet device transmits if it detects that a radio signal is already being transmitted on the frequency band in use. This results in waiting times until the frequency band is free again. The longer these waiting times are, the longer it takes for a device to transmit → The transmission speed decreases.</p>

Examples from daily life

Signal strength	Signal-to-noise ratio	Frequency utilisation
<p>Two people speak to each other (language as a signal). One person speaks louder (signal strength increases).                      If there is a wall between the people (unfavourable transmission medium), the speech becomes quieter (signal decreases).                      If a person does not turn towards the speaker (unfavourable alignment of antennas), speech is perceived as quieter (signal decreases).                      People with good hearing (sensitive receivers) can also understand soft speech (low signal strength).</p>	<p>Two people speak to each other (language as a signal). The people are standing at a busy road next to each other, which causes noise (static). The closer people get to the road, the louder the noise becomes in relation to the speech (signal-to-noise ratio decreases). If people stand too close to the road, they no longer understand each other.                      People can either move away from the street (noise decreases) or speak louder (signal increases) to improve the signal-to-noise ratio. It makes no difference whether a person can hear better (sensitivity is higher), because with speech (signal) the street (noise) is also heard louder.</p>	<p>Many people want to speak simultaneously (speech as signal). If one person is speaking (frequency band is busy), then no other person can speak (waiting time), otherwise no one will understand. People have to wait until there is a break in the conversation ("listen-before-talk") and then they can speak (start radio signal transmission).                      The more people are in a room, the longer they have to wait for a break in the conversation (frequency utilisation increases).                      People can either spread out spatially (to avoid hearing when other people are talking at the same time) or be short (to shorten the waiting time), so that more people can talk in the same period of time (reduce the load on the frequency).</p>

Possible causes for deteriorating environmental conditions in WaveNet

(List without claim to completeness)

Signal strength	Signal-to-noise ratio	Frequency utilisation
<ul style="list-style-type: none"> <li>❑ Devices too far away</li> <li>❑ Absorption by unfavourable transmission media (e.g. metal surfaces or metal doors)</li> <li>❑ Absorption due to unfavourable environmental conditions (e.g. humidity, temperature)</li> <li>❑ Unfavourable alignment of the antennas</li> </ul>	<ul style="list-style-type: none"> <li>❑ Many devices on the 868 MHz band nearby</li> <li>❑ Electromagnetic sources of interference                             <ul style="list-style-type: none"> <li>❑ Electromagnetic fields (e.g. from switching power supplies)</li> <li>❑ Jammers</li> </ul> </li> <li>❑ Reflective surfaces</li> </ul>	<ul style="list-style-type: none"> <li>❑ Many devices on the 868 MHz band nearby</li> <li>❑ Unauthorised use of spectrum</li> <li>❑ Jammers</li> <li>❑ Long transmission times or large data volumes</li> </ul>

### 5.5 Safety and alarms

Security is a top priority for SimonsVoss as a manufacturer of high-quality equipment.



#### NOTE

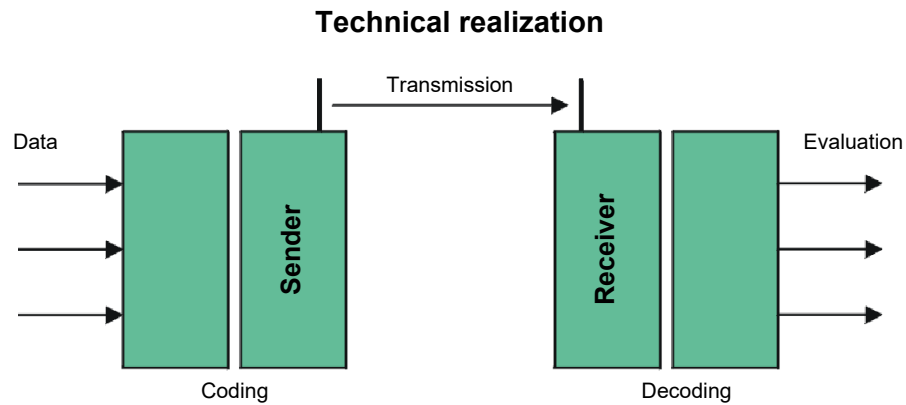
#### Redundant protection of the network infrastructure

In addition to SimonsVoss security measures, the network infrastructure in which you use WaveNet must also comply with current security standards.

1. You can meet these security standards by, for example using virtual networks or active network monitoring (the list does not claim to be complete).
2. talking to your IT infrastructure specialist.

#### 5.5.1 Encryption (WaveNet)

Advanced cryptography protects the data that is transported in your WaveNet.



**End-to-end encryption**

End-to-end means in this context: between central software and locking devices. The data is encrypted and leaves the central software. It is only decrypted again when the locking device is closed.

Communication	Encryption
End-to-end (general)	3DES (112 bit)
Access lists (against unauthorised reading)	Single DES (56 bit)
Broadcast signals	AES (128 bit)

**Digitally signed data packages**

The 128-bit signing of the data packets protects against manipulation on the radio link. If the signature of a data packet is not correct, the data packet is ignored.

**Protection against replay attacks**

Each safety-relevant data packet contains a counter. This counter is incremented for each new data packet. If a data packet with the same counter reading arrives again, the data packet is ignored. This means that if an attacker records a data packet and sends it again (replay attack), the counter of the data packet is the same as that of the original packet and the copy of the attacker is recognized and therefore ignored.

**5.5.2 Monitoring the devices in the network**

The devices on your WaveNet can be distributed over large parts of the building. You can monitor the devices partially remotely:

the status of your locking devices

If you use door monitoring locking devices, the current status of your locking device is transmitted to LSM via WaveNet and displayed there (DM column). As an alternative to the display in LSM, you can also monitor the status of your locking devices using Smart.Surveil.

For additional information, see the LSM manual and the Smart.Surveil manual.

Network connections of your WaveNet

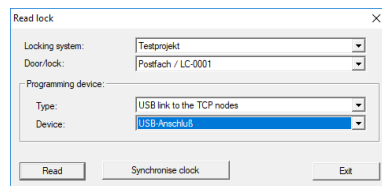
The current status of the connections between the LSM and your WaveNet devices is displayed in the LSM (column N).

- No entry: Network connection not created.
- W (turquoise): Last connection attempt successful.
- W (yellow): Last connection attempt up to LockNode successful, but not up to locking device (door open?).
- W (red): Last connection attempt failed.

Additional information can be found in the chapters *WaveNet and LSM* [▶ 30] and *Assigning LockNodes to the locking devices* [▶ 68] as well as *Fault rectification* [▶ 152].

Battery status

You can also use LSM to read the battery status of the marked lock via your WaveNet (| Programming | - [Read highlighted locking device/set time](#) - [Read](#) ).



You can find additional information in the LSM manual.

### 5.5.3 Alarms

You can use the WaveNet to transmit status changes to LSM and thus react to them. In this context, alarms are messages to which you must respond (e.g. break-in attempts).



#### WARNING

##### Redundant protection against hazards

The WaveNet system is not suitable as a replacement for monitoring systems such as burglar or fire alarm systems. Undetected fires or burglaries can pose a risk to persons and property.

- In addition to WaveNet, use a redundant monitoring system.

## 5.6 WaveNet and LSM

WaveNet and LSM are formally separate. LSM "thinks" in locking devices and communication nodes and WaveNet manager "thinks" in LockNodes. You create your locking system with access authorisations independently of one another in LSM and the WaveNet Manager creates WaveNet.

WaveNet does not "know" your locking devices, only the LockNodes connected to them. The LockNodes are physically connected to the locking devices (Inside LockNodes) or within radio range (external LockNodes). The LockNodes therefore "know" in which locking device they are installed. The LSM can therefore read both information (locking device and LockNode) from the LockNodes via WaveNet and then establish the logical connection between LockNode and locking device (see *Assigning LockNodes to the locking devices* [▶ 68]).

## 5.7 Firmware

### 5.7.1 Reading out firmware

You can read out the firmware versions of your devices (for information on firmware versions see *Firmware information* [▶ 39]).

#### RouterNodes

You can either see the firmware of the RouterNodes in the overview of the OAM tool (for RN2, older ones only listed as "Digi Device") and update it (see *Updating firmware* [▶ 32]) or read it out with LSM (for RN and RN2).

- ✓ LSM is open.
  - ✓ RouterNodes connected to LSM (for testing, see *Test reachability (LSM)* [▶ 186])
1. Via | Network | open the entry **Administer WaveNet node**.
    - ↳ You see a list of WaveNet-relevant components.
  2. If necessary, activate the checkbox  Display all WaveNet nodes.
    - ↳ You will see a list of WaveNet-relevant components.
  3. Select the RouterNode whose firmware you want to read out.
  4. Click the button **Properties**.
    - ↳ The window "WaveNet network node properties" opens.

WaveNet network node properties

Name:

Node type:

Interfaces:

Chip ID:

Address:

Firmware:  Firmware TM:

Connection device:

Description:

State

Output is set

Input 1

Input 2

Input 3

Battery state critical

Configuration

Activate event forwarding

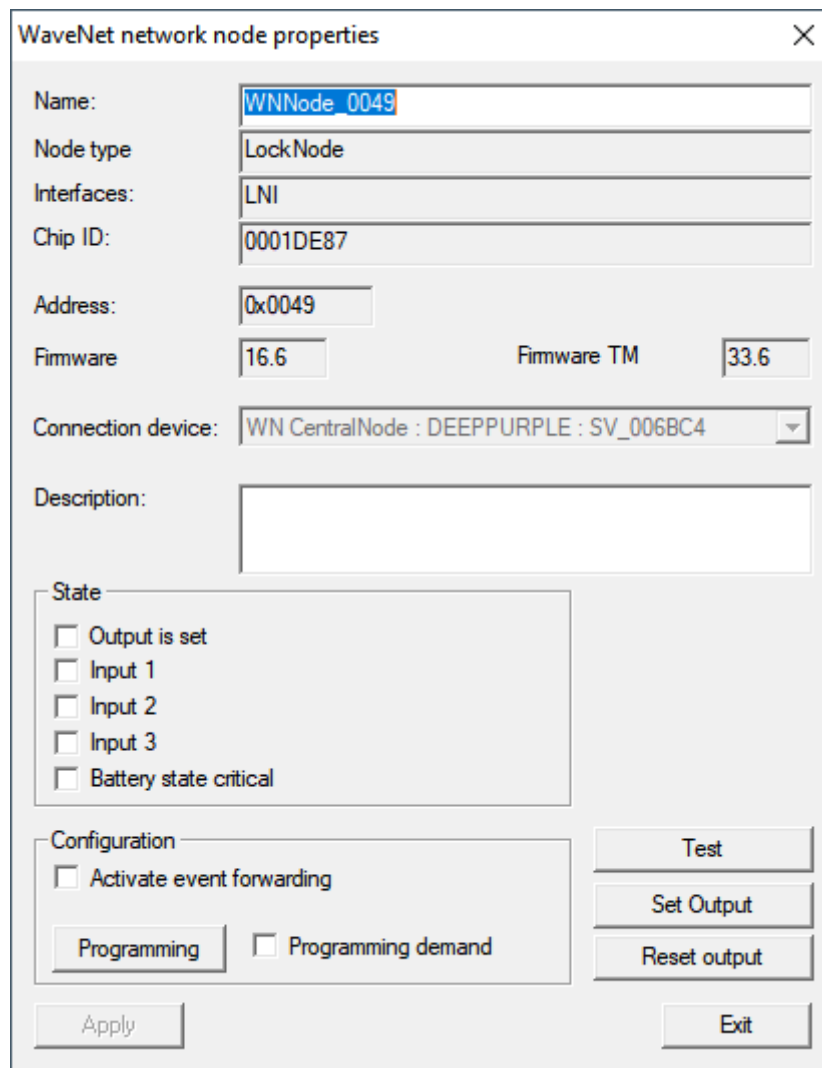
Programming demand

Buttons: Test, Set Output, Reset output, Apply, Exit

↳ You see the firmware version in the line **Firmware TM**.

### LockNodes

- ✓ LSM is open.
  - ✓ LockNodes connected to LSM (for testing, see *Test reachability (LSM)* [[▶ 186](#)]).
1. Via | Network | open the entry [Administer WaveNet node](#).
    - ↳ You see a list of WaveNet-relevant components.
  2. If necessary, activate the checkbox  Display all WaveNet nodes.
    - ↳ You will see a list of WaveNet-relevant components.
  3. Select the LockNode whose firmware you want to read out.
  4. Click on the button [Properties](#).
    - ↳ The window "WaveNet network node properties" opens.



The screenshot shows a dialog box titled "WaveNet network node properties" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** WNNode\_0049
- Node type:** LockNode
- Interfaces:** LNI
- Chip ID:** 0001DE87
- Address:** 0x0049
- Firmware:** 16.6
- Firmware TM:** 33.6
- Connection device:** WN CentralNode : DEEPPURPLE : SV\_006BC4 (dropdown menu)
- Description:** (empty text box)
- State:** A group box containing five unchecked checkboxes:
  - Output is set
  - Input 1
  - Input 2
  - Input 3
  - Battery state critical
- Configuration:** A group box containing two unchecked checkboxes:
  - Activate event forwarding
  - Programming demand
- Buttons:** Test, Set Output, Reset output, Apply, and Exit.

↳ You see the firmware version in the line **Firmware TM**.

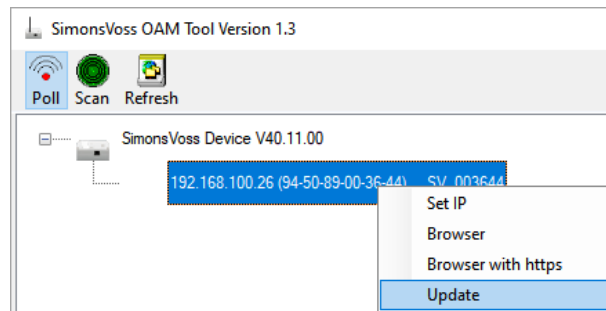
### 5.7.2 Updating firmware

Newer firmware versions improve your products and may also enable new features (see *Firmware information* [▶ 39]).

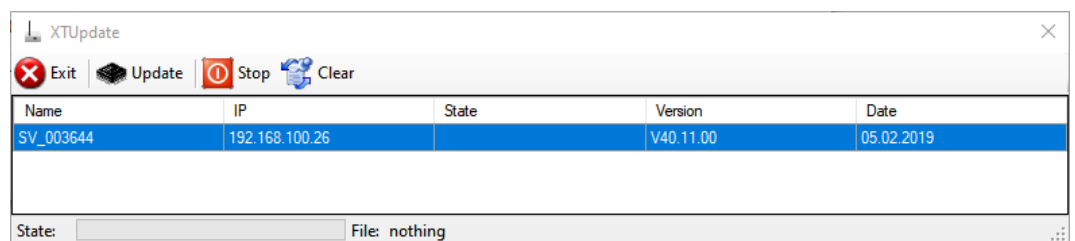
#### RouterNodes with Ethernet connection

You can update the firmware yourself by using the Operation, Administration and Maintenance Tool (OAM tool) (only RN2). The OAM tool is available free of charge in the download area on the SimonsVoss website (<https://www.simons-voss.com>). You do not need to install the OAM tool.





- ✓ Latest version of the OAM tool opened (see *Determining and setting the IP address* [▶ 49]).
  - ✓ RouterNode listed (see *Determining and setting the IP address* [▶ 49]).
  - ✓ Change of IP allowed via the OAM tool (see *Browser interface* [▶ 148]).
  - ✓ Current firmware of RouterNode 40.1X or higher.
  - ✓ RouterNode type RN2
  - ✓ Firmware file (.REL) available (contact your dealer or system partner)
1. Right-click on the entry of the RouterNode you want to update to open the context menu.
  2. Select the entry **Update**.
    - ↳ Window "XTUpdate" with a RouterNode list opens.



## NOTE

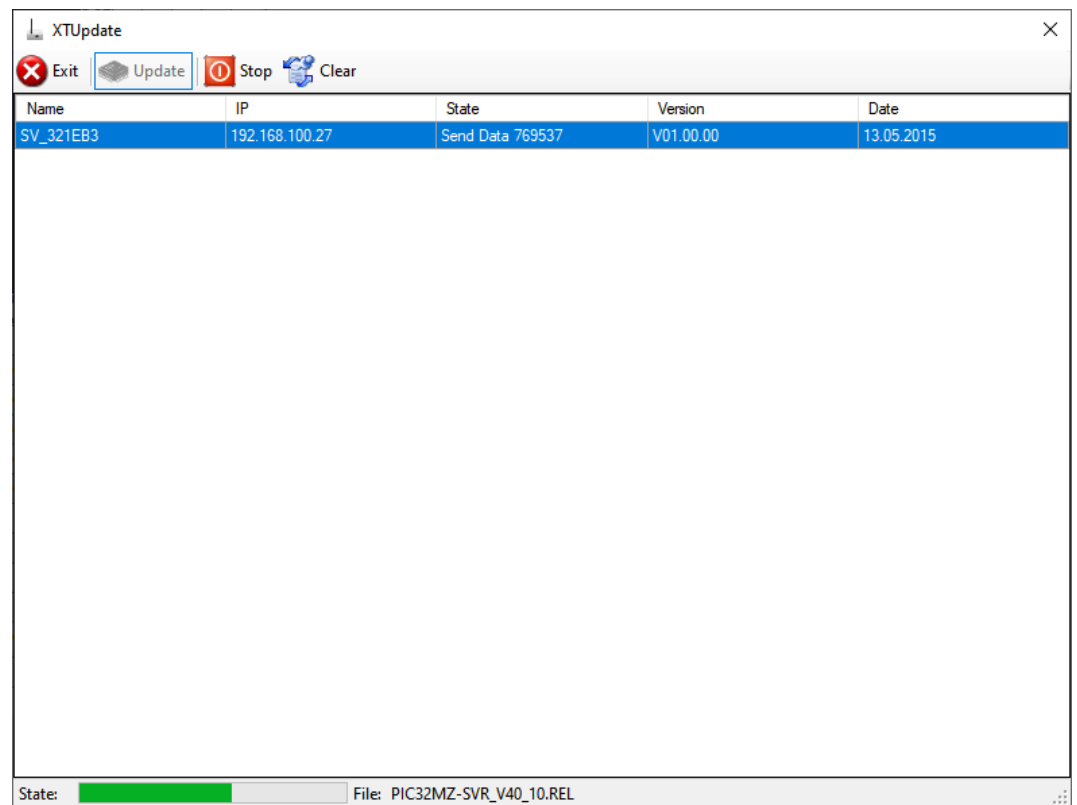
### Updating multiple RouterNodes

The OAM tool stays open. You can add more entries to the update list in the "XTUpdate" window.

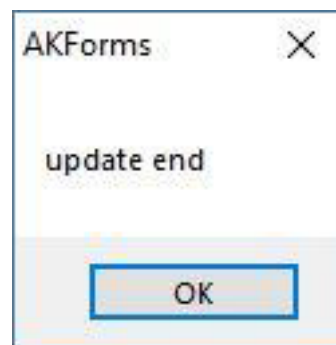
1. Select another RouterNode in the OAM tool.
  2. Select the entry **Update** aus.
    - ↳ RouterNode is added to the update list in the "XTUpdate" window.
  3. Repeat the steps until all RouterNodes you want to update are in the update list.
- ↳ RouterNodes are added to the update list in the "XTUpdate" window.

3. Make sure that the RouterNodes you want to update are highlighted.
4. Click on the button **Update**.
  - ↳ Explorer window opens.

5. Navigate to the location of the firmware file.
6. Highlight the firmware file.
7. Click on the button **Open**.
  - ↳ The Explorer window closes.
  - ↳ The firmware of the RouterNodes is updated.



- ↳ The window "AKForms" opens.



8. Click on the **OK** button.
  - ↳ The "AKForms" window closes.
9. Click on the button **Exit**.
  - ↳ The "XTUpdate" window closes.
- ↳ The firmware of the RouterNodes is updated.

## 6. WaveNet Manager

### 6.1 System requirements

#### General

- Local administrator rights
- Communication: TCP/IP
- LAN connection (recommendation: 100 MBit or higher)
- Help function: PDF Reader, for example Adobe Reader

Additionally the following preconditions apply for the inclusion of Ethernet routers with host names:

- Communication: TCP/IP with activated NetBios
- Windows domain with name resolution

Contact your IT department.

#### Client

Requirements same as LSM.

- Monitor: 19" and 1024x768 (or better)
- Computer: 2,66 GHz and 2 GB RAM (or better)
- Operating system with static IP and name resolution for LSM
- Windows Operating system (7, 8/8.1 or 10 Professional)
- LSM: .NET-Framework 2.0 (or higher)
- USB interface or LAN connection

### 6.2 Unpacking, updating and starting the software

#### 6.2.1 Unpacking

If you work with several LSM databases: Use a separate WaveNet Manager folder (e.g. subfolder) for each LSM database. This will help you avoid differently configured strings.

#### LSM Basic Online

Unpack the WaveNet Manager into a suitable directory.

SimonsVoss recommends creating the output folder of the WaveNet Manager in the same directory. Therefore, select a directory with free write access, e.g:

*C:\WaveNet-Manager.*

### LSM Business/Professional

Unpack the WaveNet Manager into a suitable directory (usually a folder on a network drive). SimonsVoss recommends creating the output folder of the WaveNet Manager in the same directory.

Follow these recommendations for the directory:

- The directory is located on the LSM Business server. The server and client can have different port releases. The WaveNet Manager should therefore always be started from the server. Otherwise, client-side port releases may be missing and communication problems may occur during subsequent operation.
- All clients or users who are to work with the WaveNet Manager have *read/execute* permission for the released folder. Grant the clients or users this right if it does not exist.
- If you are working with several LSM databases: Create a separate subdirectory for each database, which contains a separate output folder. Unpack the WaveNet Manager into each subdirectory. From the respective LSM databases, call up the WaveNet Manager in the appropriate subdirectory and select the output folder of the appropriate subdirectory.

#### 6.2.2 Update

If WaveNet Manager has already been installed, you only need to replace the following files in the WaveNet installation folder to implement the update:

- boost\_threadmon.dll
- WaveNetManager.exe
- WNIPDiscoveryLib.dll

The latest version of the WaveNet Manager can be found on the website:

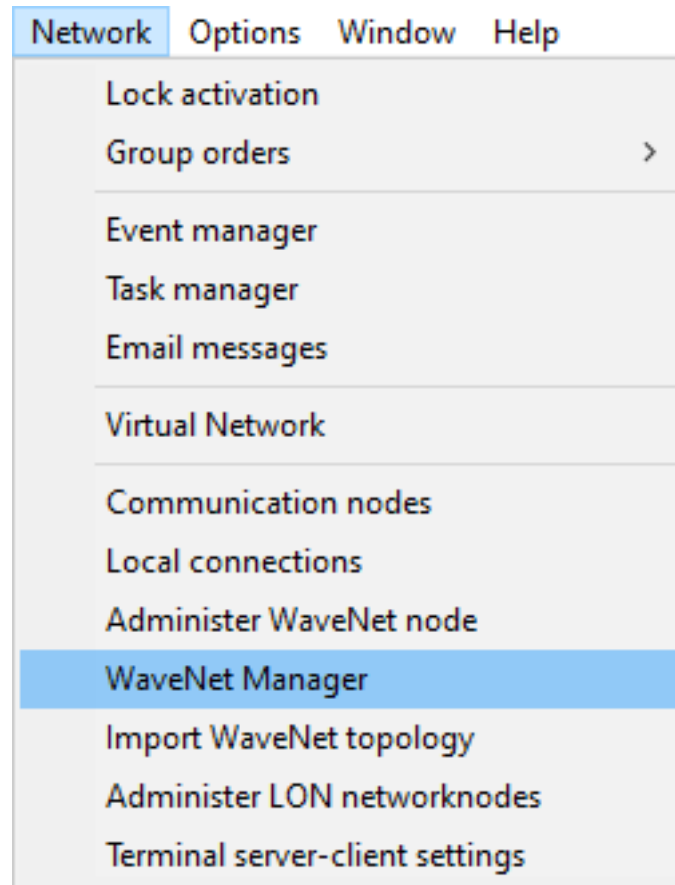
<https://www.simons-voss.com/en/service/software-downloads.html>

## 6.2.3 Start

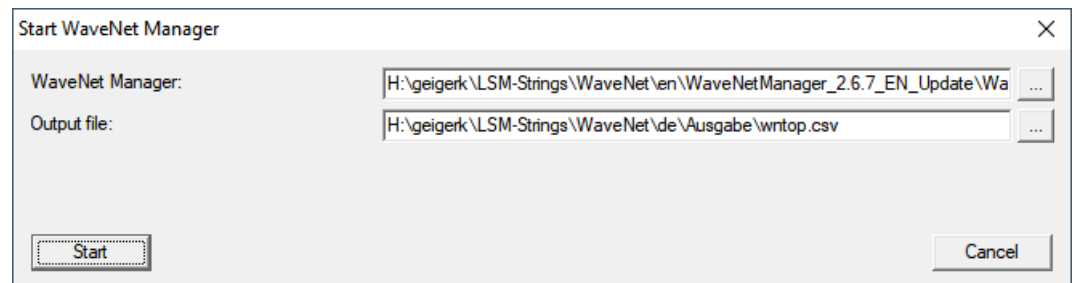
### 6.2.3.1 Best Practice: From the LSM software

✓ LSM is started with administrator rights.

1. Open the WaveNet Manager via | Network | - **WaveNet Manager**.



2. Check the file paths.



**NOTE****Error during saving due to missing write permissions**

The WaveNet Manager cannot write to protected storage locations (such as C:\Program Files). The output is then redirected to the Virtual Store (see Checking and fixing the Virtual Store).

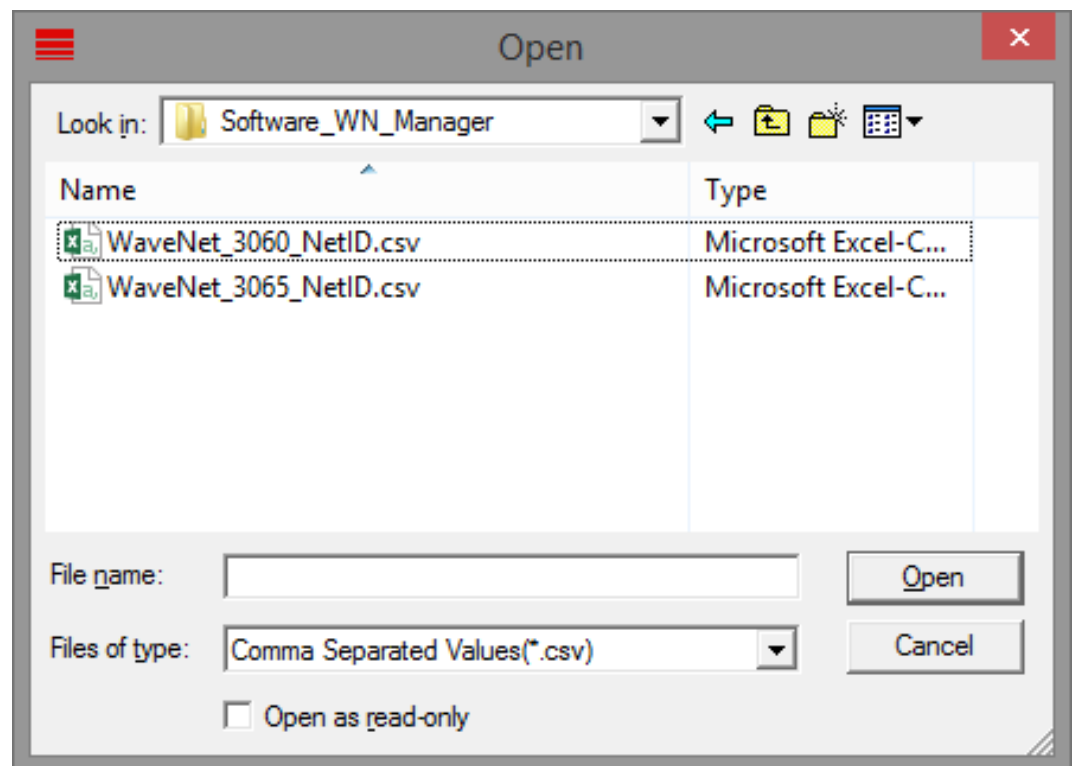
- ❑ Select a storage location for the output for which all users have write permission.

3. Click the button **Start**.
- ↳ WaveNet Manager opens.

### 6.2.3.2 Manually

Only start the WaveNet Manager manually if you do not want to connect the WaveNet to be configured directly to the LSM and only want to use the I/O function, for example.

1. Execute the file "WaveNetManager.exe" in the installation directory.
2. Select your topology or create a new network using the **Cancel**.



- ↳ The WaveNet Manager opens.

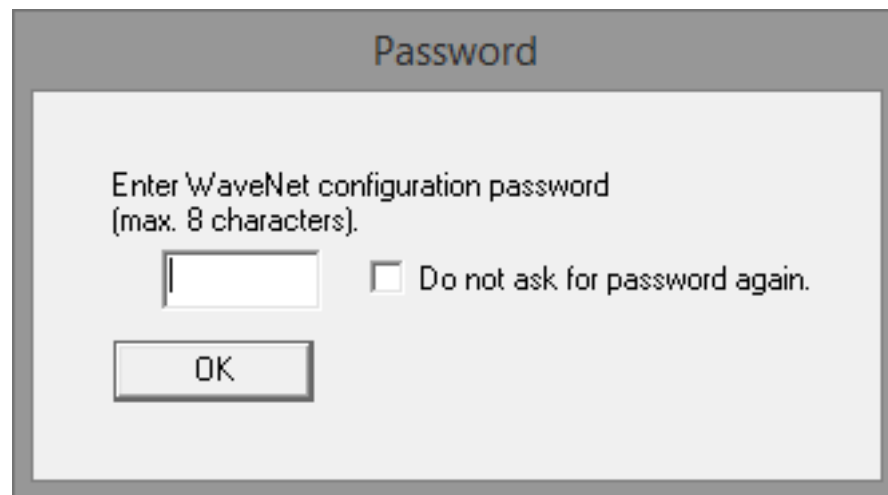
If more than one WaveNet topology is available, a dialogue box appears. In the dialogue box, select the network that you would like to edit. If you do not select a topology (**Cancel**), the WaveNet Manager starts and a new network can be created.

If you previously started the WaveNet Manager via LSM and are now starting it locally, LSM cannot tell the WaveNet Manager what the previous WaveNet looks like. In this case you create a new WaveNet.

#### 6.2.4 Password

The password must contain 1-8 characters. Otherwise you can choose your password freely. This password is programmed into all WaveNet components. It is not possible to change the password retroactively!

The password prevents accidental reprogramming of your existing or third-party networks. It is imperative that you only use one password per WaveNet database.



### IMPORTANT

#### Password assignment at first start

You can only assign the password when you first start the WaveNet Manager. If you do not assign a password when you first start the WaveNet Manager, you will not be able to assign a password afterwards. The password is then empty.

- Assign a password the first time you start the WaveNet Manager.

### 6.3 Firmware information

The availability of individual functions is firmware dependent. You can read out the firmware yourself (see *Reading out firmware* [▶ 30]) and possibly update it yourself (see *Updating firmware* [▶ 32]).

#### RouterNodes

The following functions are only available from certain firmware versions:





### LockNodes

The following functions are only available from certain firmware versions:

<30.8.16.0	≥ 30.8.16.0	≥ 30.8.16.2	≥ 30.8.16.3	≥ 33.3.16
Protection functions (IO) see <i>I/O configuration and protection functions</i> [▶ 69]				
✗	✓	✓	✓	✓
Send acknowledgement after broadcast see <i>RingCast</i> [▶ 95]				
✗	✗	✗	✓	✓
Fast wake-up see <i>Maximum transmission time in RingCast</i> [▶ 130]				
✗	✗	✓	✓	✓
LockNodes for triggering an input event individually selectable see <i>I/O configuration and protection functions</i> [▶ 69]				
✗	✗	✗	✗	✓

## 6.4 Management

### 6.4.1 Basic principles

**Network options**

Network parameters for RN\_ER - 192.168.100.26.

Network ID:

Radio frequency:

Network mask:

Do you want to add this node?

### 6.4.1.1 Addressing

You define the addressing during initial setup (when you add your first RouterNode). If you want to change these settings later, you must reset all WaveNet devices (see [Resetting/Deleting \[▶ 168\]](#)).

#### Network ID

The WaveNet uses a network ID. The network ID must meet the following requirements:

- Length: Four characters
- Permitted characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
- Invalid combinations: 0000, 0001, DDDD, FFFF

The Network ID, in combination with a password, ensures that your WaveNet is unique and prevents accidental reprogramming of networks.

#### Address in network/network mask

Devices in WaveNet have a network address (16-bit). The WaveNet uses a network mask for the address in the network. The network mask defines the division of bits between GROUP-ID (RouterNode) and MEMBER-ID (LockNode) and therefore the maximum number of RouterNodes and the maximum number of LockNodes and RouterNodes.

An 11\_5 network mask sees 11 bits ( $2^{11}=2048$  addresses, of which 1790 can be used. Some addresses are reserved for addressing serially accessible RouterNodes, i.e. "RouterNodes behind RouterNodes" and addressing the entire network or for broadcasts) for the RouterNodes and 5 bits ( $2^5=32$  addresses, of which 25 can be used) for the LockNodes.

You can choose from the following network masks:

Network mask	Number of Router-Nodes	Number of LockNodes
8_8	Max. 249	Max. 249 per Router-Node
11_5	Max. 1790	Max. 25 per Router-Node
12_4	Max. 3200	Max. 9 per RouterNode

If you do not make any other selection, the network mask is preset with 11\_5. Based on experience, this value has proven to be universally applicable.

#### Convert address to GROUP-ID and MEMBER-ID

You can convert the displayed address to the binary system to read the GROUP-ID and MEMBER-ID from the displayed address. Example:

Displayed address	0xA23F			
Division hexadecimal	A	2	3	F
Division decimal	10	2	3	15
Division binary	1010	0010	0011	1111
Total binary	1010001000111111			
Distribution after 8_8	8 GROUP-ID: 10100010 (=A2), 8 MEMBER-ID: 00111111 (=3F)			
Distribution according to 11_5	11 GROUP-ID: 10100010001, 5 MEMBER-ID: 11111			
Distribution after 12_4	12 GROUP-ID: 101000100011 (=A23), 4 MEMBER-ID: 1111 (=F)			

In the case of 8\_8 and 12\_4 network masks, you can also read the GROUP-ID and MEMBER-ID in the hexadecimal system directly from the displayed address.

#### 6.4.1.2 Radio channel

Select a radio channel for your WaveNet during initial setup. Each radio channel uses a different frequency range. Once you have selected the radio channel, all WaveNet devices use the same radio channel. The available radio channels for devices for the US market differ from those for the European market. For more information on setting up the radio network, see *Radio network* [▶ 21]).

You can only set the radio channel during the initial setup. To change the radio channel later, you must reset the WaveNet (see *Resetting/Deleting* [▶ 168]).



#### NOTE

##### Licensing or registration requirements

The operation of radio equipment may be subject to authorisation or registration in some areas.

1. Please enquire about the legal requirements in your area.
2. For new projects in Europe, use channel 1 or 2.

Channel number	Frequency range	Recommended geographical region of use
0 (only for searching for components)	868.1 MHz (standard version)	Europe
	920.1 MHz (australian version)	Australia
1	868.3 MHz (standard version)	Europe
	920.3 MHz (australian version)	Australia
2	868.5 MHz (standard version)	Europe
	920.5 MHz (australian version)	Australia
9	869.9 MHz	Europe
	921.9 MHz	Australia

#### 6.4.2 Auto-configuration

If your devices support automatic configuration, you can also configure the network automatically. You then no longer need to add the devices manually (for manual adding, see [Finding and adding devices \[▶ 48\]](#)).

Depending on the size of your WaveNet, the complete autoconfiguration may take some time. You can therefore restrict automatic configuration to branches of your WaveNet (manually select RouterNodes or select them directly). This does not check all connections and it is possible that the LockNodes are not assigned to the most accessible RouterNode. Only make use of the limited auto-configuration if you are absolutely sure.

##### Optimized autoconfiguration

If you select the Optimized checkbox Optimised, the system searches for both new and already configured devices.

If the WaveNet Manager discovers that nodes that have already been configured are much easier to reach from other segments (from other RouterNodes), the WaveNet Manager will move these nodes to the segments with the better accessibility.

You can also move the nodes manually afterwards (see [Assigning LockNodes to another RouterNode \[▶ 153\]](#)).

1. The WaveNet Manager searches for accessible RouterNodes.

- The WaveNet Manager searches for reachable LockNodes on every RouterNode that is reached (six searches).

Once auto-configuration is complete, the WaveNet Manager will display all devices that have been reached, together with their hex address and chip ID.



### NOTE

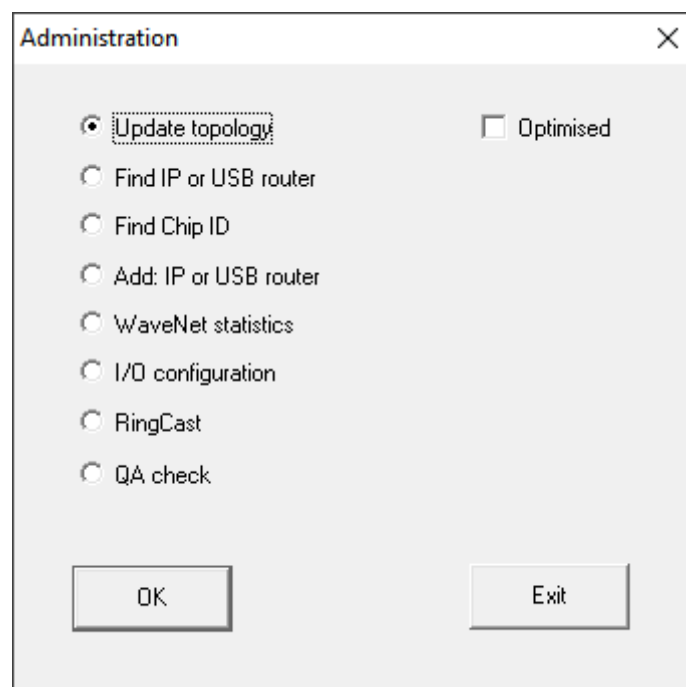
#### Time estimate

Depending on the size of your WaveNet, the automatic configuration may take a few minutes.

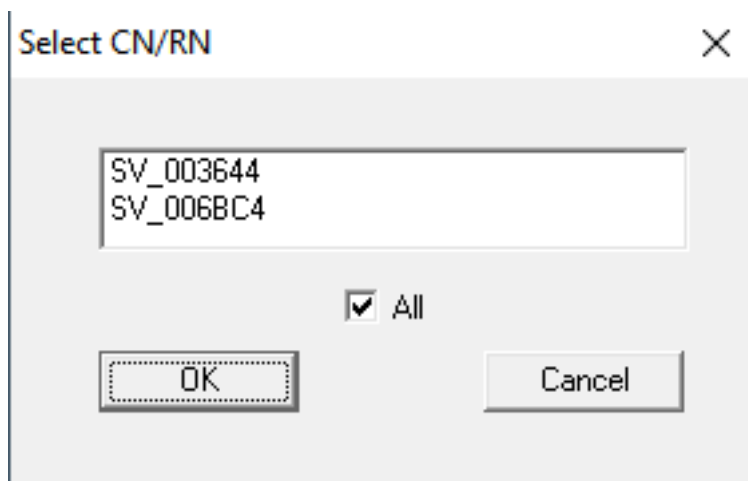
- ▣ You can expect about two minutes per router.

#### 6.4.2.1 Complete or limited (select RouterNodes from list)

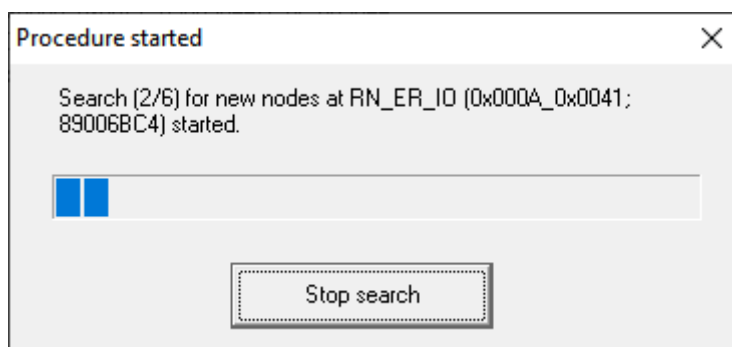
- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes/LockNodes within range.
- Right-click on the WaveNet\_XX\_X entry.
    - ↳ The window "Administration" opens.



- Select the option  Update topology.
- Click on the  button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Select CN/RN" opens.



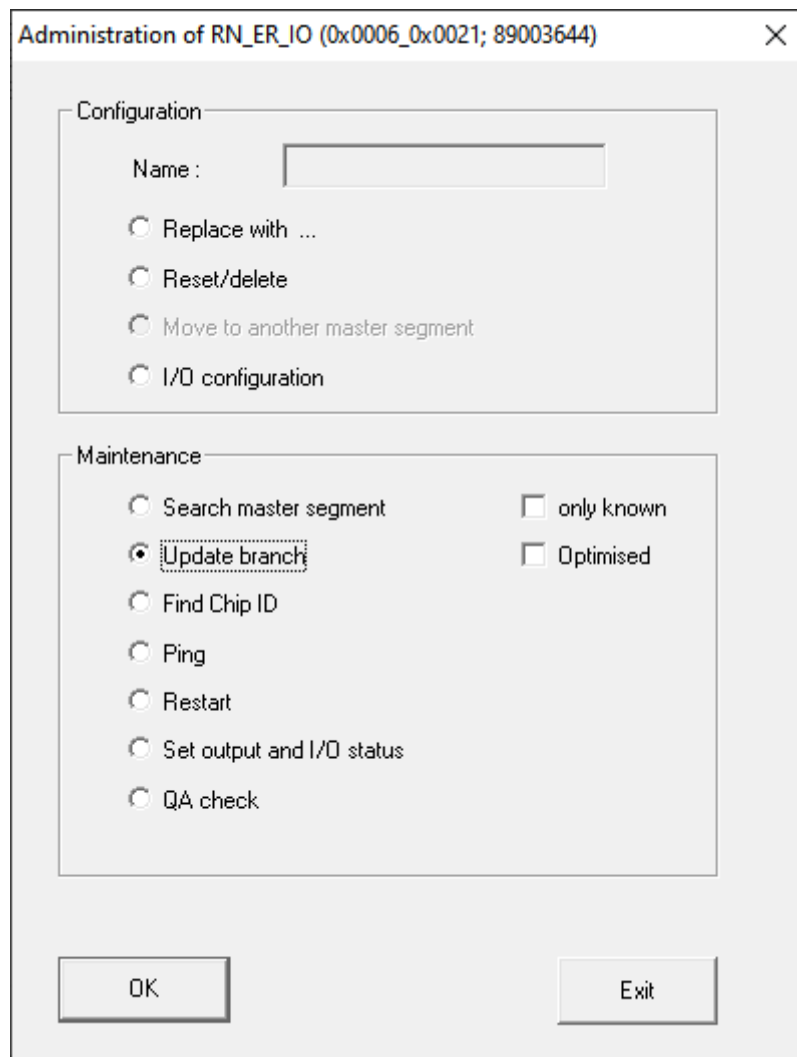
4. Select all RouterNodes you want to search with or check the  all checkbox to automatically configure your entire WaveNet.
5. Click on the **OK** button.
  - ↳ The window "Select CN/RN" closes.
  - ↳ The "Procedure started" window opens temporarily.



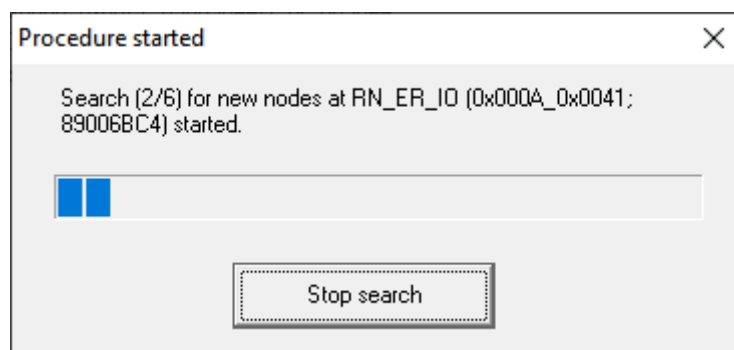
- ↳ Accessed devices (RouterNodes, LockNodes) are listed.
6. Click on the button **Save**.
    - ↳ Accessed devices (RouterNodes, LockNodes) are added. LockNodes have been assigned to the RouterNodes from your selection that are best accessible.

#### 6.4.2.2 Restricted (select RouterNode directly)

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes/LockNodes within range.
1. Right-click on the entry of the RouterNode from which you want to automatically search and configure.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Update branch.
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The "Procedure started" window opens temporarily.



- ↳ Accessed devices (RouterNodes, LockNodes) are listed.
4. Click on the button **Save** .
  - ↳ Accessed devices (RouterNodes, LockNodes) are added.

## Search with a single RouterNode

### 6.4.3 Finding and adding devices

You can optionally assign your RouterNodes to a communication node during the setup of your WaveNet. In this case, before setting up your WaveNet, make sure that at least one free communication node is available in your locking system. If necessary, create one and transfer the changes (see LSM manual).

In standalone operation (for example, with an LSM Basic) you do not need to create or use a communication node. Instead, you connect the WaveNet via local connections. Note that closing the LSM software interrupts the connection to WaveNet.

#### 6.4.3.1 Connecting RouterNode

You have two options for connecting your Ethernet RouterNode to your computer:

##### Option 1: Direct connection with CAT.5 patch cable

- ✓ Computer not connected to a network.
- ✓ Computer with assigned static IP address.
- Connect the Ethernet port on the RouterNode to the computer's Ethernet port.

You can set the IP address for the later location (see *Determining and setting the IP address* [▶ 49]) or operate the RouterNode permanently directly on the Ethernet port of your computer.

##### Option 2: Connect to the local network

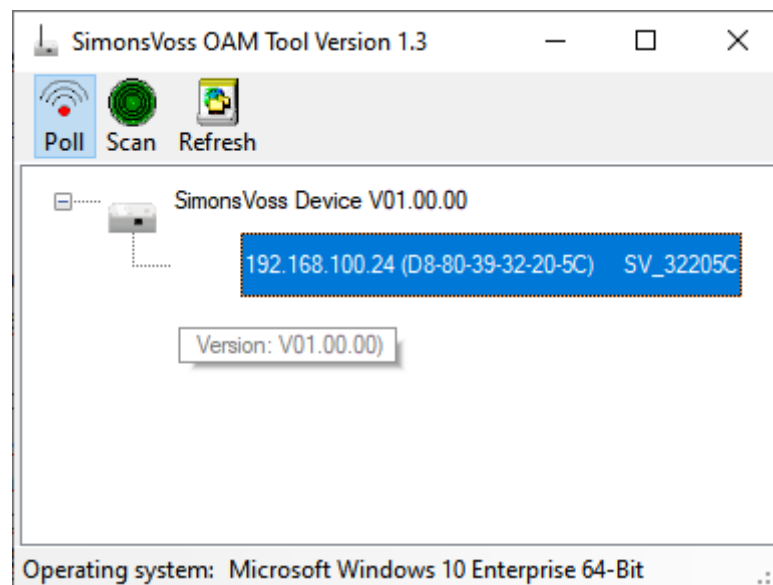
- ✓ RouterNode and computer in the same network (subnet).
  - ✓ DHCP server available.
1. Connect the Ethernet port of the RouterNode to a free network port on the network.
  2. Connect the Ethernet port of your computer to an available network port on the network.

You can set the IP address for the later location (see *Determining and Setting the IP Address* (*Determining and setting the IP address* [▶ 49]) or operate the RouterNode permanently on the same network as your computer.



### 6.4.3.2 Determining and setting the IP address

With the Operation, Administration and Maintenance Tool (OAM tool) you can both read and set the IP address. The OAM tool is available free of charge in the download area of the SimonsVoss website (<https://www.simons-voss.com>). You do not need to install the OAM tool.



#### IMPORTANT

##### Unauthorised changing of the IP address

The OAM tool is freely accessible. The OAM tool can be misused by unauthorized persons to change the IP address of your RouterNodes, GatewayNodes or SmartBridges.

- Block changing the IP address in the OAM Tool via the browser interface (see *Browser interface* [▶ 148]).



#### NOTE

##### Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

## Determining the IP



### NOTE

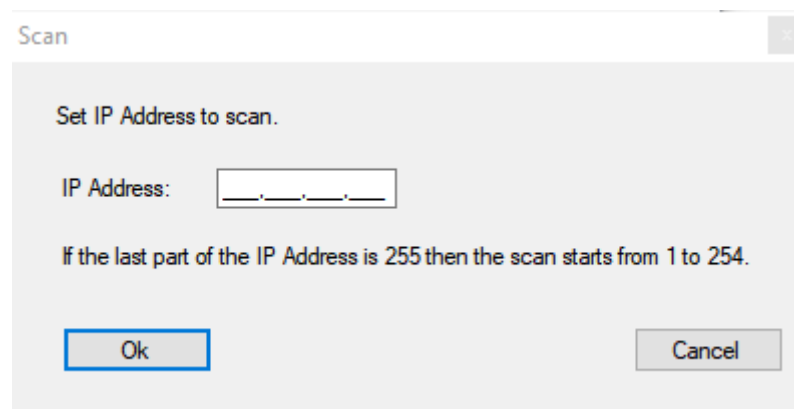
#### Error when connecting to several networks at the same time

The OAM tool searches the network for SimonsVoss network devices. Computers can be connected to several networks (e.g. cable and WiFi). In such a case, it is not clear to the OAM tool which network is to be searched and not all SimonsVoss network devices may be found.

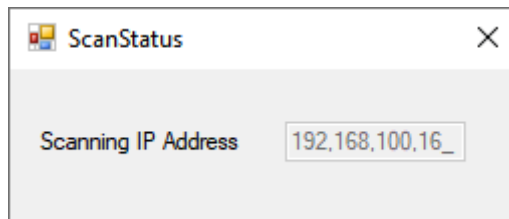
1. Disconnect network connections that are not needed.
2. Only connect the computer to the network that contains the network devices.

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
  - ✓ Subnet known.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Scan** button.
    - ↳ The "Scan" window will open.



3. Enter a known IP address of a device in the (WaveNet) network (other or new devices will also be found. If you do not know an IP address, then use the following IP address: 192.168.100.255 - may differ depending on the subnet).
4. Click on the **OK** button.
  - ↳ "Scan" window closes.
  - ↳ OAM tool scans the address range.



↳ OAM tool displays detected devices in the list.

Choose between DHCP server or static IP. You can also make the settings described below in the browser interface (see *Browser interface* [▶ 148]).

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

### Set IP for DHCP mode (default)

If you use a DHCP server, a DHCP server will configure the IP address.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Refresh** button.
    - ↳ RouterNode's IP address updated.
  3. Right-click the entry for the RouterNode's IP address you want to update to open the context menu.



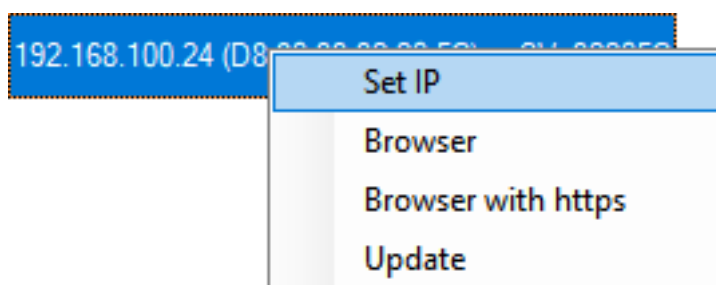
### NOTE

#### Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- ❑ Compare the MAC address of the entry with the label on your RouterNode.

4. Click the **Set IP** entry.



↳ The "Network configuration" window will open.

5. Make sure that the checkbox  Enable DHCP is activated.

6. If no address reservation is provided for this RouterNode on the DHCP server, note down the *hostname* (e.g. *SV\_32205C*). You will need it later when you carry out configuration in WaveNet Manager (see WaveNet manual - *Add RouterNode to WaveNet* [▶ 53]).
7. Click on the **OK** button.
  - ↳ "Network configuration" window closes.
  - ↳ RouterNode restarts.
8. Close the reboot notification window.
9. Close the OAM tool.
  - ↳ DHCP mode is configured.

### Configuring the IP for operation with static IP address

If you do not use a DHCP server, the IP address is configured with the default factory setting. You must change the IP address in this case; if you don't, several RouterNodes will have the same IP (i.e. the default factory IP) and will not be able to communicate.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Refresh** button.
    - ↳ The RouterNode's IP address is now updated.
  3. Right-click the entry for the RouterNode's IP address you want to update to open the context menu.



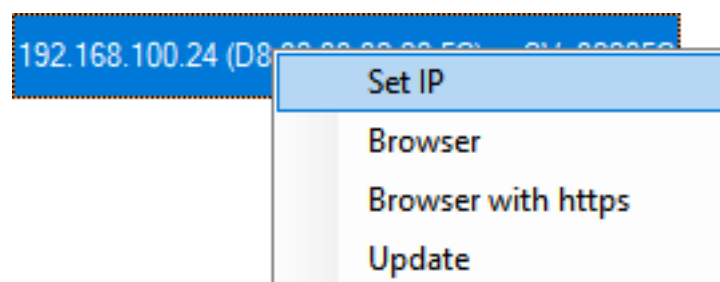
#### NOTE

#### Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click the **Set IP** entry.



↳ The "Network configuration" window will open.

5. Disable the  Enable DHCP check box.
6. Enter a new IP address if required.
7. Click on the **OK** button.
  - ↳ "Network configuration" window closes.
  - ↳ RouterNode restarts.
8. Close the reboot notification window.
9. Close the OAM tool.
  - ↳ IP address is now configured.

#### 6.4.3.3 Add RouterNode to WaveNet

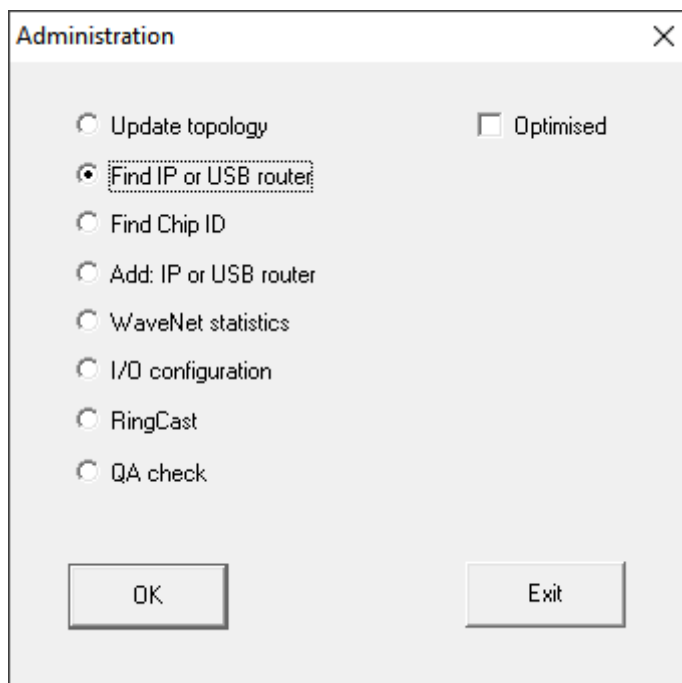
If you want to use RouterNodes in your WaveNet, you must first import the RouterNodes into your WaveNet topology in the WaveNet Manager.

Option	Application situation
<input checked="" type="radio"/> Find IP or USB router	<p>Use this option if you have many RouterNodes with Ethernet interface connected to the same network. They must be on the same subnet, otherwise use <input checked="" type="radio"/> Add: IP or USB router.</p> <p>With this option, you do not have to determine each IP and then enter it manually.</p>

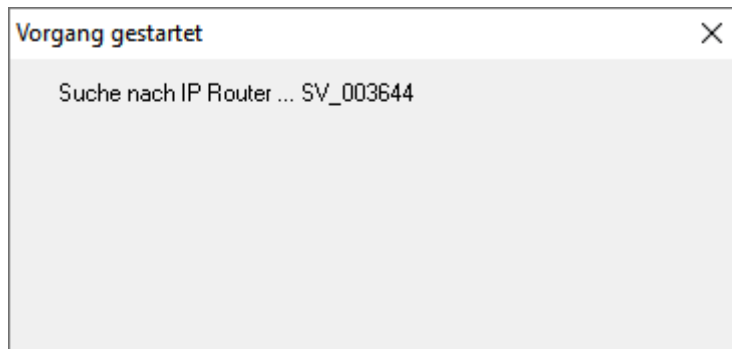
Option	Application situation
<input checked="" type="radio"/> Find Chip ID	Use this option to add RouterNodes without an Ethernet interface (see <i>Transmission paths</i> [▶ 13]). Routers without an Ethernet interface do not have an IP address and can therefore only be found and added using the chip ID.
<input checked="" type="radio"/> Add: IP or USB router	Use this option if you specifically want to add a RouterNode with Ethernet interface to your network. You must know the IP address (static / reserved) or the host name (DHCP). These can also be located in a different subnet.

### Find IP or USB router

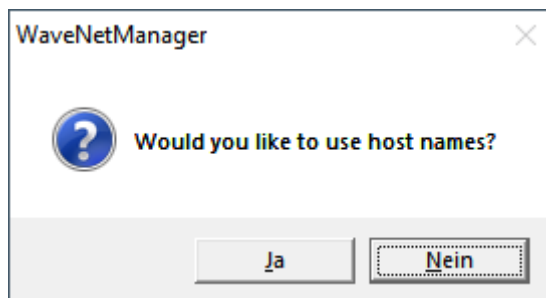
- ✓ RouterNode connected to the network.
  - ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
1. Right-click on the WaveNet\_XX\_X entry.
    - ↳ The window "Administration" opens.
  2. Select the option  Find IP or USB router.



3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The "Procedure started" window opens temporarily.



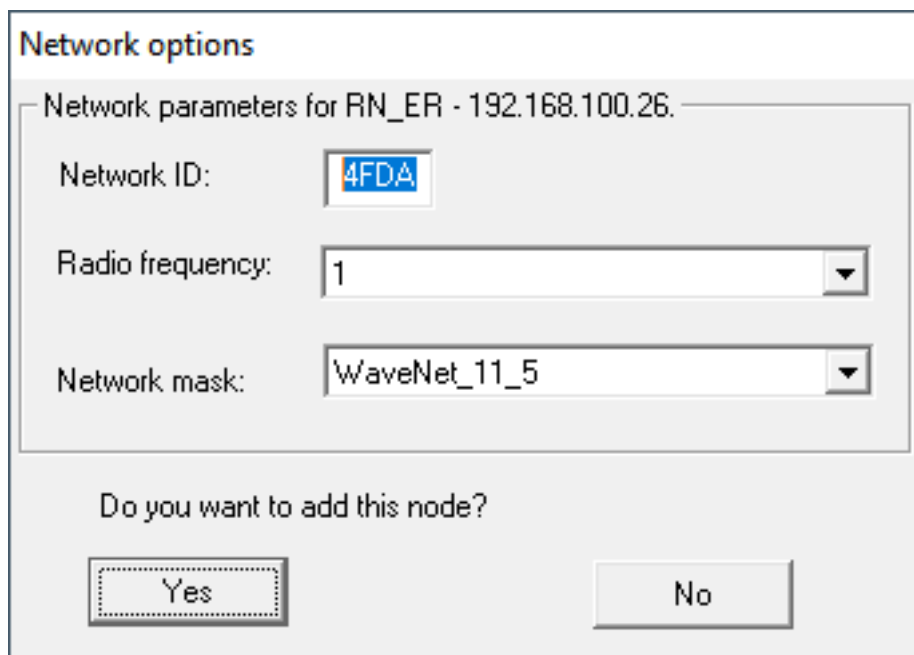
↳ The window "Use host names?" opens.



4. If the router is connected via DHCP and you have a working name resolution in the network, confirm with the button **Yes** to use the host name. If you have connected the router using a static IP address, click the **No**.

↳ The window "Use host names?" closes.

↳ The window "Network options" opens.



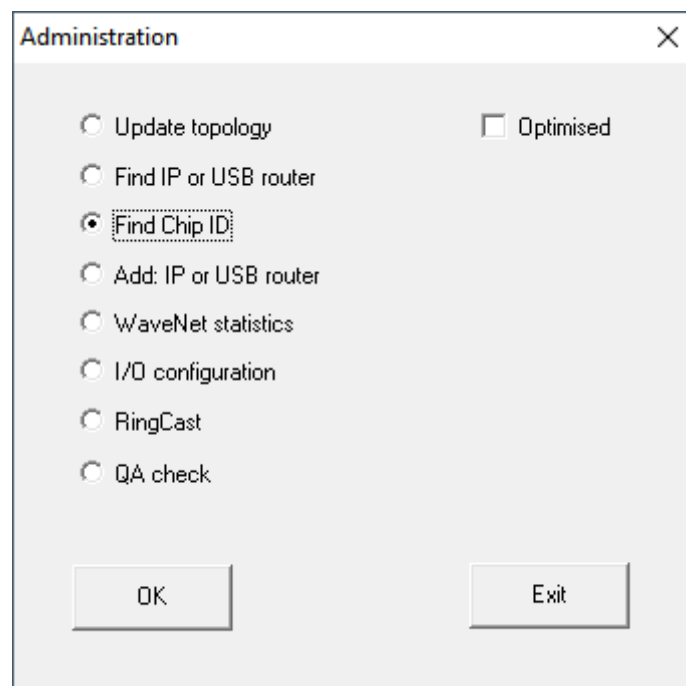
**NOTE****Setting network parameters**

If you set up a new WaveNet and add your first RouterNode, you can set network options here (see *Addressing* [▶ 42] and *Radio channel* [▶ 43]). After setting up your WaveNet, you can no longer change these settings without resetting your WaveNet devices.

5. Click on the **Yes** button.
  - ↳ The "Network options" window closes.
6. Click on the button **Save**.
  - ↳ RouterNode is added and listed. All other unconfigured RouterNodes are automatically added.

**Find Chip ID**

- ✓ RouterNode connected to the network.
  - ✓ Chip ID of the RouterNode still to be configured known.
  - ✓ WaveNet Manager is open.
1. Right click the entry WaveNet\_XX\_X.
    - ↳ The window "Administration" opens.
  2. Select the option  Find Chip ID.



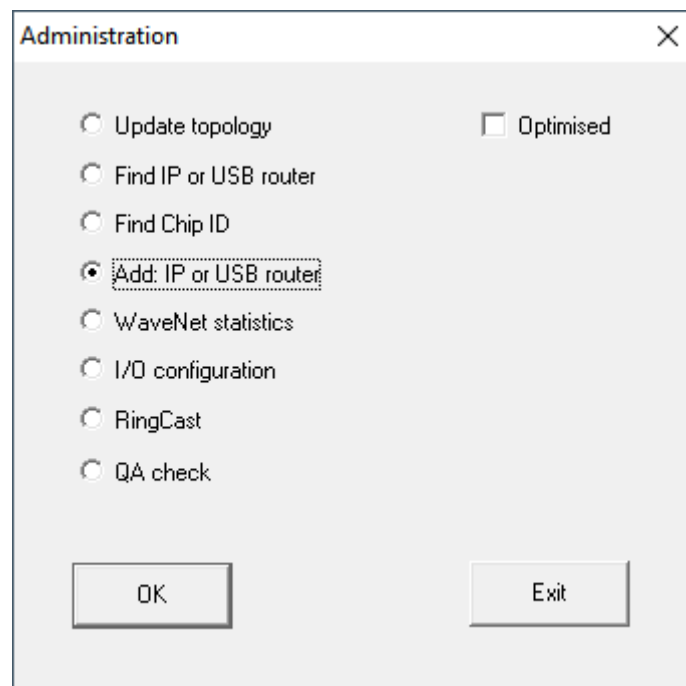
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Search for node" opens.
4. Enter the chip ID.



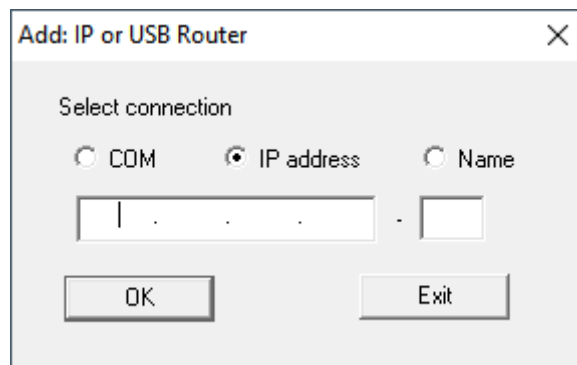
5. Click on the button **Start**.
  - ↳ The window "Search for node" closes.
  - ↳ The window "Procedure started" opens temporarily.
6. Add the RouterNode.
  - ↳ RouterNode is listed.
7. Click on the button **Save**.
  - ↳ RouterNode is added.

#### Add: IP or USB router

- ✓ RouterNode is connected to the network.
  - ✓ The IP of the RouterNode is known (see *Determining and setting the IP address* [▶ 49]).
  - ✓ WaveNet-Manager opened.
1. Right click the entry WaveNet\_XX\_X.
    - ↳ The window "Administration" opens.
  2. Select the option  Add: IP or USB router.



3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Add: IP or USB Router" opens.



4. Select the option  IP address.
5. Enter the IP address of your RouterNode.

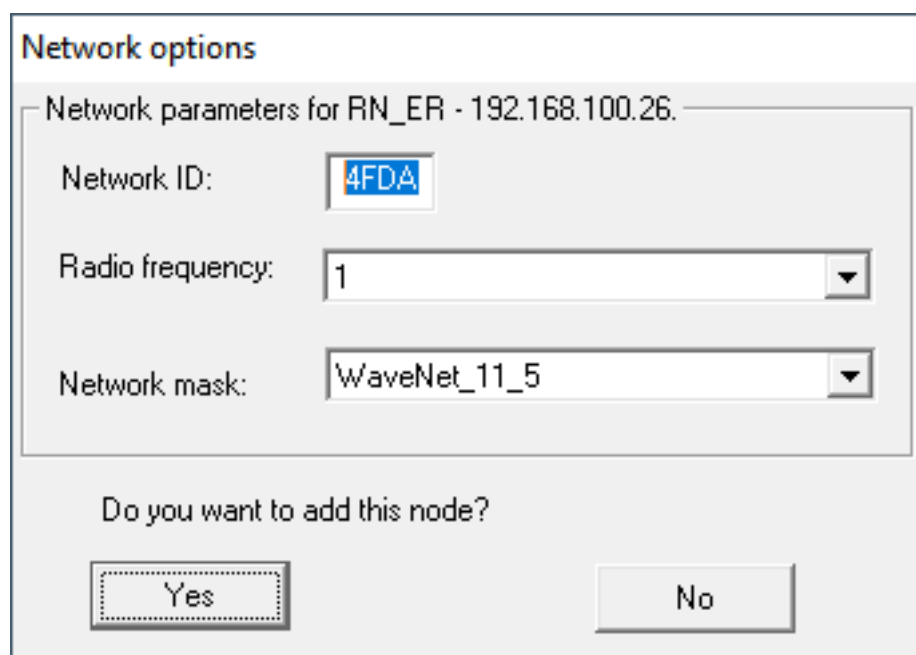


## NOTE

### IP range

You can specify a range of IP addresses. For example, if you use 192.168.100.XX to 192.168.100.YY, enter the first IP address of your range (192.169.100.XX) and the extension of the last IP address (YY). The WaveNet Manager will then add any router nodes it finds in this range.

6. Click on the **OK** button.
  - ↳ The window "Add: IP or USB Router" closes.
  - ↳ The window "Network options" opens.



**NOTE****Setting network parameters**

If you set up a new WaveNet and add your first RouterNode, you can set network options here (see [Addressing \[▶ 42\]](#) and [Radio channel \[▶ 43\]](#)). After setting up your WaveNet, you can no longer change these settings without resetting your WaveNet devices.

7. Click on the **Yes** button.
  - ↳ The "Network options" window closes.
8. Click on the button **Save**.
  - ↳ RouterNode is added and listed.

#### 6.4.3.4 Adding Lock Nodes to WaveNet

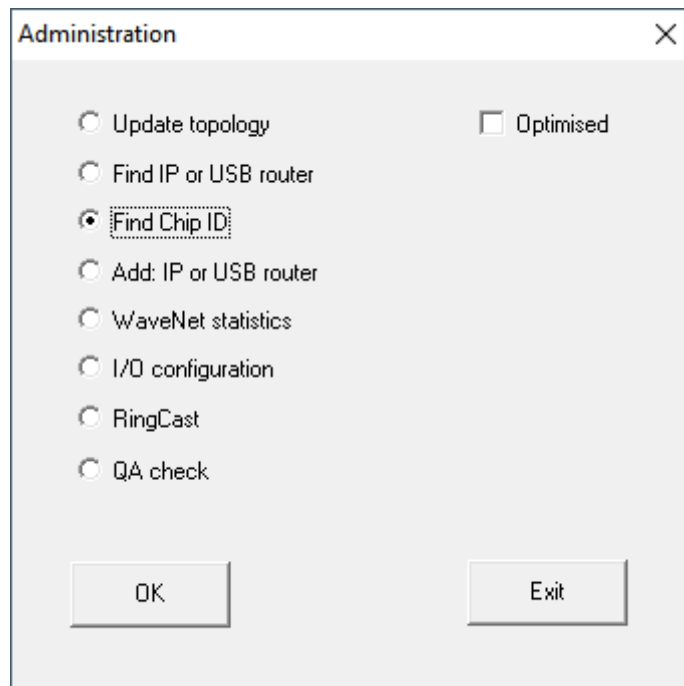
If you want to use LockNodes in your WaveNet, you must first add the LockNodes in the WaveNet Manager. LockNodes do not have an IP address and can therefore only be found using the Chip ID. You can find the Chip ID on the LockNode itself, on the supplied sticker or on its packaging.RouterNode connected to the network.

You can later manually assign the LockNode to another RouterNode (see [Assigning LockNodes to another RouterNode \[▶ 153\]](#)).

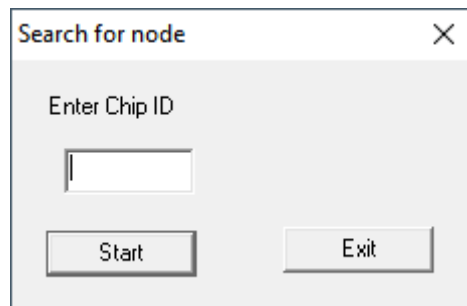
**Single LockNode: Find Chip ID**

- ✓ RouterNode is connected to the network.
  - ✓ WaveNet Manager opened via LSM (see [Best Practice: From the LSM software \[▶ 37\]](#))
  - ✓ LockNode installed or supplied with power.
  - ✓ LockNode within range of the WaveNet.
  - ✓ The chip ID of the LockNode is known.
1. Right click the entry WaveNet\_XX\_X.
    - ↳ The window "Administration" opens.

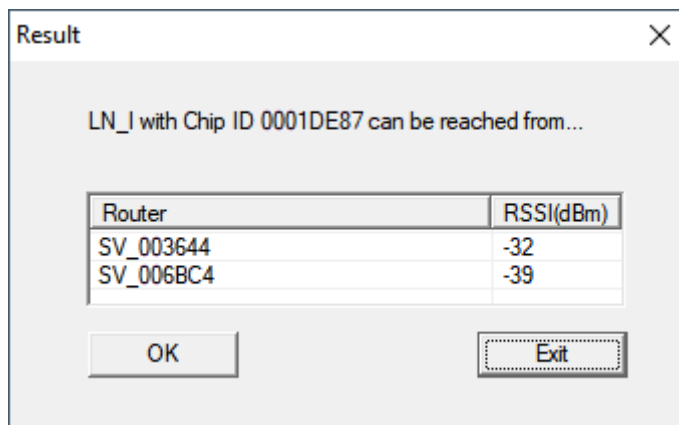
2. Select the option  Find Chip ID.



3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Search for node" opens.



4. Enter the chip ID.
5. Click on the button **Start**.
  - ↳ The "Search for node" window closes.
  - ↳ WaveNet Manager searches for reachable chip IDs.
  - ↳ The window "Result" opens. You will see a list of router nodes that reach the LockNode.



6. Select the RouterNode with which you want to spark the LockNode.



### NOTE

#### Observe the signal strength

The signal strength in the WaveNet Manager should be between 0 dBm and -70 dBm.

If the signal strength is between -75 dBm and -90 dBm, the connection and communication between the devices may become slow or interrupted, and there will also be higher power consumption.

1. Select the RouterNode with the best signal strength.
2. If no RouterNode has sufficient signal strength, position a RouterNode closer to the LockNode (see *Improving signal quality* [▶ 152]).

7. Click on the **OK** button.
  - ↳ The window "Result" closes.
  - ↳ The "Procedure started" window opens temporarily.
8. Click on the button **Save**.
  - ↳ LockNode is imported and linked to the selected RouterNode.

LockNodes are displayed in the WaveNet topology below the RouterNode to which they are assigned.

```

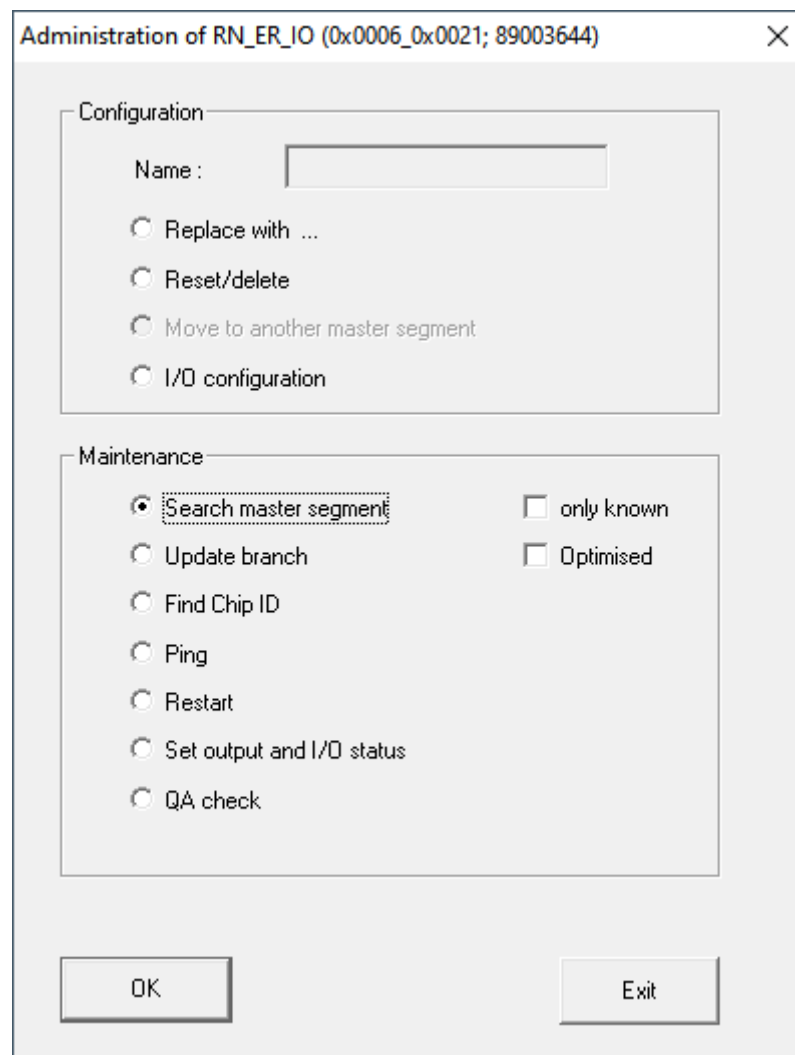
WaveNet_11_5
├── RN_ER_ID (0x0006_0x0021; 89003644) | 192.168.100.26
│   └── LN_I (0x0026; 0001DE87) -45dBm

```

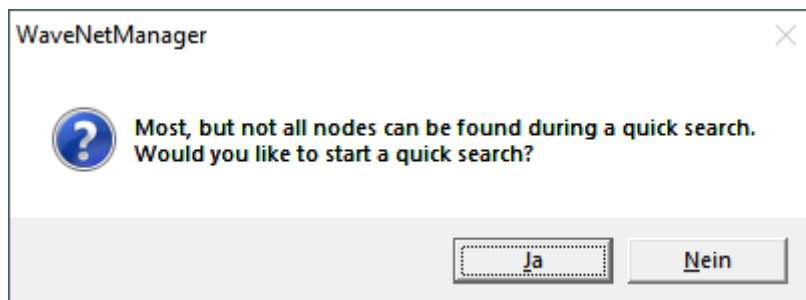
#### Multiple LockNodes: Search by RouterNode

Alternatively, you can also use a RouterNode to search for accessible LockNodes and then select the LockNodes you want to assign to this RouterNode from a list of LockNodes.

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes and LockNodes connected to power.
  - ✓ RouterNodes connected to WaveNet (for testing, see *Testing accessibility (WaveNet)* [▶ 183]).
1. Right-click on the RouterNode you want to use to search for new LockNodes.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Search master segment.
3. Make sure that the  only known is disabled.
4. Click on the  button.
  - ↳ The window "Administration" closes.
  - ↳ The window "WaveNetManager" opens.



5. Click button **Yes** (quick search) or **No** (regular search).

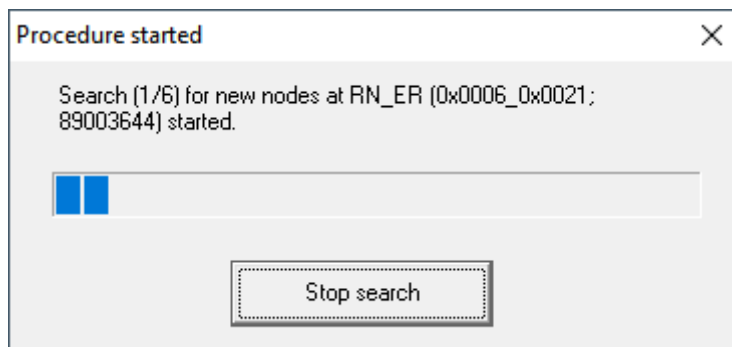


## NOTE

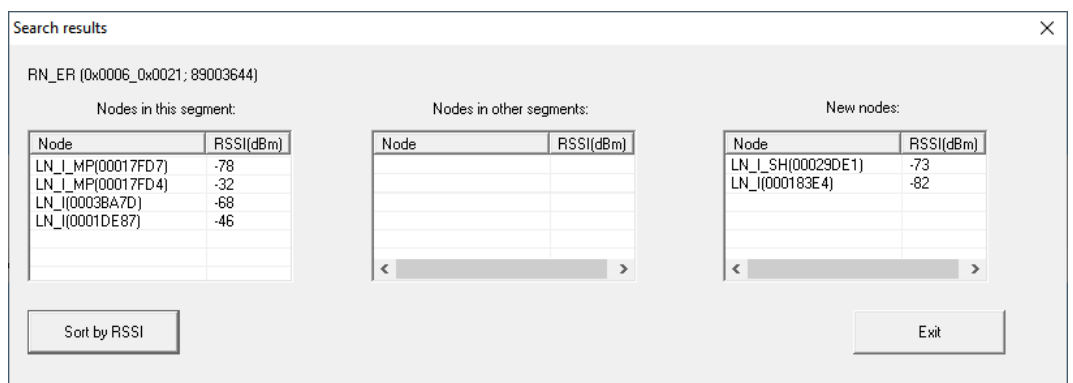
### Quick search

If you perform a fast search, the RouterNode will only send a single broadcast. If you perform a regular sweep, the RouterNode sends a total of six broadcasts. The quick search is completed faster, but the normal scan is more thorough and finds LockNodes that were not reached during a quick search.

- ↳ The "WaveNetManager" window closes.
- ↳ The "Procedure started" window opens temporarily.



- ↳ The window "Search results" opens.



You will see an overview table of the LockNodes found by the RouterNode during the search. This table has three columns:

Nodes in this segment	Nodes from other segments	New nodes
These LockNodes are located in the WaveNet topology and are already assigned to the RouterNode.	These LockNodes are located in the WaveNet topology, but are assigned to a different RouterNode.	These RouterNodes are un-configured and are not located in any topology.

Each column contains two sub-columns:

Node	RSSI
Name of the LockNode	Signal strength of the connection of the LockNode to the searching RouterNode

### Unit of signal strength

The WaveNet Manager displays the signal strength as an RSSI value (Received Signal Strength) in dBm. This value is:

- Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.
- Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm (i.e. the smaller the amount), the better the reception.

1. Select the LockNodes of the right column (New Nodes) that you want to assign to the RouterNode.
2. Drag and drop the LockNodes to the left column (Nodes in this segment) to assign them to the current RouterNode (the one you used to search).
  - ↳ LockNodes are assigned to the current RouterNode.



### NOTE

#### Assignment duration

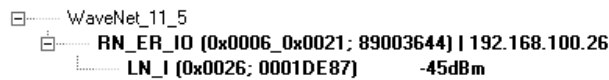
When you reassign LockNodes, the WaveNet Manager communicates with the LockNodes to transfer the configuration and check the LockNode. This check takes a few seconds

3. If necessary, confirm the IO configuration of the LockNode by clicking the **OK** (you can change the IO configuration at any time, see *I/O configuration and protection functions* [▶ 69]).

↳ LockNode is imported and linked to the selected RouterNode.

LockNodes are displayed in the WaveNet topology below the RouterNode to which they are assigned.



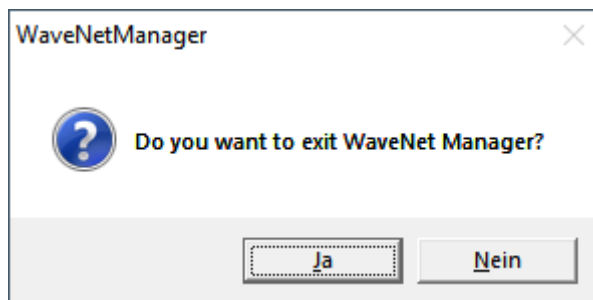


### 6.4.3.5 LSM import

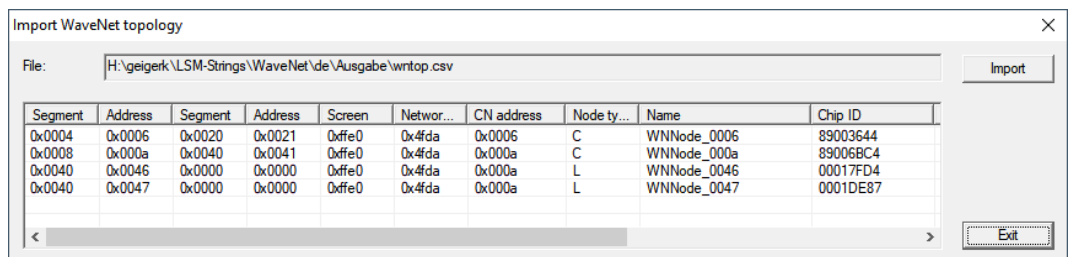
You must import the created WaveNet topology into the LSM so that you can use the WaveNet topology there.

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
- ✓ Free communication node available in the LSM (or local connection for operation without communication node).
- ✓ WaveNet topology created and saved (see *Add RouterNode to WaveNet* [▶ 53] and *Adding Lock Nodes to WaveNet* [▶ 59]).

1. Click on the **Exit** button.
  - ↳ The window "WaveNetManager" opens.



2. Click on the **Yes** button.
  - ↳ The "WaveNetManager" window closes.
  - ↳ The window "Import WaveNet topology" opens. You see a list of the devices to be imported.



3. Click on the button **Import**.
  - ↳ The window "Assignment" opens.

**Zuordnung**

Central Node: 192.168.100.26

Adresse: 0x0006

Kommunikationsknoten: GUINode\_1

nicht weiter fragen

OK Abbrechen

4. In the drop-down menu ▼ **Communication nodes** select the communication node in the LSM that you want to use for the RouterNode (for creation, see *Finding and adding devices* [▶ 48] or LSM manual).
5. Click on the **OK** button.
  - ↳ The "Assignment" window closes.
  - ↳ The window "Result" opens.

**Result**

Net IDs  
In the database: 0x4fda In the WaveNet topology file: 0x4fda

Central Nodes

Address	Name	State
0x0006	SV_003644	already exists
0x000a	SV_006BC4	already exists

Error: 0 Present: 2 Are being added: 0 **Select all**

Segments

Address	State
0x0020	is being inserted
0x0040	is being inserted

Error: 0 Present: 0 Are being added: 2 **Select all**

Node

Segm...	Address	Segm...	Address	Screen	Netw...	CN a...	No...	Name	State
0x0020	0x0026	0x0000	0x0000	0xffe0	0x4fda	0x0006	L	WNNode_0026	can be inserted
0x0040	0x0046	0x0000	0x0000	0xffe0	0x4fda	0x000a	L	WNNode_0046	can be inserted
0x0040	0x0048	0x0000	0x0000	0xffe0	0x4fda	0x000a	L	WNNode_0048	can be inserted

Error: 0 Present: 0 Are being added: 3

OK Cancel

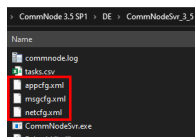
6. Click on the **OK** button.
  - ↳ The "Result" window closes.
  - ↳ The window "LockSysMgr" opens.



7. Click on the **OK** button.
  - ↳ The "LockSysMgr" window closes.
  - ↳ WaveNet Manager closes.
- ↳ WaveNet topology is imported and RouterNode is listed in the list of ports for the communication node.

Transfer to communication nodes

- ✓ LSM open.
1. Via | Network | select the entry **Communication nodes**.
2. Use the buttons **◀** or **▶** to select the communication node you just used.
3. Click the button **Config files**.
  - ↳ The window "Search Folder" opens.
4. Ensure that the installation directory of the CommNode server is selected.
5. Click on the button **OK**.
  - ↳ The "Search Folder" window closes.
6. Click on the button **No** to avoid saving to a node-specific folder.
  - ↳ XML configuration files are saved.

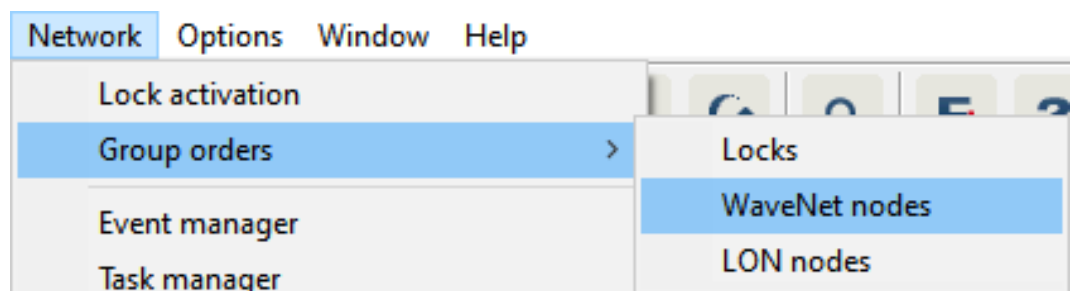


7. Click on the button **Transmit**.
  - ↳ The window "LockSysMgr" opens.
8. Click on the **OK** button.
  - ↳ The "LockSysMgr" window closes.
- ↳ Data is transferred to the communication node.

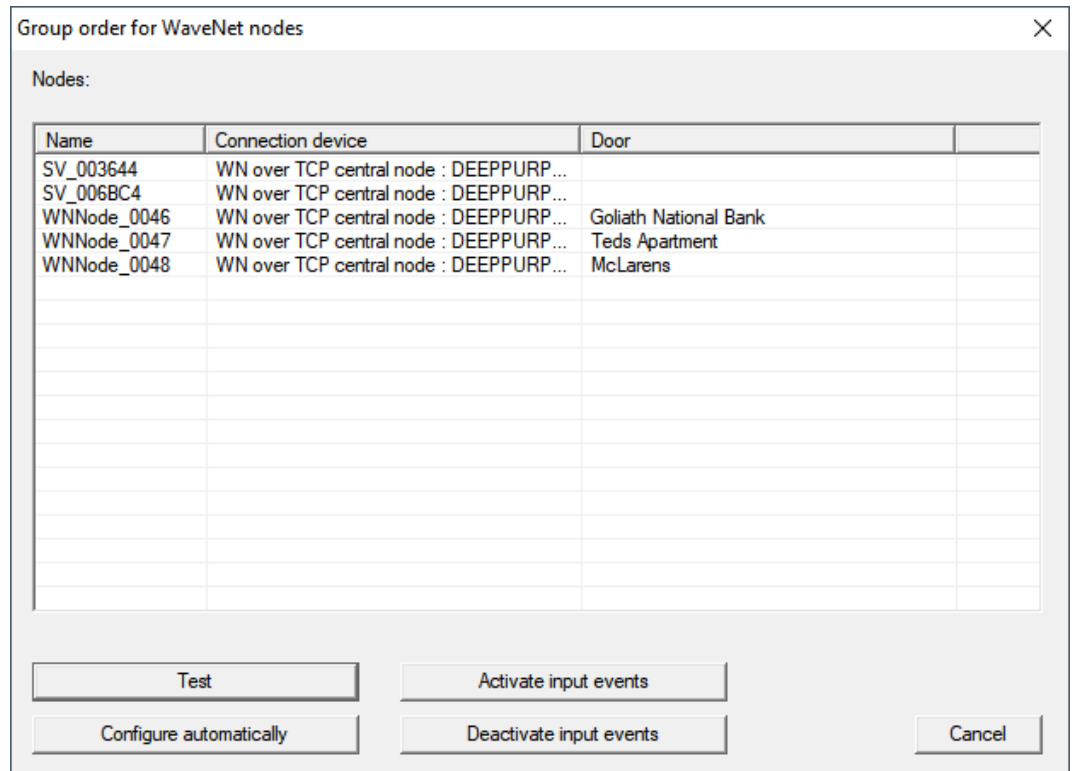
## 6.4.3.6 Assigning LockNodes to the locking devices

- ✓ LSM is open.
- ✓ Locks to be networked have already been initially programmed (with local programming device).
- ✓ WaveNet created (see *Add RouterNode to WaveNet* [▶ 53] and *Adding Lock Nodes to WaveNet* [▶ 59]).
- ✓ WaveNet topology imported (see *LSM import* [▶ 65]). You will see a list of WaveNet-relevant components.

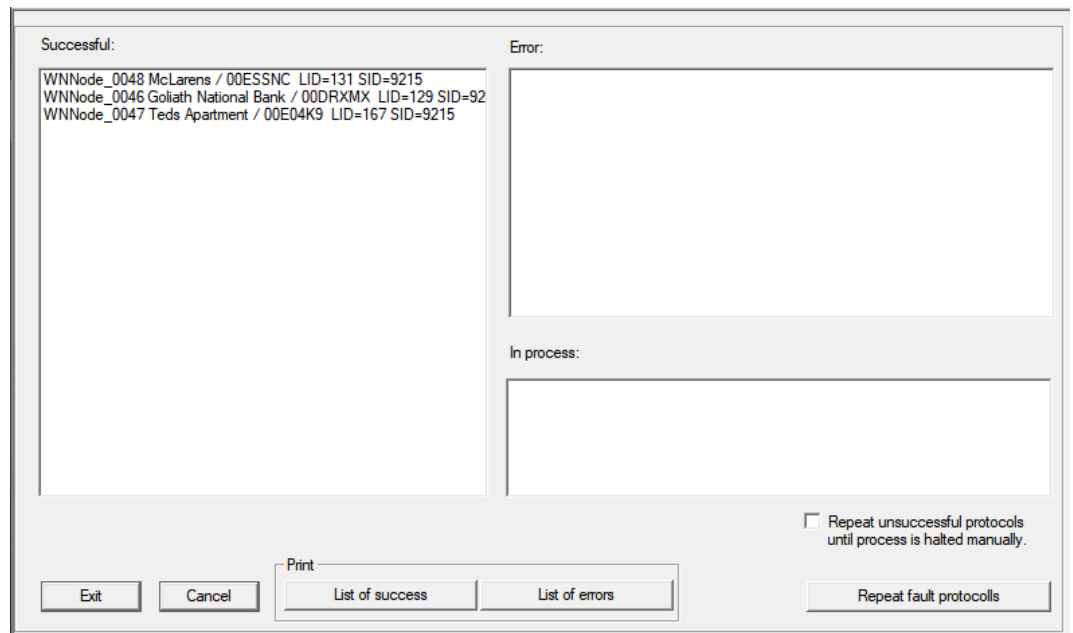
1. Open the assignment via | Network | - **Group orders** - **WaveNet nodes**.



- ↳ The window "Group order for WaveNet nodes" opens.



2. Select the LockNodes you want to assign.
  3. Click on the button **Configure automatically**.
    - ↳ The "Group order for WaveNet nodes" window closes.
    - ↳ LSM assigns LockNodes.
- ↳ LockNodes are assigned to locks.



You can address your locks with LockNodes via your WaveNet after they have been successfully assigned.

#### 6.4.4 I/O configuration and protection functions

You can use the protective functions to deactivate, activate or open locking devices remotely via radio (868 MHz). To do this, you define the IO configuration in the WaveNet Manager:

- When an event is triggered (by an identification medium or an input, see *Input (relay contact)* [[▶ 88](#)]) and
- how to react to this event (triggering of a protection function)

Protective functions are basically independent of LSM or its services. If you use protective functions, you can increase the level of security with your WaveNet – in conjunction with the security measures that are required in public buildings anyway.



**WARNING**

**Personal injury or damage to property due to non-redundant safety concept**

The protective functions of your WaveNet system are only one element of an entire safety concept. They are not suitable as the only protection against hazards such as fire, burglary or similar.

1. Make use of redundant systems to protect against your individual risks (burglar alarms, fire alarms and the like).
2. Have a technical risk manager (Certified Security Manager or the like) create and evaluate a security concept.
3. Please pay particular attention to relevant regulations on escape and rescue routes.




**NOTE**

**Proprietary WaveNet without legal requirements**

WaveNet is a SimonsVoss in-house development, designed to further enhance the security of your building with the protective functions offered in addition to existing security concepts. There are currently no known legal requirements for these protective functions.

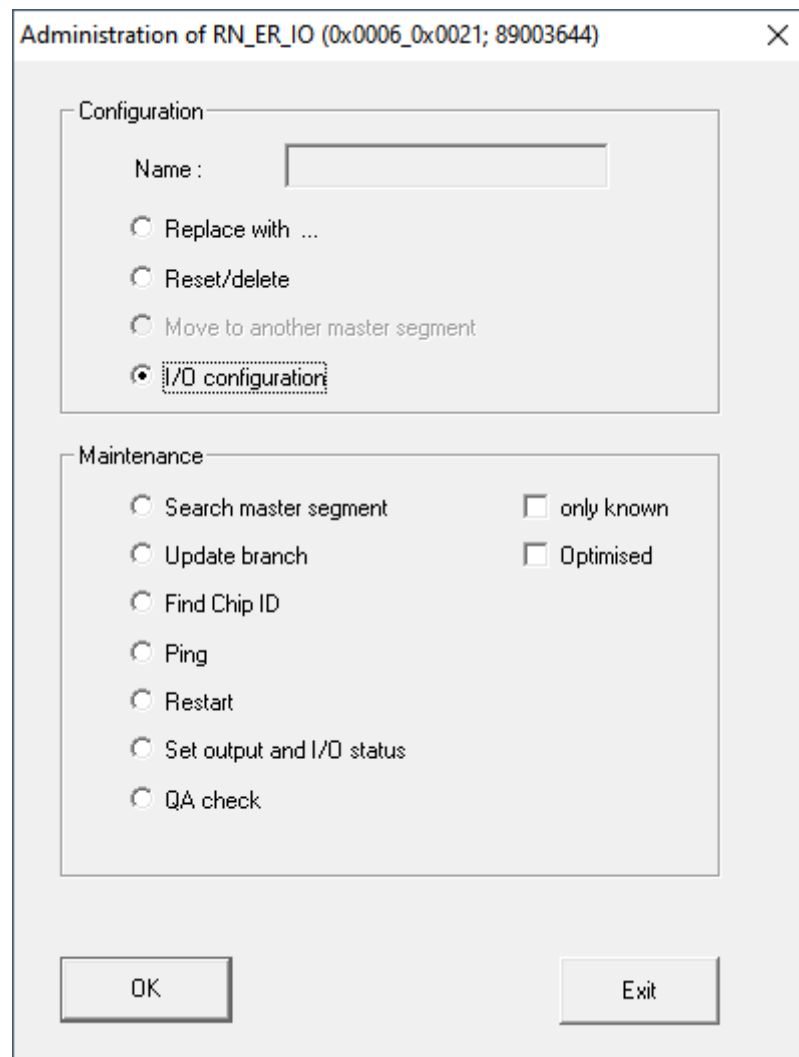
You can set the inputs and outputs of your RouterNodes to suit your needs:

Outputs	Inputs (digital)	Input (analogue)
Respond to identification media or acknowledge completed reactions that were triggered by the digital inputs. Switch the outputs depending on detected identification media (see <i>RouterNode: Digital output</i> [▶ 76]).	Respond to changes in the status of the digital inputs. Trigger a reaction at the connected locks (see <i>RouterNode: Digital input</i> [▶ 79]).	Respond to status changes at the analog input. Trigger an event in the LSM (see <i>RouterNode: Analogue input</i> [▶ 84]).

The  Set output and I/O status option shows you the current status and the result of the last responses (see *IO Status and LockNode responsiveness* [▶ 188]).

**Single RouterNode**

1. Right-click on the entry of the router node whose I/O configuration you want to change.
  - ↳ The window "Administration" opens.



2. In the area "Configuration" select the option  I/O configuration.
3. Click on the  button.
  - ↳ The "Administration" window closes.
  - ↳ The window "I/O configuration" opens.

I/O configuration for RN\_ER\_IO (0x0006\_0x0021; 89003644)

Digital output configuration

I/O application : Standard

1 2 3

Output : Output Output Output

Select LN Report events to management system : None

Digital input configuration

1 2 3

Input : Input Input Input

Delay [s] : 0 0 0

Report events to management system :  Yes  Yes  Yes

Select LN : For all inputs For Input 1 For Input 2 For Input 3

Protocol generation : Password hidden

G1 Locking system password :

G2 Locking system password :

Analogue input configuration

Event handling : No event

Threshold [mV] : Low : 1050 High : 1250

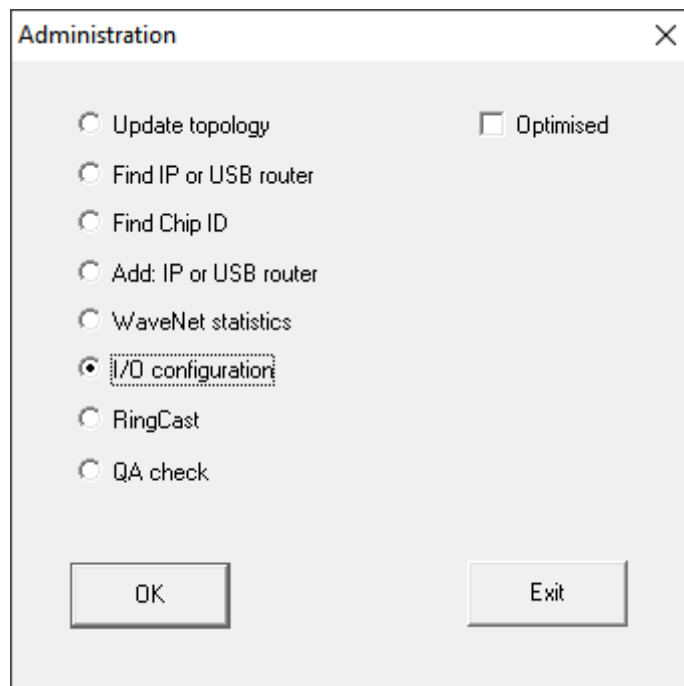
Sampling interval [s] : 600

OK Cancel

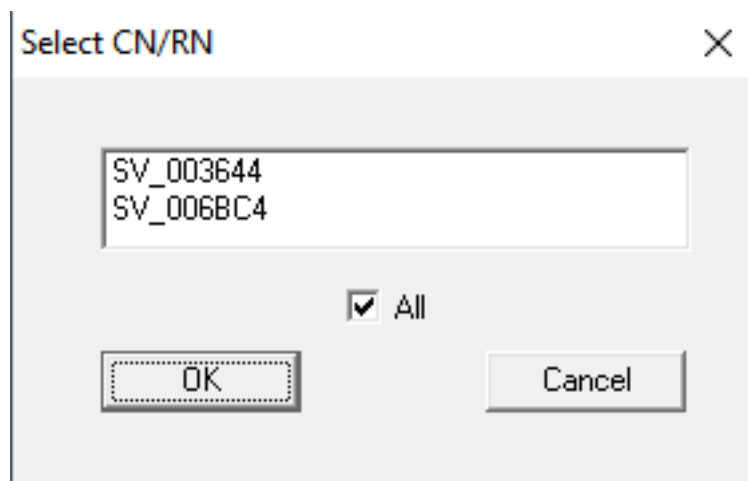
### Multiple RouterNodes

1. Right click the entry WaveNet\_XX\_X.
  - ↳ The window "Administration" opens.





2. Select  I/O configuration.
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Select CN/RN" opens.



4. Either select all desired RouterNodes or activate the checkbox  all.
5. Click on the **OK** button.
  - ↳ The "Select CN/RN" window closes.
  - ↳ The window "I/O configuration" opens.

I/O configuration for RN\_ER\_IO (0x0006\_0x0021; 89003644)

Digital output configuration

I/O application : Standard

	1	2	3
Output :	Output	Output	Output
Report events to management system :	None		

Select LN

Digital input configuration

	1	2	3
Input :	Input	Input	Input
Delay [s] :	0	0	0
Report events to management system :	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes

Select LN : For all inputs For Input 1 For Input 2 For Input 3

Protocol generation : Password hidden

G1 Locking system password :

G2 Locking system password :

Analogue input configuration

Event handling : No event

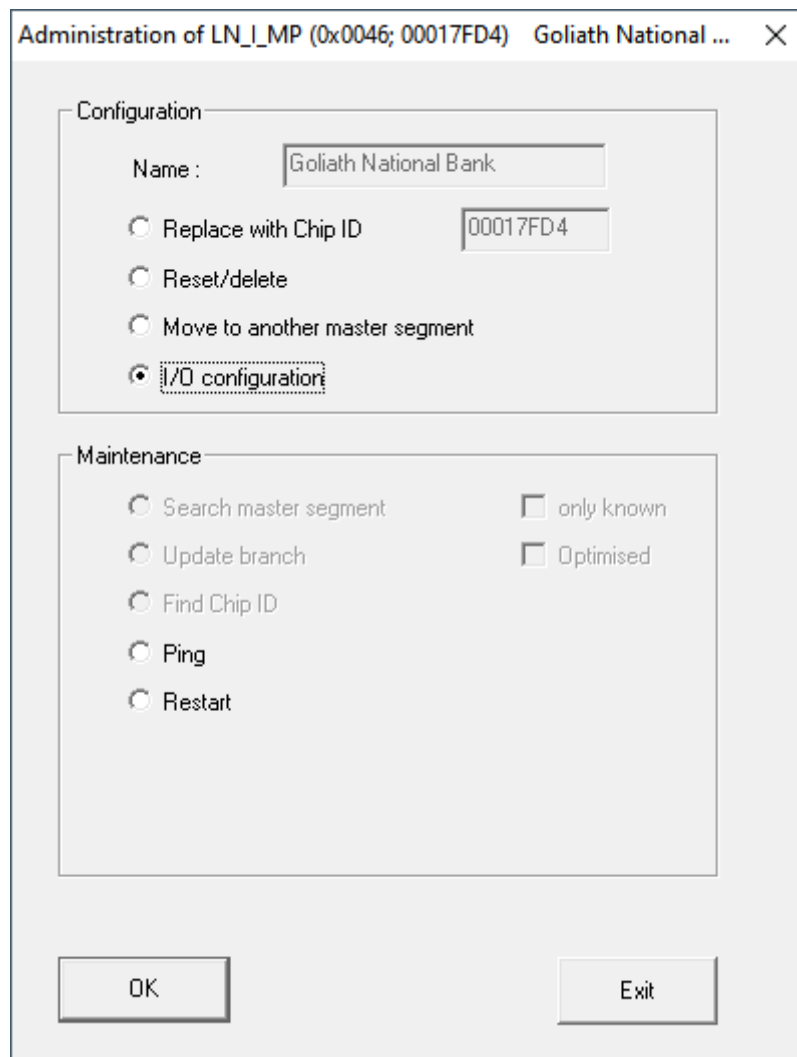
Threshold [mV] : Low : 1050 High : 1250

Sampling interval [s] : 600

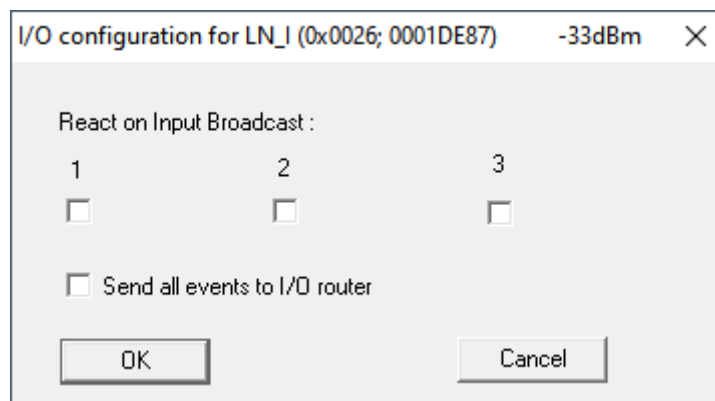
OK Cancel

### Single LockNode

1. Click with the right mouse button on the entry of the LockNode whose I/O configuration you want to change.
  - ↳ The window "Administration" opens.

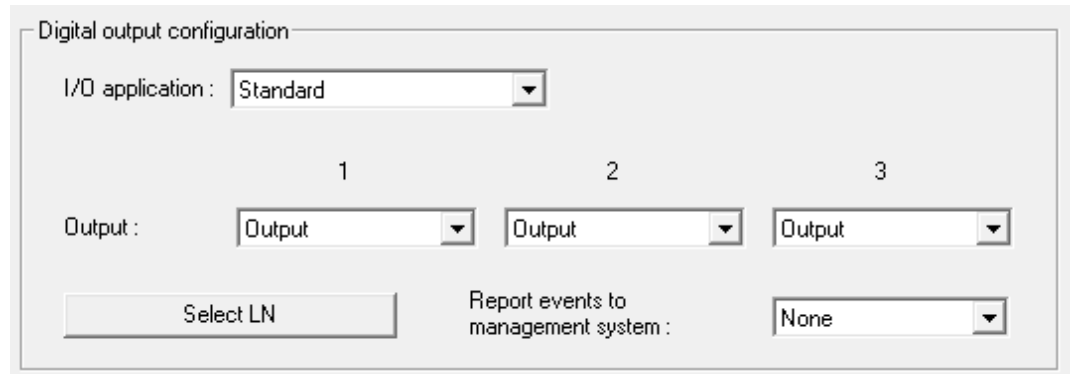


2. Select  I/O configuration.
3. Click on the  button.
  - ↳ The "Administration" window closes.
  - ↳ The window "I/O configuration" opens.



6.4.4.1 Description of the options

RouterNode: Digital output



You can select the following entries from the dropdown list ▼ I/O application:

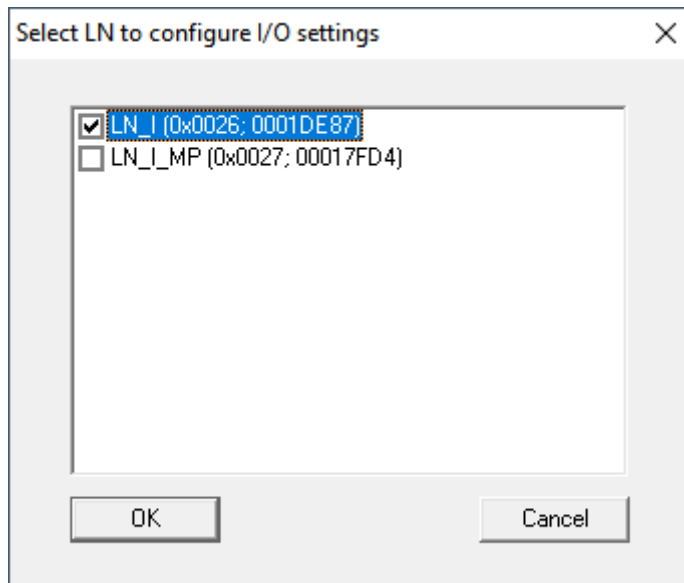
"Standard"	Standard entry:
------------	-----------------

In the dropdown list ▼ Output, you can set when the output in the RouterNode triggers:

"Output"	Standard entry: The RouterNode does not switch the output. You can switch the output manually (see <i>IO Status and Lock-Node responsiveness [▶ 188]</i> ).
"Authorised"	The output switches at one or more freely selectable locking devices with a LockNode assigned to the RouterNode for about one second in case of an authorised identification medium. The identification medium must be present in the locking system.
"Unauthorised attempt"	If an unauthorised identification medium is present on one or more freely selectable locking devices with a LockNode assigned to the RouterNode, the output switches for about one second. The identification medium must be present in the locking system.
"All LN events"	The output switches at any identification medium at one or more freely selectable locks with a LockNode assigned to the RouterNode for about one second. The identification medium must be present in the locking system.

"Input receipt short" (at all LockNodes)	The output switches when the response (see <i>RouterNode: Digital input [▶ 79]</i> ) to a signal at the corresponding input on all LockNodes has been performed (=input event) for about one second.
"Input receipt static" (at all LockNodes)	The output switches when the response (see <i>RouterNode: Digital input [▶ 79]</i> ) to a signal at the corresponding input has been performed on all LockNodes. As long as the input event is present after the response is completed, the output remains switched.
Output 1	<p>O1</p> <p>Relay output, consisting of O1.NC, O1.NO and O1.COM</p> <ul style="list-style-type: none"> <li>■ NC=Normally connected, is connected to COM in idle state.</li> <li>■ NO=Normally open, is not connected to COM in idle state.</li> </ul> <p>When the output is switched, the relay picks up and changes from the idle state to the energized state.</p>
Output 2	<p>O2</p> <p>Digital output (Open Drain), max. 12 V<sub>DC</sub>, max. 100 mA (resistive load)</p> <p>When the output is switched, the output is connected to the ground potential.</p>
Output 3	<p>O3</p> <p>Digital output (Open Drain), max. 12 V<sub>DC</sub>, max. 100 mA (resistive load)</p> <p>When the output is switched, the output is connected to the ground potential.</p>

With the button **Select LN** you can open the window "Select LN to configure I/O settings". Select the LockNodes in locking devices here. Authorised access or unauthorised access attempts at these locks (LockNodes) are forwarded to the LSM.



In LSM, you can react to the forwarded event using the Event manager.

In the ▼ **Report events to management system** dropdown list (WNM IO Config), you can set which events at the LockNodes selected previously are forwarded to LSM:

"None"	Default entry. There is no event and no forwarding.
"Authorised"	Authorised access attempts at the marked locks (LockNodes) are forwarded to the LSM (= event that is forwarded to the LSM).
"Unauthorised attempt"	Unauthorised access attempts at the marked locks (LockNodes) are forwarded to the LSM (=event that is forwarded to the LSM).
"All LN events"	Authorised accesses and unauthorised access attempts at the marked locks (LockNodes) are forwarded to the LSM (=event that is forwarded to the LSM).

Alternatively, you can also set directly on the LockNodes whether the LockNodes forward events to the RouterNode (see [LockNode \[▶ 86\]](#)).

Select the event here that triggers forwarding to LSM. If the event specified here ("Authorised", "Unauthorised attempt" or "All LN events") occurs at the locking devices (LockNodes) that you have previously defined (**Select LN**), the event is forwarded to the LSM.

**NOTE****Same event for forwarding**

You cannot select LockNodes (and thus the lock in which the LockNode is built in) and thus exclude them from event forwarding. If you use event forwarding, the same event applies to all LockNodes selected (in **Select LN**).

For example, you cannot only forward authorised accesses for one LockNode and unauthorised access attempts for another.

**RouterNode: Digital input**

Digital input configuration

	1	2	3
Input :	<input type="text" value="Input"/>	<input type="text" value="Input"/>	<input type="text" value="Input"/>
Delay [s] :	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Report events to management system :	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Select LN :	<input type="button" value="For all inputs"/>	<input type="button" value="For Input 1"/>	<input type="button" value="For Input 2"/>
Protocol generation :	<input type="text" value="Password hidden"/>		
G1 Locking system password :	<input type="text"/>		
G2 Locking system password :	<input type="text"/>		

In the dropdown list ▼ **Input**, you can set how the LockNodes of the RouterNode should react to a signal applied to the respective RouterNode input. (= applied voltage is higher than the fixed reference voltage).

**Comparison voltages (RN and RN2)**

$<0,9 V_{DC}$	LOW (no signal)
$>2.1 V_{DC}$	HIGH (signal)

"Input"	Standard entry. The RouterNode does not respond to an applied signal. However, you can forward the signal changes to LSM.
---------	---

"Block lock"	<p>If a signal is present at the input (input event, level change low to high), the RouterNode sends a broadcast to all LockNodes. You can set whether the LockNodes should respond to the broadcast (see <a href="#">LockNode [▶ 86]</a>). The LockNodes then deactivate the locking devices in which they are installed for the duration of the input event.</p> <p>They then no longer react to authorised identification media, no access is possible. When the signal is no longer present (= no input event, level change from high to low), the locks are reactivated.</p> <p>If you apply a signal to the input by an intrusion alarm system during arming, you can thus deactivate the locks of the outer shell for the duration of the arming of the alarm system (and prevent the unintentional triggering of the alarm system). However, you can also freely choose which locks you want to deactivate.</p> <p>With the outputs (see <a href="#">RouterNode: Digital output [▶ 76]</a>) you can send an acknowledgement back to the intrusion alarm system after successful deactivation.</p> <p>Using this function is not VdS-compliant.</p>
"Amok function"	<p>Similar to the block lock function: If a signal is applied to the input (level change Low to High), the RouterNode sends a broadcast to all LockNodes. You can set whether the LockNodes should respond to the broadcast (see <a href="#">LockNode [▶ 86]</a>). If there is a signal at the input, the RouterNode sends a broadcast to all LockNodes which should react to the input.</p> <p>They then reject all identification media (even normally authorised ones); one-time access is only possible with special identification media (red level).</p> <p>They then reject all identification media (even normally authorised ones), no access is possible. You must explicitly reactivate the locks with an activation command:</p> <ul style="list-style-type: none"> <li>■ Use WaveNet (response "Activation")</li> <li>■ LSM</li> <li>■ Activation transponder or card</li> </ul> <p>If you connect an emergency button to an input (see <a href="#">Input (button) [▶ 87]</a>) and connect it to the amok function, then you can use the emergency button to block all locks that have been reached and prevent people from entering (or in the case of a freely rotating cylinder, from leaving) rooms until they are explicitly reactivated.</p>



"Emergency release"	<p>Opposite to the gunman attack function: If a signal is applied to the input (level change Low to High), the RouterNode sends a broadcast to all LockNodes. You can set whether the LockNodes should respond to the broadcast (see <a href="#">LockNode [▶ 86]</a>). This broadcast permanently couples all locks in which the LockNodes are installed.</p> <p>The locks remain coupled even after the end of the input event. You must end the emergency release of the locks with a remote opening command (the locks uncouple immediately after the remote opening command has been received):</p> <ul style="list-style-type: none"> <li>■ Use WaveNet (response "Remote opening")</li> <li>■ LSM</li> </ul> <p>If you apply a signal to the input through a fire alarm system (see <a href="#">Application examples [▶ 87]</a>), then you can open all locking devices to enable emergency services to access them.</p>
"Remote opening"	<p>If a signal is applied to the input (level change Low to High), the RouterNode sends a broadcast to all LockNodes. You can set whether the LockNodes should respond to the broadcast (see <a href="#">LockNode [▶ 86]</a>). This broadcast carries out a remote opening.</p> <p>The locking device couples for the pulse duration set in the LSM (pulse opening). This also applies to locking devices in flip-flop operation.</p>
"Activation"	<p>If a signal is applied to the input (level change Low to High), the RouterNode sends a broadcast to all LockNodes. You can set whether the LockNodes should respond to the broadcast (see <a href="#">LockNode [▶ 86]</a>). This broadcast activates the locks in which the LockNodes are installed.</p> <p>You can then reuse locks that were previously deactivated.</p> <p>This response only works with I/O RouterNodes of type RN2 from firmware version 40.8 onwards together with WaveNet Manager version 2.6.6 or later.</p>

**NOTE****Permanent emergency opening**

A fire can damage the input cable or other parts. This would cause the locking devices to close again even though there is a fire. Persons could be locked up in the fire zone and rescue units could be prevented from entering.

Therefore, all locking devices stay in the emergency opening state (and thus passable) until an explicit remote opening command closes the locking devices again.

If you define a response to an event, you must make additional specifications.

1. Select the LockNodes that are to react.
2. Specify the protocol generation (G1, G1+G2, G2) as entered in the locking system settings.
3. Specify the locking system password.

A signal applied to the input is an input event and can also be switched by the built-in relay, see ▼ **Output** in *RouterNode: Digital output* [▶ 76]. If the RouterNode has reacted to the input event and, for example, has performed a broadcast, it can thus switch the relay as confirmation.

In the ▼ **Delay [s]** drop-down list, you can set how long the RouterNode should wait until the corresponding input responds to an event.

"0 s"	Standard entry: The input reacts immediately to an event.
"8 s"	The input reacts to an event after 8 seconds
"16 s"	The input reacts to an event after 16 seconds.
"24 s"	The input reacts to an event after 24 seconds.
"32 s"	The input reacts to an event after 32 seconds.
"RingCast"	An event at the input triggers a RingCast (see <i>RingCast</i> [▶ 95]).

**Forward triggering events to the LSM**

You can use the checkbox  Report events to management system to set whether the signals (input events) at the respective input are to be forwarded to LSM. In LSM, you can (additionally) use the event manager to react to these events.

Not all events are forwarded (see table):

Response	Forwardable signals (events)
<ul style="list-style-type: none"> <li>■ "Amok function"</li> <li>■ "Emergency release"</li> <li>■ "Remote opening"</li> <li>■ "Activation"</li> </ul>	<ul style="list-style-type: none"> <li>■ Level change Low to High</li> </ul>
<ul style="list-style-type: none"> <li>■ "Input"</li> <li>■ "Block lock"</li> </ul>	<ul style="list-style-type: none"> <li>■ Level change Low to High</li> <li>■ Level change High to Low</li> </ul>

Only events that have the responses "Input" oder "Block lock" are forwarded to the LSM. All other events are not forwarded to the LSM.

### Select LockNodes for response

You can use the **Select LN** to set which LockNodes perform the set reaction. You have two options for setting:

(Different) settings for individual inputs of the RouterNode	Same setting for all inputs of the RouterNode
<p>Click on the button of the respective input (For Input 1, 2 or 3). The window of the input opens. Select the LockNodes that should react to the events of this input.</p> <p>Proceed in the same way for the other inputs. LockNodes marked here react to all events at this input. You carry out the response that you have defined for this input.</p>	<p>Click the button <b>For all inputs</b> and select the LockNodes.</p> <p>LockNodes marked here react to all events at the inputs. They execute the response that you have defined for the relevant input.</p>

The following example illustrates the behavior depending on the setting:  
 For events at inputs 1 and 2, "Remote opening" is assumed as the response.

Example for settings				
	All inputs	Input 1	Input 2	Input 3
LockNode 1	✓			
LockNode 2		✓		
<p>LockNode 1 reacts to all events. LockNode 2 only reacts to events of input 1.</p> <p>In other words: a keystroke on Input 1 will give a remote open command to all locking devices. By pressing a key on Input 2, only the locking device with LockNode 1 receives a remote opening command.</p>				

Alternatively, you can also set directly at the LockNodes whether they perform reactions (see [LockNode \[▶ 86\]](#)).

You use the drop-down menu ▼ **Protocol generation** to specify the protocol generation of the locking system.

The LockNodes address the locking devices with the locking system password. You should therefore enter your locking system password.

Click the button **Password hidden**, to prevent your password from being displayed in plain text during entry.

### RouterNode: Analogue input

Analogue input configuration

Event handling :

Threshold [mV] :      Low :       High :

Sampling interval [s]:

In the drop-down list ▼ **Event handling** you can set when a voltage change at the analogue input of the RouterNode triggers an event (see *RouterNode: Digital output* [▶ 76]).

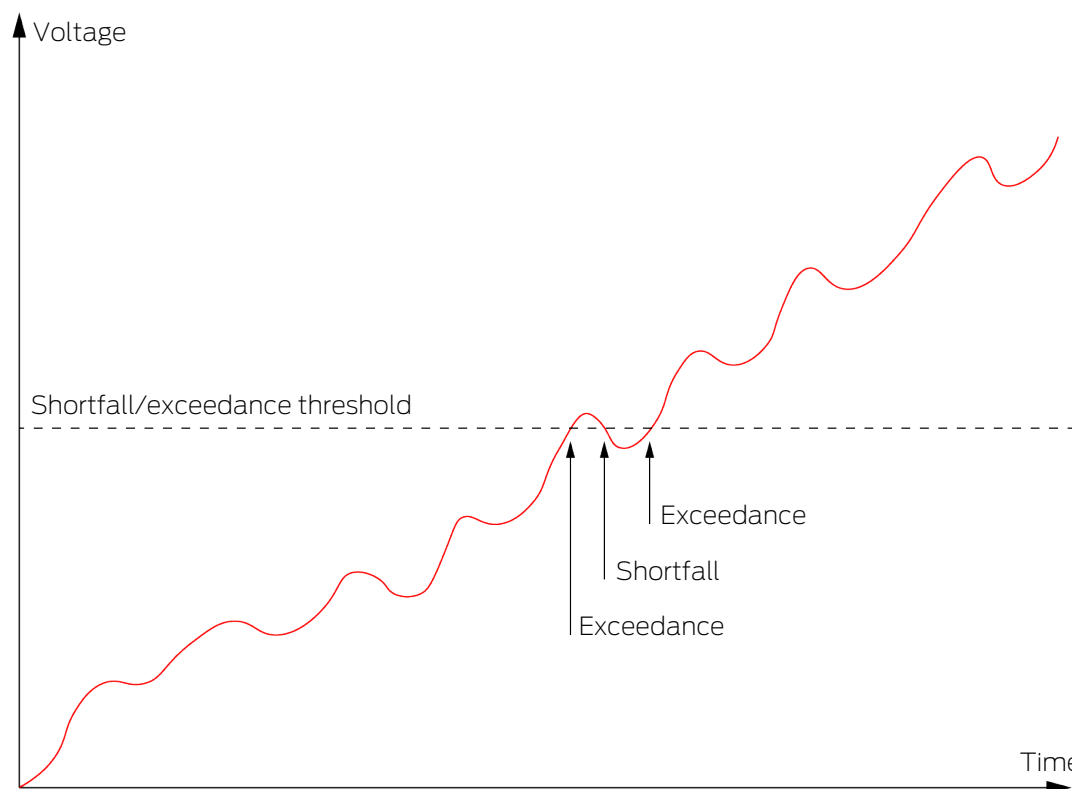
"No event"	Standard entry: The RouterNode does not respond to an applied signal.
"If too high"	If the voltage applied rises, it will at some point exceed the threshold value for exceeding it. At this moment the event is triggered.
"If too low"	If the applied voltage decreases, then at some point it falls below the threshold for falling below. At that moment, the event is triggered.
"If too high/too low"	<p>If the applied voltage changes and the following scenarios occur, then the event is triggered.</p> <ul style="list-style-type: none"> <li>■ Voltage drops and falls below the threshold value to fall below</li> <li>■ Voltage rises and exceeds the threshold value for exceeding</li> </ul>

With the sampling interval you can specify how often the applied signal is compared with the threshold values.

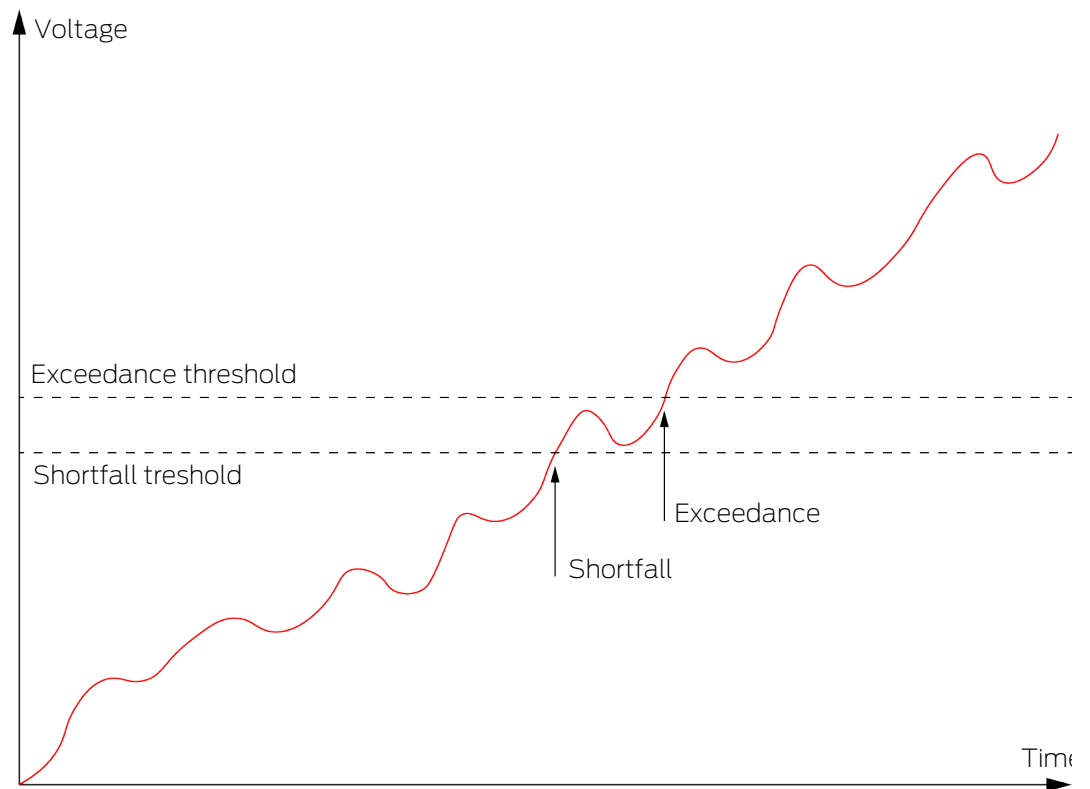
**NOTE****200 mV hysteresis band**

The analogue signal applied may be susceptible to interference and fluctuate slightly depending on its nature. If the thresholds were too close together, even small changes in the voltage would trigger several unintended events in succession.

The WaveNet Manager automatically sets the threshold value for falling below the threshold for exceeding by 200 mV (hysteresis). This increases the operational reliability of the RouterNode.



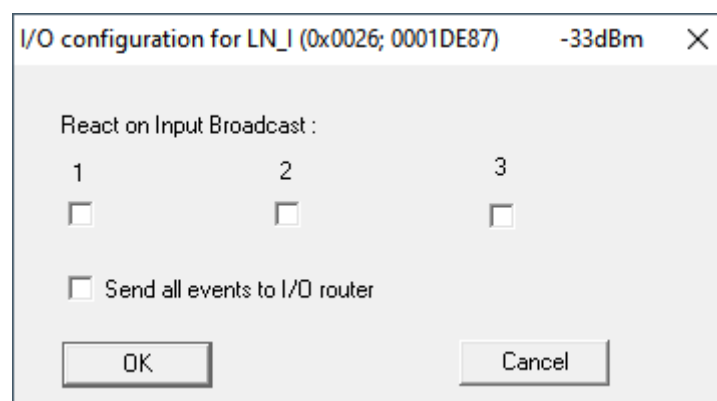
Without hysteresis, the same voltage curve will cause the threshold to be exceeded twice.



With hysteresis, the same voltage curve triggers exactly one overshoot. The overshoot is only detected again after the voltage has fallen below the thresholds.

### LockNode

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
- ✓ LockNodes reachable (see *Testing accessibility (WaveNet)* [▶ 183]).
- Right-click on the entry of the LockNode whose IO configuration you want to change.
  - ↳ Window "I/O configuration" opens (window and settings version-dependent, picture is an example).



- ↳ You can set the IO configuration.

### Activate reactions

If the RouterNode detects an input event at one of its digital inputs and a reaction is set (see *RouterNode: Digital input* [▶ 79]), then the RouterNode transmits for a broadcast. You use the upper row of checkboxes to individually specify for each of the three inputs whether the selected LockNode reacts to the broadcast caused by the event at the respective input.

Alternatively, you can activate the reaction for several LockNodes at the same time. Open the IO configuration menu of the RouterNode (see *RouterNode: Digital input* [▶ 79]).

### Activate event forwarding

The RouterNode can

- react to certain events (see *RouterNode: Digital output* [▶ 76])
- and/or forward these events to LSM.

You can set whether the LockNode forwards the events to the RouterNode directly at the LockNode. Activate the checkbox  Send all events to I/O router, to forward all events to the RouterNode. You can respond to these events either with the RouterNode (see *RouterNode: Digital output* [▶ 76]) or in the LSM.

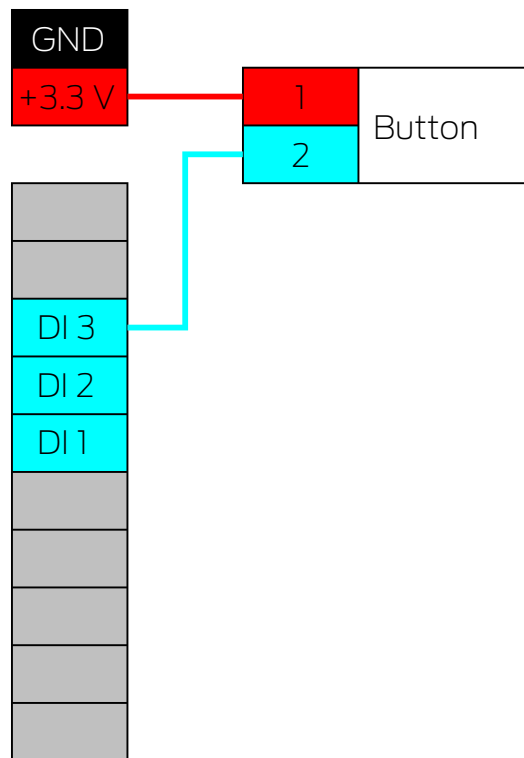
Alternatively, you can activate event forwarding for several LockNodes of a RouterNode at the same time. Open the IO configuration menu of the RouterNode (see *RouterNode: Digital output* [▶ 76]).

#### 6.4.4.2 Application examples

The following examples describe the connection at RouterNode 2. The wiring at the older RouterNode generation is similar.

#### Input (button)

Use this configuration to switch an input with a button. You can switch an input manually.

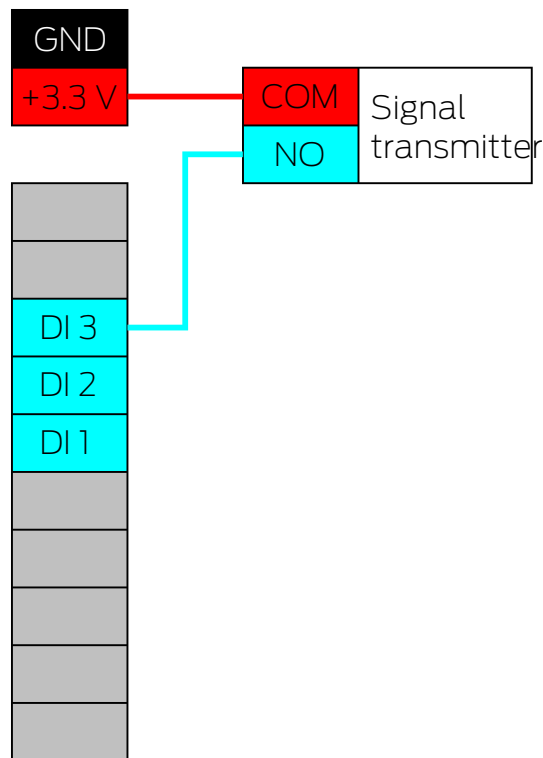


1. Connect a contact of the push button to a contact on the board, which is next to the IO-Connector and intended for  $+3.3 V_{DC}$ .
2. Connect the other contact of the push-button to one of the digital inputs DI1, DI2 or DI3.

#### Input (relay contact)

Use this configuration to switch an input with a relay contact. The relay contact can be controlled by an external system. This allows you to connect an external system to the WaveNet.



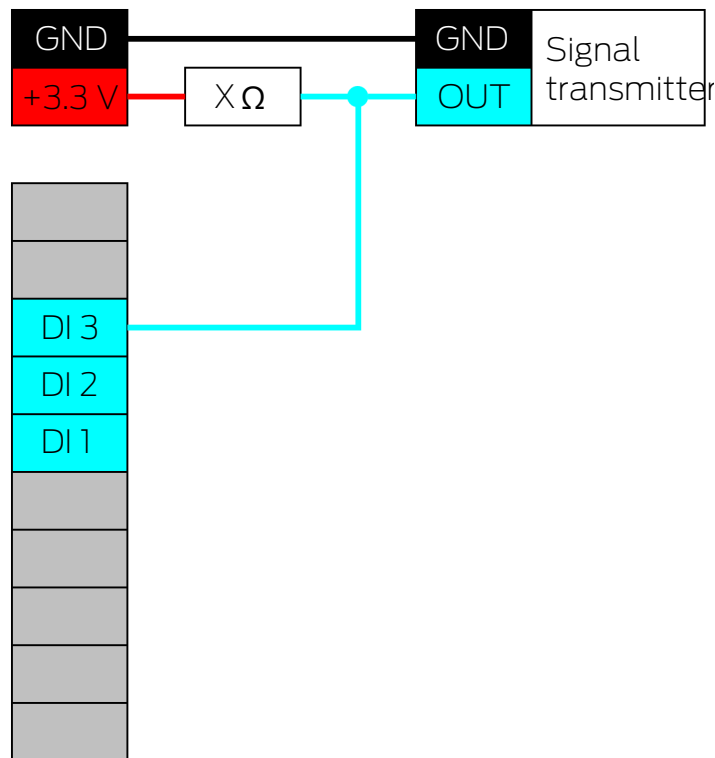


1. Connect the COM connector of the relay to the positive terminal of the power connector next to the IO-Connector.
2. Connect the relay NO port to one of the digital inputs DI1, DI2 or DI3. Buttons:

### Input (open drain)

Use this configuration to switch an open-drain output. The open-drain output can be regulated by an external system. This allows you to connect an external system to the WaveNet. Note that the switching behaviour is inverted:

- Open drain of the signal generator open/unswitched: Pull-up resistor "pulls" the digital input to +3.3 V<sub>DC</sub> (high level). An event is detected for this input.
- Open drain of the sensor closed/switched: Input is short-circuited to ground (low-level).



1. Connect the ground potentials of the signal transmitter and the router node.
2. Connect the positive terminal of the power connection next to the IO connector to the open-drain output of the signal transmitter via the pull-up resistor  $X$ .
3. In addition, connect the open drain output of the signal transmitter to one of the digital inputs DI1, DI2 or DI3.

The pull-up resistor depends on the open-drain output of the signal transmitter. A possible value is  $1 \text{ k}\Omega$ .

### IMPORTANT

#### Calculation of pull-up resistance

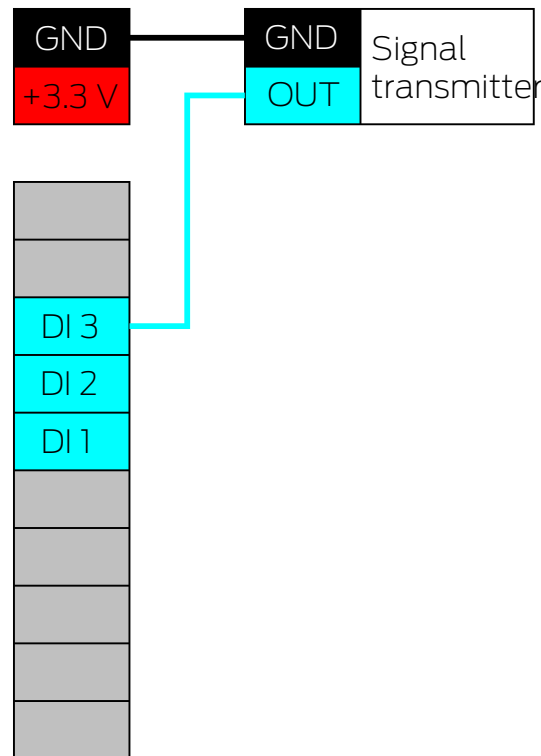
Pull-up resistors that are too small can damage the power connection next to the IO-Connector and overload the open-drain connection of the Signal Giver. Too large pull-up resistors make the signal unclear.

The pull-up resistor must be as small as possible and as large as necessary.

1. Do not select a value lower than  $16.5 \Omega$ .
2. Do not select unnecessarily large values.

### Input (push-pull)

Use this setup to switch an input with a push-pull output. The push-pull output can be regulated by an external system. This allows you to connect an external system to the WaveNet.



1. Connect the ground potentials of the signal transmitter and the router node.
2. Connect the push-pull output of the signal transmitter to one of the digital inputs DI1, DI2 or DI3.

### IMPORTANT

#### Voltage ranges of the digital inputs

The push-pull output can work with unsuitable voltages. For the signal to be reliably recognized as HIGH and LOW, it must be above or below the reference voltages, depending on the signal level. The maximum output voltage of the push-pull output must not exceed  $3.3 V_{DC}$ .

1. Do not use push-pull outputs whose voltage values for HIGH and LOW do not match the equivalent voltages of RouterNode 2.
2. Do not use push-pull outputs whose maximum output voltage exceeds  $3.3 V_{DC}$ .

#### Comparison voltages (RN and RN2)

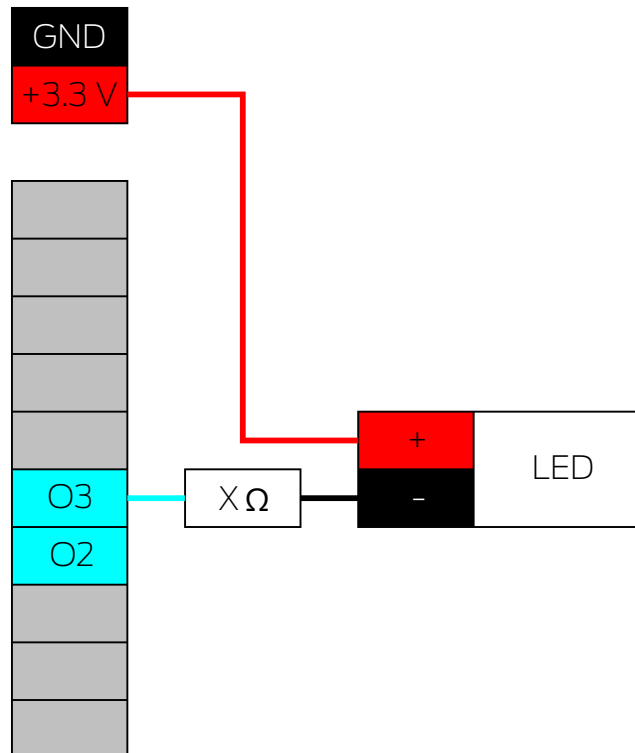
$<0,9 V_{DC}$	LOW (no signal)
---------------	-----------------

### Comparison voltages (RN and RN2)

$>2.1 V_{DC}$	HIGH (signal)
---------------	---------------

### Output (LED)

Connect the LED to O2 or O3 to indicate the second or third output.



1. Connect the cathode of the LED (-) via the series resistor X to O3 or O2.
2. Connect the anode (+) to the positive pole of the power connector next to the IO connector.

The value of the resistor X depends on the LED used.

### IMPORTANT

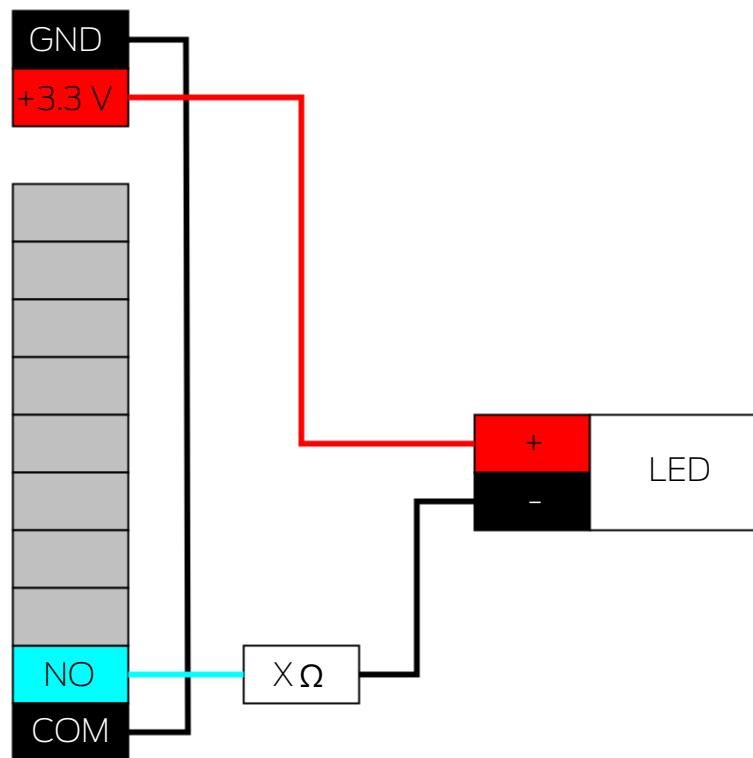
#### Current carrying capacity

The power connection next to the IO connector supplies between  $3.0 V_{DC}$  and  $3.3 V_{DC}$  and may be loaded with a maximum of 200 mA.

- Do not use the connector to operate equipment that exceeds these specifications.

### Output (LED on relay)

Connect the LED to the relay to indicate the first output.



1. Connect NO to the ground of the router node.
2. Then connect the cathode of the LED (-) via the series resistor X to COM.
3. Connect the anode (+) to the positive pole of the power connector next to the IO connector.

The value of the resistor X depends on the LED used.

### IMPORTANT

#### Current carrying capacity

The power connection next to the IO connector supplies between 3.0 V<sub>DC</sub> and 3.3 V<sub>DC</sub> and may be loaded with a maximum of 200 mA.

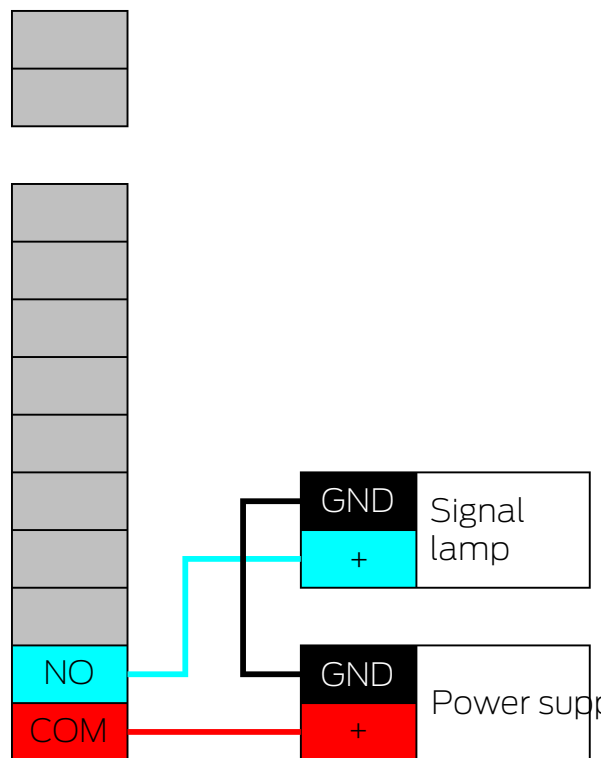
#### Output (light with increased current requirement)

In this context, lights with increased power requirements are light sources which are operated with more than 3.3 V<sub>DC</sub> and/or 200 mA. Do not connect these lamps to the power connection next to the IO connector, but use a suitable power supply unit.

**IMPORTANT****Load capacity of the relay**

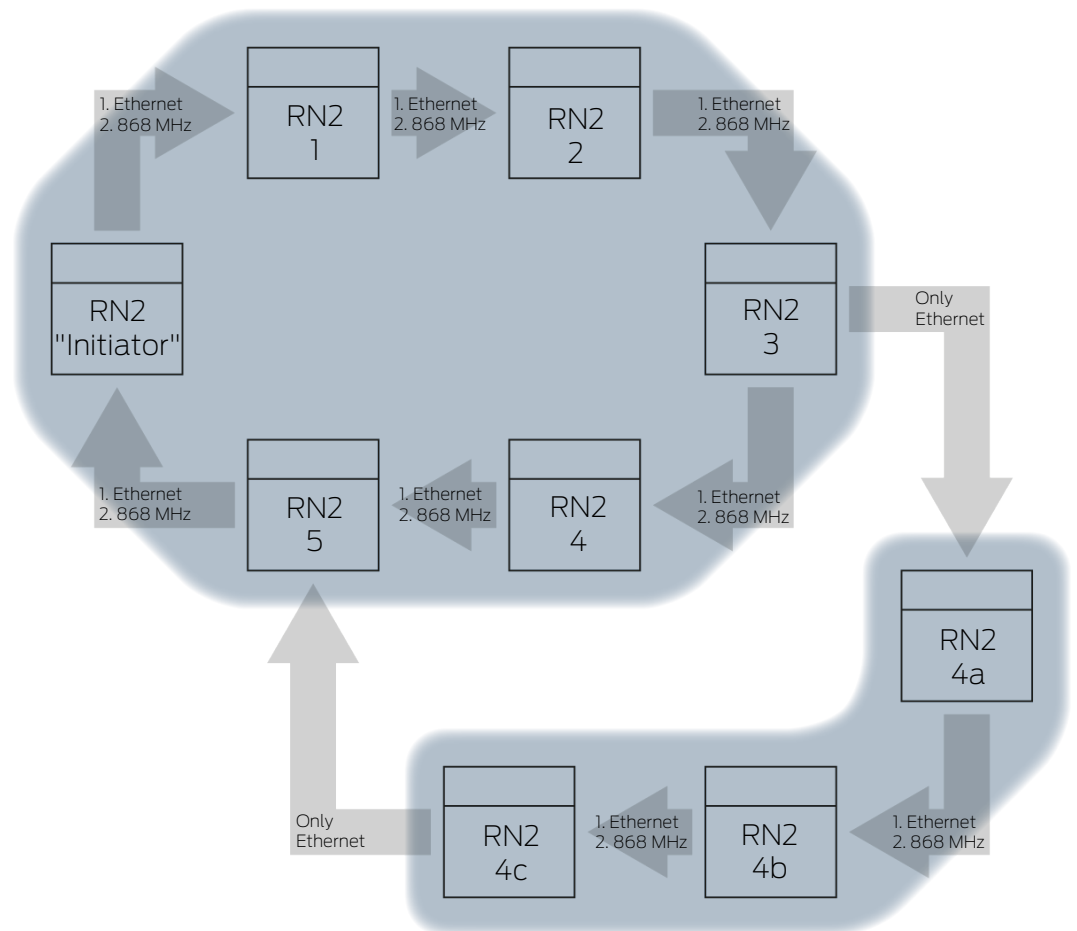
The relay in RouterNode 2 may be loaded with maximum 650 mA continuous current and 12 V<sub>DC</sub> switching voltage (see also technical data in RouterNode 2 manual).

- ❑ Do not use the relay to operate devices that exceed these specifications.



1. Connect the ground connections of the power supply unit and the signal lamp.
2. Connect the positive terminal of the power supply unit to O1.COM.
3. Connect the positive pole of the signal lamp to O1.NO.

## 6.4.5 RingCast



Depending on the firmware version of the router and LockNodes, some individual functions are not available (see *Firmware information* [▶ 39]).

**NOTE****Version-dependent availability of RingCast in WaveNet Manager**

From version 2.6.7, the WaveNet Manager supports all RingCast functions described above.

```

RingCast
├── Ringcast(0)
│   ├── CN_UR (0x000E_0x0101; 0001E0CE)
│   └── RN_ER (0x0012_0x0301; 0002013F)
│       └── CN_UR (0x000E_0x0101; 0001E0CE) ###
    
```

With RingCast, an input signal from a specific RouterNode ("Initiator") can be passed on to all networked RouterNodes without having to wire all inputs of the RouterNodes. If a signal arrives at the initiator at an input with a RingCast, the signal is forwarded to all RouterNodes connected to the RingCast and the RouterNodes react as if a signal were actually present at their input.

Meaning of the initiator	The "initiator" is the most important RouterNode in the RingCast. Connect the "Initiator" and the RouterNodes in the vicinity to Ethernet, even if the RouterNodes would reach each other wirelessly. This creates a backup and provides the RouterNode with a fallback level for passing on the signal.
Three inputs, three RingCasts	You can create a separate RingCast for each of the three inputs of a RouterNode, but you cannot start several RingCasts from one input. This means that you can connect one RouterNode to a maximum of three RingCasts. This restriction does not apply to the entire WaveNet; you can create more than three RingCasts.
RingCast calculation	After you have created the RingCast, the WaveNet Manager performs a radio scan. It then uses the results of the radio scan to calculate a three-dimensional structure.
Broadcast	<p>RouterNodes that have received an input signal and have stored a reaction for this input signal perform a broadcast to all locking devices networked with this RouterNode. Within a RingCast, these reactions can be different at the participating locking devices (depending on the reaction set at the respective RouterNodes (see <i>RouterNode: Digital input</i> [▶ 79]).</p> <p>Depending on the settings, the RouterNode repeats the broadcast up to three times (four attempts in total). These settings are decisive for repeating the broadcast:</p> <ul style="list-style-type: none"> <li>■ Selected response: "Block lock" or "Activation"</li> <li>■ Input acknowledges must be enabled: "Input receipt short" or "Input receipt static"</li> </ul> <p>When calculating the structure, the WaveNet Manager ensures that as many RouterNodes as possible can broadcast simultaneously without interfering with each other. This allows you to address your LockNodes as quickly as possible with a RingCast. After the RouterNode has completed its broadcasts, it forwards the signal in a data packet to its target partners.</p> <p>As soon as the LockNodes have received the broadcast, the LockNode locking device executes the set response.</p>
Protective functions	<p>An application purpose is, for example, the reaction to a fire alarm system. If the fire alarm system sends a signal to a RouterNode, then all networked locking devices should be opened and remain open until they are explicitly closed by remote opening. However, you can also use other functions via a RingCast, for example:</p> <ul style="list-style-type: none"> <li>■ Block lock function</li> <li>■ gunman attack function</li> <li>■ Remote opening</li> </ul>



Data package Depending on the transmission path, a RouterNode may have one or more other RouterNodes as target partners. Sending RouterNodes transmit a data packet consisting of:

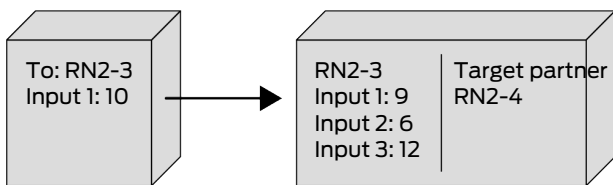
- Target partners who are to receive the data packet
- Input signal to be forwarded
- Counter reading of the corresponding input at the initiator

Stand-alone The information which RouterNodes have which target partners is also stored in the RouterNodes themselves. The RingCast therefore functions independently of connected computers.

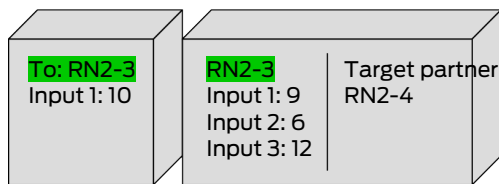
6.4.5.1 Procedure at the individual RouterNode viewed

**Sequence of the RingCast at a RouterNode 2:**

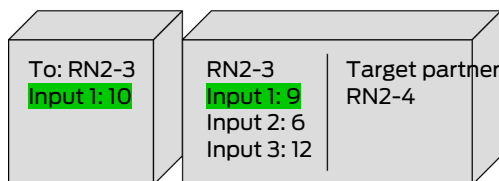
1. Receive data packet



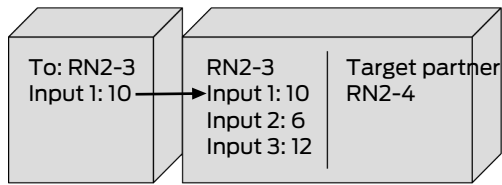
2. Check data package: **Actual target partner**  
If the check fails, the data packet is discarded.



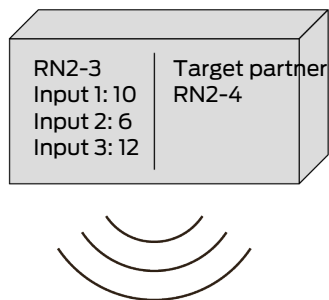
3. Check data package: **Input counter reading in data package > currently stored input counter reading**  
If the check fails, the data packet is discarded.



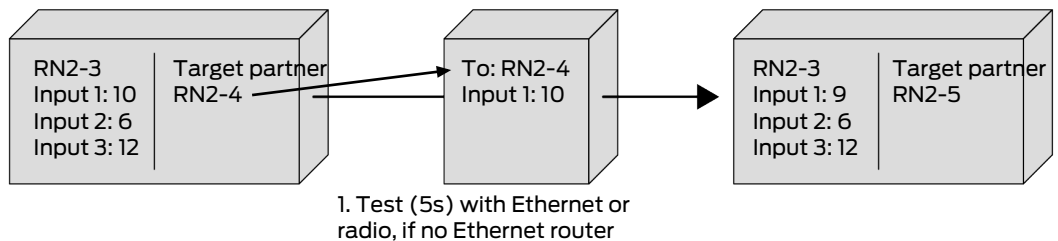
4. Save input counter reading of the package



5. Perform broadcast: Five seconds (One second for Fast Wake-Up support, see *Firmware information* [▶ 39])



6. Forward data packet with input signal and input counter reading (Ethernet or radio, if RouterNode has no Ethernet connection): Max. five seconds, then abort



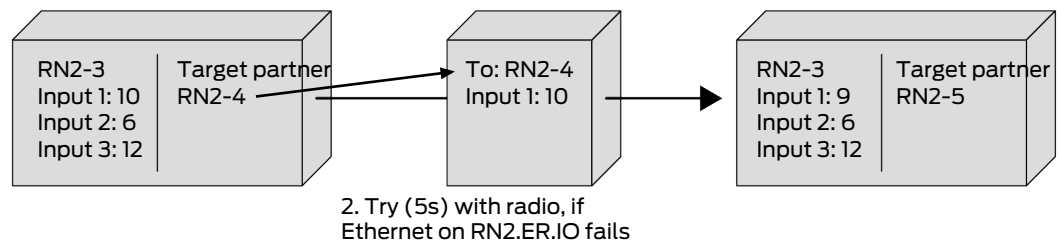
**NOTE**

**RingCast start only with existing radio connection**

The RingCast is set up according to radio accessibility. If the initiator cannot reach another RouterNode via radio, then the data packet is only sent via Ethernet to the assigned target partners. Even if the destination partners could reach further RouterNodes via radio, do not forward the data packet. The RingCast then ends at the initiator's target partners that can be reached via Ethernet.

- Make sure that the initiator of a RingCast can always establish at least one wireless connection to another RouterNode of the RingCast.

7. Forward data packet with input signal and input counter reading (radio, only after failed Ethernet connection attempt of RN2.ER.IO): Max. five seconds, then abort



Conditions that must be met for forwarding and broadcast:

1. **Actual target partner:** The RouterNode checks whether it is listed in the target partners of the data packet.
2. **Input counter reading in data package > currently stored input counter reading:** The initiator counts how often it has forwarded the input signal via the RingCast after an input event and increases the counter reading each time it is sent again. The transmitted data packet contains this counter reading. When a RouterNode receives a data packet, there are two possibilities.

The counter reading of the received packet is higher than the own counter reading: The received packet is new and has not yet been processed (otherwise the stored counter reading would be the same).

The counter reading of the received packet is less than or equal to the own counter reading: The received packet has already been processed.

If the initiator receives a data packet with an input counter reading equal to its own counter reading, the RingCast is considered complete.



#### NOTE

##### Signal distribution after RingCast termination detection

The termination detection means that the shortest possible intact path of the RingCast has been passed and all RouterNodes on this path have received the input signal.

If not all paths are intact in case of redundant paths, the RingCast is still recognized as terminated.

The terminal detection therefore does not indicate whether all router nodes involved have received the input signal.

##### Transmission behavior after terminal recognition of the RingCast

The termination detection means that the shortest possible intact path of the RingCast has been passed and all RouterNodes on this path have received the input signal.

Transmission is still possible on (longer) redundant paths or branches.

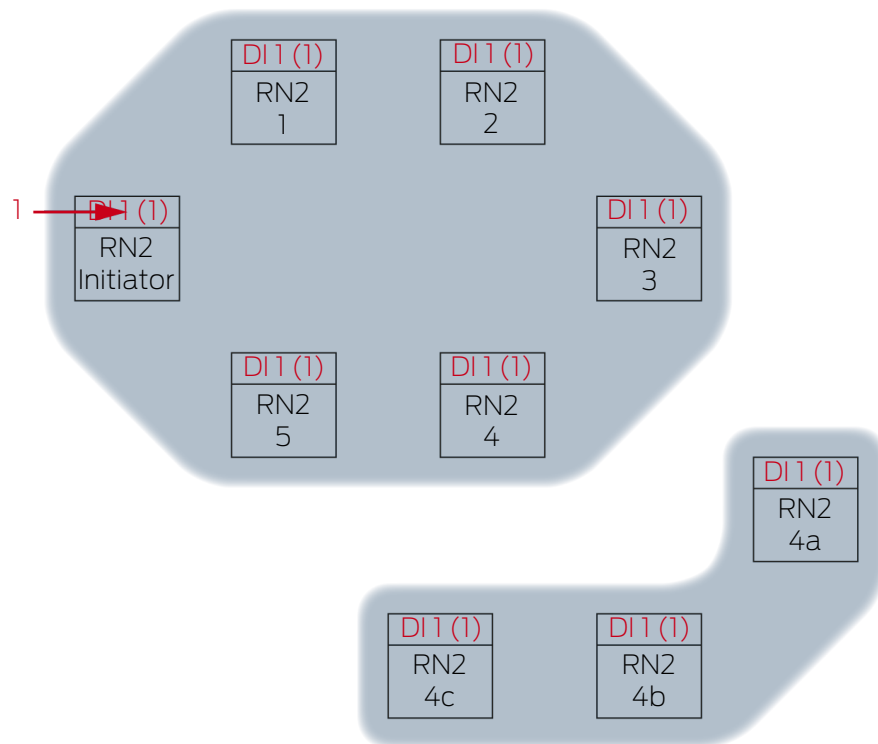
The terminal recognition therefore does not say anything about whether participating RouterNodes are still sending.

## 6.4.5.2 Sequence considered at several RouterNodes

With this example you can follow the process of a RingCast. This RingCast contains:

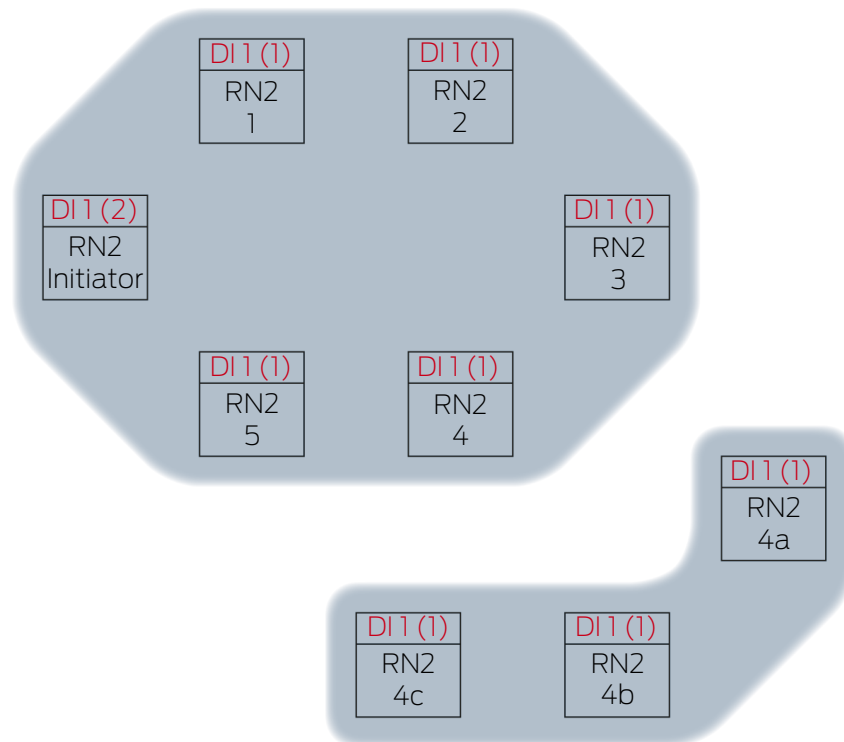
- Branches
- Redundant paths of different lengths

The input signal in this example is **1**.

**Extension 1**

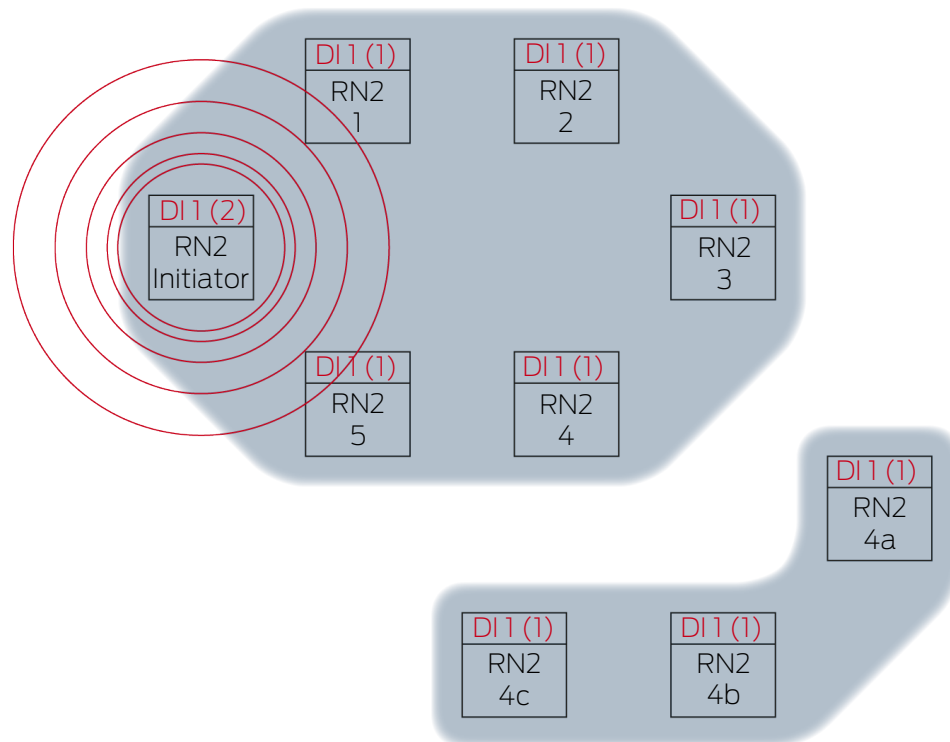
Input signal **1** at RN2 "Initiator".

## Extension 2



This is the second time in the example that the "initiator" distributes the input signal 1 via a RingCast. The input counter reading in the initiator is therefore 2. All other RouteNodes in the RingCast have first received the input signal via a RingCast and therefore the input counter reading is 1.

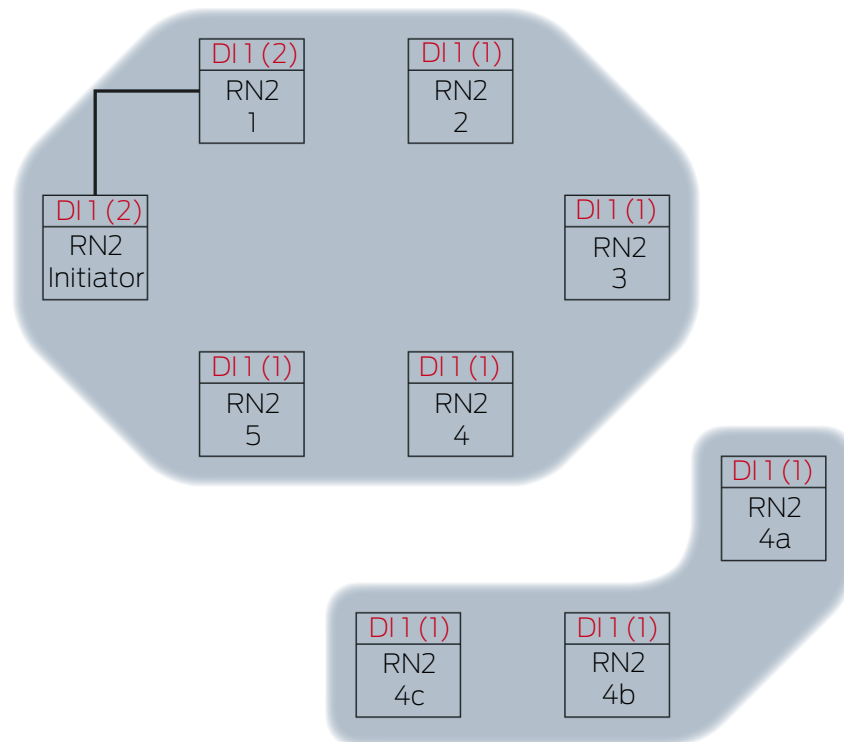
## Extension 3



The RN2 "Initiator" transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-1	1 (2)

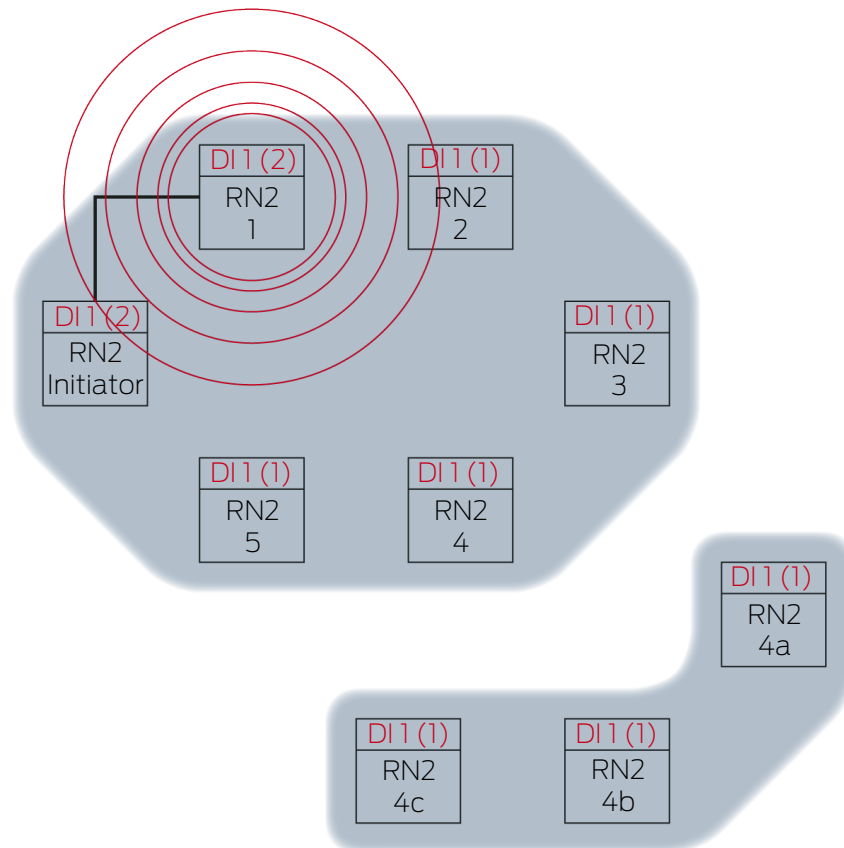
## Extension 4



The RN2-1 receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package** > **currently stored input counter reading**. Both conditions are met → RN2-1 accepts the data packet and stores the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

## Extension 5

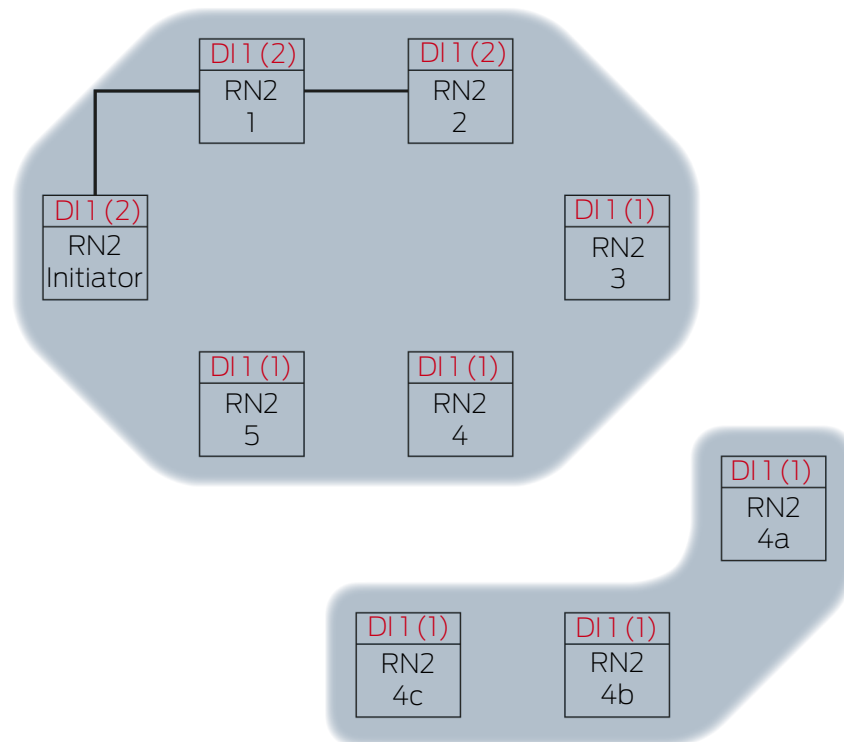


RN2-1 transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-2	1 (2)



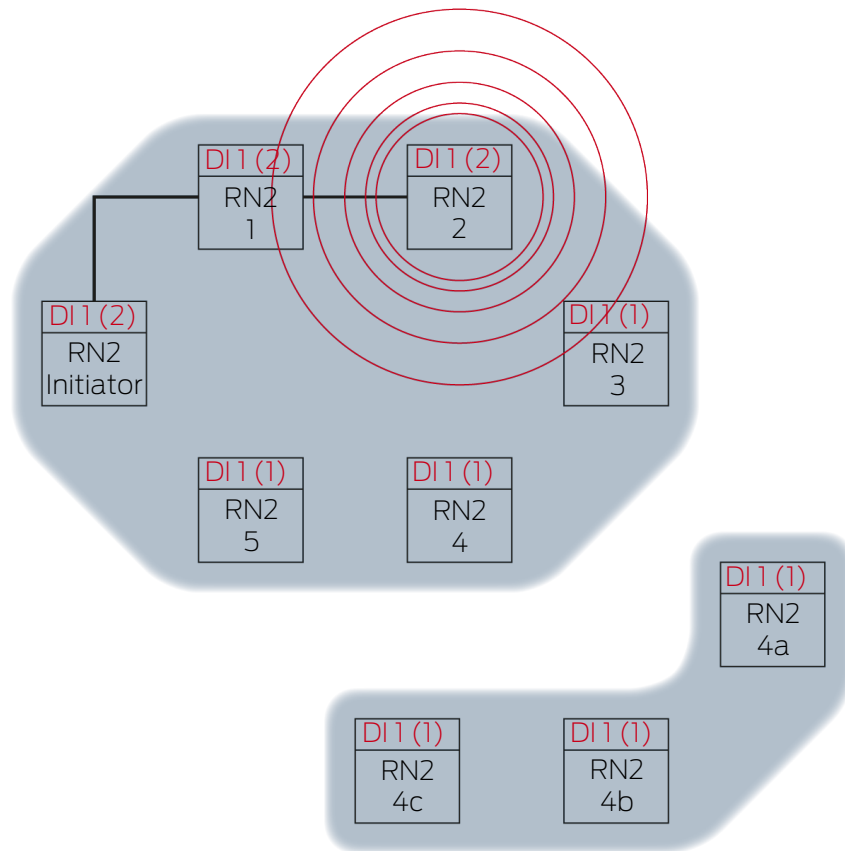
## Extension 6



The RN2-2 receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package > currently stored input counter reading**. Both conditions are met → RN2-2 accepts the data packet and saves the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

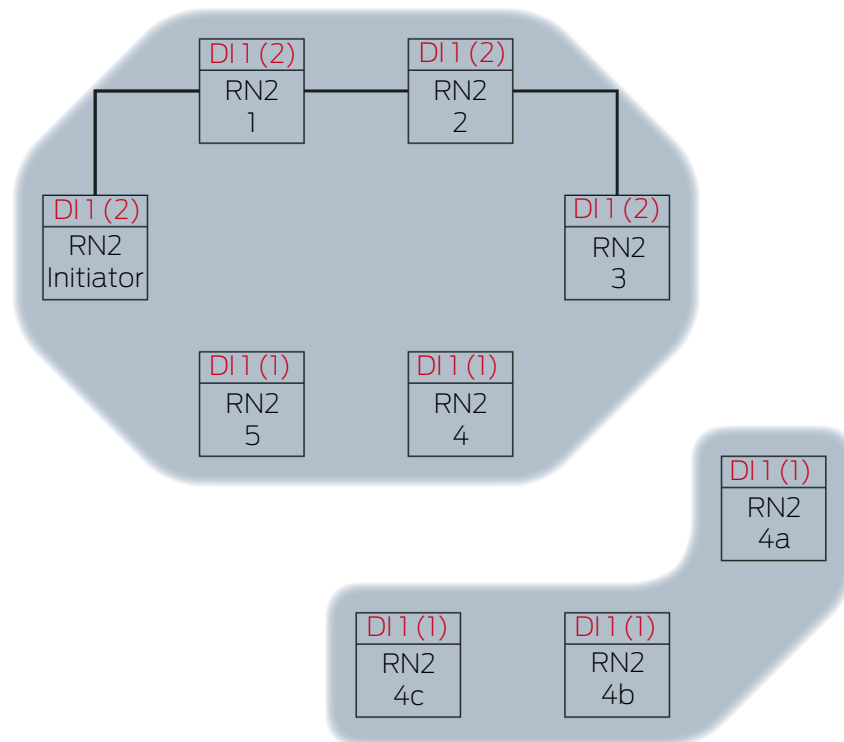
Extension 7



RN2-2 transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-3	1 (2)

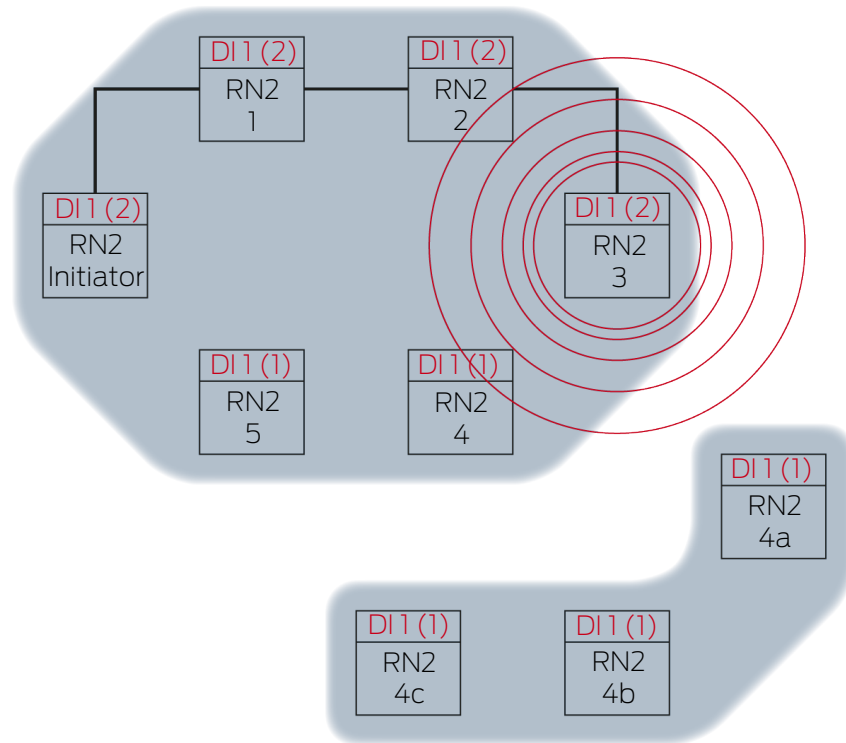
## Extension 8



The RN2-3 receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package** > **currently stored input counter reading**. Both conditions are met → RN2-3 accepts the data packet and saves the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

Extension 9

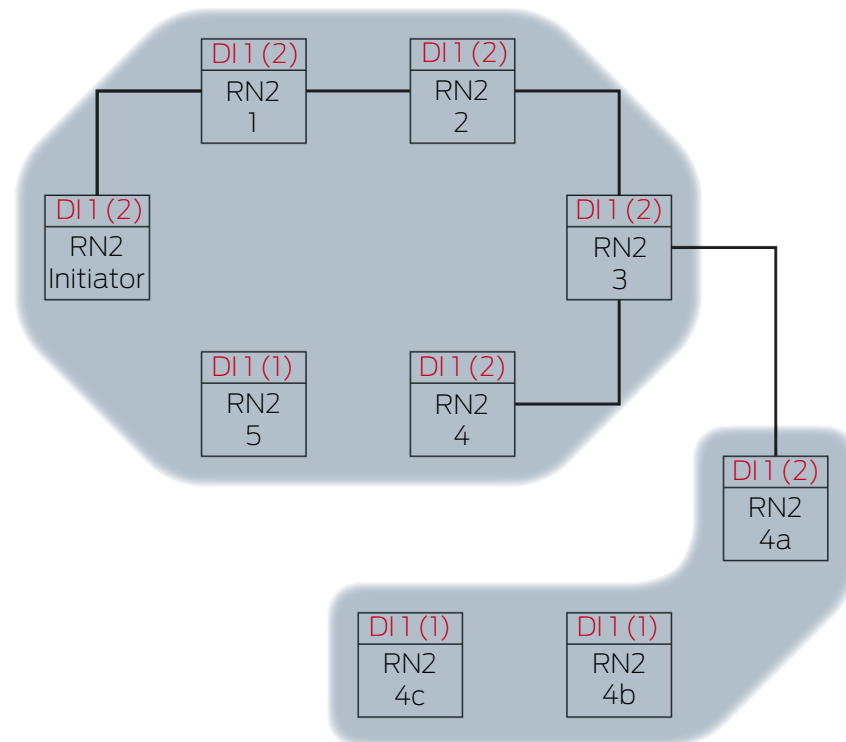


RN2-3 transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-4 RN2-4A	1 (2)

The WaveNet Manager recognises that the radio networks of RN2-4 and RN2-4A do not influence each other and can therefore simultaneously propagate the input signal. This accelerates the RingCast.

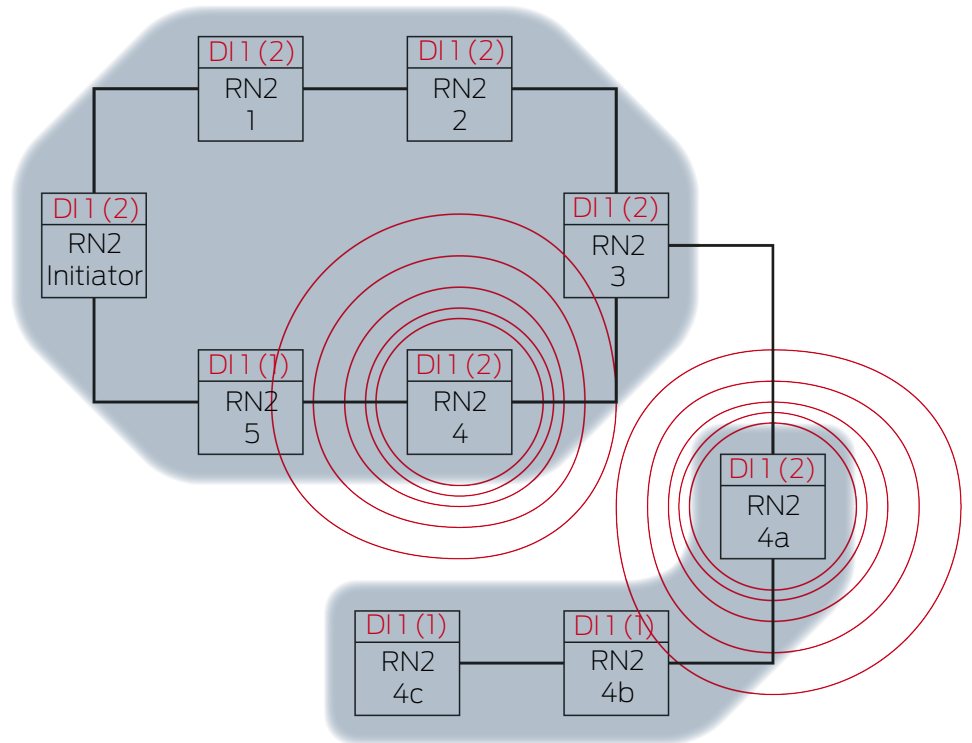
## Extension 10



RN2-4 and RN2-4 receive the data packet and checks the conditions one after the other **Actual target partner** and **Input counter reading in data package > currently stored input counter reading**. Both conditions are met → RN2-4 and RN2-4 accept the data packet and save the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

Extension 11



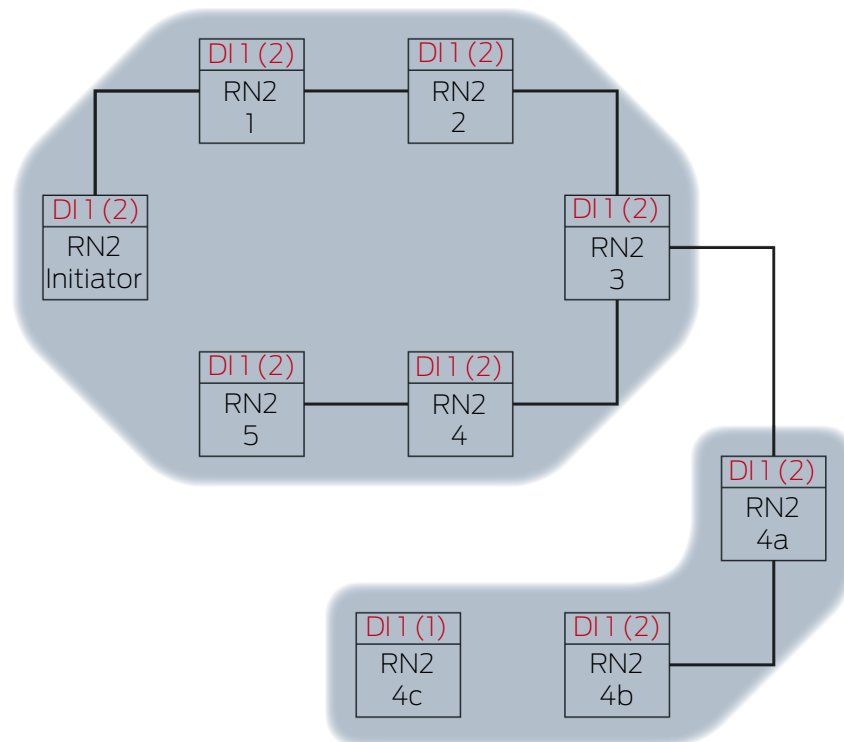
RN2-4 transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-5	1 (2)

RN2-4A transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-4B	1 (2)

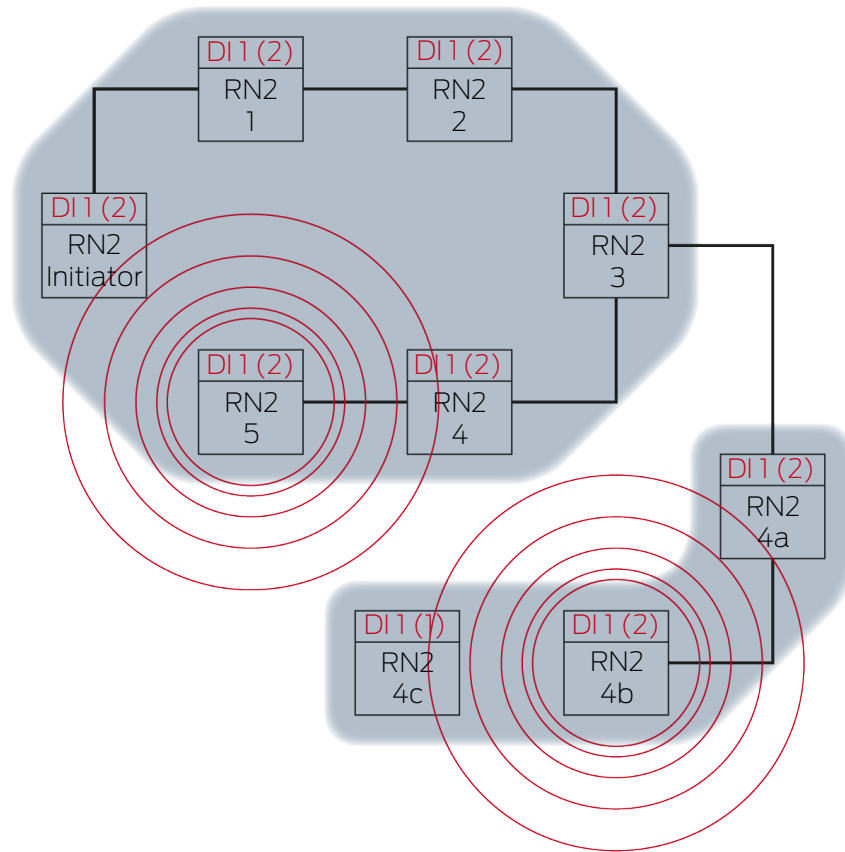
## Extension 12



RN2-5 and RN2-4B receive the data packet and checks the conditions one after the other **Actual target partner** and **Input counter reading in data package > currently stored input counter reading**. Both conditions are met → RN2-5 and RN2-4B accept the data packet and save the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition Actual target partner is not fulfilled, these RouterNodes discard the data packet.

Extension 13



RN2-5 transmits data packet (cable connection or radio connection if cable connection failed or not available).

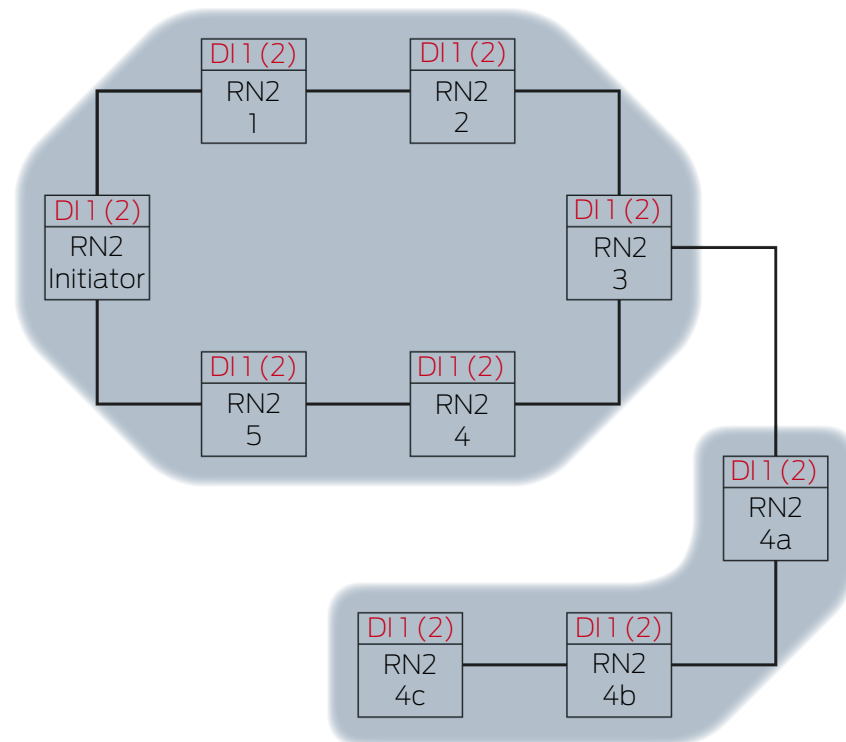
Target partner	Input signal and input counter reading
RN2 "Initiator"	1 (2)

RN2-4B transmits data packet (cable connection or radio connection if cable connection failed or not available).

Target partner	Input signal and input counter reading
RN2-4C	1 (2)



## Extension 14

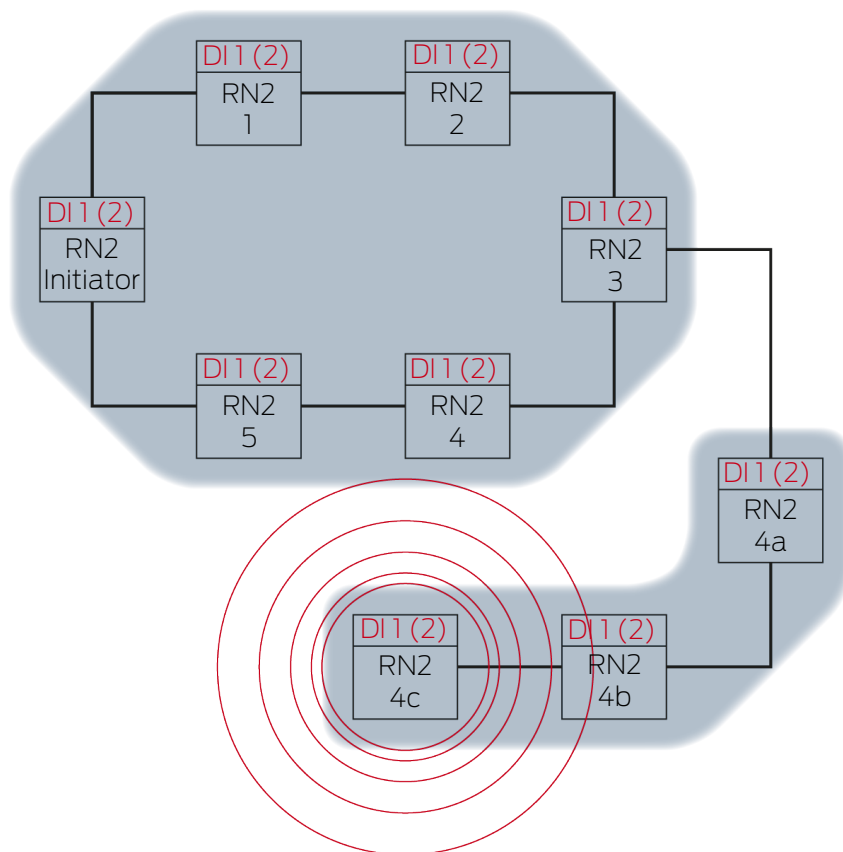


The RN2 "Initiator" receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package** > **currently stored input counter reading**. The condition **Input counter reading in the data package** > **currently stored input counter reading** is not fulfilled (same input counter reading) → The RN2-"Initiator" does not accept the data packet and terminates the RingCast as "Initiator" RouterNode.

The RN2-4C receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package** > **currently stored input counter reading**. Both conditions are met → RN2-4C accepts the data packet and saves the input counter reading of the data packet in its own input counter reading.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

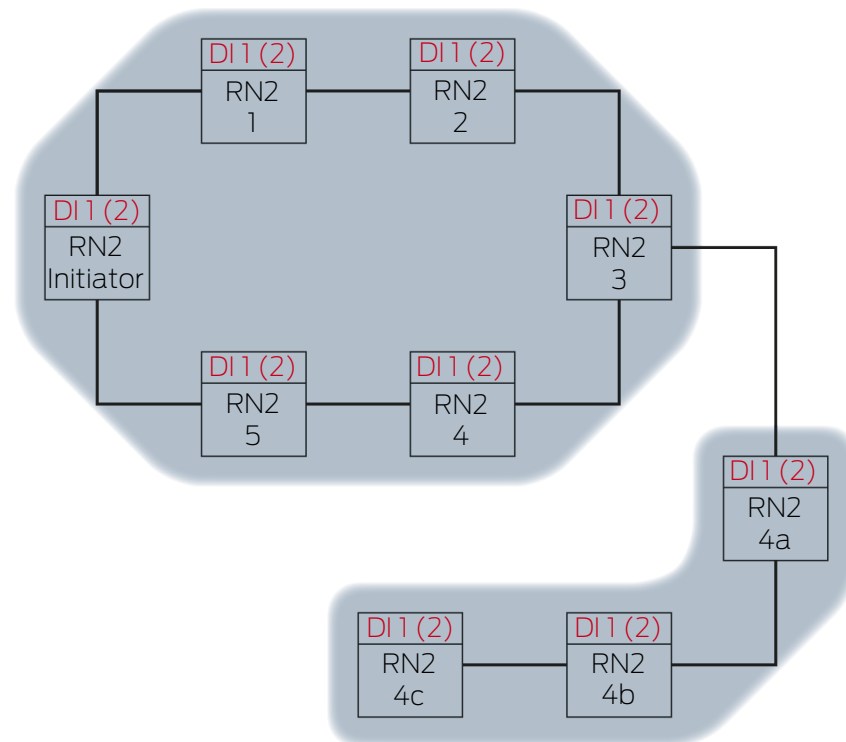
Extension 15



RN2-4C transmits data packet (cable connection).

Target partner	Input signal and input counter reading
RN2-5	1 (2)

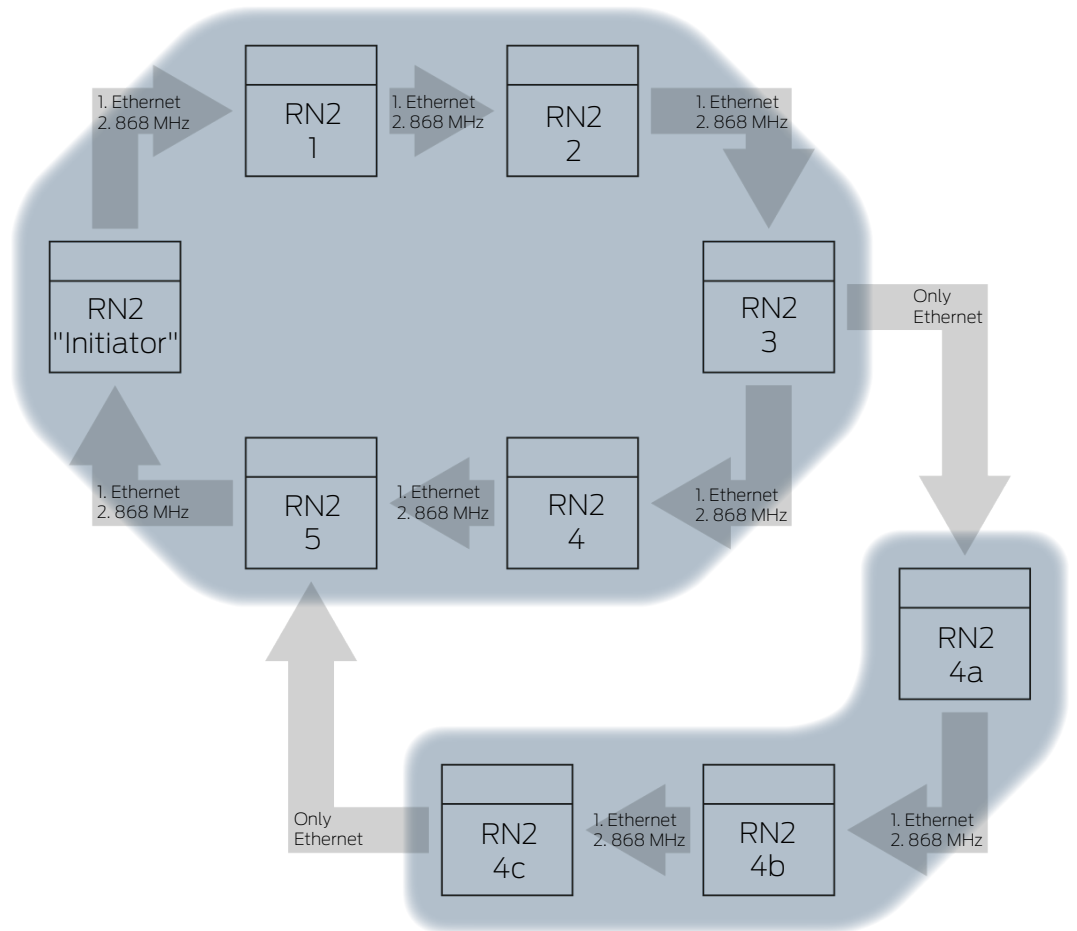
## Extension 16



The RN2-5 receives the data packet and checks the conditions one after the other. **Actual target partner** and **Input counter reading in data package > currently stored input counter reading**. The condition **Input signal not saved as received** is not satisfied (same Input counter reading) → RN2-5 discards the data packet.

If the data packet is transmitted wirelessly, then other router nodes within range will also receive the data packet. The condition **Actual target partner** is not fulfilled, these RouterNodes discard the data packet.

6.4.5.3 Redundancies in RingCast



**Redundancy through transmission media**

If you use second-generation Ethernet router nodes (=RN2), the router nodes first use the Ethernet connection and then the wireless connection as backup.

If the WaveNet Manager detects when calculating the RingCast that several RouterNodes reach each other wirelessly at the same time (in the example "Initiator", 1, 2, 3, 4, 5 or 4a, 4b and 4c), it assigns exactly one target partner to each RouterNode within this "radio cloud".

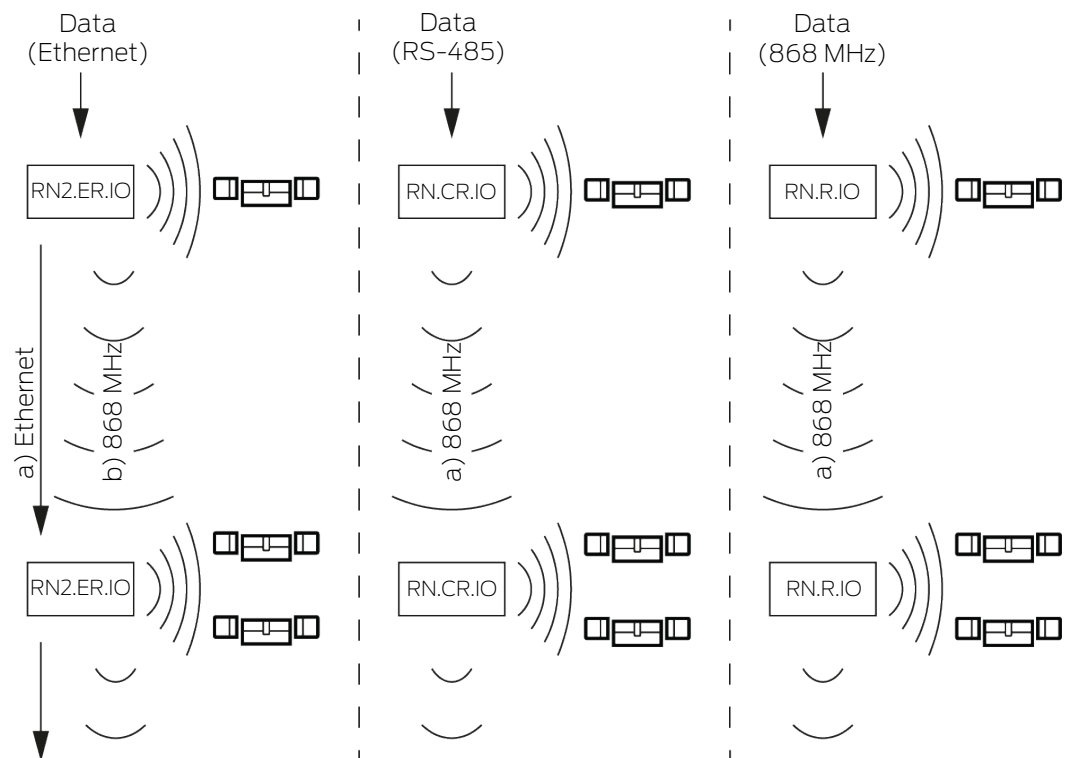
Router node	1. Transmission medium in RingCast	2. Transmission medium (backup) in RingCast
RN2.ER.IO (Ethernet and radio)	Ethernet	Radio (868 MHz)
RN.CR.IO (RS-485 and Radio)	Radio (868 MHz)	
RN.R.IO (Radio)	Radio (868 MHz)	



## NOTE

### Transmission range

The range of the radio connection is up to 30 m (depending on the building structure).



If the Ethernet RouterNode does not reach its target partner via the Ethernet connection after five seconds with a RingCast, it attempts to reach the target partner via the wireless connection. Since the RouterNode is physically unable to address its target partners in a wireless connection, all RouterNodes within range receive the data packet. Subsequently, all RouterNodes that have received the data packet check whether the condition **Actual target partner** is fulfilled. If the condition is not fulfilled, the router nodes that are not target partners of the sending RouterNode discard the packet again.

If the RouterNode does not reach its target partner via the wireless connection, the RingCast is interrupted at this point.

### Redundancy through branching

Regardless of the transmission medium, it is possible for the WaveNet Manager to establish multiple connections between two RouterNodes when calculating the RingCast. If one of these connections fails or is disturbed, then the RingCast can partially continue to run over the intact

connections. The data packet with the same input counter reading as the input counter reading stored in the initiator arrives at the initiator again and the RingCast is recognised as completed.

### Redundancy of the power supply

#### Interruption of the RingCast due to power failure

Power in buildings may fail. If RouterNodes are not supplied with power, you cannot forward your data packets and the RingCast is interrupted.

- Use an uninterruptible power supply (UPS) to protect the RouterNodes from a power failure.

### Redundancy through events in LSM



#### NOTE

#### Event management only in LSM Business

This chapter describes how to use the Event Manager. The Event Manager is only available in LSM Business/Professional.

Various influences can (temporarily) interfere with radio transmission (see *Radio network* [▶ 21] and *Signal quality* [▶ 23]). If interference occurs during a broadcast, not all LockNodes and therefore not all locking devices may be reached.

You can add an additional transmission using the LSM. Since you can also forward input events to the LSM when a connection to the LSM is established (see *RouterNode: Digital output* [▶ 76]), you can also react to them in the LSM (| Network | - **Event manager**). In the window "I/O configuration" activate the checkbox  Yes.

Report events to management system :  Yes  Yes  Yes

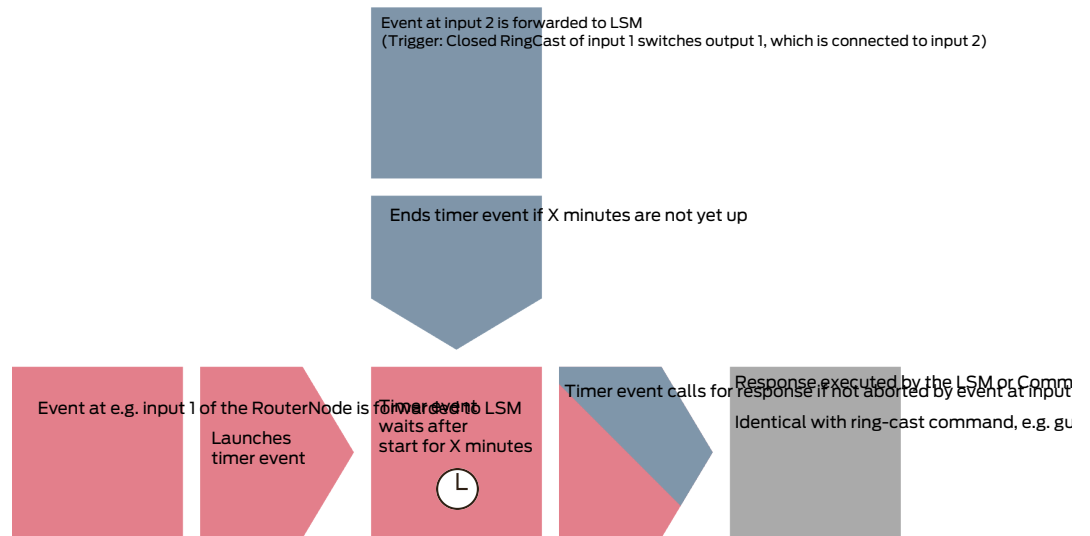
This additional broadcast requires the following:

- Initiator and central output router are the same device
- Only Ethernet RouterNodes are involved in RingCast

If you use a central output router and forward its input acknowledgement to LSM, you can also cancel the additional transmission (in LSM, cancel the timer as a response). To do this, connect the output of the input acknowledgement (e.g. 1) to a free input (e.g. 2).

The event in LSM is processed in three parts.

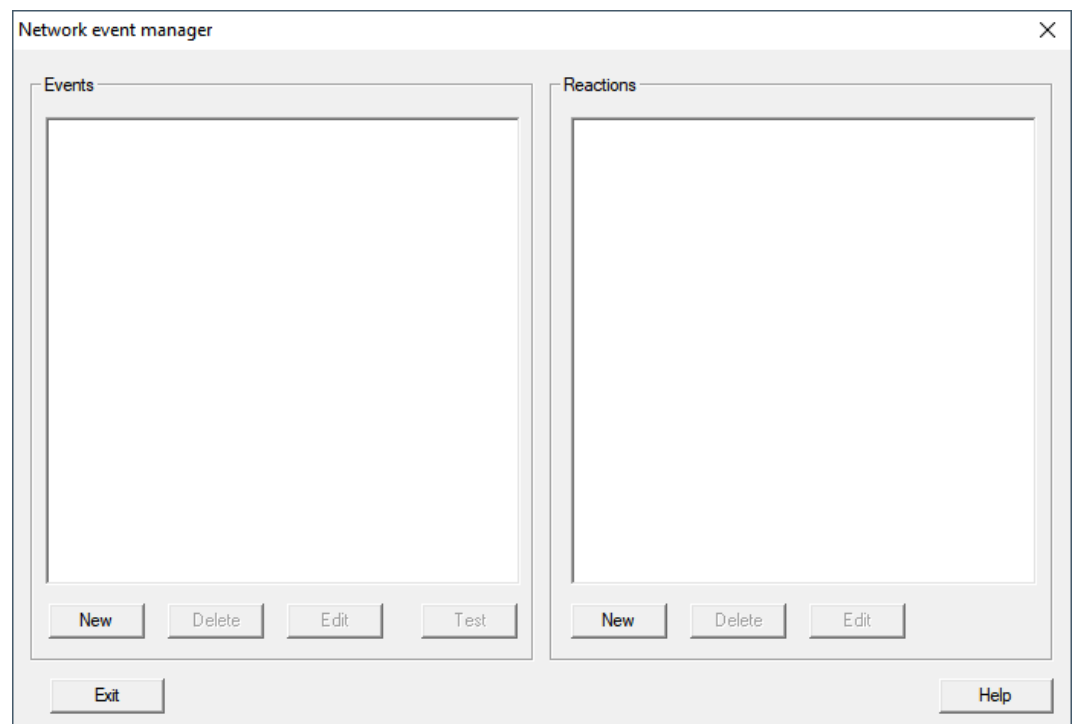
1. WaveNet input starts a timer event.
2. Timer event starts after event expires and starts reaction.
3. Reaction sends the RingCast command to all specified locking devices.



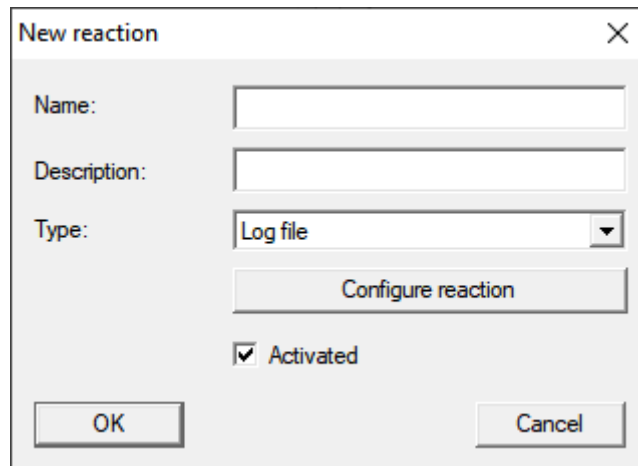
### Repeating the broadcast

✓ LSM open.

1. Via | Network | select the entry **Event manager**.
  - ↳ The window "Network event manager" opens.



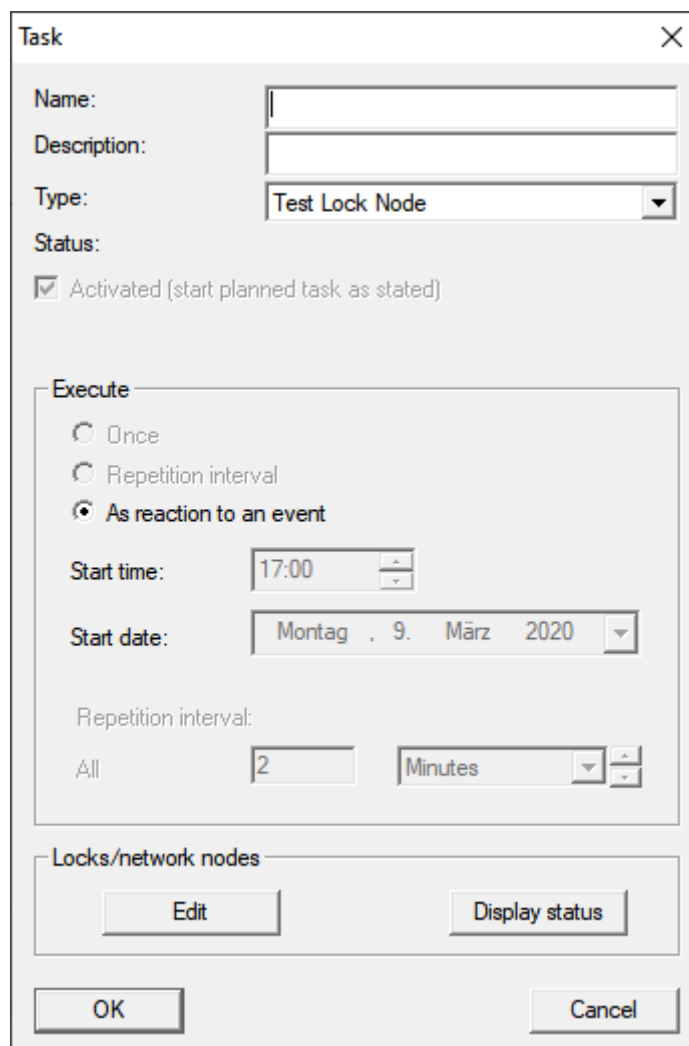
2. In the area "Reactions" click the button **New**.
  - ↳ The window "New reaction" opens.



The 'New reaction' dialog box contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Type:** A dropdown menu with 'Log file' selected.
- Configure reaction:** A button.
- Activated:** A checked checkbox.
- OK** and **Cancel** buttons at the bottom.

3. Enter a name and a description.
4. In the dropdown menu ▼ **Type** select the entry "Network task".
5. Click on the button **Configure reaction**.
  - ↳ The window "Task" opens.



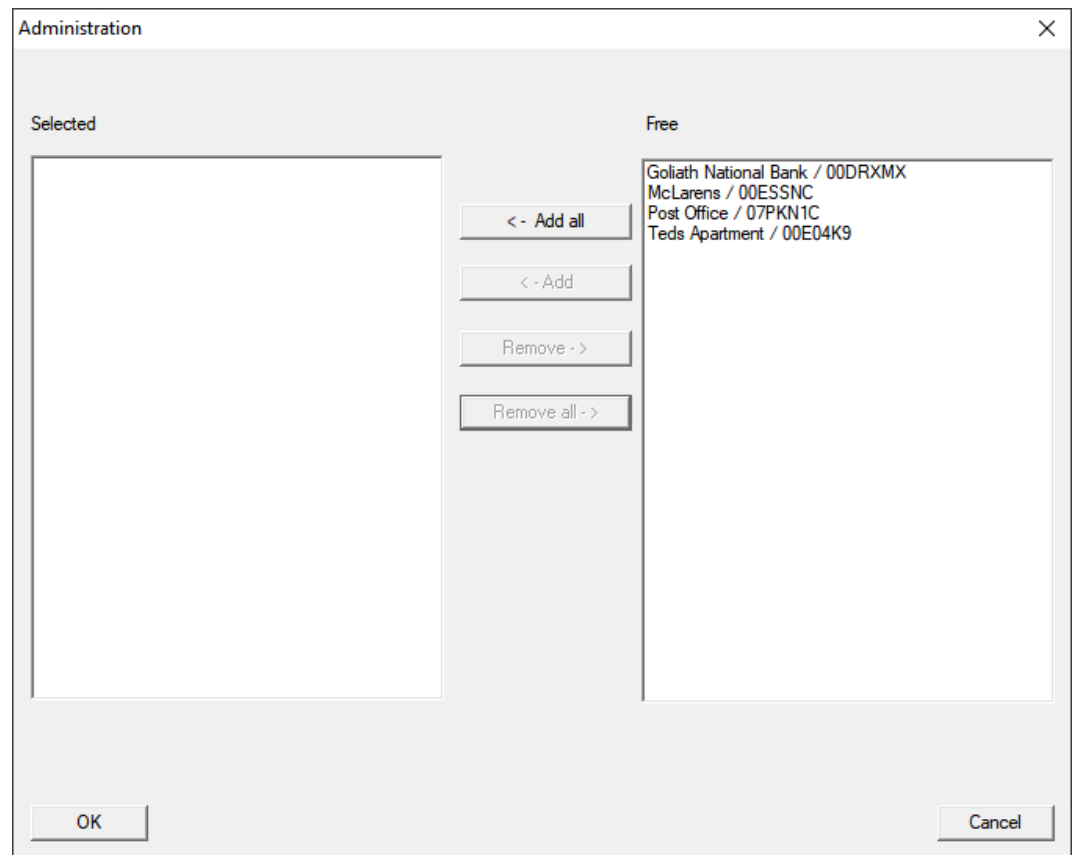
The 'Task' dialog box contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Type:** A dropdown menu with 'Test Lock Node' selected.
- Status:** A checked checkbox labeled 'Activated (start planned task as stated)'.
  - Execute:** A section with three radio buttons: 'Once', 'Repetition interval', and 'As reaction to an event' (selected).
  - Start time:** A time picker set to 17:00.
  - Start date:** A date picker set to Montag, 9. März 2020.
  - Repetition interval:** A section with 'All' selected, a text input field with '2', and a dropdown menu with 'Minutes'.
- Locks/network nodes:** A section with 'Edit' and 'Display status' buttons.
- OK** and **Cancel** buttons at the bottom.

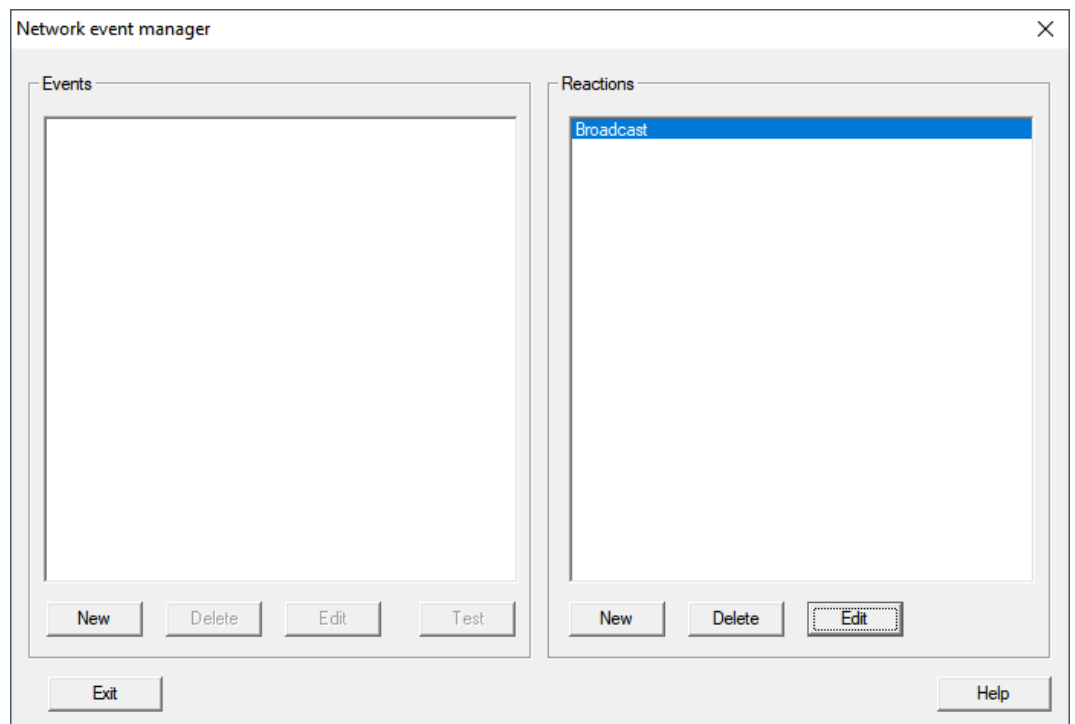
6. Enter a name and a description.



7. In the dropdown menu ▼ **Type** select the command that your RingCast transmits.
8. In the area "Locks/network nodes" click the button **Edit**.
  - ↳ The window "Administration" opens.

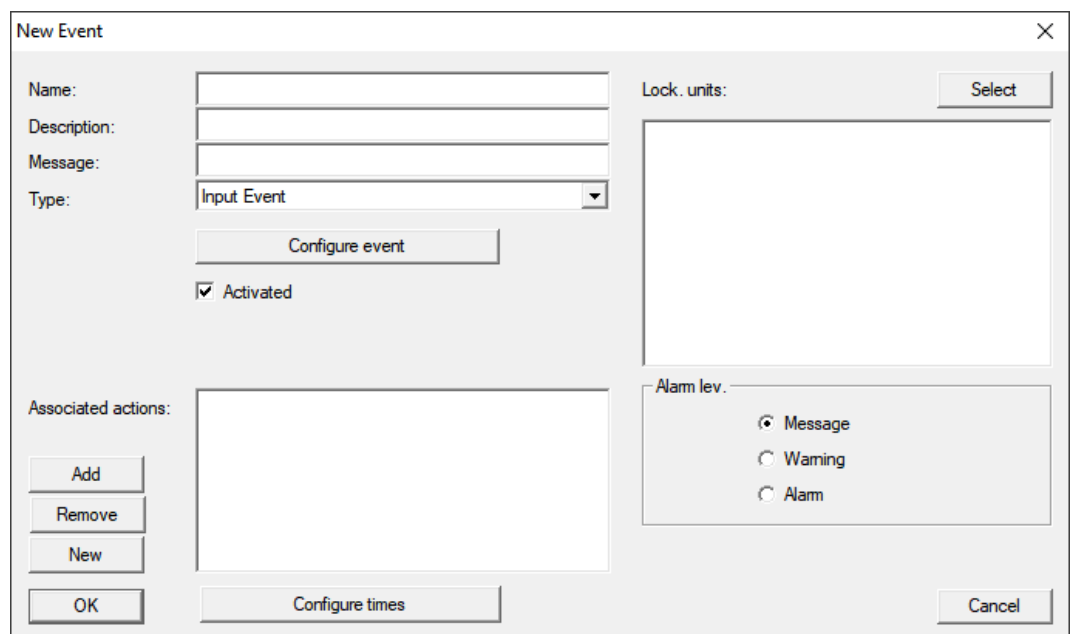


9. Mark all locking devices that are controlled by the RingCast.
10. Click on the button **Add**.
11. Click on the **OK** button.
  - ↳ The "Administration" window closes.
12. Click on the **OK** button.
  - ↳ The window "Task" closes.
13. Click on the **OK** button.
  - ↳ The "New reaction" window closes.
  - ↳ The reaction is listed in the area "Reactions".

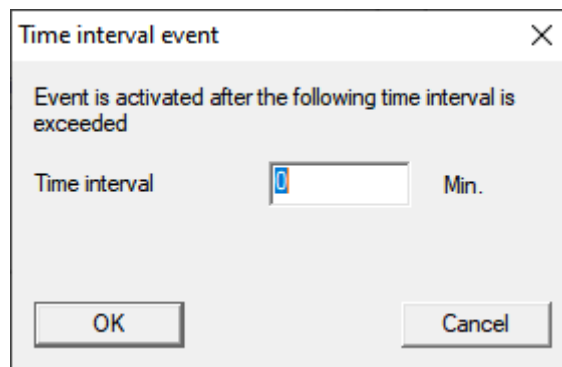


Wait for timer

1. In the area "Events" click the button **New**.  
↳ The window "New Event" opens.



2. Enter a name and a description.
3. In the dropdown menu ▼ **Type** select the entry "Time interval".
4. Click on the button **Configure event**.  
↳ The window "Time interval event" opens.



5. Specify the time delay between RingCast start and LSM backup start.



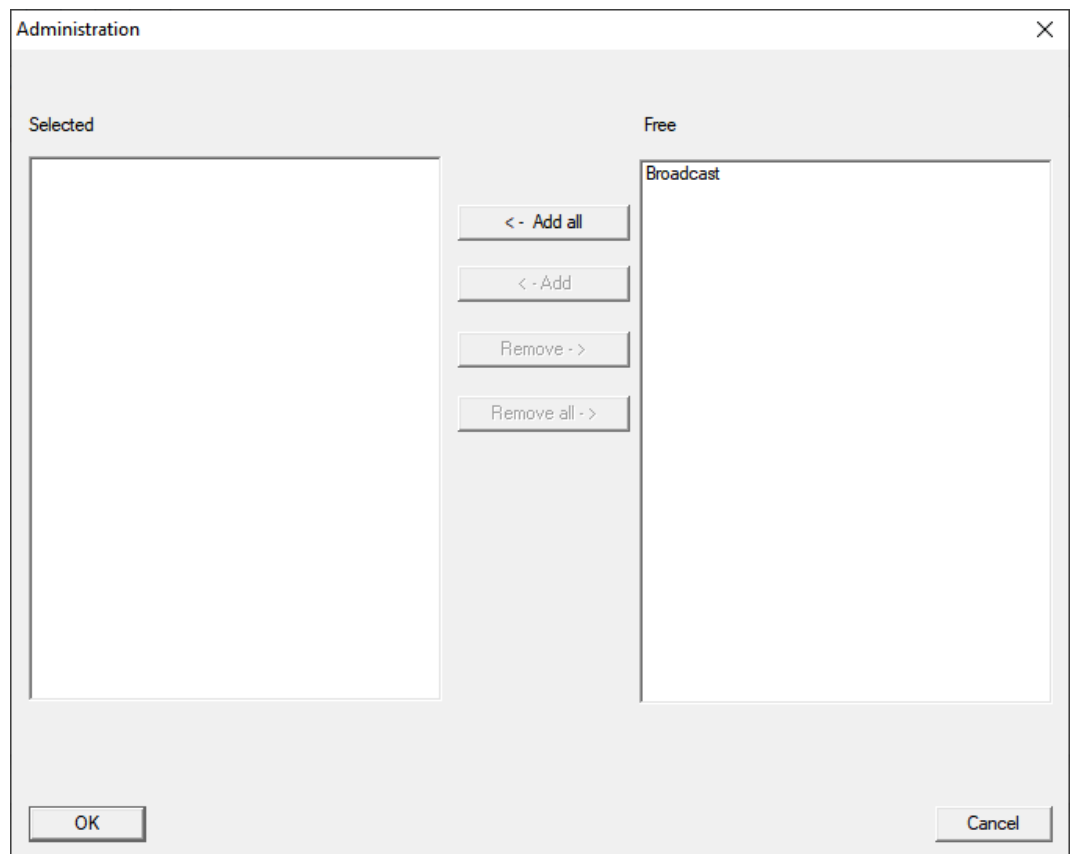
#### NOTE

##### RingCast malfunction due to parallel transmission

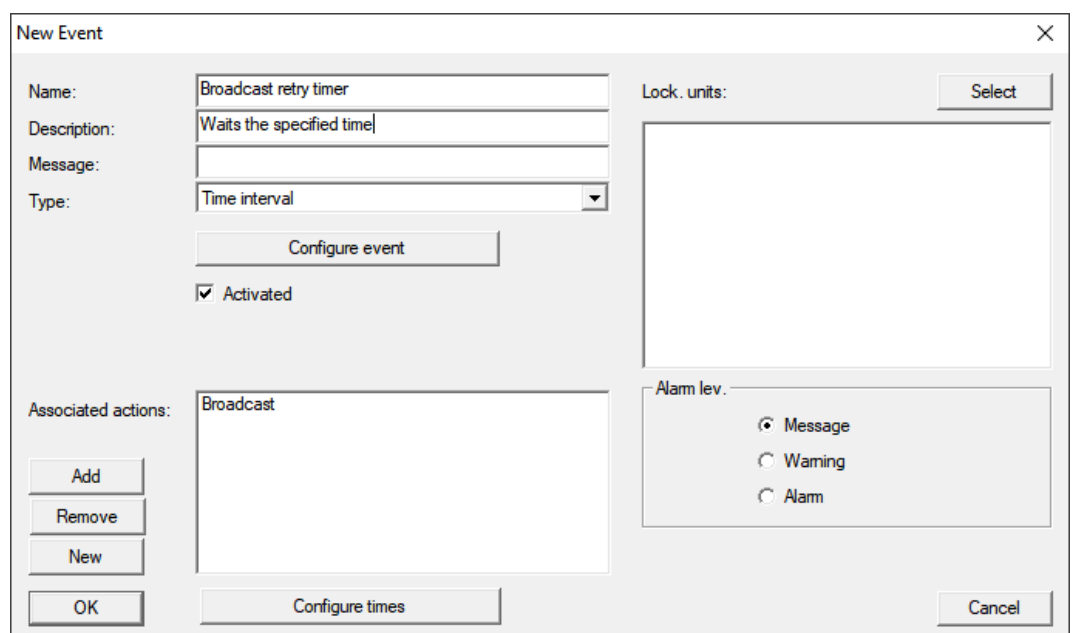
If LSM executes the reaction immediately, then the affected router nodes are already sending while the RingCast is not yet complete. This can interrupt the RingCast.

- Set a delay that is one minute longer than the maximum transmission time of the RingCast (see *Maximum transmission time in RingCast* [▶ 130]).

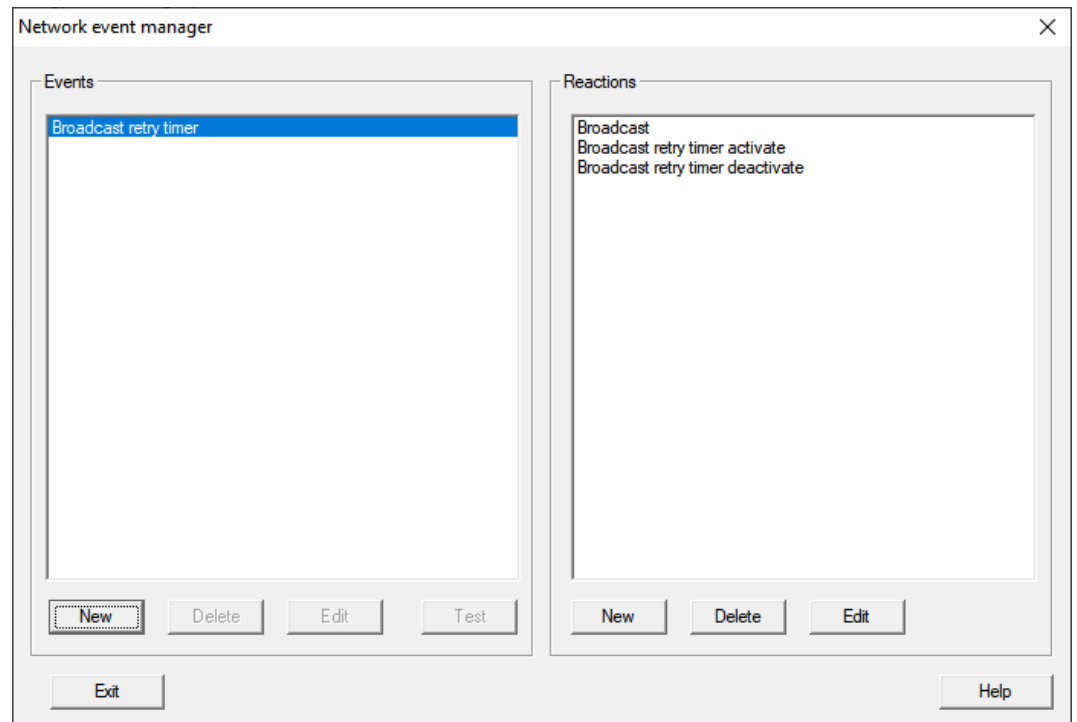
6. Click on the **OK** button.
  - ↳ The window "Time interval event" closes.
7. Click on the button **Add**.
  - ↳ The window "Administration" opens.



8. Mark the response which you have just created and which is to be triggered when the timer event expires without being interrupted.
9. Click the button  Add.
10. Click on the  OK button.
  - ↳ The "Administration" window closes.
  - ↳ Action is displayed in the list of actions associated with the event.

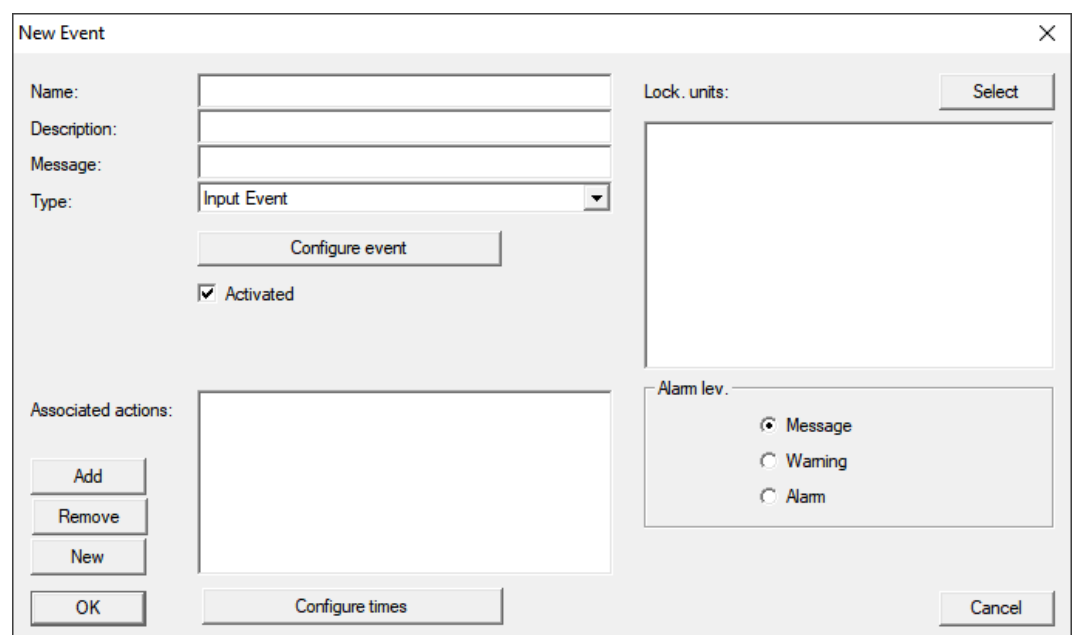


11. Click on the **OK** button.
  - ↳ The "New Event" window closes.
  - ↳ "Reactions" receives two additional entries with the endings "Deactivate" and "Activate".



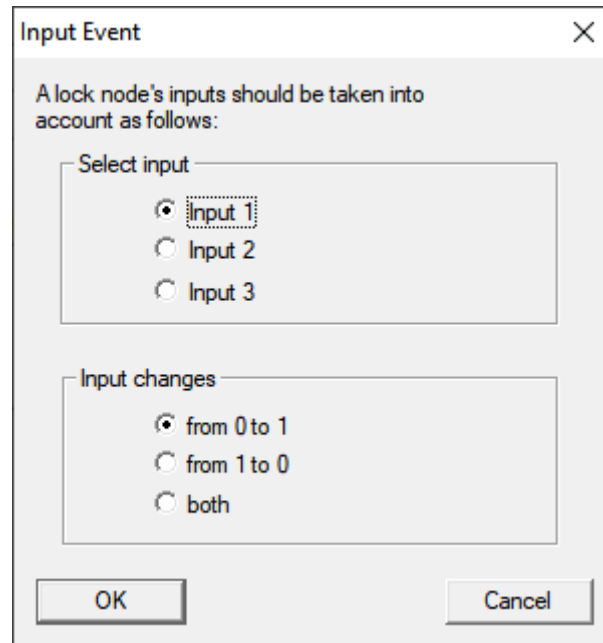
### Starting the timer

1. In the area "Events" click the button **New**.
  - ↳ The window "New Event" opens.

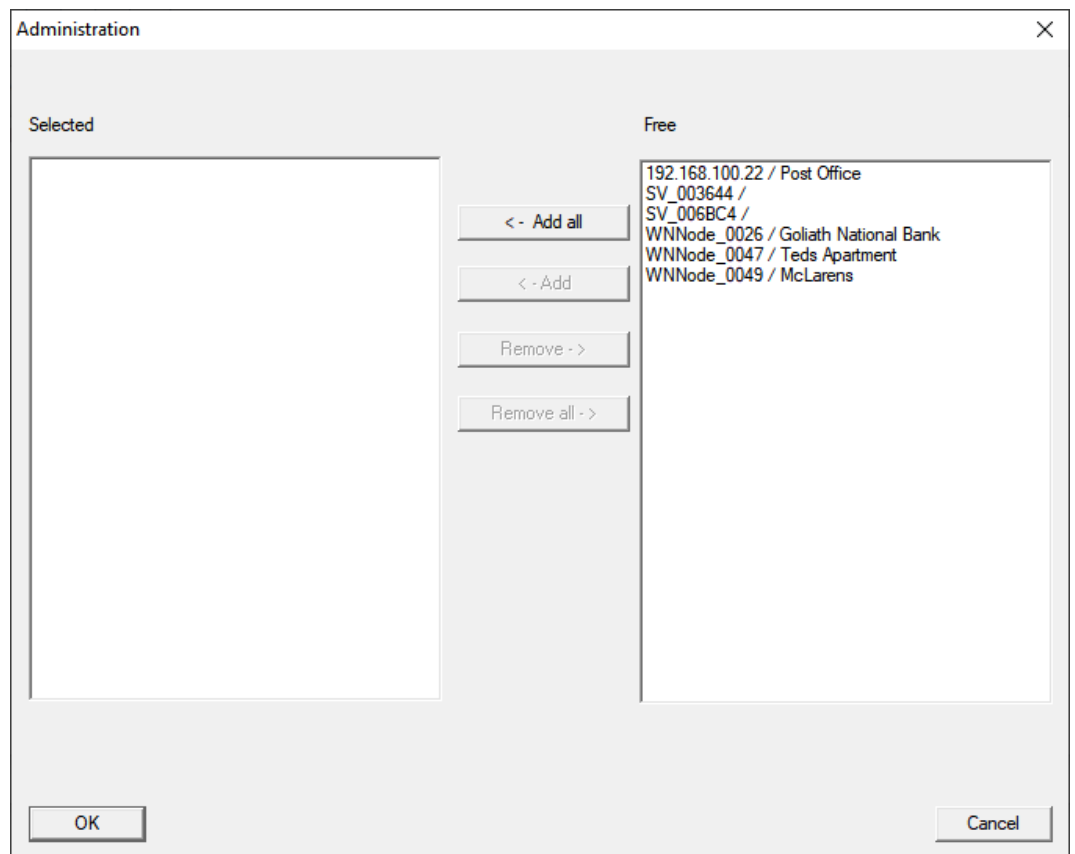


2. Enter a name and a description.

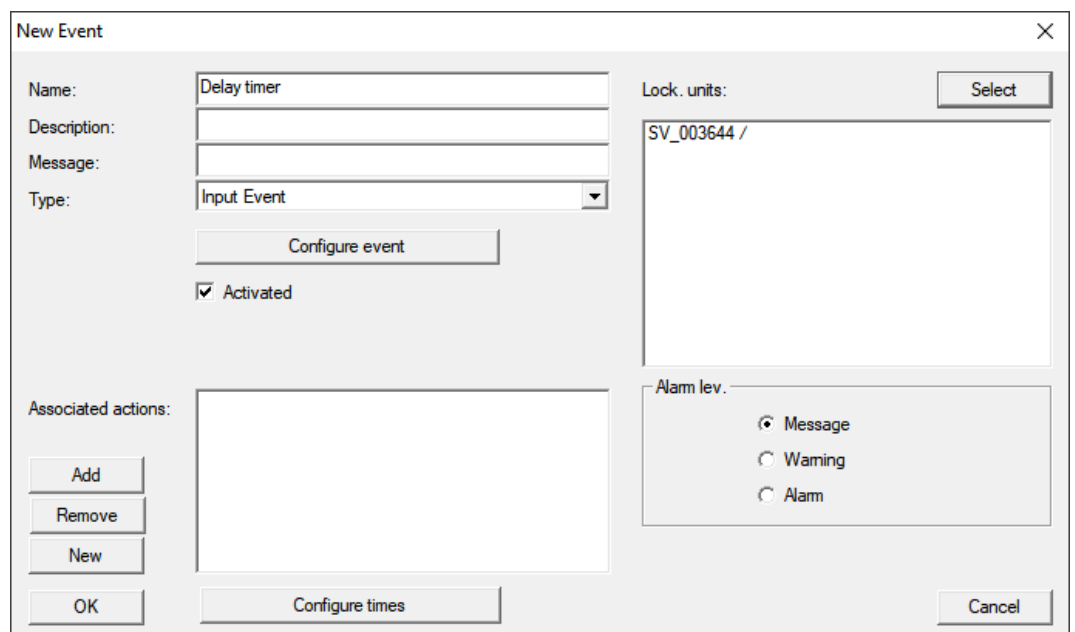
3. In the dropdown menu ▼ **Type** select the entry "Input Event".
4. Click on the button **Configure event**.
  - ↳ The window "Input Event" opens.



5. In the area "Select input" select the input that triggers your RingCast.
6. In the area "Input changes" select when your RingCast starts.
  - from 0 to 1: RingCast starts when the signal is present.
  - from 1 to 0: RingCast starts when the signal is no longer present.
  - both: RingCast starts when the signal is present and when it is no longer present.
7. Click on the **OK** button.
  - ↳ The "Input Event" window closes.
8. Click on the button **Select**.
  - ↳ The window "Administration" opens.



9. Mark the router that is the initiator in your RingCast (the RouterNode that gets the input first).
10. Click on the button  Add.
  - ↳ The "Administration" window closes.
  - ↳ RouterNode is displayed in the list of locking devices associated with the event.

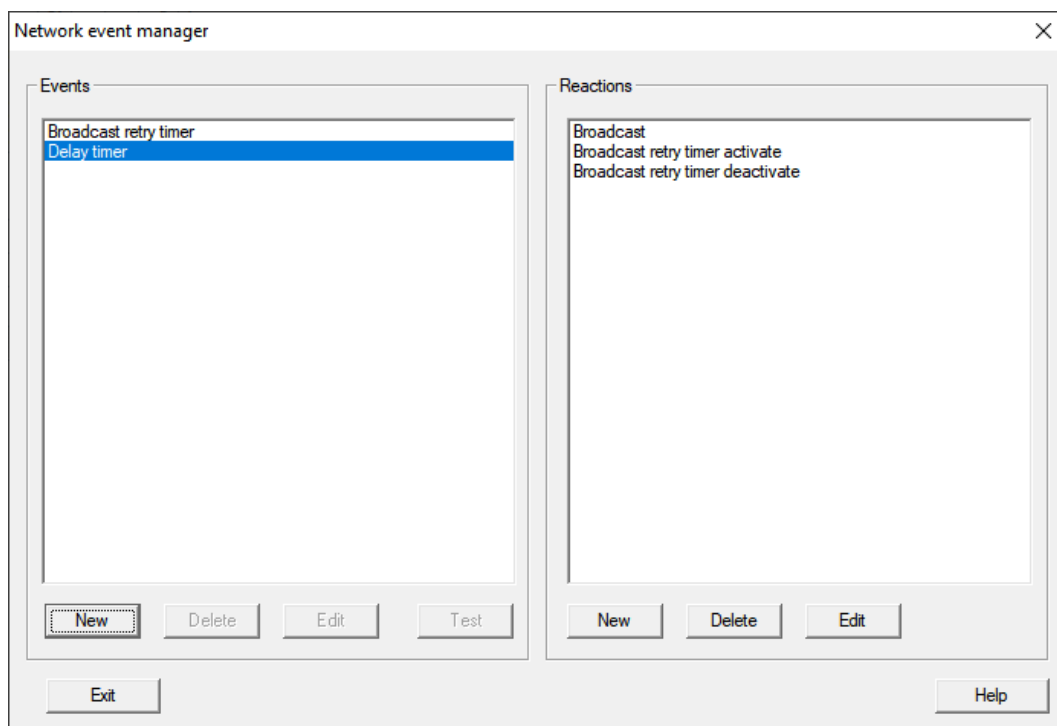


11. Click on the button **Add**.
  - ↳ The window "Administration" opens.
12. From the responses you created earlier, mark the one with the ending "activate".
13. Click the button **Add**.
14. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ Action is displayed in the list of actions associated with the event.

The screenshot shows the "New Event" dialog box. The "Name" field is filled with "Delay timer". The "Type" dropdown is set to "Input Event". The "Activated" checkbox is checked. The "Associated actions" list contains "Broadcast retry timer activate". The "Alarm lev." section has "Message" selected. The "Lock units" section shows "SV\_003644 /". The "Add" button in the "Associated actions" section is highlighted with a dotted border.

15. Click on the **OK** button.
  - ↳ The "New Event" window closes.
- ↳ LSM backup is set up.





### Cancel timer event

- ✓ On the central output router, at least one digital output is set to "Input receipt short" or "Input receipt static" eingestellt (see *RouterNode: Digital output* [▶ 76]).
1. At the central output router, connect a free input input to a digital output with input acknowledgement (see *Central output router* [▶ 137]).
  2. Via | Network | select the entry **Event manager**.
    - ↳ The window "Network event manager" opens.
  3. In the area "Events" click the button **New**.
    - ↳ The window "New Event" opens.
  4. Enter a name for the event, e.g. "Backup abort".
  5. In the dropdown menu ▼ **Type** select the entry "Input Event".
  6. Click on the button **Configure event**.
    - ↳ The window "Input Event" opens.
  7. In the "Select input" area, select the input to which the central output router's acknowledgement is to be created.
  8. In the area "Input changes" select the option  from 1 to 0.
  9. Click on the **OK** button.
    - ↳ The window "Input Event" closes.
  10. Click on the button **Add**.
    - ↳ The window "Administration" opens.
  11. From the responses created earlier, select the one with the ending "activate".

12. Click the button `+` Add .
    - ↳ Response is
  13. Click on the `OK` button.
    - ↳ window "Administration" closes.
    - ↳ Action is displayed in the list of actions associated with the event.
  14. Click on the `OK` button.
    - ↳ The "Network event manager" window closes.
- ↳ LSM backup is set up.

Transfer the changes to the communication node assigned to your router node (see *LSM import* [▶ 65]).

For more information on setting up an event and a reaction, refer to the LSM manual.

#### 6.4.5.4 Maximum transmission time in RingCast

The RingCast also transmits data wirelessly. Wireless transmission is naturally slower than the Ethernet interface. Depending on the protection function selected, the broadcast to the locking devices is also repeated. This results in a total transmission time for the RingCast. You can calculate the maximum transmission time of your RingCast using the following formula:

**Transmission time = Number of RouterNodes in the RingCast \* Broadcast duration \* Number of Broadcasts per RouterNode + forwarding time \* Number of RouterNodes in the RingCast**

Number of RouterNodes	You can see the number of RouterNodes in the overview (see <i>Overview</i> [▶ 178]) or when creating and editing the RingCast (see <i>Adding a RingCast</i> [▶ 133]).
Broadcast duration	The duration of the broadcast is five seconds. If all LockNodes as well as all RouterNodes in the RingCast support Fast Wake-Up (see <i>Firmware information</i> [▶ 39]), the broadcast duration is one second. If a device does not support Fast Wake-Up, you will have to count with five seconds for the calculation.

Number of Broadcasts per RouterNode (depending on the response set in ▼ Input)	"Input"	No broadcast
	"Block lock"	1x (if input acknowledgement is not active) 4x (if input acknowledgement is active)
	"Amok function"	1x
	"Emergency release"	1x
	"Remote opening"	1x
	"Activation"	1x (if input acknowledgement is not active) 4x (if input acknowledgement is active)
Forwarding time	The maximum forwarding time is five seconds. The forwarding time depends on the transmission medium (see <i>Transmission paths</i> [▶ 13]) and can be shorter.	

#### Calculation example (50 RouterNodes) with long broadcast duration and Block lock with input acknowledgement

Transmission time = 50 RouterNodes in the RingCast \* 5 s \* 4 Broadcasts + 5 s \* 50 RouterNodes in RingCast

The transmission time is up to 1000 seconds.

#### Calculation example (50 RouterNodes) with short broadcast duration and Block lock without input acknowledgement

Transmission time = 50 RouterNodes in RingCast \* 1 s \* 1 Broadcast + 5 s \* 50 RouterNodes in RingCast

The transmission time is up to 300 seconds.

#### 6.4.5.5 Preparing RouterNode for RingCast



#### NOTE

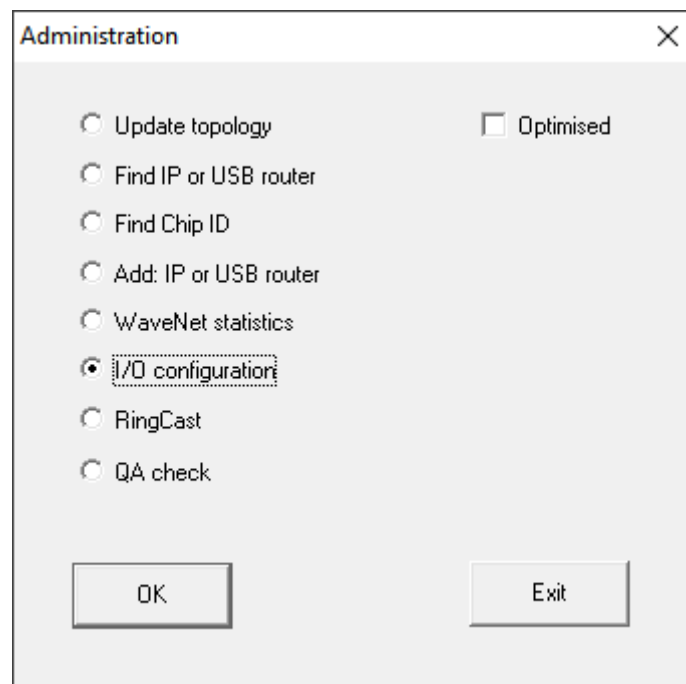
#### Firmware dependent availability of RingCast for RouterNodes

RingCast support is firmware dependent (see *Firmware information* [▶ 39]).

■ If necessary, update the firmware (see *Updating firmware* [▶ 32]).

Prepare the RouterNodes for the RingCast:

- ✓ In the Wavenet radio network, at least two different RingCast-capable RouterNodes are configured and "online" (see *Firmware information* [[▶ 39](#)]).
  - ✓ At least one locking device is assigned to each RouterNode of the planned RingCast. Both locking devices are "online".
1. Open the WaveNet Manager.
  2. Right-click on the first RouterNode 2.
    - ↳ Window "Administration" opens.



3. Select the option  I/O configuration.
4. Click on the button **OK**.
  - ↳ Window "Administration" closes.
  - ↳ Window "I/O configuration" opens.
5. Optional: For example, for ▼ **Output 1** "Input receipt static", to be able to control a signal device during deactivation.
6. In the drop-down menu ▼ **Input** select the desired entry of the corresponding response (see *RouterNode: Digital input* [[▶ 79](#)]).
7. In the drop-down menu ▼ **Delay [s]** select the entry "RingCast".
8. Click on the button **Select LN**.
9. Check whether all required LockNodes are selected. (*When the I/O configuration of the router is set up for the first time, all LockNodes are included.*)
10. Select your protocol generation from the drop-down menu ▼ **Protocol generation**

**NOTE****Protocol generation in the LSM**

The log generation is displayed in the LSM in the locking system properties on the tab page [Name] in the area "Protocol generation".

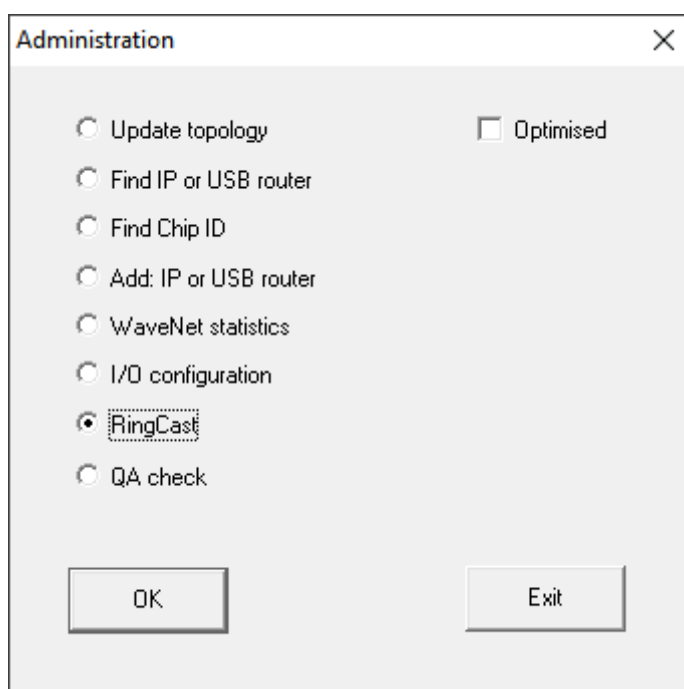
11. Enter the locking system password.
12. Click on the **OK** button.
13. Make the same settings on the other RouterNodes 2 as well.

## 6.4.5.6 Adding a RingCast

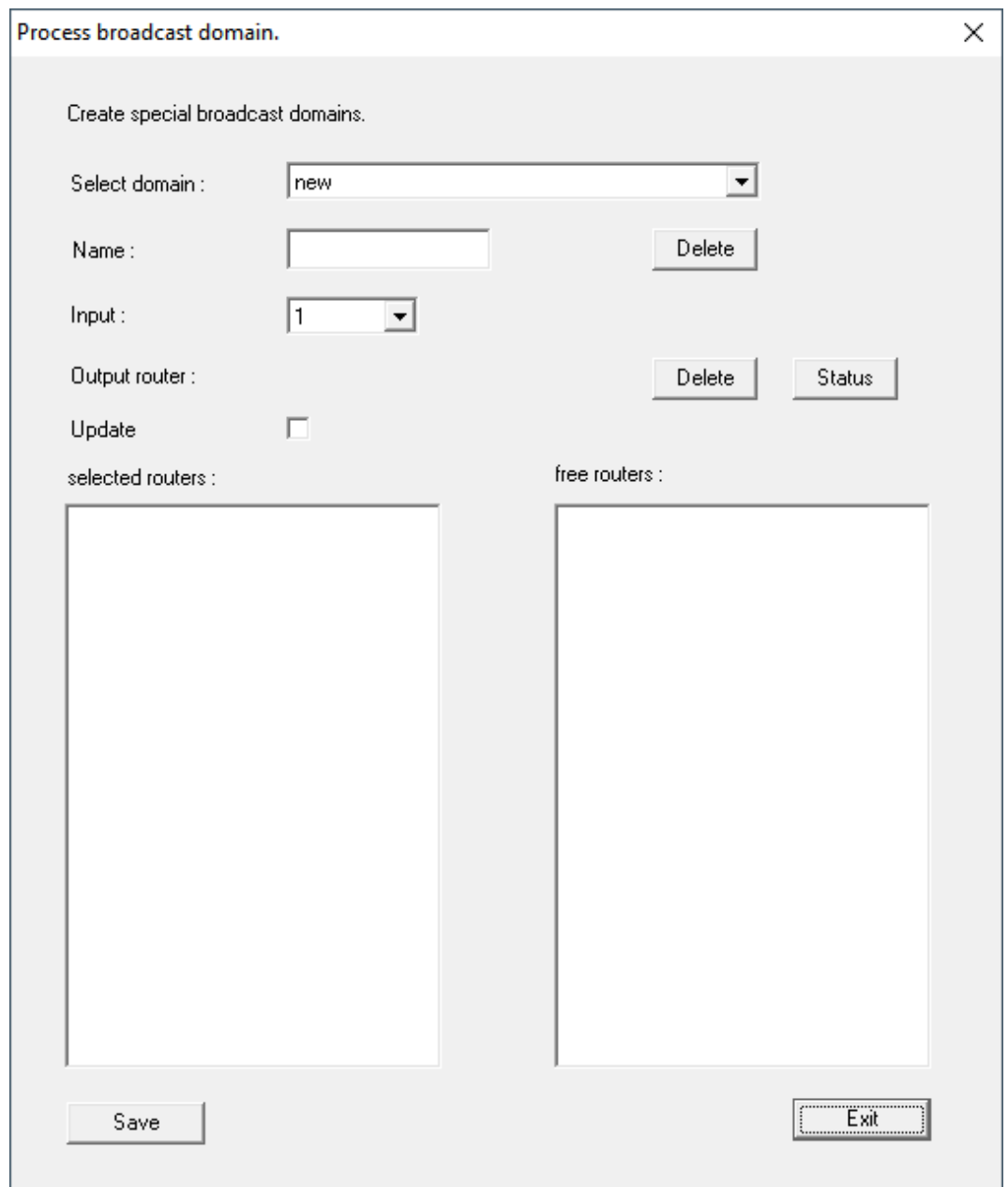
**NOTE****Recalculating the RingCast**

If you replace or delete a RouterNode in the RingCast or change its RingCast-relevant IO configuration, the RingCast is automatically recalculated after saving the changes and confirming the request.

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes and LockNodes connected to power.
  - ✓ RouterNodes and LockNodes imported into WaveNet topology (see *Finding and adding devices* [▶ 48]).
  - ✓ RouterNodes for RingCast prepared (see *Preparing RouterNode for RingCast* [▶ 131]).
1. Right-click on the WaveNet XX\_X entry.
    - ↳ The window "Administration" opens.



2. Select the option  RingCast.
3. Click on the button .
  - ↳ The "Administration" window closes.
  - ↳ The window "Edit radio domains" opens.



Process broadcast domain. [X]

Create special broadcast domains.

Select domain : new

Name : [ ] [Delete]

Input : 1

Output router : [ ] [Delete] [Status]

Update

selected routers : [ ]

free routers : [ ]

[Save] [Exit]

4. In the dropdown menu ▼ **Select domain** select an input for which in ▼ **Delay [s]** you have selected "RingCast".



- ↳ In the field "selected routers" all RouterNode2 appear for which at the beginning at ▼ **Delay [s]** you have selected the input "RingCast" (=Domain).

The dialog box titled "Process broadcast domain." contains the following fields and controls:

- Create special broadcast domains.**
- Select domain :** A dropdown menu with "Input1" selected.
- Name :** A text box containing "Input1" and a "Delete" button.
- Input :** A dropdown menu with "1" selected.
- Output router :** A text box containing "0x5530" and "Delete" and "Status" buttons.
- Update** checkbox, which is checked.
- selected routers :** A list box containing two entries: "RN\_ER (0x0006\_0x0021; 89003644)" and "RN\_ER (0x000A\_0x0041; 890068C4)".
- free routers :** An empty list box.
- Save** and **Exit** buttons at the bottom.

5. Click the button **Save**.
6. Click the button **Exit**.
  - ↳ The "Edit radio domains" window closes.
  - ↳ The window "WaveNetManager" opens.

The dialog box titled "WaveNetManager" displays a question mark icon and the text: "Changes have been made. Do you want to update the broadcast domain?". At the bottom, there are two buttons: "Ja" (Yes) and "Nein" (No).



7. Click on the button **Yes**.
  - ↳ The "WaveNetManager" window closes.
  - ↳ Changes will be updated.
- ↳ The RingCast is created and will be visible in the WaveNet Manager after a short time.

```

RingCast
├── Input1(0)
│   ├── RN_ER (0x0006_0x0021; 89003644)
│   │   └── RN_ER (0x000E_0x0041; 0002A8B2)
│   │       └── RN_ER (0x0006_0x0021; 89003644) ###

```

Save the new settings and exit the WaveNet Manager.

#### 6.4.5.7 Central output router

The availability of this function is firmware dependent (see [Firmware information](#) [▶ 39]).

You can read out the firmware version of your RouterNode via the browser interface (see [Browser interface](#) [▶ 148]) or the OAM tool (see [Updating firmware](#) [▶ 32]).

#### Adding the central output router

In RingCast you can configure any second generation RouterNode (with Ethernet interface, WNM.RN2.ER.IO from firmware version 40.10) as central output router. The central output router first collects the received input acknowledgements of all other Ethernet router nodes (ER) involved in the RingCast and only then sends its own input acknowledgement or sets the output as set in [RouterNode: Digital output](#) [▶ 76]. All other RouterNodes set the input acknowledgement / output as previously set.

Transmission takes place via Ethernet. Its output is therefore always switched as the last output of the entire RingCast and indicates that all locking devices involved in the RingCast via Ethernet RouterNodes have received the command.



#### NOTE

#### Central output router in RingCast with R/CR router nodes

The central output router receives the input acknowledgement of the participating router nodes exclusively via an Ethernet connection. The central output router therefore ignores the status of router nodes that are not Ethernet router nodes (.ER). If you are using the central output router and your

RingCast also contains router nodes without an Ethernet interface, the central output router's input acknowledgement only means that all locking devices assigned to an Ethernet router node have received the command.

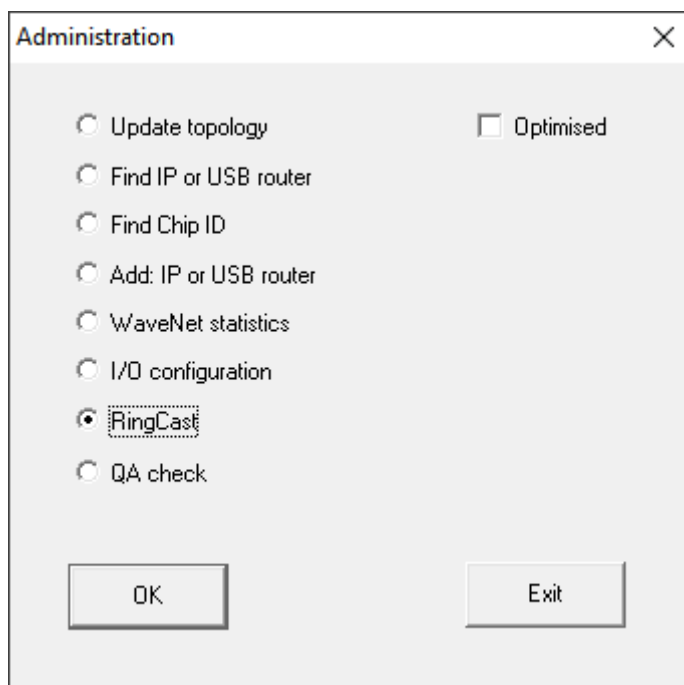
- ❑ Check the status of other router nodes (R/CR) independently of the central output router manually (see *Test reachability (LSM)* [▶ 186] and *RouterNodes* [▶ 183] or *IO Status and LockNode responsiveness* [▶ 188]).

---

If the central output router does not set its input acknowledgement or does not switch its output, this may be due to these reasons, among others:

- ❑ One or more RouterNodes have not received the data packet.
- ❑ One or more RouterNodes have not reached one or more LockNodes.
- ❑ Ethernet connection to one or more RouterNodes is interrupted. The RouterNodes could have received the data packet wirelessly, but could no longer return their input acknowledgements due to the interrupted Ethernet connection.

1. Right-click on the entry "WaveNet\_xx\_x" in the WaveNet Manager.
  - ↳ The window "Administration" opens.



2. Select the option  RingCast.
3. Click on the button .
  - ↳ The "Administration" window closes.
  - ↳ The window "Edit radio domains" opens.

Process broadcast domain. [X]

Create special broadcast domains.

Select domain :

Name :

Input :

Output router :

Update

selected routers :

```
RN_ER (0x0006_0x0021; 89003644)
RN_ER (0x000A_0x0041; 890068C4)
```

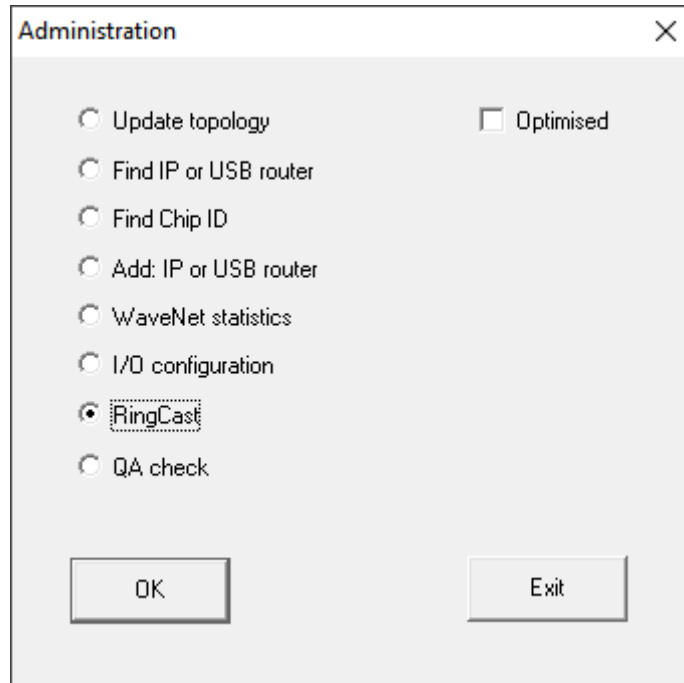
free routers :

4. In the drop-down list ▼ **Select domain** select the name of the domain whose central output router you want to specify.
  5. Select the RouterNode you want to set as the central output router.
  6. Click on the button **Set**.
  7. Click on the button **Save**.
  8. Click on the **Exit** button.
- ↳ The central output router is set.

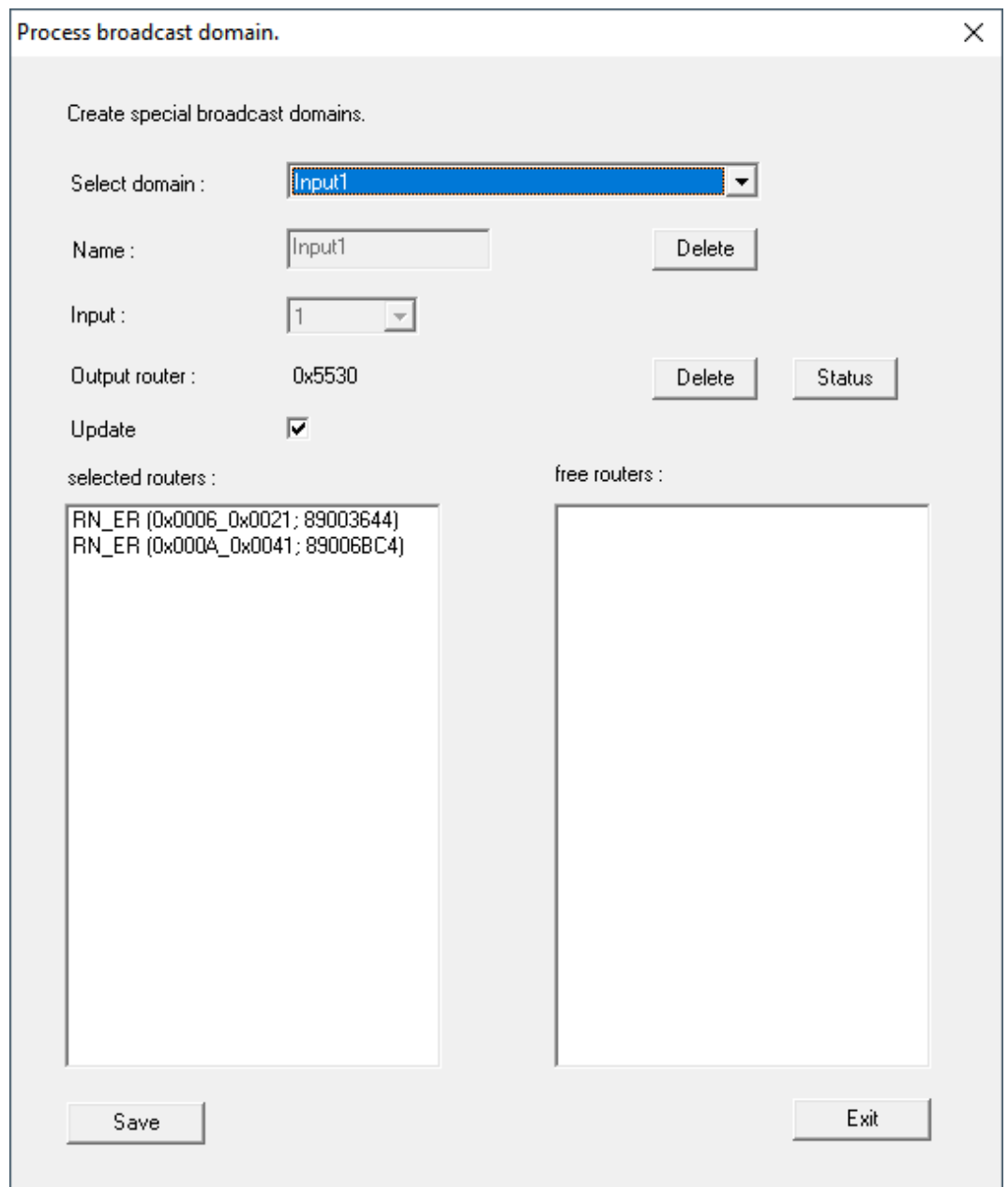
#### Delete central output router

Without a central output router, all RouterNodes (including the former central output router) set the input acknowledgement / output as previously set.

1. Right-click on the entry "WaveNet\_xx\_x" in the WaveNet Manager.
  - ↳ The window "Administration" opens.



2. Select the option  RingCast.
3. Click on the button .
- ↳ The "Administration" window closes.
- ↳ The window "Edit radio domains" opens.



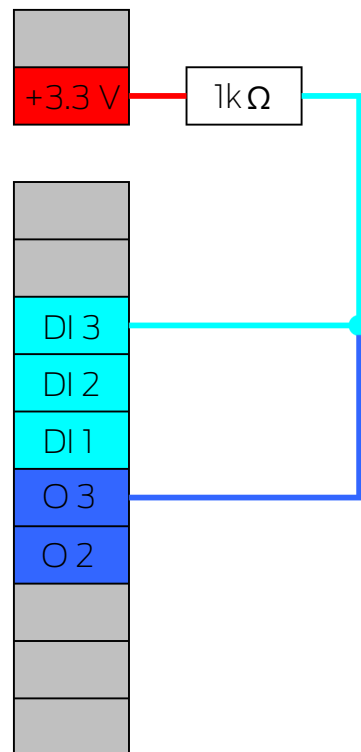
4. Click on the lower button **Delete**.
  - ↳ Central output router is flagged for deletion.
5. Click on the button **Save**.
6. Click on the **Exit** button.
  - ↳ Central output router is deleted. The completion of the RingCast is no longer displayed.

### Report completion of RingCast to LSM

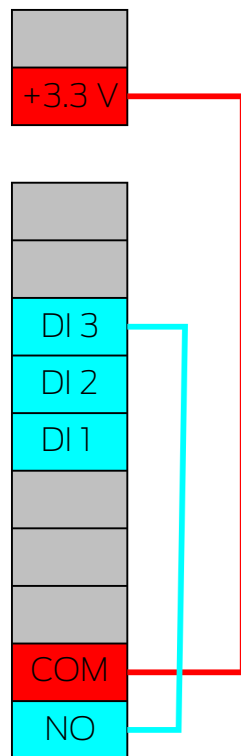
RouterNodes cannot report the input acknowledgement (or the switching of an output) directly to LSM. To do this, use a digital input and forward its status to LSM (see *RouterNode: Digital input* [▶ 79]). This allows you to react to the successful completion of a RingCast in the event manager.

This illustration shows the wiring when the input acknowledgement is output on O3 or O2. Connect O3/O2 to a free digital input as shown and forward this to the LSM. The switching behaviour is inverted by the pull-up resistor:

- Input acknowledgement active: Level at digital input 0 (Low)
- Input acknowledgement not active: Level at digital input 1 (High)



This illustration shows the wiring when the input acknowledgement is output on O1. Connect O1 to a free digital input as shown and forward this to the LSM.



#### 6.4.5.8 RingCast function test

The RingCast has no self-test function.



### WARNING

#### Impairment or failure of protective functions due to changed conditions

The activation of the protection functions in RingCast is based on wireless connections and Ethernet connections. Wireless connections in particular can be affected by changing environmental conditions (see *Radio network* [▶ 21] und *Challenges in wireless networks* [▶ 24]). This also influences the activation of the protective functions in the RingCast and can jeopardise the safety of persons and property that are additionally protected by the protective functions in the RingCast, for example.

1. Test the protective functions at least once a month (see *RingCast function test* [▶ 143]).
2. If necessary, also observe other guidelines or regulations that are relevant for your locking system (especially for escape and rescue routes and fire protection. You are solely responsible for ensuring compliance with these guidelines and regulations).

## Change in the sequence of emergency functions due to malfunctions

SimonsVoss and "Made in Germany" stand for maximum safety and reliability. In individual cases, however, malfunctions of your devices cannot be ruled out. This may pose a risk to the safety of persons and property, which are additionally protected by the protective functions in the RingCast.

1. You should test your devices at least once a month (see *Device function test* [▶ 187] Shorter intervals may also be required according to other regulations concerning your overall system).
2. Test the protective functions at least once a month (see *RingCast function test* [▶ 143]).

---

Switch the corresponding input on the initiator and check:

- whether the locks react as desired (see also *RouterNode: Digital input* [▶ 79]).
- whether the output set on the RouterNode shows the acknowledgement by switching as desired (see also *RouterNode: Digital output* [▶ 76]).

### Test with central output router



#### NOTE

#### Central output router in RingCast with R/CR router nodes

The central output router receives the input acknowledgement of the participating router nodes exclusively via an Ethernet connection. The central output router therefore ignores the status of router nodes that are not Ethernet router nodes (.ER). If you are using the central output router and your RingCast also contains router nodes without an Ethernet interface, the central output router's input acknowledgement only means that all locking devices assigned to an Ethernet router node have received the command.

- Check the status of other router nodes (R/CR) independently of the central output router manually (see *Test reachability (LSM)* [▶ 186] and *RouterNodes* [▶ 183] or *IO Status and LockNode responsiveness* [▶ 188]).

---

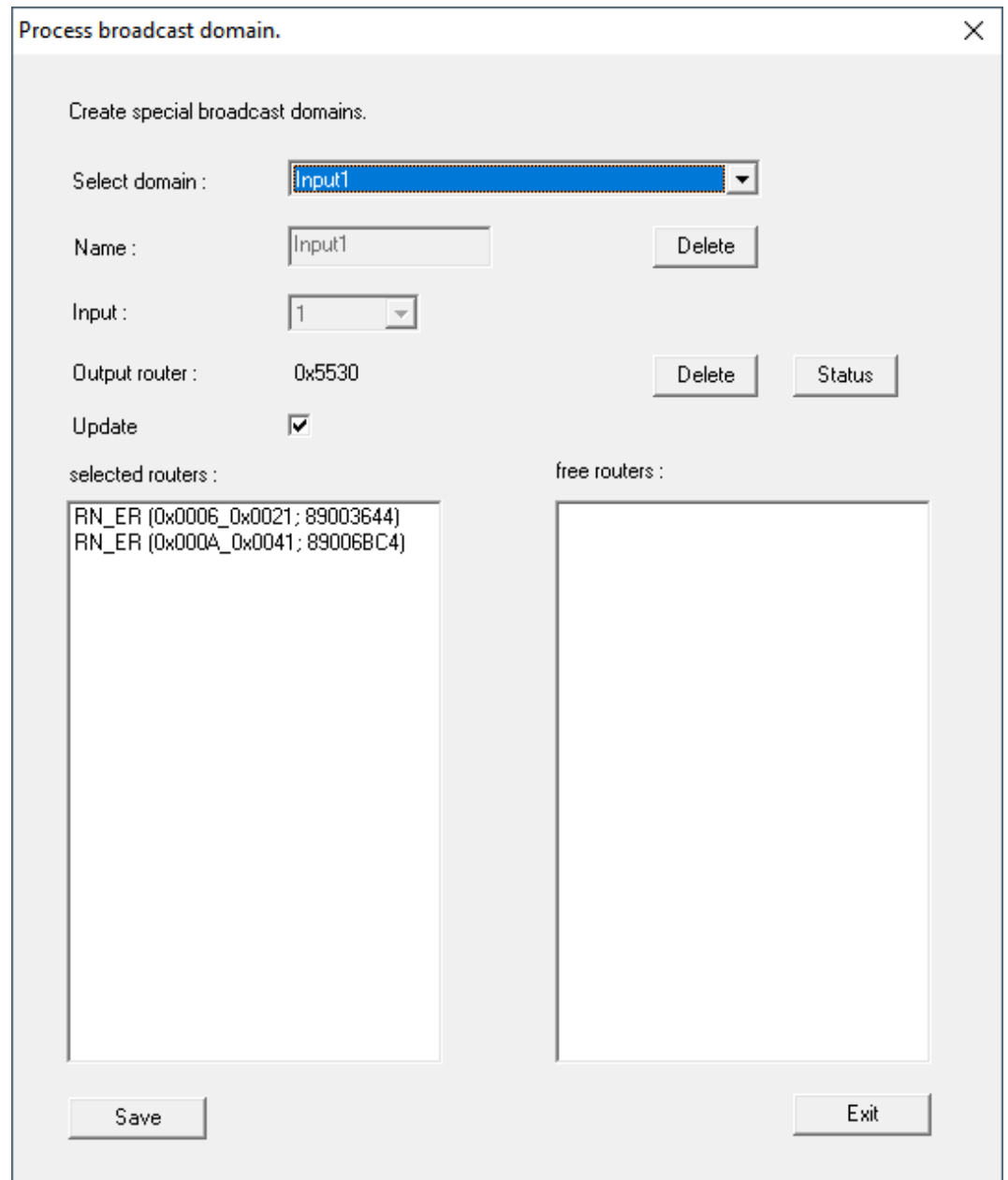
The use of a central output router (see *Central output router* [▶ 137]) simplifies the test of the RingCast considerably. Switch the corresponding input at the initiator and check whether the central output router sends an input acknowledgement or switches the corresponding output. If the output does not switch, then check which RouterNodes have caused problems:

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
1. Click with the right mouse button on the RingCast entry you want to test.



- In the drop-down menu ▼ **Select domain** select the input whose RingCast you want to test.

↳ The window "Edit radio domains" opens.

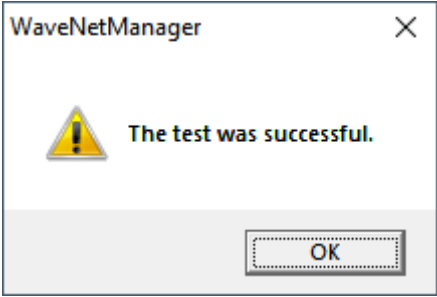

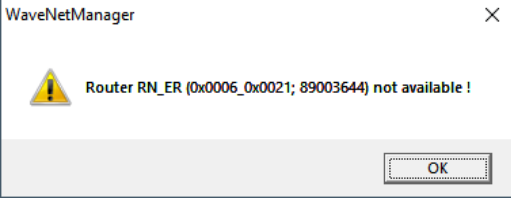

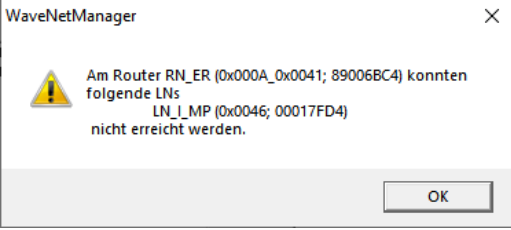



The screenshot shows a dialog box titled "Process broadcast domain." with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Create special broadcast domains.**
- Select domain :** A dropdown menu with "Input1" selected.
- Name :** A text input field containing "Input1" and a "Delete" button to its right.
- Input :** A dropdown menu with "1" selected.
- Output router :** A text input field containing "0x5530" and two buttons to its right: "Delete" and "Status".
- Update :** A checked checkbox.
- selected routers :** A list box containing two entries: "RN\_ER (0x0006\_0x0021; 89003644)" and "RN\_ER (0x000A\_0x0041; 890068C4)".
- free routers :** An empty list box.
- Save** and **Exit** buttons at the bottom.

- Click on the button **Status**.

↳ RingCast is tested.

 <p>WaveNetManager</p> <p> <b>The test was successful.</b></p> <p>OK</p>	 <p>WaveNetManager</p> <p> Router RN_ER (0x0006_0x0021; 89003644) not available !</p> <p>OK</p>  <p>WaveNetManager</p> <p> Am Router RN_ER (0x000A_0x0041; 89006BC4) konnten folgende LNs LN_LMP (0x0046; 00017FD4) nicht erreicht werden.</p> <p>OK</p>
<p>The RingCast was able to address all locking devices.</p>	<p>The RingCast could not be closed. Possible causes (see also <i>Central output router</i> [<a href="#">▶ 137</a>):</p> <ul style="list-style-type: none"> <li>■ One or more RouterNodes have not received the data packet.</li> <li>■ One or more RouterNodes have not reached one or more LockNodes.</li> <li>■ Ethernet connection to one or more RouterNodes is interrupted. The RouterNodes could have received the data packet wirelessly, but could no longer return their input acknowledgements due to the interrupted Ethernet connection.</li> </ul> <ol style="list-style-type: none"> <li>1. Check the reachability of the RouterNodes mentioned (see <i>RouterNodes</i> [<a href="#">▶ 183</a>] und <i>Test reachability (LSM)</i> [<a href="#">▶ 186</a>]).</li> <li>2. Check the reachability of the LockNodes (see <i>LockNodes</i> [<a href="#">▶ 185</a>] und <i>Test reachability (LSM)</i> [<a href="#">▶ 186</a>]).</li> <li>3. Check the last responses of the LockNodes (see <i>IO Status and LockNode responsiveness</i> [<a href="#">▶ 188</a>]).</li> </ol>

## 6.4.5.9 Deleting RingCast

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes and LockNodes connected to power supply.
1. In the overview, right-click on the top entry of the RingCast you want to delete.
    - ↳ The window "Edit radio domains" opens.

Process broadcast domain. [X]

Create special broadcast domains.

Select domain : new [v]

Name : [ ] [Delete]

Input : 1 [v]

Output router : [ ] [Delete] [Status]

Update

selected routers : [ ]

free routers : [ ]

[Save] [Exit]

2. In the drop-down menu ▼ **Select domain** select the domain (input) whose RingCast you want to delete.
3. Click the Delete button [Delete] below the drop-down menus ▼ **Select domain**.
  - ↳ RingCast of the domain is flagged for deletion.

4. Click on the button **Save**.
  5. Click on the **Exit** button.
- ↳ RingCast of the domain is deleted and is no longer displayed in the overview.

Repeat the steps until you have deleted all desired RingCasts. You can then reconfigure the IO configuration of the RouterNodes at the corresponding inputs (see *RouterNode: Digital input* [▶ 79]).

## 6.4.6 Device-specific settings

### 6.4.6.1 RouterNodes

You can set the IO configuration for each RouterNode individually (see *I/O configuration and protection functions* [▶ 69]) and set router-specific settings (interface password and IP change by the OAM tool) in the browser interface (see *Browser interface* [▶ 148]).

#### Browser interface

You can use the Ethernet interface in the browser to configure the following for RouterNodes, GatewayNodes and SmartBridges:

- Allow changes using the OAM tool
- Password for the web interface
- IP address/DHCP mode
- Opening and closing the SMTP port

#### Launching

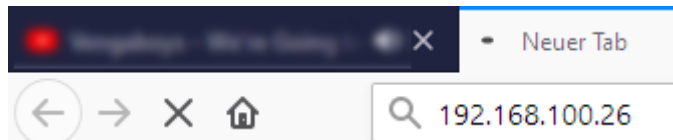
You receive the device with the following factory configuration:

IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

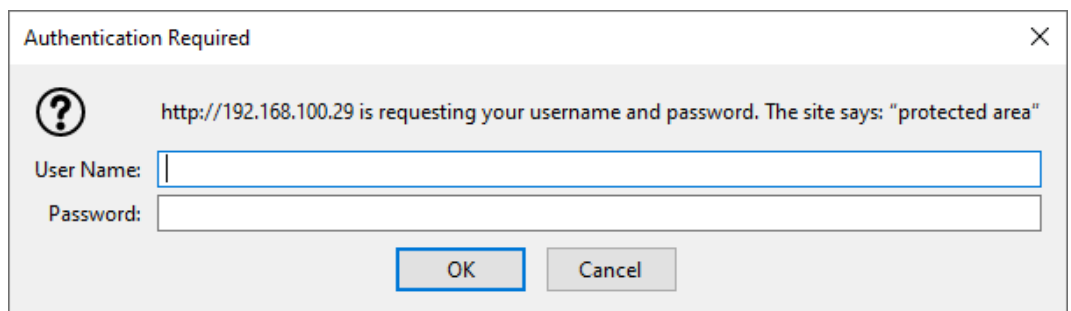
The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

Change the default password after you launch for the first time.

- ✓ RouterNode IP known (see *Determining and setting the IP address* [▶ 49]).
  - ✓ Browser open.
  - ✓ User credentials known for the browser interface (name and password).
1. Enter the IP address in your browser's address field.



2. Press the Enter key to confirm.
  - ↳ The "Authentication required" window will open.



3. Enter the login credentials.
4. Click on the **OK** button.
  - ↳ The browser interface system overview is visible.

OVERVIEW  
WAVENET  
CONNECTION

## System Information: Overview

### Version:

**Firmware version:** 40.11.00

### Basic network settings:

<b>MAC Address:</b>	94:50:89:00:36:44
<b>Host Name:</b>	SV_003644
<b>DHCP:</b>	On
<b>IP-Address:</b>	192.168.100.26
<b>Subnetmask:</b>	255.255.255.0
<b>Gateway:</b>	192.168.100.1
<b>DNS-Server1:</b>	192.168.100.1
<b>DNS-Server2:</b>	0.0.0.0
<b>SV Port:</b>	2101
<b>SV SecPort:</b>	2153

**NOTE**

Web interface can no longer be used with the default password with firmware 40.12 and above

The browser interface remains blocked in firmware version 40.12 or above until the default password has been changed.

- Change the default password.
- ↳ Browser interface is unblocked and settings can be changed.

**NOTE**

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

**Blocking/enable change to the IP address using the OAM tool**

If you do not enable the ▼ **OAM-Tool allow**, you will not be able to use the OAM tool to perform updates.

- ✓ Browser interface opened.
- 1. Open the [PORT] tab using | CONFIGURATION |.
  - ↳ You will see an overview of the TCP port settings for RouterNode 2.

NETWORK  
PORT  
ETHERNET INTERFACE  
WAVENET

## Configuration: port settings

**TCP port settings:**

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV connection timeout [s]:	<input type="text" value="30"/>
HTTP:	<input type="text" value="On"/> ▼
Telnet:	<input type="text" value="Off"/> ▼
OAM-Tool allow:	<input type="text" value="Yes"/> ▼

2. Select the option "Yes" (enable the OAM tool to change the IP) or the option "No" (block change to the IP by the OAM tool) from the ▼ **OAM-Tool allow** drop-down menu.

3. Click on the button **Save**.

↳ Changing the IP address using the OAM tool is locked/allowed.

### Change password

Some browsers do not register any spaces included at the start of a password, so do not begin your password with spaces.

✓ Browser interface opened.

1. Open the [PASSWORD] tab using | ADMINISTRATION |.

PAS SWORD  
CERTIFICATE  
FACTORY  
REBOOT

---

## Administration: Change password

---

**New password:**

<b>New password:</b>	<input type="text"/>
<b>Confirm password:</b>	<input type="text"/>

**Save password**

2. Enter your new password.

3. Repeat your new password.

4. Click on the **Save password** button.

↳ Password is now changed.

### Opening and closing the SMTP port

The SMTP port is open ex works and after each reset. As a general rule, ports that are not required should be closed. If you close the SMTP port, the OAM tool will no longer find RouterNode 2.

✓ Browser interface opened.

1. Open the [PORT] tab using | CONFIGURATION |.

↳ You will see an overview of the TCP port settings for RouterNode 2.

NETWORK  
PORT  
ETHERNET INTERFACE  
WAVENET

## Configuration: port settings

### TCP port settings:

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV connection timeout [s]:	<input type="text" value="30"/>
HTTP:	<input type="button" value="On"/> ▾
Telnet:	<input type="button" value="Off"/> ▾
OAM-Tool allow:	<input type="button" value="Yes"/> ▾

2. Select the "Yes" option (open SMTP port) or the "No" option (close SMTP port) from the ▼ SMTP Port drop-down menu.
  3. Click on the button **Save**.
- ↳ The SMTP port is open or closed.

### 6.4.6.2 LockNodes

You can set for each LockNode individually whether it reacts to broadcasts (see also *I/O configuration and protection functions* [[▶ 69](#)] and *LockNode* [[▶ 86](#)]).

## 6.5 Fault rectification

### 6.5.1 Improving signal quality

You can see the signal strength in the overview of the WaveNet Manager (see also *Check signal quality* [[▶ 180](#)]).

```

┌─── WaveNet_11_5
│   ┌─── RN_ER_ID (0x0006_0x0021; 89003644) | 192.168.100.26 192.168.100.26
│       └─── LN_I (0x0026; 0001DE87) -47dBm

```

### Unit of signal strength

The WaveNet Manager displays the signal strength as an RSSI value (Received Signal Strength) in dBm. This value is:

- Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.
- Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm (i.e. the smaller the amount), the better the reception.



### External antennas

An external antenna (see [Accessories \[▶ 17\]](#)) improves reception when correctly positioned. Connect the antenna to the intended slot and adjust the antenna so that the signal strength at the LockNode is improved.

#### 6.5.1.1 Assigning LockNodes to another RouterNode

The signal quality of the radio link between RouterNodes and LockNodes (and other RouterNodes) is influenced, among other things, by the following:

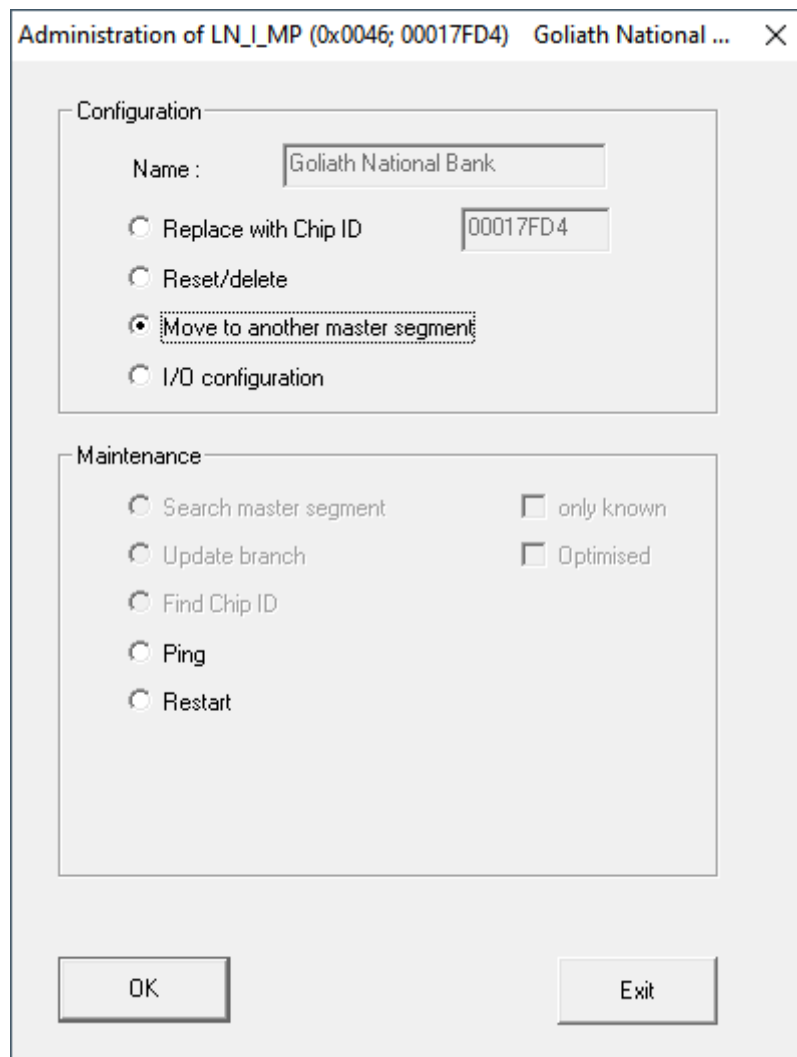
- Environmental conditions (interference signals, building materials)
- Centres distance

You can improve these conditions and thus the signal quality of the radio link between RouterNodes and LockNodes by assigning the LockNode to a RouterNode that is closer or less disturbed.

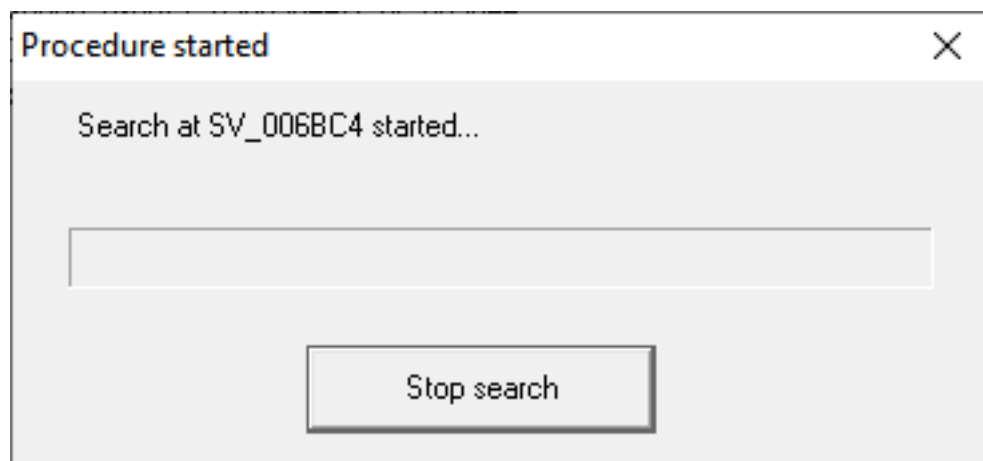
As long as you move the LockNode within the same CentralNode/Ethernet RouterNode segment, you can easily reassign the LockNode as described below. Otherwise, reset the LockNode in the WaveNet Manager and re-insert it at the planned RouterNode (see [Best Practice: Reset with the WaveNet Manager \[▶ 168\]](#) und [Adding Lock Nodes to WaveNet \[▶ 59\]](#)).

#### Reassigning a single LockNode to a RouterNode

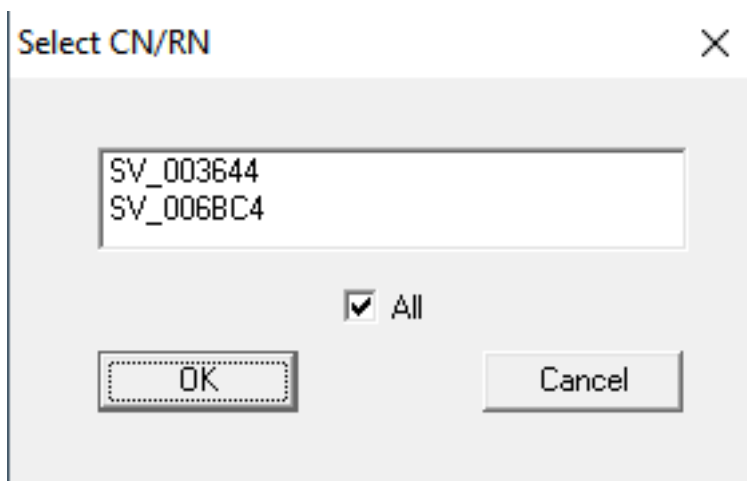
- ✓ WaveNet Manager opened via LSM (see [Best Practice: From the LSM software \[▶ 37\]](#))
1. Right-click on the LockNode entry that you want to assign to another RouterNode.
    - ↳ The window "Administration" opens.



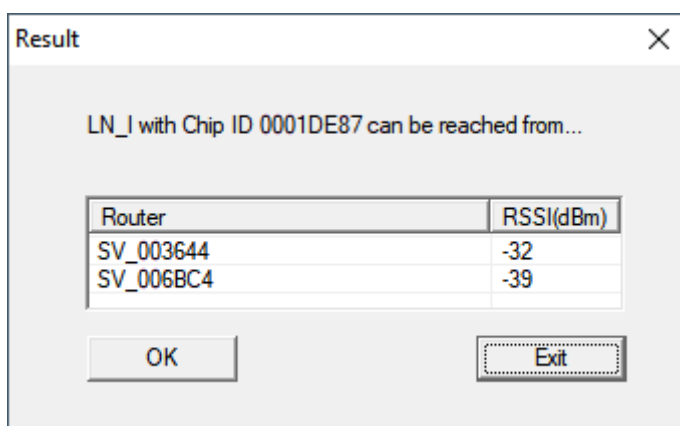
2. In the area "Configuration" select the option  Move to another master segment.
3. Click on the **OK** button.
  - ↳ The "Procedure started" window opens temporarily.



- ↳ Window "Select CN/RN" router opens (If the results window opens directly, then there are no other Router/CentralNodes in the segment. You must reset the LockNode and add it to another RouterNode).



4. Select the router/central nodes that are eligible to move the LockNode. (If necessary, select the checkbox  all.)
5. Click on the **OK** button.
  - ↳ Signal quality between LockNode and selected RouterNodes is measured.
  - ↳ The window "Result" opens. You will see the list of previously selected RouterNodes with measured values.



6. Select the RouterNode to which you want to assign your LockNode.



#### NOTE

##### Best signal quality

From the possible RouterNodes, select the RouterNode whose RSSI value is closest to 0 (0 = theoretical best value).

**NOTE****Exclamation mark before RouterNodes in the list**

For certain network structures, you can only assign the selected LockNode to certain RouterNodes. RouterNodes to which you cannot assign the selected LockNode are marked with an exclamation mark in front of the entry (e.g. if the maximum number of LockNodes for this RouterNode has already been reached). These RouterNodes are displayed for completeness only.

7. Click on the **OK** button.

↳ The "Result" window closes.

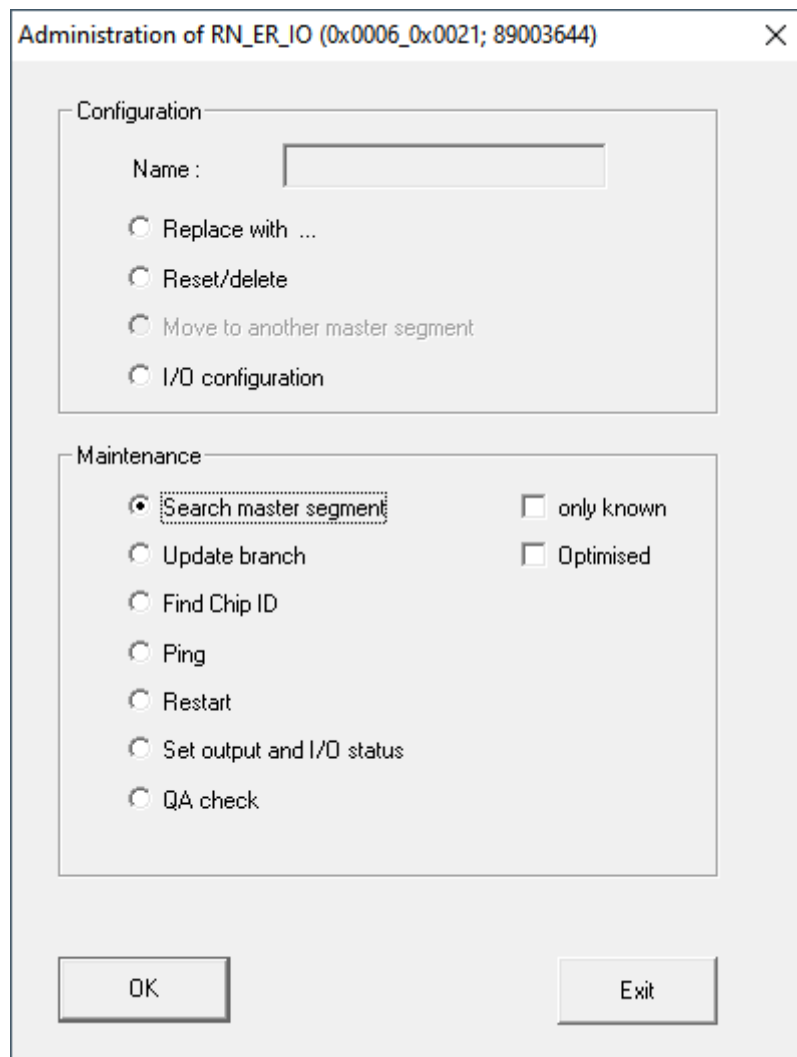
↳ LockNode is assigned to the desired RouterNode.

**Reassigning several LockNodes to one RouterNode**

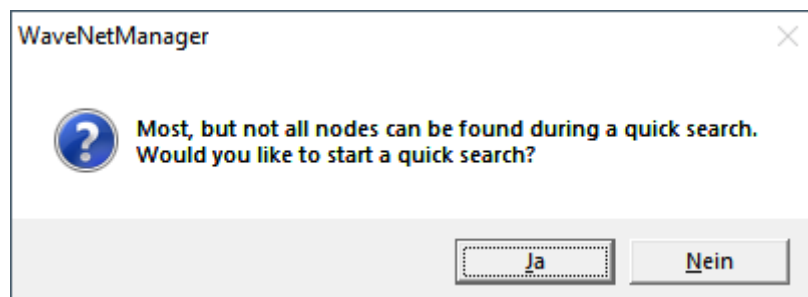
- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
- ✓ LockNodes and RouterNodes connected to power supply.
- ✓ LockNodes and RouterNodes connected to WaveNet (test see *Testing accessibility (WaveNet)* [▶ 183]).
- ✓ LockNodes with currently poor connection known (see *Check signal quality* [▶ 180]).

1. Right-click on the RouterNode to which you want to reassign LockNodes.

↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Search master segment.
3. Activate the checkbox  only known.
4. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "WaveNetManager" opens.



5. Click button **Yes** (quick search) or **No** (regular search).

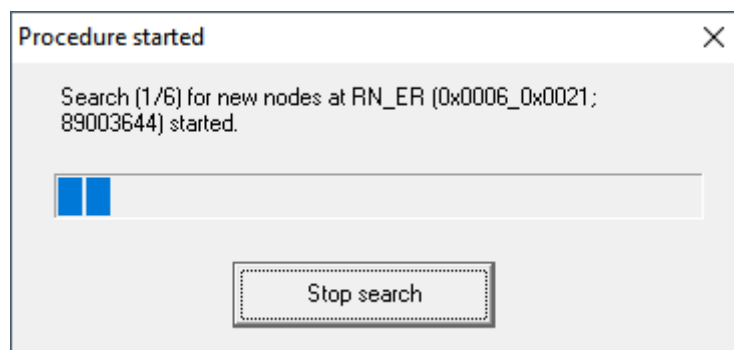


**NOTE**

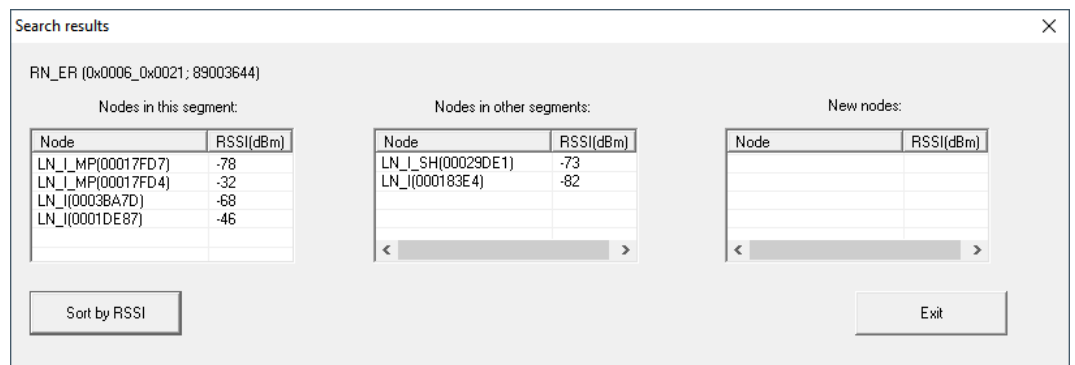
**Quick search**

If you perform a fast search, the RouterNode will only send a single broadcast. If you perform a regular sweep, the RouterNode sends a total of six broadcasts. The quick search is completed faster, but the normal scan is more thorough and finds LockNodes that were not reached during a quick search.

- ↳ The "WaveNetManager" window closes.
- ↳ The "Procedure started" window opens temporarily.



- ↳ The window "Search results" opens.



You will see an overview table of the LockNodes found by the RouterNode during the search. This table has three columns:

Nodes in this segment	Nodes from other segments	New nodes
These LockNodes are located in the WaveNet topology and are already assigned to the RouterNode.	These LockNodes are located in the WaveNet topology, but are assigned to a different RouterNode.	These RouterNodes are not in the WaveNet topology.

Each column contains two sub-columns:

Nodes	RSSI
Name of the LockNode	Signal strength of the LockNode connection to the searching RouterNode

### Unit of signal strength

The WaveNet Manager displays the signal strength as an RSSI value (Received Signal Strength) in dBm. This value is:

- Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.
  - Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm (i.e. the smaller the amount), the better the reception.
1. Mark the known LockNodes with bad connection in the middle column (nodes of other segments) if the RSSI value is better.  
You can see the current RSSI values in the main window of the WaveNet Manager.
  2. Use drag and drop to move the LockNodes to the left-hand column (nodes in this segment) to assign them to the current RouterNode (which you used to search).
    - ↳ LockNodes are assigned to the current RouterNode.



### NOTE

#### Assignment duration

When you reassign LockNodes, the WaveNet Manager communicates with the LockNodes to transfer the configuration and check the LockNode. This check takes a few seconds

3. If necessary, confirm the IO configuration of the LockNode by clicking the **OK** (you can change the IO configuration at any time, see *I/O configuration and protection functions* [[▶ 69](#)]).
  - ↳ LockNodes are assigned to the RouterNode.

## 6.5.2 Device restart

### 6.5.2.1 RouterNodes

#### Restarting Ethernet Router Nodes via the Browser Interface

- ✓ Browser interface open (see *Browser interface* [[▶ 148](#)]).
1. Via | ADMINISTRATION | open the tab [REBOOT].
    - ↳ Now you see the restart menu.

PASSWORD  
CERTIFICATE  
FACTORY  
REBOOT

---

## Administration: Reboot the router

---

Reboot

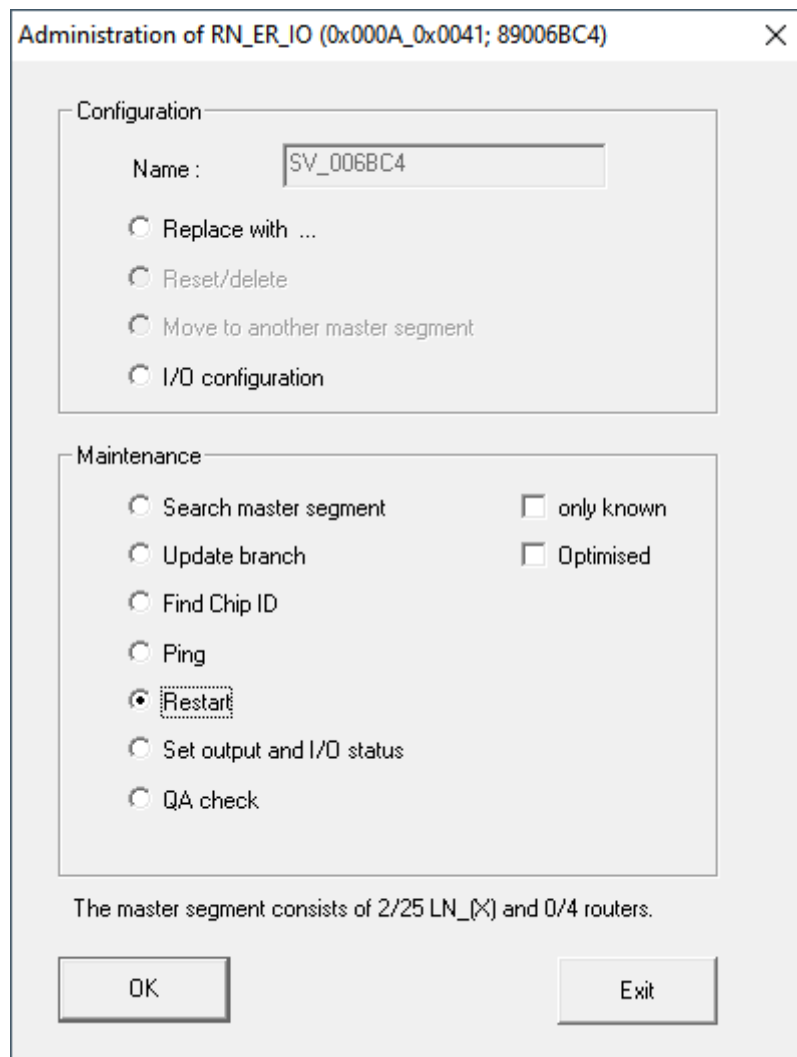
**Information:** The reboot process will take approximately 10 seconds to complete.

2. Click on the button **Reboot**.
  - ↳ Restart is performed.
  - ↳ Ethernet RouterNode is restarted.

### Restarting RouterNodes in the WaveNet Manager

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [[▶ 37](#)])
  - ✓ RouterNode connected to WaveNet (see *Add RouterNode to WaveNet* [[▶ 53](#)]).
1. Right-click on the entry of the RouterNode you want to restart.
    - ↳ The window "Administration" opens.





2. In the area "Maintenance" select the option  Restart.
3. Click on the **OK** button.
  - ↳ The "Procedure started" window opens temporarily.



- ↳ RouterNode will be restarted.
- ↳ RouterNode is restarted.

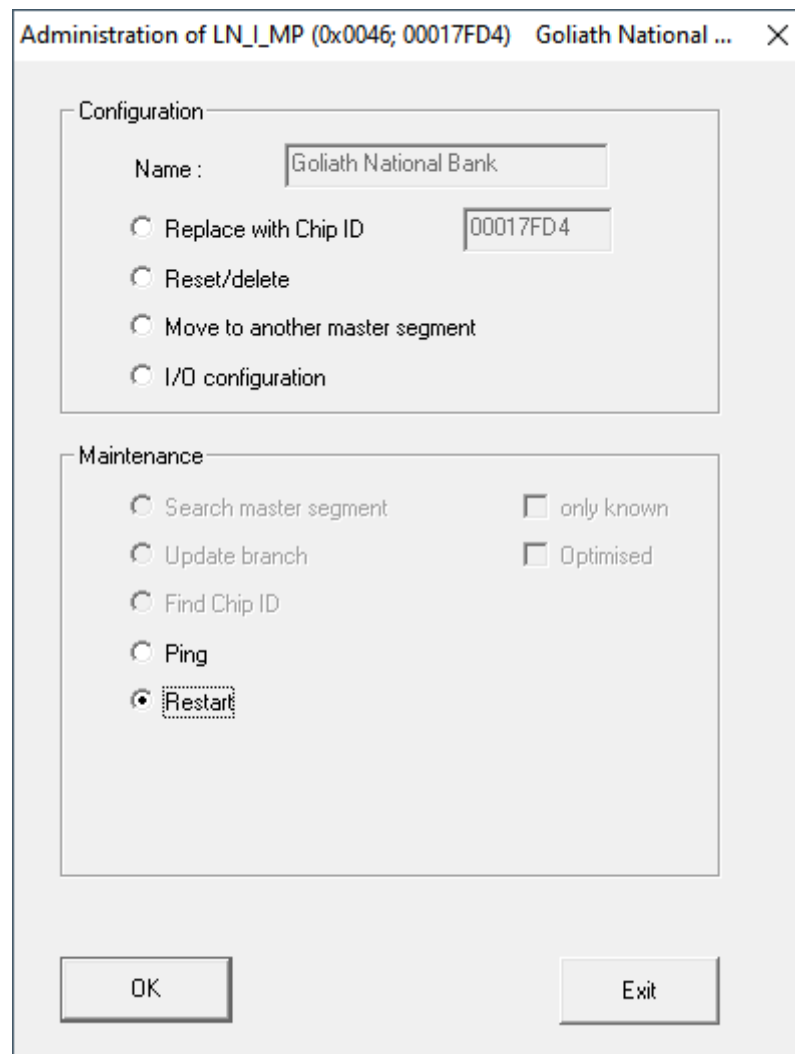
### Restart RouterNodes via power connection

Your RouterNodes will restart when you disconnect the power supply, wait about half a minute and reconnect.

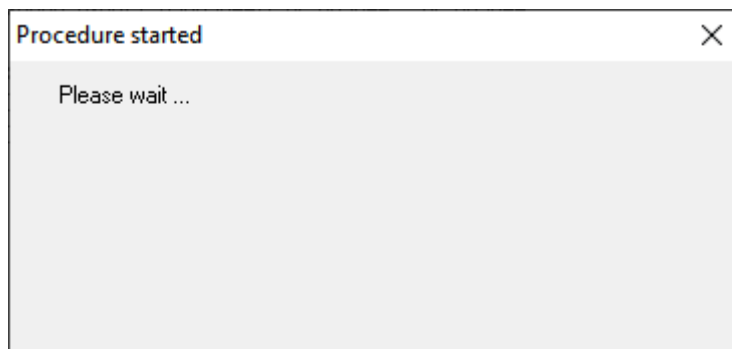
## 6.5.2.2 LockNodes

**Restarting LockNodes in the WaveNet Manager**

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ LockNode connected to WaveNet (see *Adding Lock Nodes to WaveNet* [▶ 59]).
1. Right-click on the entry of the LockNode you want to restart.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Restart.
3. Click on the  button.
  - ↳ The "Procedure started" window opens temporarily.



- ↳ LockNode will restart.
- ↳ LockNode is restarted.

### Restarting LockNodes via power connection

Your LockNodes are reset and restart when you disconnect the power (or remove the LNI), wait half a minute and reconnect (or reinstall the LNI). After the restart the LockNodes beep four times.

### 6.5.3 Reprogram or replace the device

If you have problems with a device, try the following before replacing it:

- Reprogram the device
- Reset and re-program the device (see *Resetting/Deleting* [▶ 168])

#### Reprogram the device

The flash symbol in the overview indicates a problem with your device. Try to reprogram the configuration on the same device. To do this, perform the replacement procedure as described (see *RouterNodes* [▶ 164] and *LockNodes* [▶ 166]) with the same IP address or chip ID of the device you want to reprogram. You transfer the configuration of the device you want to replace to the device that has that chip ID. If this is the same Chip ID, then the configuration is reprogrammed on the device.

#### Replace device

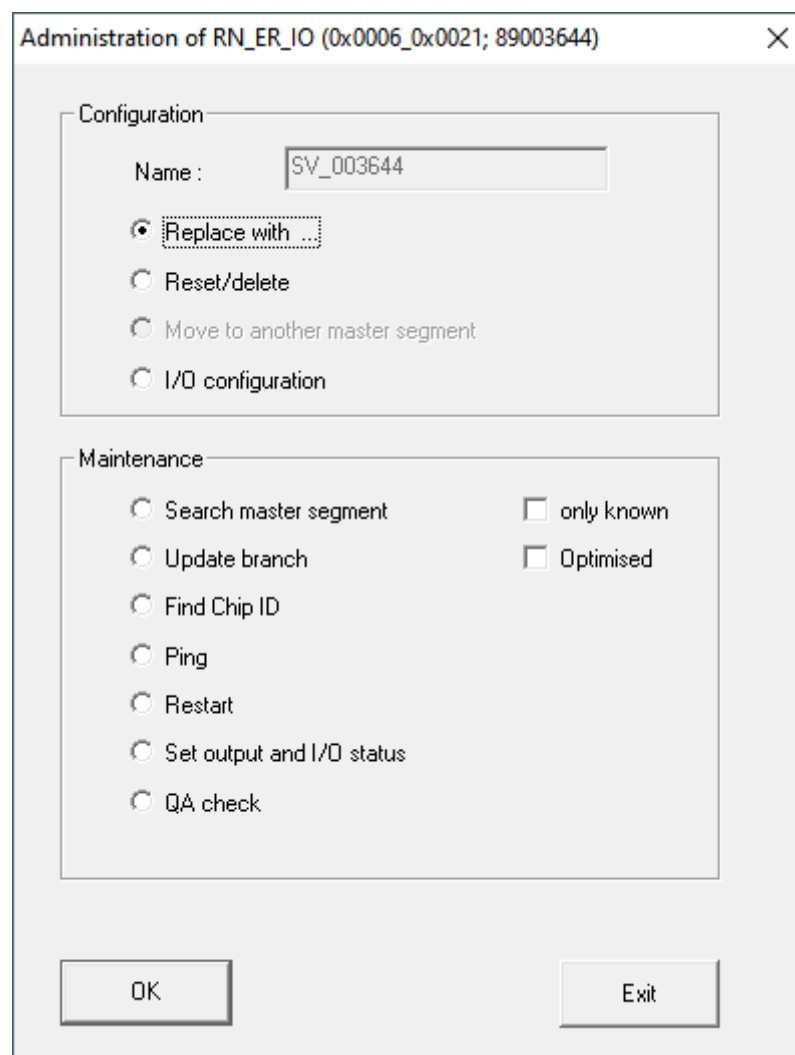
You can replace devices in WaveNet if a device is no longer to be used for the following reasons, for example:

- Replacement
- Vandalism
- Theft
- Defects

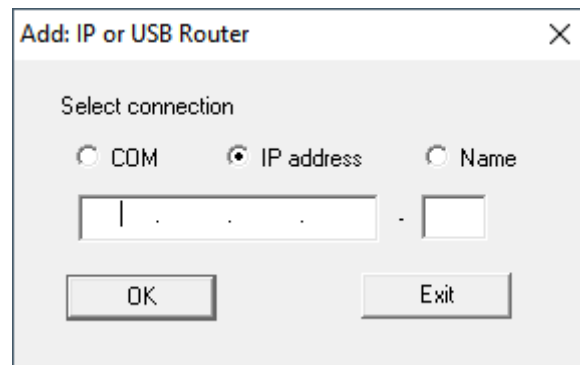
- ✓ Replacement RouterNode or replacement LockNode already installed at the final operating location.
  - ✓ Replacement RouterNode can already be resolved via valid IP address/ host names (determine/set IP address see *Determining and setting the IP address* [▶ 49])
1. For reprogramming, use the IP address/chip ID of the replacement unit instead of the same IP address/chip ID.
  2. Proceed in the same way as when reprogramming a WaveNet configuration on a device (see *RouterNodes* [▶ 164] und *LockNodes* [▶ 166]).
- ↳ Device replaced.

### 6.5.3.1 RouterNodes

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
1. Right-click on the entry for the RouterNode you wish to replace.
    - ↳ The window "Administration" opens.



2. In the area "Configuration" select the option  Replace with ....
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Add: IP or USB Router" opens.



4. Select the option  IP address or  Name.
5. Check the IP address or name (and correct it if necessary).
6. Click on the **OK** button.
  - ↳ The window "Add: IP or USB Router" closes.
  - ↳ If you use the IO functions in the RouterNode you want to replace: The window "I/O configuration" opens.

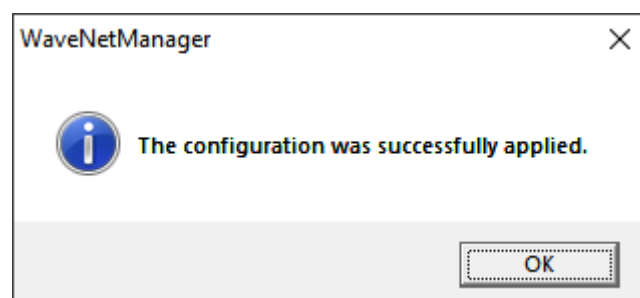


## NOTE

### Check IO configuration

Check the IO configuration. You can also set the IO configuration later (see *I/O configuration and protection functions* [[▶ 69](#)]).

7. Click on the **OK** button.
  - ↳ The "I/O configuration" window closes.
  - ↳ The window "WaveNetManager" opens.

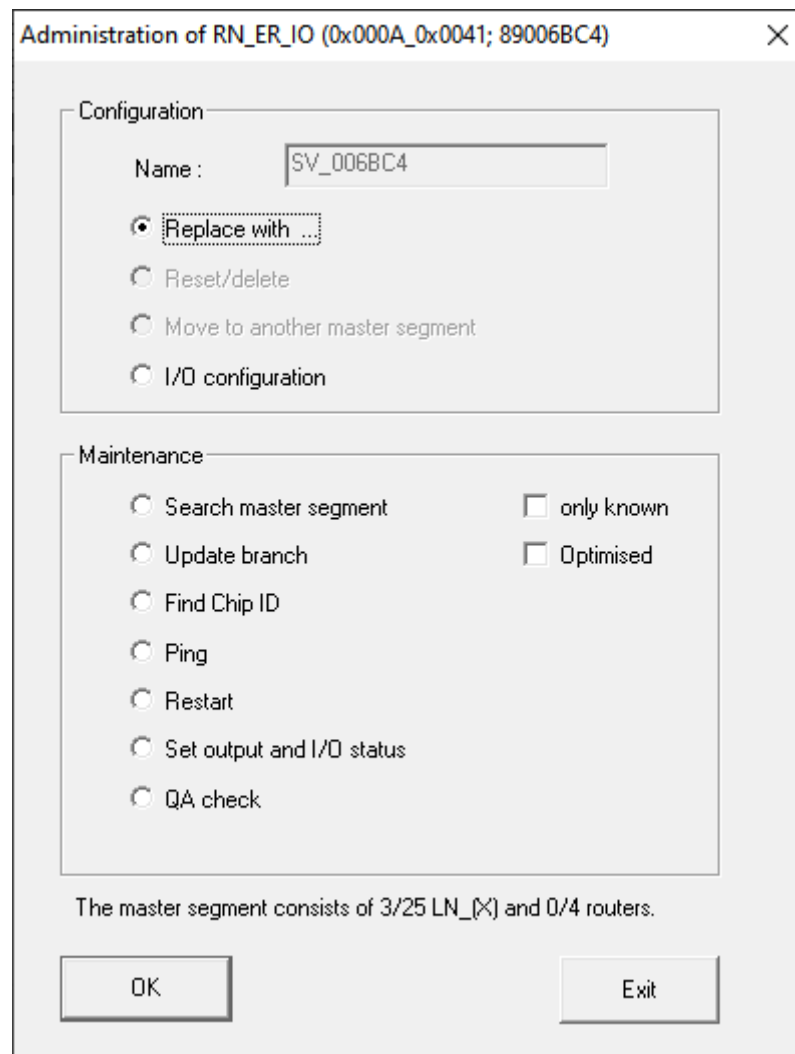


8. Click on the **OK** button.
  - ↳ The "WaveNetManager" window closes.
  - ↳ RouterNode is replaced.

## 6.5.3.2 LockNodes

✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])

1. Right-click on the entry of the LockNode you want to replace.
  - ↳ The window "Administration" opens.

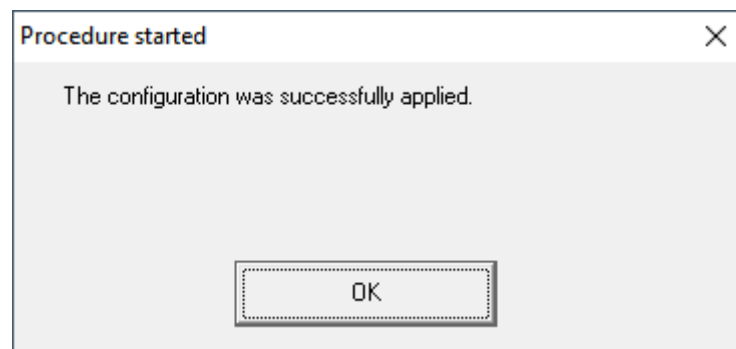


2. In the area "Configuration" select the option  Replace with Chip ID.
3. Enter the chip ID of the new LockNode (you will find the chip ID on the packaging of the LockNode or on the LockNode itself).
4. Click on the  button.
  - ↳ The "Administration" window closes.
  - ↳ The window "I/O configuration" opens.

**NOTE****Check IO configuration**

Check the IO configuration. You can also set the IO configuration later (see *I/O configuration and protection functions* [▶ 69]).

5. Click on the **OK** button.
  - ↳ The "I/O configuration" window closes.
  - ↳ The window "Procedure started" opens.



6. Click on the **OK** button.
  - ↳ The "Procedure started" window closes.
  - ↳ LockNode is replaced.

Do not use replaced LockNodes within range of the WaveNet.

**6.5.4 Delete netcfg.xml**

If you have problems with incorrect entries or your WaveNet, delete netcfg.xml before starting WaveNet Manager. The netcfg.xml may contain incorrect entries, especially if you are working with several WaveNet networks.

- ✓ WaveNet Manager not open.

1. Navigate to the WaveNet Manager directory.

appcfg.xml	10.09.2019 12:56	XML-Dokument	1 KB
boost_threadmon.dll	23.07.2002 19:15	Anwendungserwe...	24 KB
msgcfg.xml	10.09.2019 12:56	XML-Dokument	1 KB
netcfg.xml	10.09.2019 12:56	XML-Dokument	3 KB
Readme.txt	08.03.2019 07:09	Textdokument	2 KB
WaveNetManager.exe	07.03.2019 11:38	Anwendung	804 KB
WNIPDiscoveryLib.dll	17.10.2014 09:21	Anwendungserwe...	32 KB
WNM_Handbook.pdf	14.12.2016 16:02	Adobe Acrobat D...	1.571 KB
WNM_move_node	08.08.2019 15:28	Datei	1 KB
WNM_Ring_report	06.09.2019 10:57	Datei	1 KB
WNM_RSSI_report	10.09.2019 12:57	Datei	1 KB
WNMManager	10.09.2019 12:57	Datei	1 KB

2. Delete the file `netcfg.xml`.

↳ You can start the WaveNet Manager (see *Best Practice: From the LSM software* [▶ 37]).

### 6.5.5 Resetting/Deleting

Reset devices are deleted from your WaveNet topology and no longer displayed in the overview.

Resetting the entire WaveNet consists of four parts:

1. Resetting LockNodes (see *LockNodes* [▶ 168])
2. Resetting RouterNodes (see *RouterNodes* [▶ 170])
3. Edit communication nodes (see *WaveNet* [▶ 173])
4. Delete empty segments from the LSM, if not done by importing the empty topology (see *WaveNet* [▶ 173])

In general, you should reset your devices in the WaveNet Manager and then import the topology. This allows the WaveNet Manager to tell LSM which devices are actually present in WaveNet and you can keep the data synchronised.

You can also reset LockNodes and RouterNodes independently of the other parts.



#### NOTE

##### LockNodes cannot be reached after resetting

If you reset a RouterNode, you will not be able to reach its LockNodes afterwards.

- Reset LockNodes connected to the RouterNode beforehand (see *LockNodes* [▶ 152]).

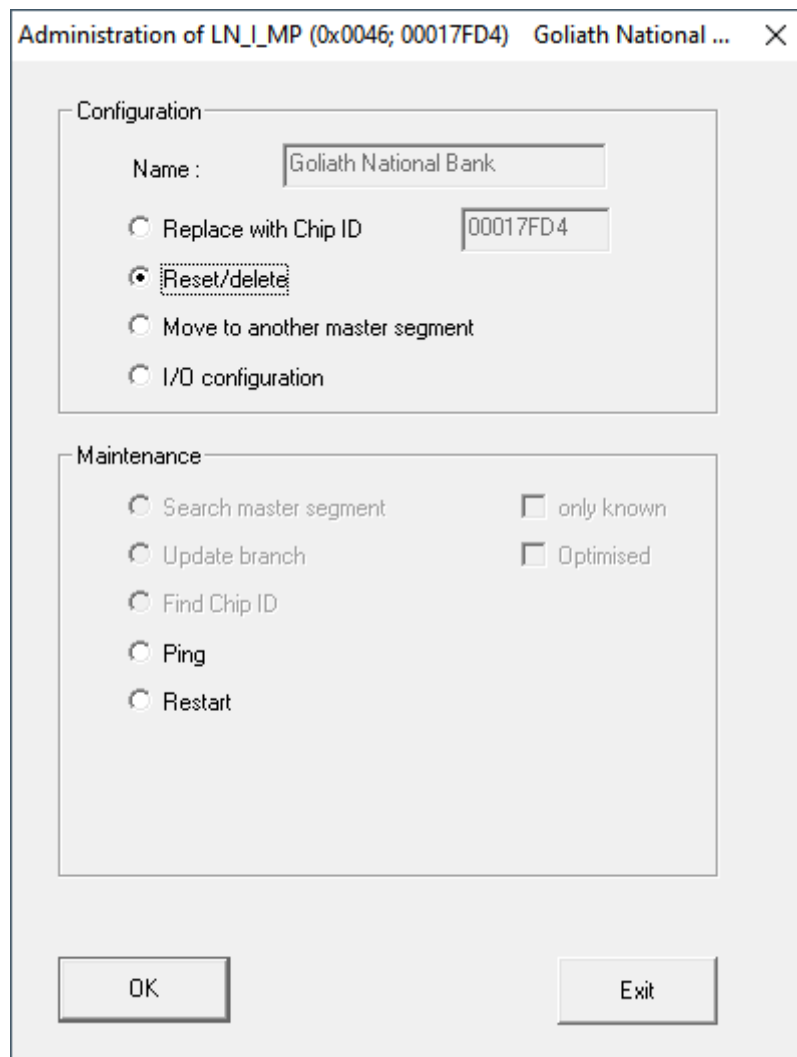
If you can no longer reach the LockNodes, you can also reset the LockNodes with a hardware reset (disconnect and restore power, see *LockNodes* [▶ 162]).

#### 6.5.5.1 LockNodes

##### Best Practice: Reset with the WaveNet Manager

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ LockNode connected to WaveNet (see *Adding Lock Nodes to WaveNet* [▶ 59]).
1. Right-click on the entry of the LockNode you want to reset.
    - ↳ The window "Administration" opens.





2. In the area "Configuration" select the option  Reset/delete.
3. Click on the **OK** button.
  - ↳ The window "Procedure started" opens.



4. Click on the **OK** button.
  - ↳ The "Procedure started" window closes.
5. Click on the button **Save**.
  - ↳ LockNode is reset and deleted from the WaveNet topology.

### Hardware reset of external LockNodes

You can reset WaveNet Manager-enabled LockNodes (recognisable by **WNM** in the article number):

1. Disconnect the LockNode from the power supply or remove the batteries.
2. Wait for about 20 seconds.
3. Press and hold the Init button.
4. Reconnect the power supply or replace the batteries.
  - ↳ LED lights up constantly red.
5. Release the Init button while the LED is constantly red.
  - ↳ All WaveNet information in the LockNode is deleted.

You can re-integrate the LockNode into your WaveNet (see WaveNet manual).

The SmartIntego variant (SI.N.IO) can only be reset in the SmartIntego Manager.

### Hardware reset of internal LockNodes

Internal LockNodes are completely reset if you install the LockNode in a lock of another locking system.

1. Remove the LockNode (see manual/quick guide for the LockNode or locking device).
2. Reinstall the LockNode in a programmed lock of another locking system.
  - ↳ Lock beeps/flashes four times.
  - ↳ LockNode is reset.

You can then remove the LockNode from the lock of the other locking system. You can then use the LockNode again in your WaveNet.

#### 6.5.5.2 RouterNodes



#### NOTE

#### LockNodes cannot be reached after resetting

If you reset a RouterNode, you will not be able to reach its LockNodes afterwards.

- Reset LockNodes connected to the RouterNode beforehand (see *LockNodes* [[▶ 152](#)]).

Reset RouterNodes have the default radio configuration:


Network ID	DDDD This ID is always changed during commissioning. Therefore, do not set this ID in the WaveNet Manager or LSM.
Radio channel	Channel 0 (868.1 MHz)

### Best Practice: Resetting RouterNodes in the WaveNet Manager



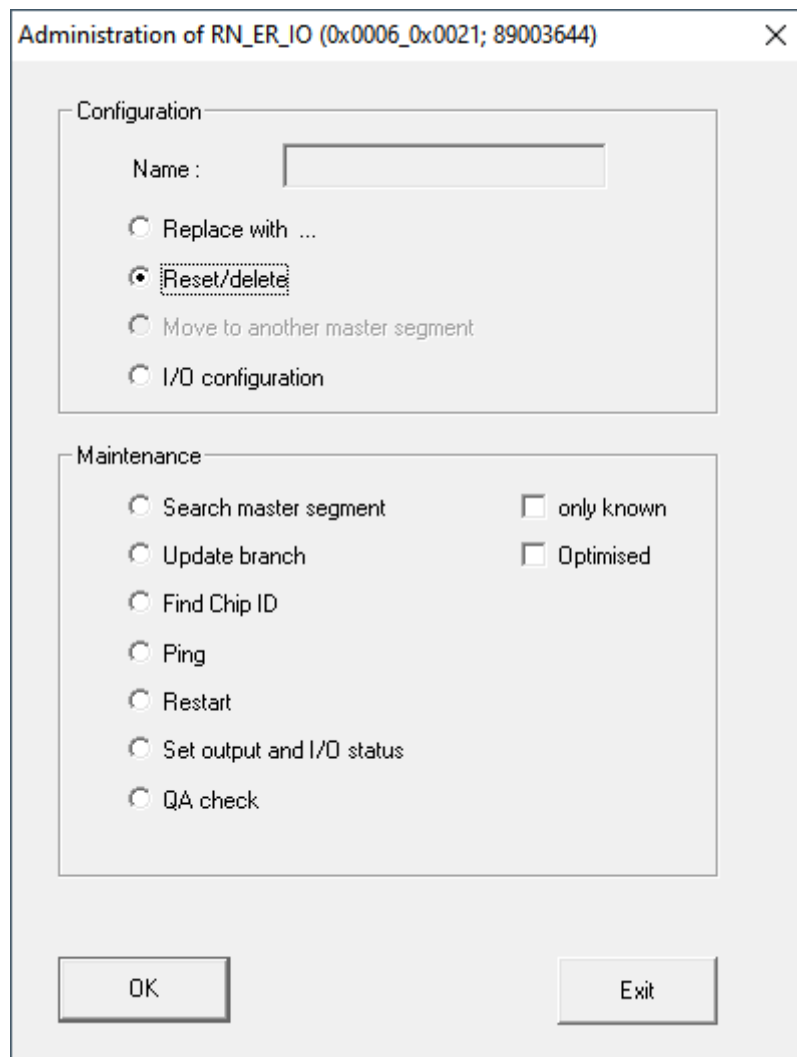
#### NOTE

##### Reset locked

LockNodes assigned to the RouterNode can no longer be reached after resetting the RouterNode. Therefore, the option  Reset/delete is disabled if LockNodes are still assigned to the RouterNode.

- First reset or delete all LockNodes assigned to the RouterNode (see [LockNodes \[▶ 168\]](#)).

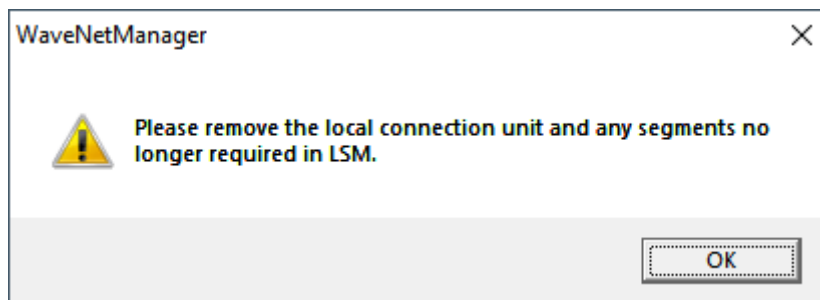
- ✓ WaveNet Manager opened via LSM (see [Best Practice: From the LSM software \[▶ 37\]](#))
  - ✓ RouterNode connected to WaveNet (see [Add RouterNode to WaveNet \[▶ 53\]](#)).
1. Right-click on the entry of the router node you want to reset.
    - ↳ The window "Administration" opens.



2. In the area "Configuration" select the option  Reset/delete.
3. Click on the **OK** button.
  - ↳ The window "Procedure started" opens.



4. Click on the **OK** button.
  - ↳ The "Procedure started" window closes.
  - ↳ The window "WaveNetManager" opens.



5. Click on the **OK** button.
  - ↳ The "WaveNetManager" window closes.
6. Click on the button **Save**.
  - ↳ RouterNode is reset and deleted from the WaveNet topology.

### Resetting Ethernet RouterNodes via the Browser Interface

- ✓ Browser interface open (see [Browser interface \[▶ 148\]](#)).
1. Via | ADMINISTRATION | open the tab [FACTORY].
    - ↳ You will see the restore menu.

PASSWORD  
CERTIFICATE  
FACTORY  
REBOOT

---

## Administration: Factory reset

---

**Reset**

**Information:** Perhaps the device is not more reachable after the reset and reboot process.

2. Click on the button **Reset**.
  - ↳ Restore is performed.
  - ↳ Ethernet RouterNode is reset to factory setting.

### Resetting RouterNodes via Hardware

All RouterNodes support a hardware reset. You can reset these RouterNodes with the reset button on the board. For further information, please refer to the manual or the short manual of the respective RouterNode.

#### 6.5.5.3 WaveNet

Importing the WaveNet topology also removes reset LockNodes from LSM.

The segments of RouterNodes and CentralNodes/RouterNodes with Ethernet connection remain. You must remove these later:

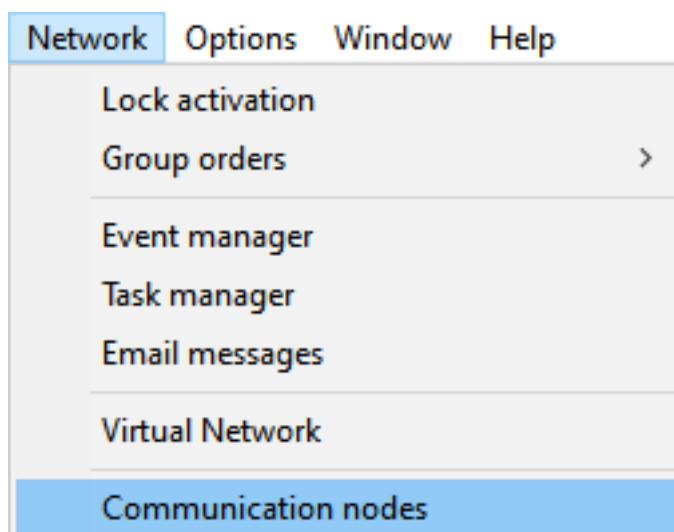
1. Remove RouterNodes from communication nodes or local connections
2. Remove segments

## Editing communication nodes

Proceed in the same way for local connections (if you are not using a CommNode server).

- ✓ RouterNodes and LockNodes are reset in the WaveNet Manager (see *Best Practice: Reset with the WaveNet Manager* [▶ 168] and *Best Practice: Resetting RouterNodes in the WaveNet Manager* [▶ 171]).
- ✓ WaveNet topology imported.
- ✓ LSM open.

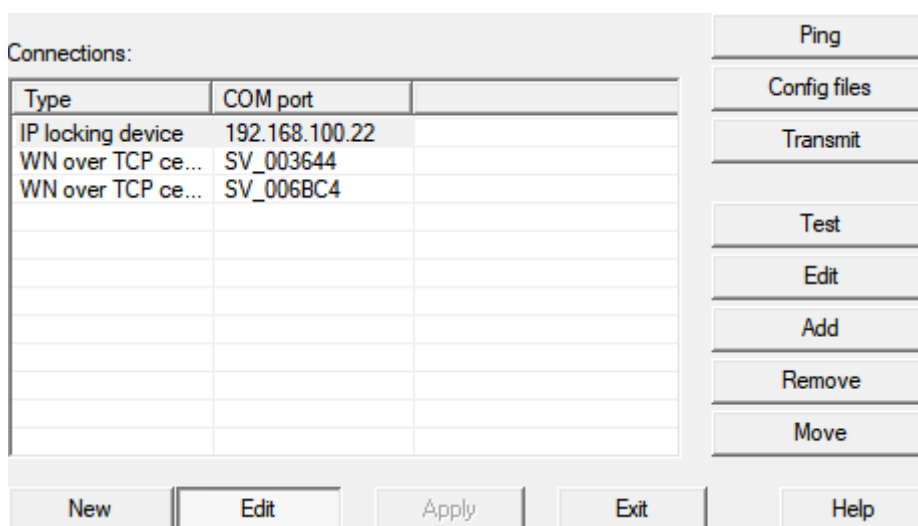
1. Via | Network | select the entry **Communication nodes**.



↳ Communication node overview opens.

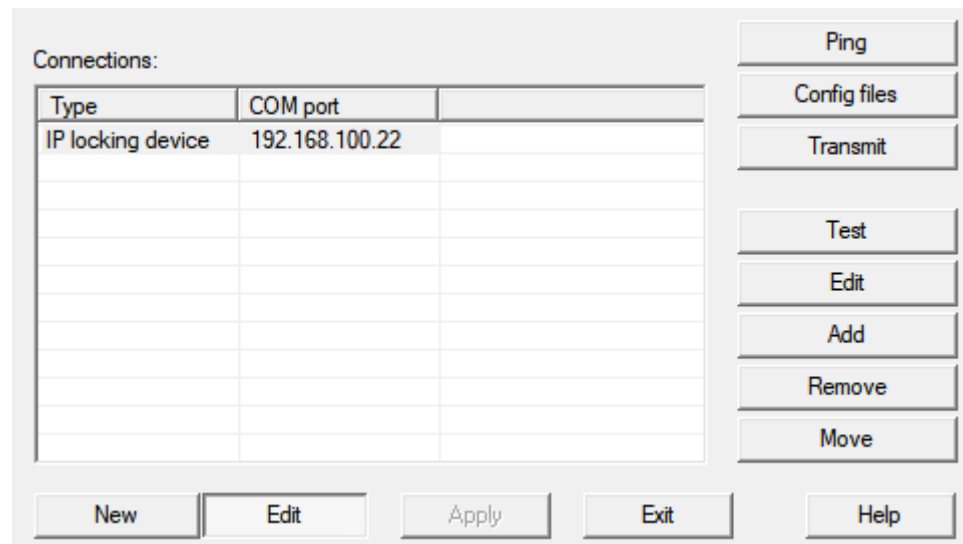
2. If necessary, use the **⏪**, **⏩**, **⏴** and **⏵** buttons to select the communication node used for WaveNet.

↳ The overview shows the entries of your RouterNodes that have not been deleted.

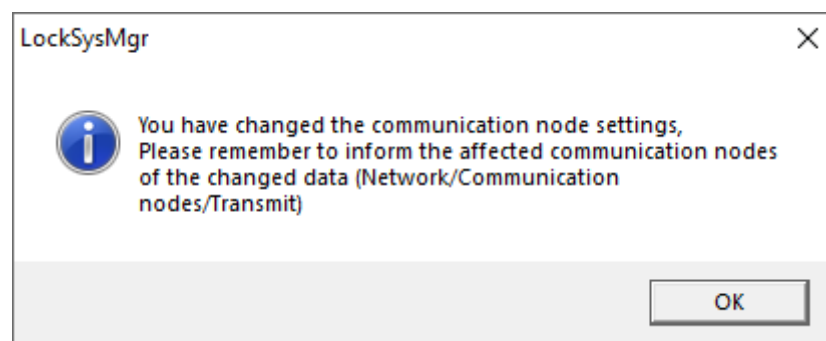


3. Select your RouterNodes.

- Click the button **Remove**.
  - RouterNodes are removed from the list.



- Click on the **Apply** button.
  - The window "LockSysMgr" opens.

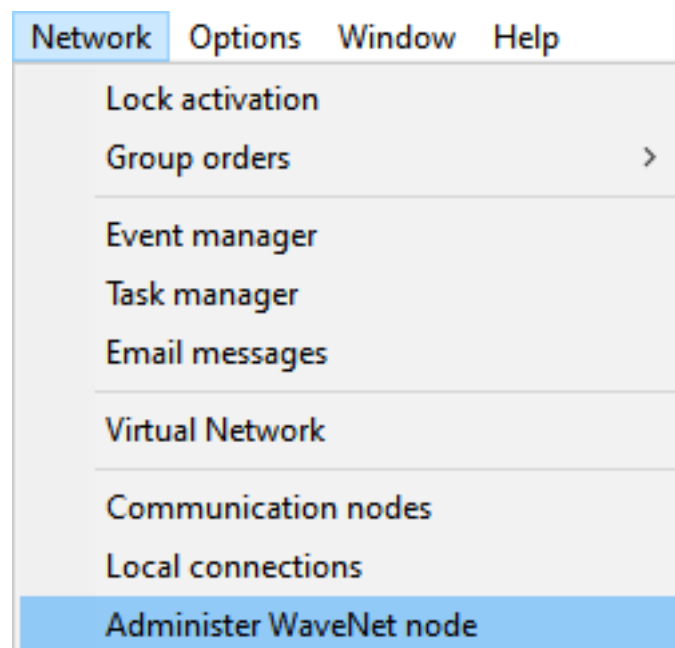


- Click on the **OK** button.
  - The "LockSysMgr" window closes.
- Click on the **Config files** button.
- Click on the **OK** button.
  - A query about the node-specific storage location opens.
- Click the button **No**.
  - A query about the node-specific storage location closes.
  - Confirmation message opens.
- Click on the **OK** button.
  - Confirmation message closes.
- Click the button **Transmit**.
  - Data is transmitted to the communication node.
  - Confirmation message opens.
- Click on the **OK** button.
  - Confirmation message closes.

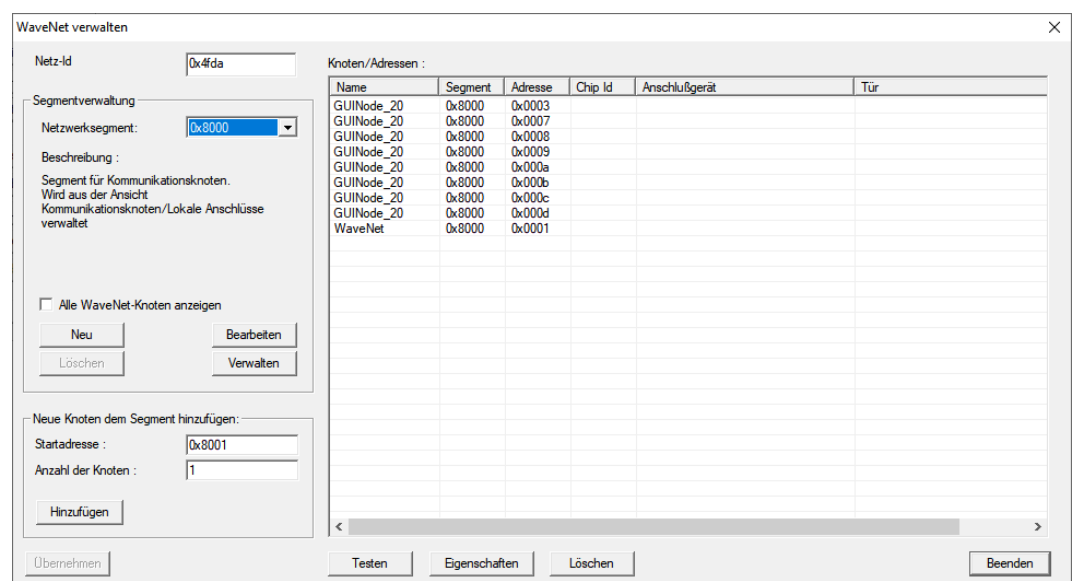
## Remove segments

- ✓ RouterNodes and LockNodes are reset in the WaveNet Manager (see *Best Practice: Reset with the WaveNet Manager* [▶ 168] and *Best Practice: Resetting RouterNodes in the WaveNet Manager* [▶ 171]).
- ✓ WaveNet topology imported.
- ✓ RouterNodes are removed from communication nodes or local connections.
- ✓ LSM open.

1. Via | Network | select the entry **Administer WaveNet node**.



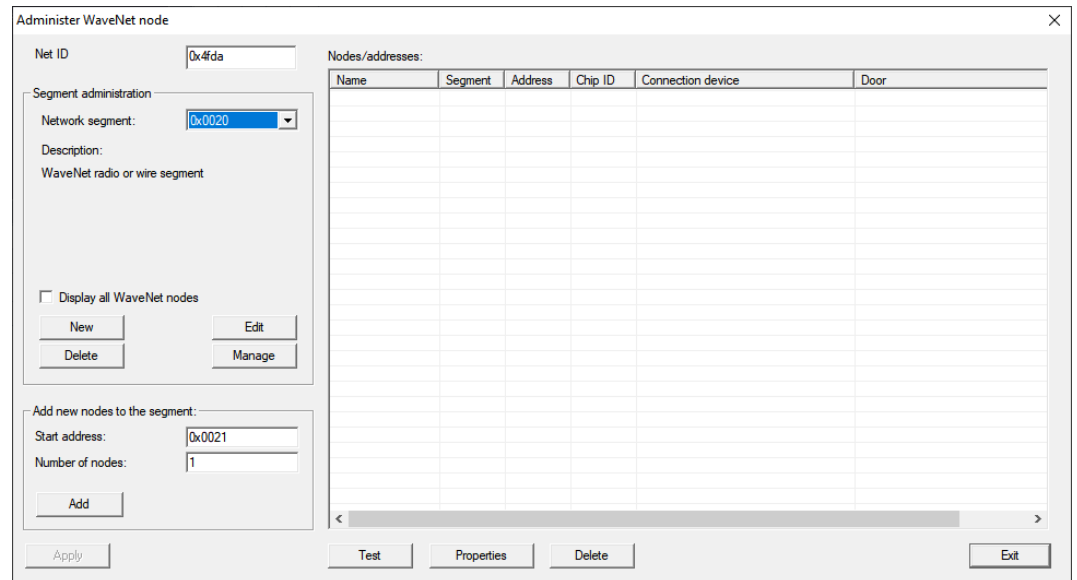
↳ The window "Administer WaveNet node" opens.



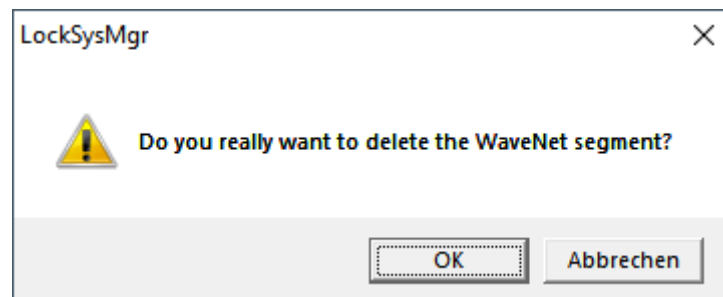


- In the dropdown menu ▼ **Network segment** select your network segment.

You can recognize the segment by the fact that there are no more entries in the table.



- In the area "Segment administration" click the button **Delete**.  
↳ The window "LockSysMgr" opens.



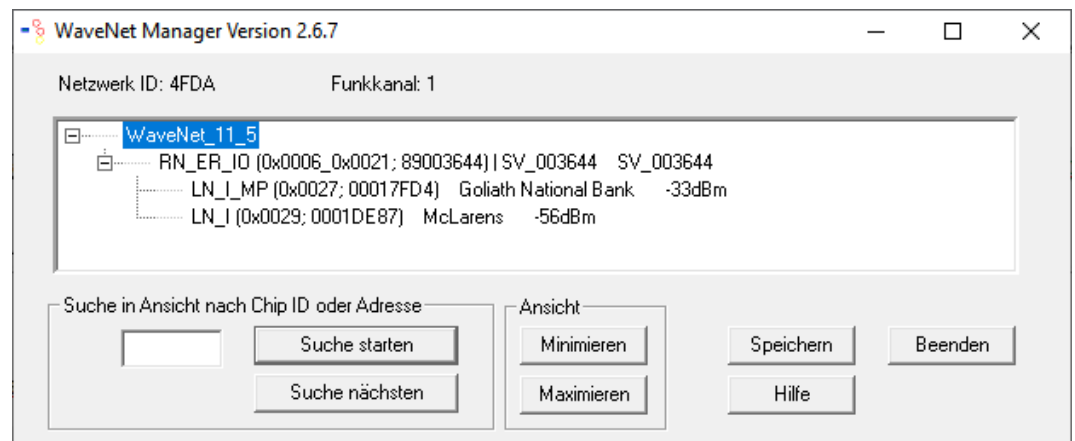
- Click on the **OK** button.  
↳ The "LockSysMgr" window closes.
- Click on the **Apply** button.  
↳ Segment is deleted.

## 6.6 Maintenance

- For information on maintaining a RingCast, see Ring *RingCast function test* [▶ 143].
- For information on battery status or battery replacement, see *Battery management* [▶ 193].

### 6.6.1 Overview

You can see the topology of your WaveNet in the WaveNet Manager on the start page.



The overview provides the following information:

#### Router node

- RouterNode type (e.g. RN\_ER\_IO)
- Input address (for example 0x0006)
- Chip ID (e.g. 89003644)
- Host name (If you do not use host names, the IP address is displayed instead of the host name).
- RSSI value (if radio interface only. Not used in the example)

#### LockNode

- LockNode type (e.g. LN\_I)
- Address (e.g. 0x0027)
- Chip ID (e.g. 00017023)
- Name of the linked locking device
- RSSI value (e.g. -33 dBm)

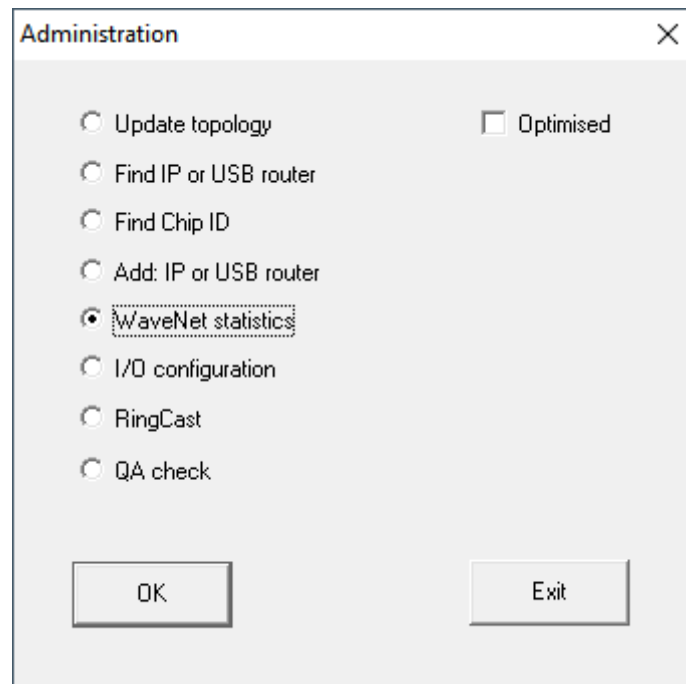
You can determine the segments with the displayed address (see [Addressing \[▶ 42\]](#)).

#### Number of device types

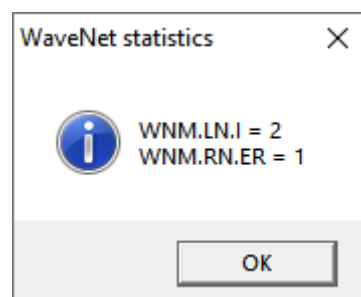
The WaveNet Manager provides you with a way to display the number of different device types.

✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])

1. Right click the entry WaveNet\_XX\_X.  
↳ The window "Administration" opens.



2. Select the option  WaveNet statistics.
3. Click on the **OK** button.  
↳ The "Administration" window closes.  
↳ The window "WaveNet statistics" opens. You will see a list of device types with the number.



### Memory status

The overview also shows the memory status of the devices.

Bold	WaveNet entry changed, but not yet saved. Click on the button <b>Save</b> .
Normal	Entry saved in WaveNet

### Configuration status

You can recognise problems by the configuration of RouterNodes or LockNodes by a black flash in front of the respective entry. Repeat the configuration by reprogramming the device (see *Reprogram or replace the device* [▶ 163]).

#### 6.6.2 Check signal quality

##### IMPORTANT

##### Recommended signal strength

The signal strength in the WaveNet Manager should be between 0 dBm and -70 dBm.

If the signal strength is insufficient, the connection and communication between devices can become slow or interrupted, and there will also be higher power consumption.

- ❑ If the signal strength is between -75 dBm and -90 dBm, there may be limited functionality. Improve the signal quality (see *Improving signal quality* [▶ 152]).

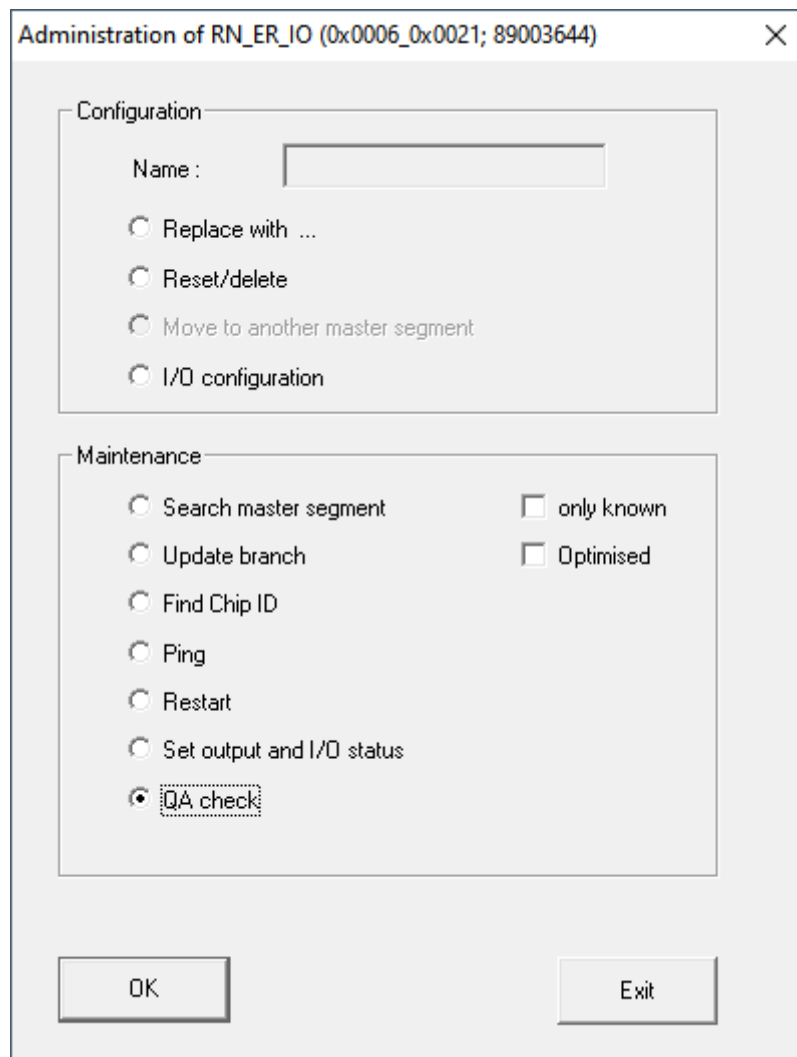
##### Unit of signal strength

The WaveNet Manager displays the signal strength as an RSSI value (Received Signal Strength) in dBm. This value is:

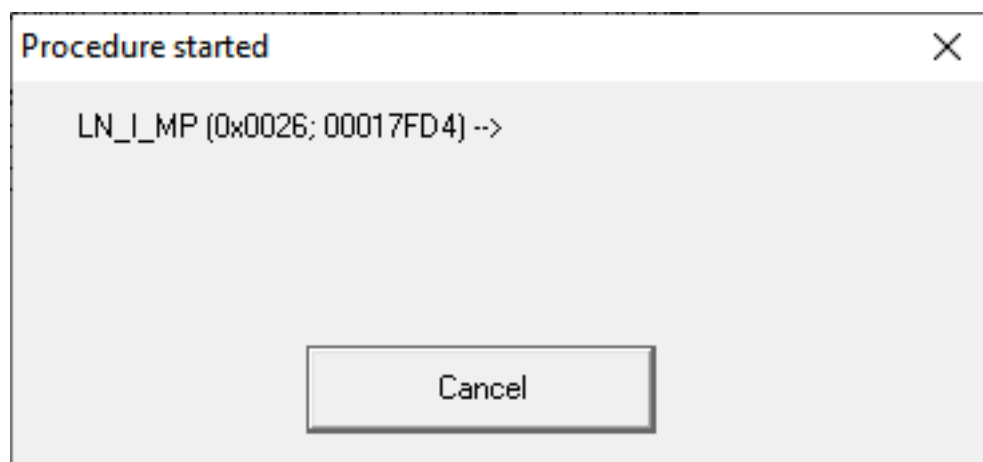
- ❑ Logarithmic: In practice, an improvement of 10 dBm means twice the signal strength.
- ❑ Negative: The theoretical best value is 0 dBm and is only achieved by cable connections. The closer the value is to 0 dBm (i.e. the smaller the amount), the better the reception.

##### Single RouterNode

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNodes and LockNodes connected to WaveNet (see *Finding and adding devices* [▶ 48]).
1. Right-click the entry of the RouterNode whose signal quality to its LockNodes you want to check.
    - ↳ The window "Administration" opens.



2. Select the option  QA check.
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The "Procedure started" window opens temporarily.

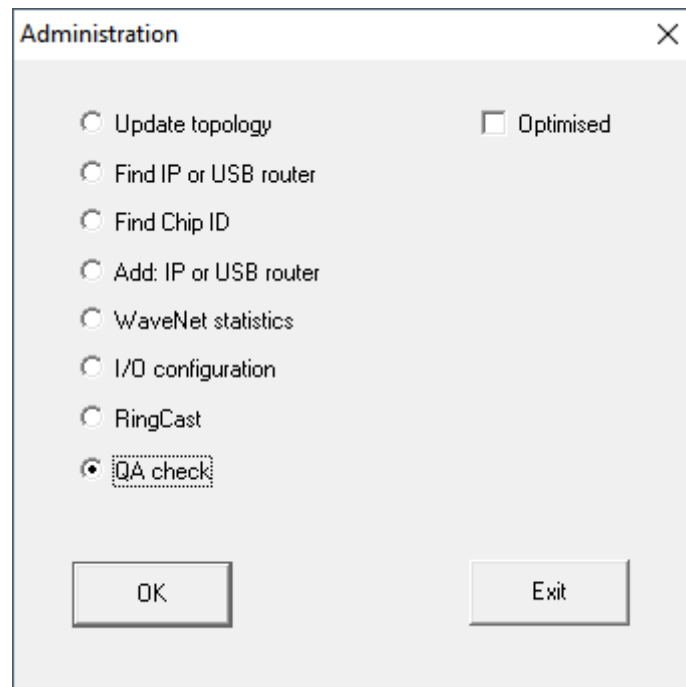


- ↳ RSSI values in the overview are updated for the corresponding Router-Node.

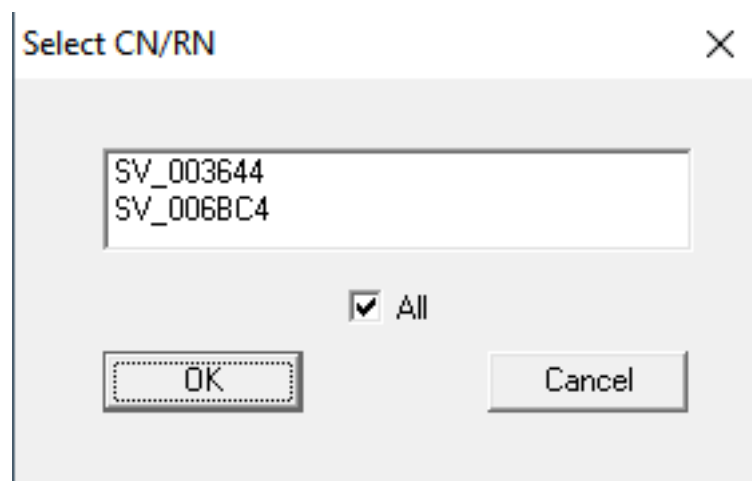
### Multiple RouterNodes

- ✓ WaveNet-Manager opened.
- ✓ RouterNodes and LockNodes connected to WaveNet.

1. Right click the entry WaveNet\_XX\_X.
  - ↳ The window "Administration" opens.

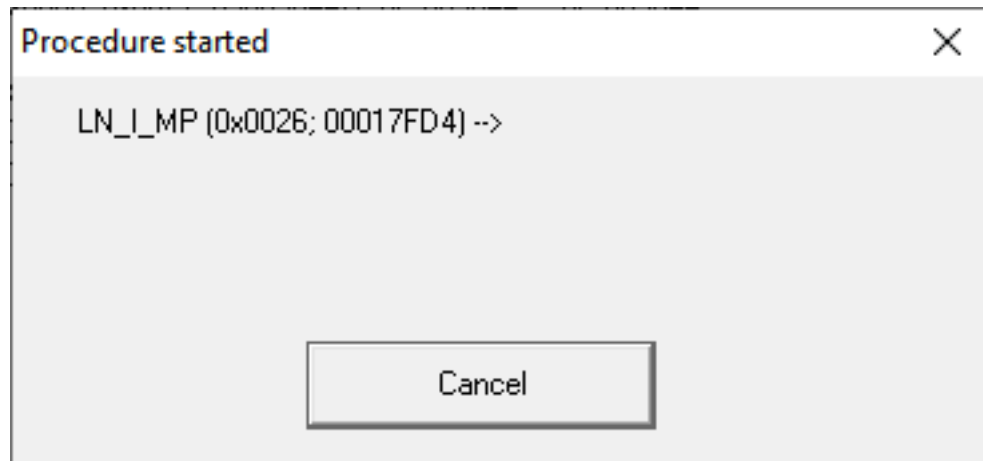


2. Select the option  QA check.
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Select CN/RN" opens. You will see a list of RouterNodes in your WaveNet.



4. Either select all desired RouterNodes or activate the checkbox  all.

5. Click on the **OK** button.
  - ↳ The "Select CN/RN" window closes.
  - ↳ The "Procedure started" window opens temporarily.



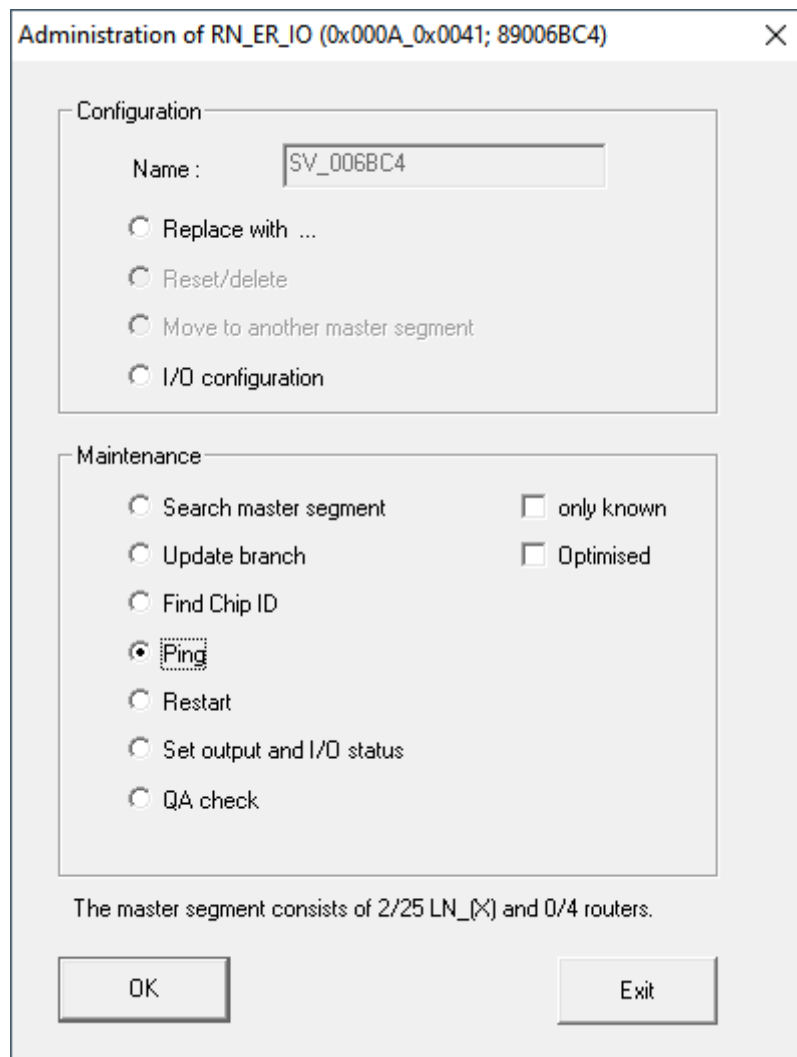
- ↳ RSSI values in the overview are updated for the corresponding Router-Nodes.

### 6.6.3 Testing accessibility (WaveNet)

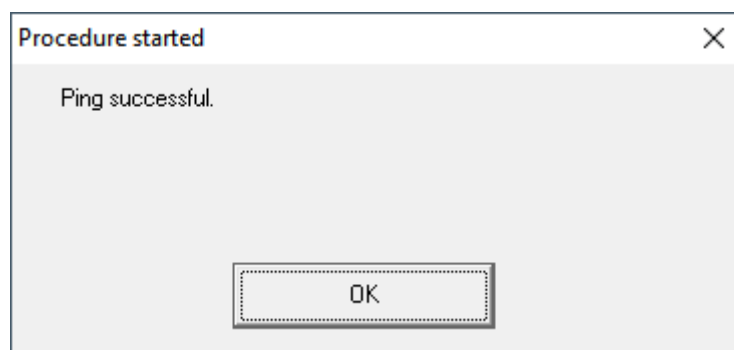
You can use the WaveNet Manager to test whether the WaveNet Manager reaches your RouterNodes and LockNodes.

#### 6.6.3.1 RouterNodes

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNode connected to WaveNet (see *Add RouterNode to WaveNet* [▶ 53]).
1. Right-click on the entry of the router node whose availability you want to test.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Ping.
3. Click on the **OK** button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Procedure started" opens.

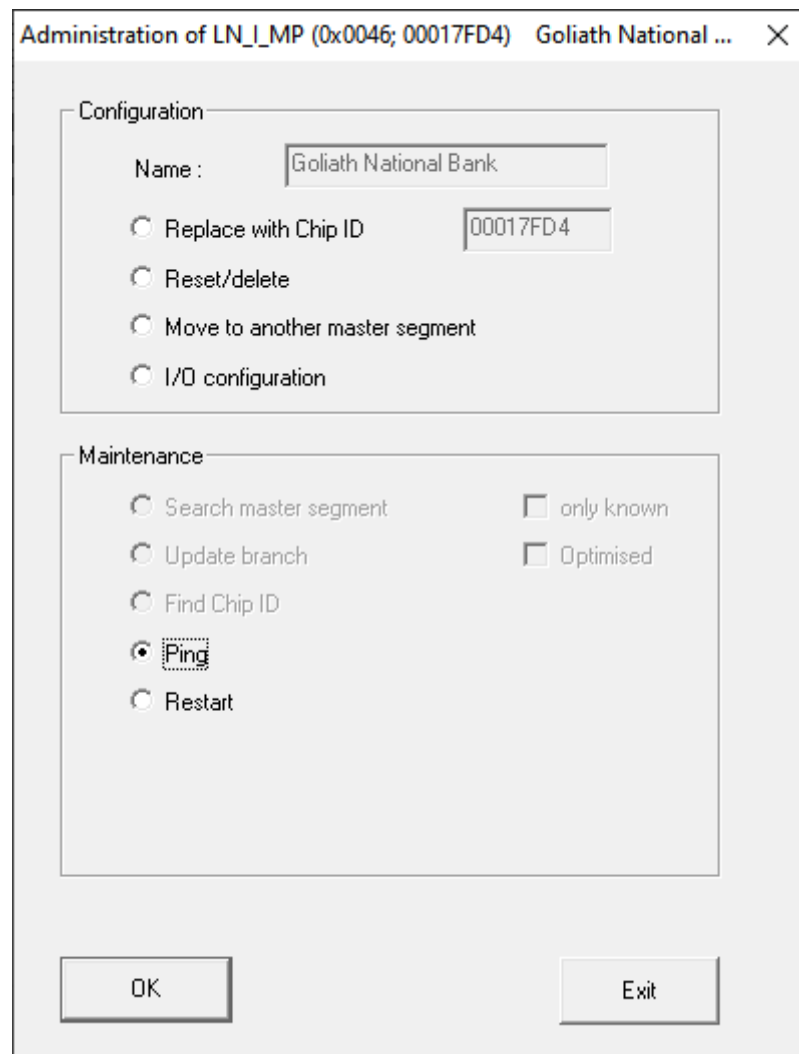


4. Click on the **OK** button.
  - ↳ The "Procedure started" window closes.
  - ↳ WaveNet Manager reaches RouterNode.

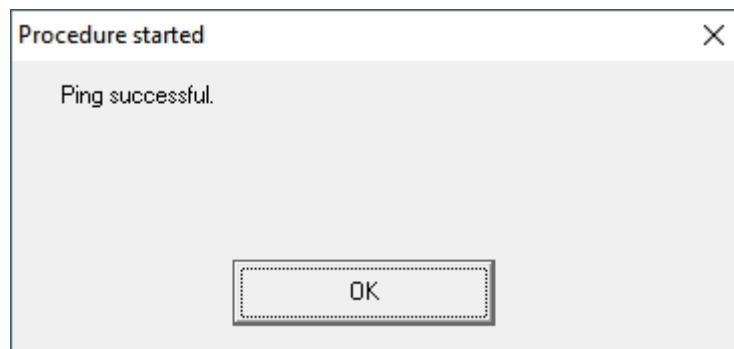


## 6.6.3.2 LockNodes

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ LockNode connected to WaveNet (see *Adding Lock Nodes to WaveNet* [▶ 59]).
1. Right-click the entry of the LockNode whose availability you want to test.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Ping.
3. Click on the  button.
  - ↳ The "Administration" window closes.
  - ↳ The window "Procedure started" opens.



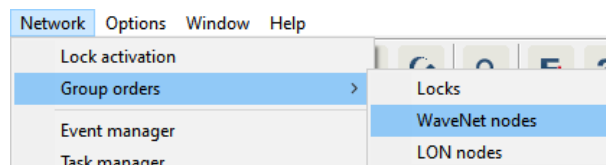
4. Click on the **OK** button.
  - ↳ The "Procedure started" window closes.
  - ↳ WaveNet Manager reaches LockNode.

#### 6.6.4 Test reachability (LSM)

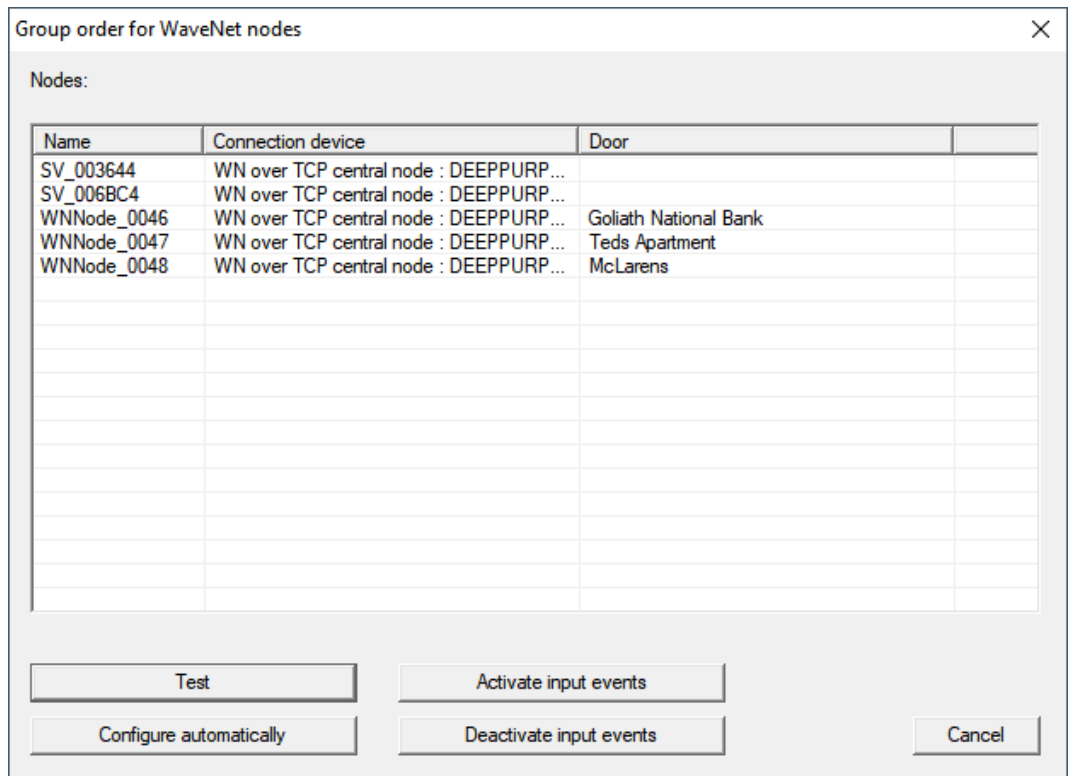
You can use LSM to test whether the network node of a WaveNet locking device is functioning properly and can be reached by LSM.

- ✓ LSM is open.
- ✓ WaveNet is created.
- ✓ WaveNet topology imported (see *LSM import* [▶ 65]). You will see a list of WaveNet-relevant components.

1. Open the assignment via | Network | - **Group orders** - **WaveNet nodes**.



- ↳ The window "Group order for WaveNet nodes" opens.



- 2. Select the LockNodes you want to test.
- 3. Click on the button **Test**.
  - ↳ The "Group order for WaveNet nodes" window closes.
  - ↳ LSM tests the accessibility of the LockNodes.
- ↳ LSM displays test results.

If a LockNode cannot be reached, the problem may be either the LockNode or the RouterNode.

Single LockNode of a segment not reachable	LockNode probably has problems.
No LockNode of a segment reachable	RouterNode probably has problems.

### 6.6.5 Device function test

Check the functionality of your WaveNet devices once a month. Please also refer to the documentation of the devices.

**WARNING****Change in the sequence of emergency functions due to malfunctions**

SimonsVoss and "Made in Germany" stand for maximum safety and reliability. In individual cases, however, malfunctions of your devices cannot be ruled out. This may pose a risk to the safety of persons and property, which are additionally protected by the protective functions in the RingCast.

1. You should test your devices at least once a month (see *Device function test* [▶ 187]) Shorter intervals may also be required according to other regulations concerning your overall system).
2. Test the protective functions at least once a month (see *RingCast function test* [▶ 143]).

**Locking devices and identification media**

1. Activate the locking device.
  - ↳ Locking device is free-running.
2. Activate an authorised identification medium.
  - ↳ The locking device indicates authorised access (or battery warning, then replace batteries).
  - ↳ Locking device opens when the battery condition is good.
3. Wait until the locking device disengages.
  - ↳ Locking device indicates disengagement (or nothing if battery is low).
4. Activate an unauthorised identification medium.
  - ↳ Lockdevice indicates no authorisation (or battery warning, then change batteries).
5. Check the battery level (see *Battery management* [▶ 193]).

**WaveNet devices**

1. Check the signal quality (see *Check signal quality* [▶ 180]).
2. Check accessibility (see *Test reachability (LSM)* [▶ 186] and *Testing accessibility (WaveNet)* [▶ 183]).
3. Check the battery level (see *Battery management* [▶ 193]).

**6.6.6 IO Status and LockNode responsiveness**

You can check the following:

- Signal at the respective input
- Results of the last broadcast for each device
- Status of the outputs
- Analogue voltage present

You can also switch the outputs manually.

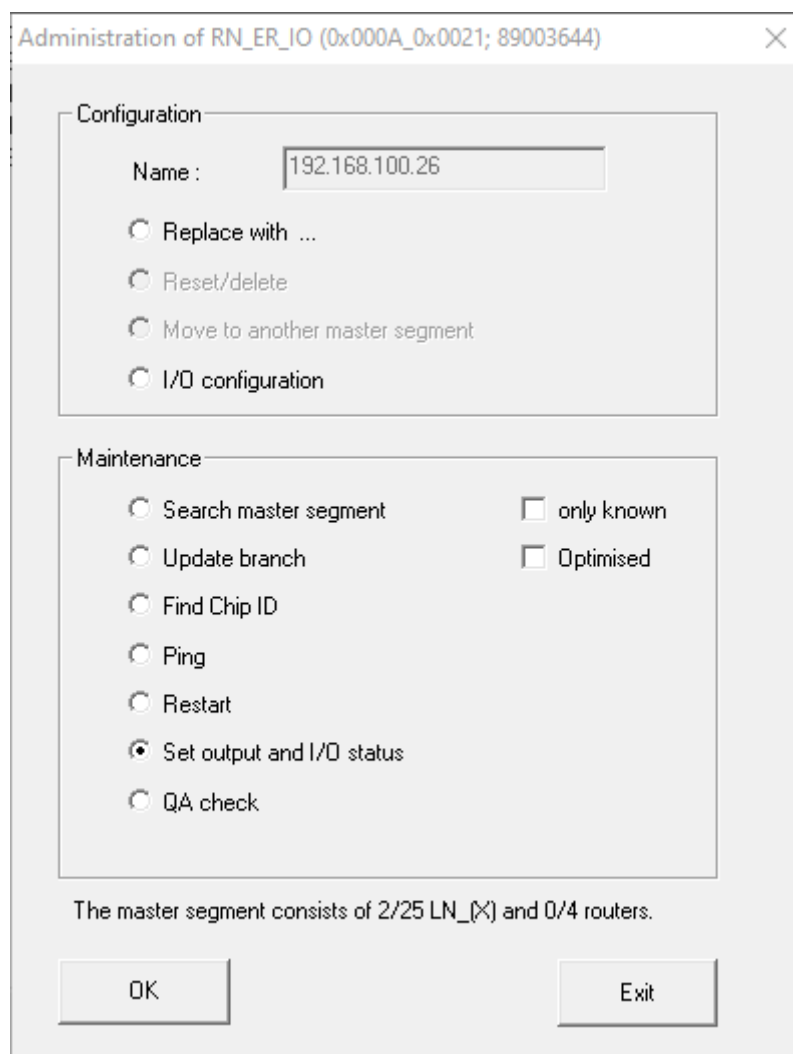


#### NOTE

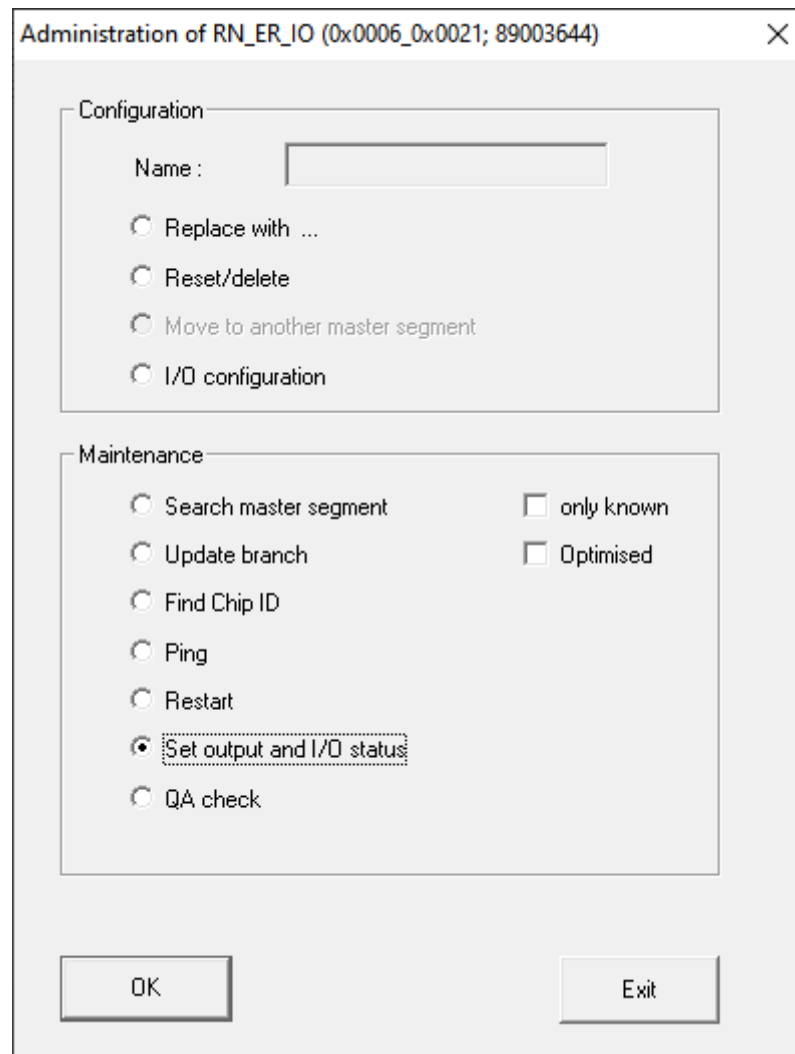
##### Manual switching disabled

You can switch the output depending on identification media or completed reactions (see *I/O configuration and protection functions* [▶ 69]). Outputs controlled by the IO configuration cannot be switched manually.

- ✓ WaveNet Manager opened via LSM (see *Best Practice: From the LSM software* [▶ 37])
  - ✓ RouterNode supplied with power.
  - ✓ RouterNode connected to WaveNet (see *Add RouterNode to WaveNet* [▶ 53]).
1. Click with the right mouse button on the entry of the RouterNode whose IO status you want to read out.
    - ↳ The window "Administration" opens.



2. In the area "Maintenance" select the option  Set output and I/O status.
  - ↳ The "Administration" window closes.
  - ↳ The window "I/O status" opens.



### Status of the inputs

In the area "Status of inputs" you can see the status of the inputs (valid for RN and RN2):

Status of the inputs	Meaning
Off	There is no signal at the input. The applied voltage is lower than the reference voltage.
On	A signal is present at the input. The applied voltage is higher than the reference voltage.

**Comparison voltages (RN and RN2)**

$<0,9 V_{DC}$	LOW (no signal)
$>2.1 V_{DC}$	HIGH (signal)

**Status/responsiveness of the LockNodes**

In the area "Status of inputs" you can also see the behaviour of the LockNodes during the last broadcast:

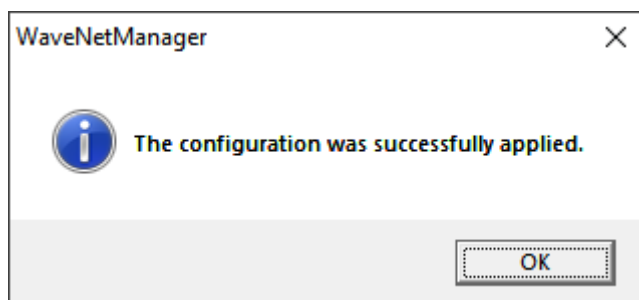
Error	No reply	Successful
Processing of the command in the LockNode of the locking device faulty.	<p>There are two possibilities here:</p> <ul style="list-style-type: none"> <li>■ Locking device with LockNode did not receive command and therefore did not respond.</li> <li>■ Locking device with LockNode has received command but RouterNode has not received response.</li> </ul>	The LockNode locking device has received the command and the RouterNode has received the response.

**Status of the outputs**

In the area "Status and settings of outputs" you can see the status of the outputs and can switch outputs manually.

Status of the inputs	Meaning
<input checked="" type="checkbox"/> Output	Output is switched.
<input type="checkbox"/> Output	Output is not switched.

1. Activate the checkbox  Output of the output that you want to switch or deactivate the checkbox  Output that you no longer want to switch.
2. Click on the button **Set**.
  - ↳ The "I/O status" window closes.
  - ↳ The window "WaveNetManager" opens.



↳ Output is switched.



## 7. Battery management

### 7.1 LockNodes

You can identify a communication problem (failed connection attempt) by a red W in the LSM (see *Monitoring the devices in the network* [▶ 28]). If the communication problem persists even after repeated connection attempts, this can have a number of causes:

- Radio shadow through open door
- Routing problem between CommNode server and RouterNode
- Communication problem between CommNode server and RouterNode, e.g. due to blocked port 2101
- (Partial) network failure, e.g. due to defective switches
- Temporarily suspended IP allocation, e.g. due to maintenance work in the network
- Low batteries

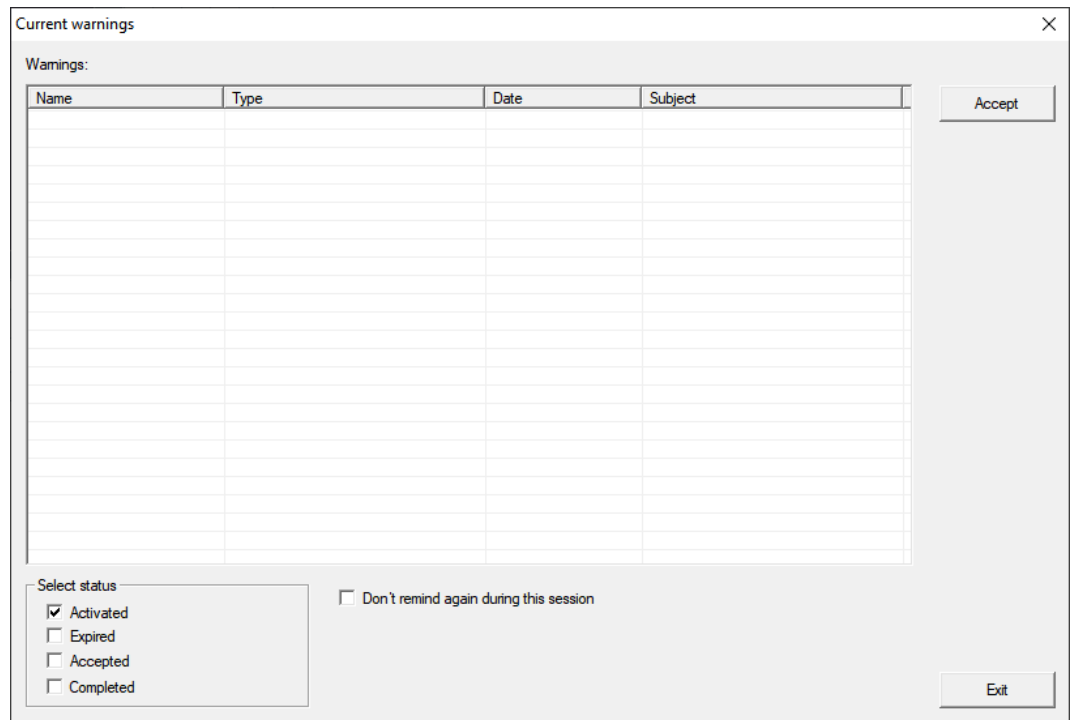
You can easily check the battery condition yourself.

#### Signalling

The signalling of the battery status depends on the LockNode used (see *Signalling the operating status* [▶ 201]).

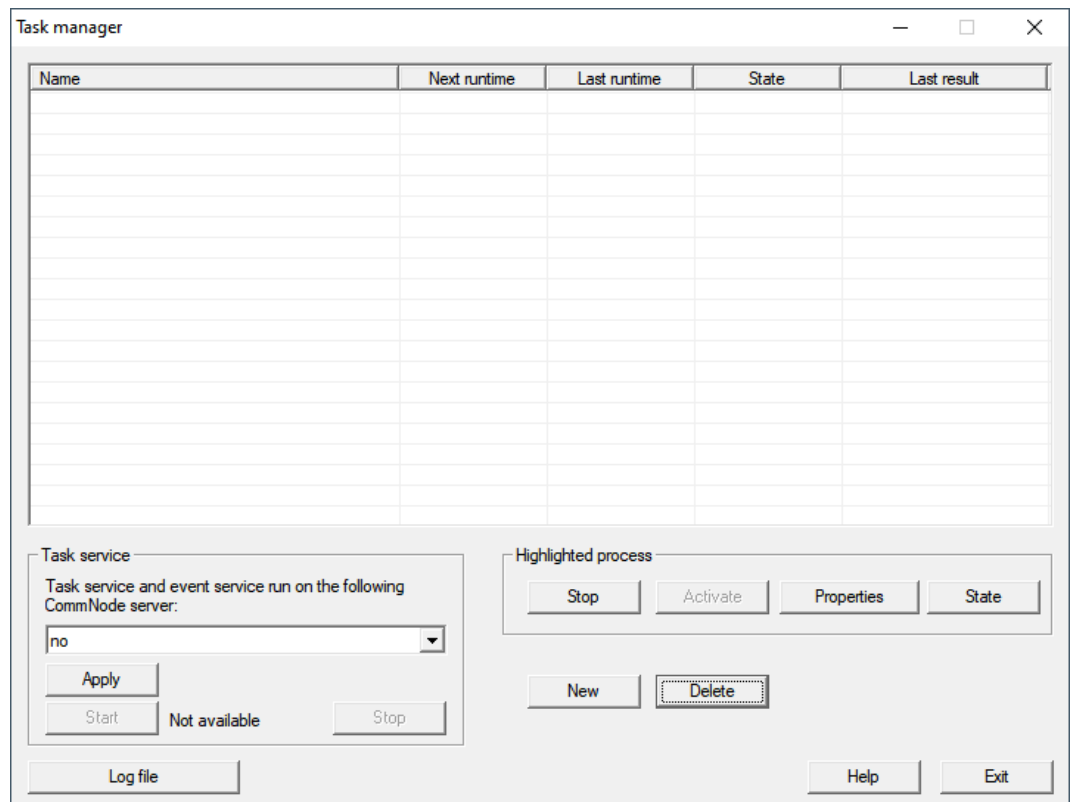
#### Warning monitor (LSM)

The LSM includes a warning monitor (| Reports |, entry [Warning monitor](#)). You will see battery warnings for all locking devices used in the locking system. To use this function effectively, you need a task that regularly tests the battery status of your networked LockNodes.



Setting up a task in  
LSM

1. Via | Network | select the entry **Task manager**.  
↳ The window "Task manager" opens.



2. Click on the button **New**.  
↳ The window "Task" opens.

Task

Name:

Description:

Type:

Status:

Activated (start planned task as stated)

Execute

Once

Repetition interval

As reaction to an event

Start time:

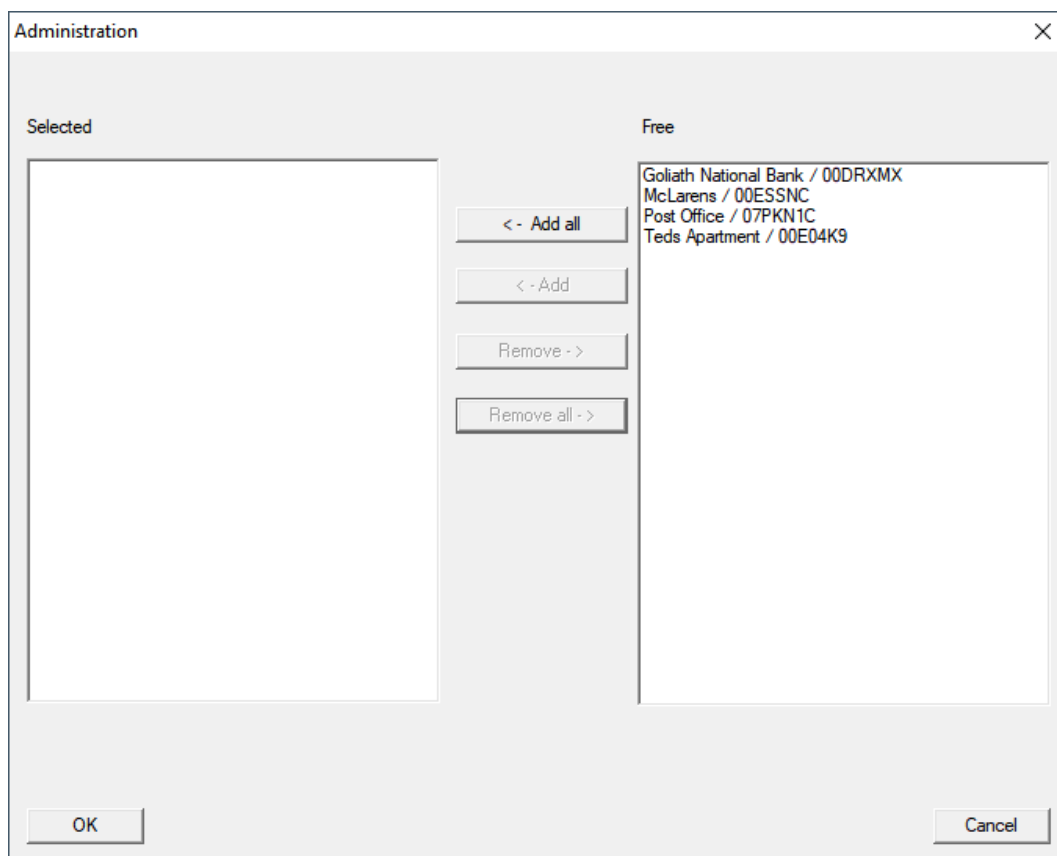
Start date:

Repetition interval:

All

Locks/network nodes

3. Enter a name for the task, e.g. "Test battery condition".
4. If necessary, enter a description.
5. In the dropdown menu ▼ **Type** select the entry "Test Lock Node".
6. Specify the repetition interval (e.g. weekly=168 hours).
7. In the area "Locks/network nodes" click the button **Edit**.
  - ↳ The window "Administration" opens.



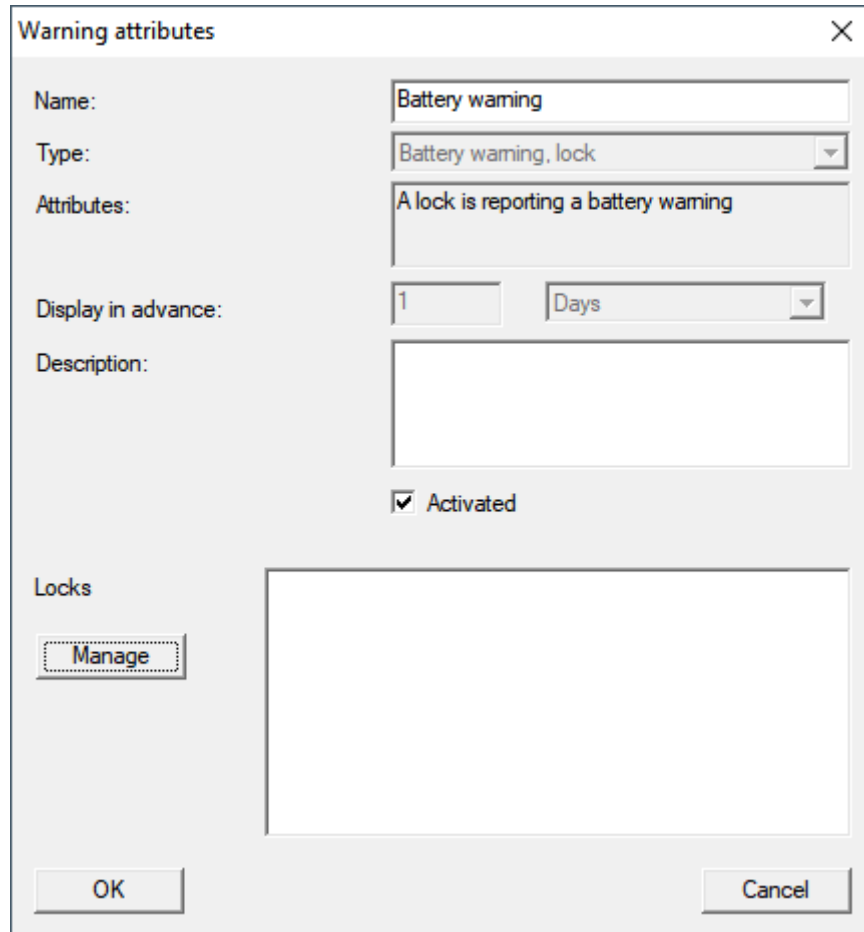
8. Select all locks whose battery status you want to monitor (usually all locks that are battery operated and networked).
9. Click the button **Add**.
  - ↳ The selected locks are now in the left-hand column.
10. Click on the **OK** button.
  - ↳ The window "Administration" closes.
11. Click on the **OK** button.
  - ↳ The "Task" window closes.
12. In the area "Task service" in the dropdown menu **▼ Task service and event service run on the following CommNode server**, select the CommNode you want to use for testing the LockNodes.
13. Click the button **Apply**.
14. Click on the **Exit** button.
  - ↳ Reminder window opens.
15. Click on the **OK** button.
  - ↳ Reminder window closes.
  - ↳ The window "Task manager" closes.
- ↳ Task set up in LSM.

Transfer to communication nodes

1. Via | Network | select the entry **Communication nodes**.
2. Make sure that the communication node you just used is selected.



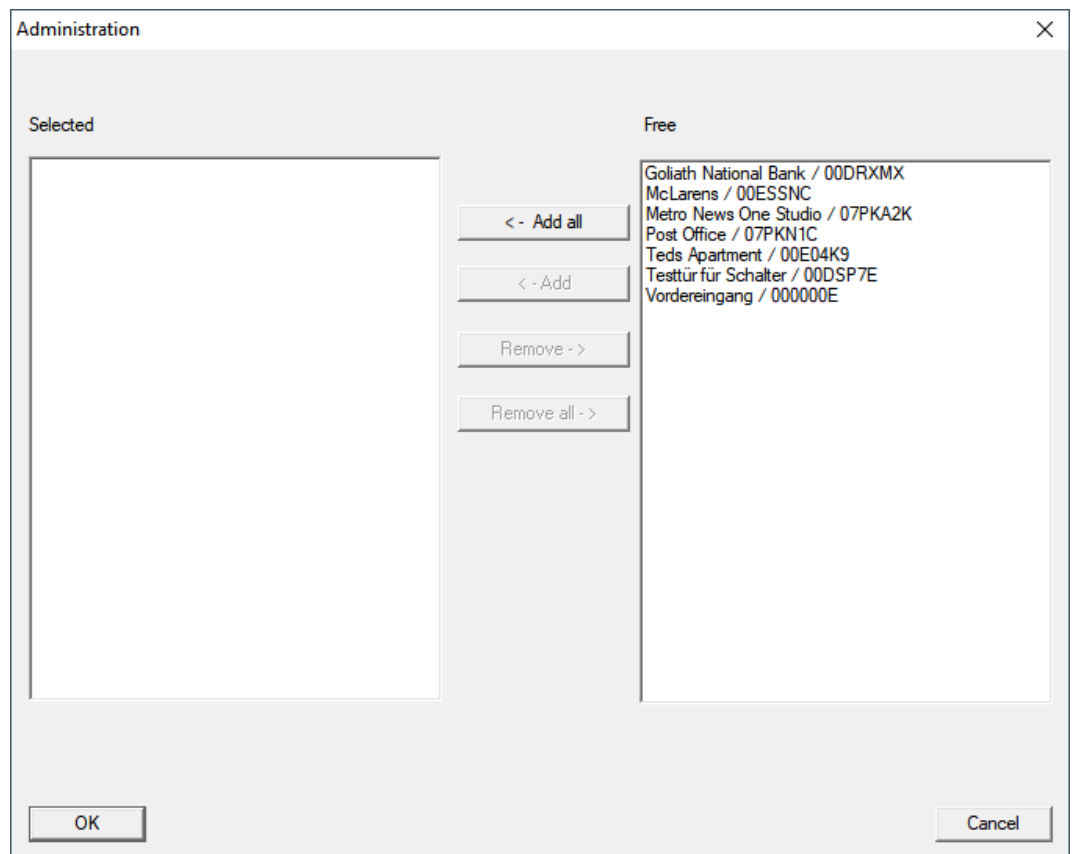
3. Click on the button **Edit**.
  - ↳ The window "Warning attributes" opens.



The screenshot shows a dialog box titled "Warning attributes" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "Battery warning".
- Type:** A dropdown menu showing "Battery warning, lock".
- Attributes:** A text area containing "A lock is reporting a battery warning".
- Display in advance:** A numeric input field set to "1" and a dropdown menu set to "Days".
- Description:** An empty text area.
- Activated:** A checked checkbox.
- Locks:** A section with a "Manage" button and an empty list area.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

4. Make sure that the checkbox  Activated is activated.
5. Click on the button **Manage**.
  - ↳ The window "Administration" opens.



6. Click on the button  .
  - ↳ All locking devices are added.
7. Click on the  button.
  - ↳ The "Administration" window closes.
8. Click on the  button.
  - ↳ The "Warning attributes" window closes.

### 7.1.1 Battery change with integrated LockNodes

LockNodes that are integrated in the locking device (LockNode Inside) are supplied with power by the locking device. When the locking device is battery powered, the battery voltage decreases over time. As soon as the battery voltage falls below a certain value, a battery warning is sent. If the value drops further, the LockNode is deactivated to protect the remaining capacity and the lock can no longer be addressed via WaveNet.

Replace the lock's batteries if there is a battery warning. For details, please refer to the short instructions or the manual for the corresponding lock.

### 7.1.2 Battery change for external LockNodes

1. Remove external LockNodes from the mounting position (for example, open the flush-mounted box).
2. Remove the rear inlay.
3. Remove the old batteries.

4. Insert new batteries.
  - ↳ LED flashes twice briefly (power-on reset).
  - ↳ LockNode is ready for operation.



#### NOTE

##### Batteries in WN.LN.R

The WN.LN.R contains a capacitor for buffering the operating voltage. After removing the batteries, this capacitor maintains the operating voltage for a few seconds. During this time, no power-on reset is triggered and the new battery status is not detected. If you use a battery with reversed polarity, you drain the capacitor and trigger the power-on reset.

1. Insert one of the new batteries into the WN.LN.R with reversed polarity.
  2. Wait five seconds.
    - ↳ Condenser emptied.
  3. Remove the battery.
  4. Insert all batteries correctly.
    - ↳ Power-On-Reset is triggered.
- ↳ New battery condition is detected.

## 7.2 Locking devices

LockNodes that are integrated in the locking devices draw their power from the batteries of the locking devices. Therefore, make sure that the batteries of your locking devices are not empty. You can view the battery status of your locking devices in LSM. If there is a repeated communication problem (red W in the LSM, see also *Monitoring the devices in the network* [▶ 28]), there are several possible causes, including

- Radio shadow through open door
- Routing problem between CommNode server and RouterNode
- Communication problem between CommNode server and RouterNode, e.g. due to blocked port 2101
- (Partial) network failure, e.g. due to defective switches
- Temporarily suspended IP allocation, e.g. due to maintenance work in the network
- Low batteries

You can easily check the battery condition yourself.

Further information on battery replacement at your locking device can be found in the brief instructions or the manual for your lock.



## 8. Signalling the operating status

### RouterNodes

Device	Signalling	Meaning	reaction
WNM.RN2.ER.IO	Flashing, ~1.5 Hz (green LED on cover)	WaveNet configuration available, RouterNode is ready for operation.	
	Flashing, ~0.3 Hz (green LED on cover)	no WaveNet configuration present.	1. Add the RouterNode to your WaveNet (see <i>Add RouterNode to WaveNet</i> [▶ 53]).
	Flashing, briefly (red LED on cover)	Power-on reset.	
	Flickering (green LED on cover)	Data transfer.	
	Continuous lights (red LED on cover)	Software or hardware defect.	1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]). 2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).
WNM.RN.R.IO WNM.RN.CC.IO WNM.RN.CR.IO WNM.RN.EC.IO	Flashing, ~1.5 Hz (green LED)	Ready to receive.	
	Flashing (green LED)	Data transfer.	
	Permanent light (red LED)	<ul style="list-style-type: none"> <li>❑ Software problem</li> <li>❑ Problem with the power supply</li> <li>❑ Hardware problem</li> </ul>	1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]). 2. Check the power supply. 3. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).

## LockNodes

Device	Signalling	Meaning	reaction
WNM.LN.I WNM.LN.I.MP	4x beeping (after contacting)	LockNode and locking device connected.	
	No signal (after contacting)	LockNode and locking device not connected.	<ol style="list-style-type: none"> <li>1. Check the batteries (see leaflet on locking cylinders).</li> <li>2. Reset the LockNode (see <i>LockNodes</i> [▶ 168]).</li> </ol>
WNM.LN.I.S2	4x beeping (after contacting)	LockNode and locking device connected.	
	No signal (after contacting)	LockNode and locking device not connected.	<ol style="list-style-type: none"> <li>1. Check the batteries (see SmartHandle AX manual).</li> <li>2. Reset the LockNode (see <i>LockNodes</i> [▶ 168]).</li> </ol>
WNM.LN.I.SH	4x beeping (after contacting)	LockNode and locking device connected.	
	No signal (after contacting)	LockNode and locking device not connected.	<ol style="list-style-type: none"> <li>1. Check the batteries (see SmartHandle manual).</li> <li>2. Reset the LockNode (see <i>LockNodes</i> [▶ 168]).</li> </ol>
WNM.LN.I.SREL2.G2 WNM.LN.I.SREL.G2	4x flashing (after contacting)	LockNode and SmartRelay connected.	
	No signal (after contacting)	LockNode and SmartRelay not connected.	<ol style="list-style-type: none"> <li>1. Check the power supply of the SmartRelay.</li> </ol>

Device	Signalling	Meaning	reaction
CompactReader Lock-Node (not retrofit-table)	3x flashing, followed by 4x flashing (after battery change)	Power-On-Reset CompactReader, LockNode and CompactReader connected.	
	3x flashing (after battery change)	Power-On-Reset CompactReader, LockNode and CompactReader not connected.	LockNode and CompactReader are permanently connected. <ol style="list-style-type: none"> <li>1. Reset the CompactReader.</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
	4x flashing (after configuration)	LockNode configured in the CompactReader.	
	No signal (after configuration)	LockNode not configured in the CompactReader.	<ol style="list-style-type: none"> <li>1. Check the batteries (see CompactReader Quick Reference Guide).</li> <li>2. Reset the CompactReader.</li> <li>3. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>

Device	Signalling	Meaning	reaction
WNM.LN.R	Flickering (signal LED)	no WaveNet configuration present.	1. Add the RouterNode to your WaveNet (see <i>Add RouterNode to WaveNet</i> [► 53]).
	1x (signal LED)	Transmission/reception power between LockNode and WN.XN.XR poor (check by pressing the button marked <i>Init</i> )	Improve the signal quality (see <i>Improving signal quality</i> [► 152]).
	2x (signal LED)	Transmission/reception power between LockNode and WN.XN.XR sufficient (check by pressing the button marked <i>Init</i> )	
	3x (signal LED)	Transmission/reception power between LockNode and WN.XN.XR optimum (check by pressing the button marked <i>Init</i> )	
WNM.LN.C	2X short (red LED)	Power-on reset.	
	Flickering (alternating red and green)	Data transfer from/to LockNode.	

## Discontinued products

Device	Signalling	Meaning	reaction
WN.RN.XX	2X short (red LED)	Power-on reset.	
	1x (signal LED)	Transmit/receive power between two WN.RN.R poor (test by pressing button on baseboard).	Improve the signal quality (see <i>Improving signal quality</i> [▶ 152]).
	2x (signal LED)	Transmit/receive power between two WN.RN.R sufficient (test by pushing button on baseboard).	
	3x (signal LED)	Transmit/receive power between two WN.RN.R optimum (test by pressing button on baseboard).	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
WN.LN.C	2X short (red LED)	Power-on reset.	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>

Device	Signalling	Meaning	reaction
WN.RN.R	Slow flashing (green LED)	Ready to receive.	
	Fast flashing (green LED)	Data transfer from/to LockNode.	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
WN.RN.XC (Master) WN.RN.CN.XC (Master)	Flickering (red LED) and green LED off.	No slave found in segment.	<ol style="list-style-type: none"> <li>1. Check the cable connection to the slave.</li> <li>2. Check the functionality of the slave.</li> </ol>
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
WN.RN.CX (Slave) WN.LN.C (Slave)	Flickering (red LED) and green LED off.	No master found in segment.	<ol style="list-style-type: none"> <li>1. Check the cable connection to the master.</li> <li>2. Check the functionality of the master.</li> </ol>
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>

Device	Signalling	Meaning	reaction
WN.LN.R	2X short (red LED)	Power-on reset.	
	1x (signal LED)	Transmit/receive power between Lock-Node and WN.XN.XR poor (check by pressing a button on the LockNode baseboard).	Improve the signal quality (see <i>Improving signal quality</i> [▶ 152]).
	2x (signal LED)	Transmit/receive power between Lock-Node and WN.XN.XR sufficient (test by pressing a button on the LockNode baseboard).	
	3x (signal LED)	Transmit/receive power between Lock-Node and WN.XN.XR optimal (check by pressing a button on the LockNode baseboard).	
	1x short (red LED)	Battery full (check after power-on-reset).	
	1x long (red LED)	Battery low (check after power-on reset).	1. Replace the batteries (see <i>Battery change for external LockNodes</i> [▶ 199]).
	1X long, four seconds (red LED)	Battery very weak (check after power-on reset).	1. Replace the batteries (see <i>Battery change for external LockNodes</i> [▶ 199]).
	Permanent light (red LED)	Software or hardware defect.	1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]). 2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 162]).

Device	Signalling	Meaning	reaction
WN.RN.CC	1x long (yellow LED)	Power-on reset.	
	Light (green LED)	Upstream data transmission (slave sends to master).	
	Lights (dark green LED)	Downstream data transmission (master sends to slave).	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
WN.CN.UX	1x long (yellow LED)	USB correctly detected and power-on reset.	
	Flashing, slow (green LED)	Ready to receive	
	Flashing, fast (green LED)	Data transfer from/to LockNode.	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>



Device	Signalling	Meaning	reaction
WN.RP.CC	Permanent lights (yellow LED)	Power supply available.	
	Light (green LED)	Upstream_Data transmission.	
	Lights (dark green LED)	Downstream data transmission.	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>
WN.RN2	Flashing (alternating red and green)	Reset is performed (firmware dependent).	
	Flashing, 1.5 (green)	no WaveNet configuration present.	<ol style="list-style-type: none"> <li>1. Add the RouterNode to your WaveNet (see <i>Add RouterNode to WaveNet</i> [▶ 53]).</li> </ol>
	Flashing, 1 s	WaveNet configuration available, RouterNode is ready for operation.	
	Flashing, 0.5 s	Data transfer.	
	Permanent light (red LED)	Software or hardware defect.	<ol style="list-style-type: none"> <li>1. Perform a power-on reset (see <i>RouterNodes</i> [▶ 159]).</li> <li>2. Replace the device (see <i>Reprogram or replace the device</i> [▶ 163]).</li> </ol>

### 8.1 In LSM

You can view some information about the operating status directly from LSM. This includes:

- Battery status (read lock)

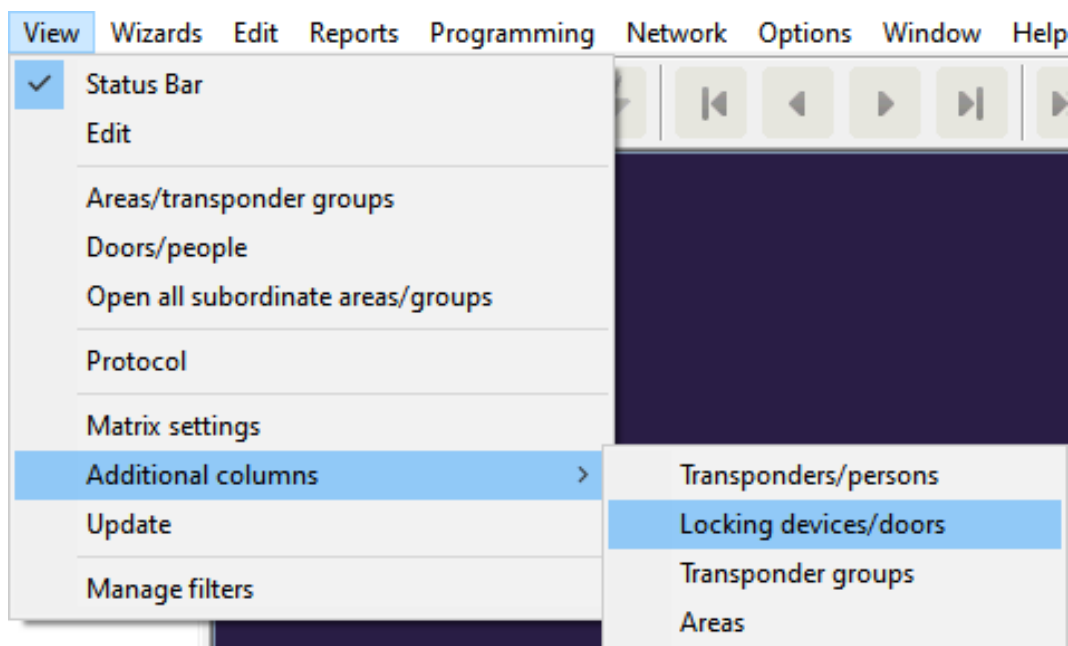
- Status of the network connection (matrix)
- Locking device status (DoorMonitoring) (Matrix or Smart.Surveil)
- Battery warning of the locking device with LockNodes via warning monitor (| Reports | - [Warning monitor](#)), see *LockNodes* [[▶ 193](#)]. To use it effectively, a task for testing the battery status must be set up using the Task Manager. This function is only available in LSM Business/Professional.

Use the button  to refresh the view.

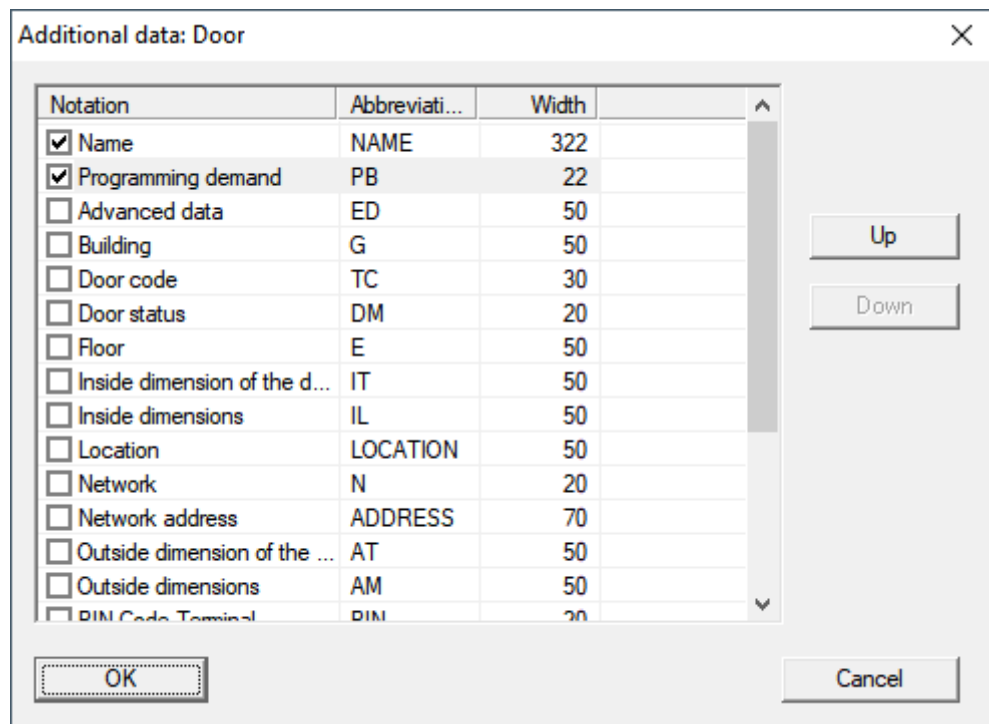
### Show network and door monitoring status

The network connection status is not displayed by default. Activate the network status display as follows:

- ✓ LSM open.
- 1. Via | View | select the entry [Additional columns](#) and there [Locking devices/doors](#).



- ↳ The window "Additional data: Door" opens.



2. Activate the checkboxes  Door status and  Network.
3. Click on the **OK** button.
  - ↳ The window "Additional data: Door" closes.
  - ↳ LSM matrix displays additional columns.

NAME (DOORS/LOCKS)		PE	N	DM
Buero	McLarens		W	
	Post Office		T	
	Teds Apartment	⚡	W	⚠
Entw	Goliath National Bank		W	
	Metro News One Studio			

## 9. Technical specifications

### 9.1 WaveNet in general

#### Number of devices

Also see *Addressing* [[▶ 42](#)].

Network mask	Number of Router-Nodes	Number of LockNodes
8_8	Max. 249	Max. 249 per Router-Node
11_5	Max. 1790	Max. 25 per Router-Node
12_4	Max. 3200	Max. 9 per RouterNode

#### Transmission paths

Different WaveNet devices support different transmission paths (see *Item numbers* [[▶ 14](#)]).

25 kHz	B field for communication between: <ul style="list-style-type: none"> <li>■ Transponders and locking devices</li> <li>■ External LockNodes and locking devices</li> </ul>
868 MHz	SRD field for communication between: <ul style="list-style-type: none"> <li>■ RouterNodes and LockNodes</li> <li>■ RouterNodes and RouterNodes</li> </ul>
Ethernet	Ethernet cabling for communication between: <ul style="list-style-type: none"> <li>■ Computer and RouterNodes</li> </ul>
RS-485	Bus cabling for connection to the network: <ul style="list-style-type: none"> <li>■ RouterNodes</li> <li>■ Wired LockNodes</li> </ul>

#### Radio frequencies in the ISM band

Also see *Radio channel* [[▶ 43](#)].

Channel number	Frequency range	Recommended geographical region of use
0 (only for searching for components)	868.1 MHz (standard version)	Europe
	920.1 MHz (australian version)	Australia
1	868.3 MHz (standard version)	Europe
	920.3 MHz (australian version)	Australia
2	868.5 MHz (standard version)	Europe
	920.5 MHz (australian version)	Australia
9	869.9 MHz	Europe
	921.9 MHz	Australia

### Adjustable triggers for relay output (RouterNode 2)

Also see *I/O configuration and protection functions* [► 69].

- Access to authorised identification media
- Access attempts by unauthorised identification media
- Access of authorised identification media or attempts to access unauthorised identification media
- Completed responses (except activation)

### Triggers for events

Also see *I/O configuration and protection functions* [► 69].

- Switching from input 1
- Switching from input 2
- Switching from input 3

Events at the analogue input are forwarded to the LSM and evaluated there:

- Exceeding an analogue threshold value voltage
- Undershooting of an analogue threshold voltage
- Exceeding or falling below an analogue threshold value voltage

**Adjustable reactions to events (RouterNode 2)**

Also see *I/O configuration and protection functions* [[▶ 69](#)].

- Block lock
- gunman attack function
- Emergency release
- Remote opening
- Activation

**Adjustable delay between event and reaction (RouterNode 2)**

- 0 s
- 8 s
- 16 s
- 24 s
- 32 s
- RingCast (see *RingCast* [[▶ 95](#)])

**9.2 RouterNodes****WNM.RN2.ER.IO**

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> <li>■ Ethernet</li> </ul>	<ul style="list-style-type: none"> <li>■ RJ45 (Network/PoE)</li> <li>■ Round plug <math>\varnothing</math> 5.5 mm, <math>\varnothing</math> pin 2.0 mm (power supply)</li> <li>■ Screw terminal block 2-pole, wire diameter 0.14 mm<sup>2</sup> to 1.5 mm<sup>2</sup> (IO-<math>V_{out}</math> for external applications)</li> <li>■ MCX socket (optional external antenna)</li> <li>■ Spring terminal block 10-pin, wire diameter 0.14 (rigid) or 0.2 (flexible) mm<sup>2</sup> to 0.5 mm<sup>2</sup> (IO connector)</li> </ul>	<p>9 V<sub>DC</sub> to 32 V<sub>DC</sub> or PoE according to IEEE 802.3af, 3 W</p> <p>Power supply via PoE and round plug simultaneously possible: Round plug &gt; 12 VDC → Round plug used, round plug &lt; 12 VDC □ PoE used</p>	172.1×85.9×32.8 mm

## WNM.RN.R.IO

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	<ul style="list-style-type: none"> <li>■ connecting terminals for an external plug-in power supply</li> <li>■ FME bushing (antenna)</li> <li>■ Molex PicoBlade 10-pin (IO connector)</li> </ul>	<p>9 V<sub>DC</sub> bis 24 V<sub>DC</sub>, min. 3 VA</p> <p>Non-IO versions differ, see brief instructions</p>	<p>98×64×40 mm or 98×64×130 mm with antenna</p>

## WNM.RN.CC.IO

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ RS-485</li> </ul>	<ul style="list-style-type: none"> <li>■ connecting terminals for an external plug-in power supply</li> <li>■ Connection terminals for RS-485</li> <li>■ Molex PicoBlade 10-pin (IO connector)</li> </ul>	<p>9 V<sub>DC</sub> bis 24 V<sub>DC</sub>, min. 3 VA</p> <p>Non-IO versions differ, see brief instructions</p>	<p>98×64×40 mm</p>

## WNM.RN.CR.IO

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> <li>■ RS-485</li> </ul>	<ul style="list-style-type: none"> <li>■ connecting terminals for an external plug-in power supply</li> <li>■ Connection terminals for RS-485</li> <li>■ FME bushing (antenna)</li> <li>■ Molex PicoBlade 10-pol (IO connector)</li> </ul>	<p>9 V<sub>DC</sub> bis 24 V<sub>DC</sub>, min. 3 VA</p> <p>Non-IO versions differ, see brief instructions</p>	<p>98×64×40 mm or 98×64×130 mm (with antenna)</p>

## WNM.RN.EC.IO

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ Ethernet</li> <li>■ RS-485</li> </ul>	<ul style="list-style-type: none"> <li>■ connecting terminals for an external plug-in power supply</li> <li>■ Connection terminals for RS-485</li> <li>■ RJ45 socket (Ethernet)</li> <li>■ Molex PicoBlade 10-pin (IO connector)</li> </ul>	<p>9 V<sub>DC</sub> to 48 V<sub>DC</sub>, min. 3 VA or PoE in acc. with IEEE 802.3af, 3 W</p> <p>Non-IO versions differ, see brief instructions</p>	98×64×40 mm

## 9.3 LockNodes

## WNM.LN.I

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	Contacts for locking devices	Supply from locking device	Integrated in cylinder

## WNM.LN.I.S2

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	Contacts for locking devices	Supply from locking device	Integrated in SmartHandle AX

## WNM.LN.I.SH

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	Contacts for locking devices	Supply from locking device	Integrated in SmartHandle 3062

## WNM.LN.I.SREL2.G2

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	Contacts for locking devices	Supply from locking device	Integrated in SmartRelay 2 (G2)

## WNM.LN.I.SREL.G2

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> </ul>	Contacts for locking devices	Supply from locking device	Integrated in SmartRelay (G2)



## WNM.LN.R

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 868 MHz</li> <li>■ 25 kHz</li> </ul>	<ul style="list-style-type: none"> <li>■ 3 inputs (potential-free, pulses in 2 Hz cycle : 1 ms, 35 <math>\mu</math>A)</li> <li>■ Output (open drain, max. 25 V<sub>DC</sub>, max. 650 mA continuous current (2 A inrush current - contact resistance 0.5 <math>\Omega</math>)  IO cable with 6-pin Molex connector required (WN.LN.SENSOR.CABLE)</li> </ul>	<p>2x CR<sup>2</sup>/<sub>3</sub>AA (lithium 3,6V - tadiran SL-761)</p> <p>Service life approx. 6 years</p>	37×Ø53 mm

## WNM.LN.C

transfer media	Interfaces	Power supply	Dimensions
<ul style="list-style-type: none"> <li>■ 25 kHz</li> </ul>	<ul style="list-style-type: none"> <li>■ Connection terminals for RS-485</li> <li>■ Connection terminals for external power supply</li> <li>■ Output (open drain, max. 25 V<sub>DC</sub>, max. 650 mA continuous current (2 A inrush current - contact resistance 0.5 <math>\Omega</math>)  IO cable with 6-pin Molex connector required (WN.LN.SENSOR.CABLE)</li> </ul>	9 V <sub>DC</sub> bis 24 V <sub>DC</sub> , ~15 mA	37×Ø53 mm

## 10. Help and other information

### Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

### Software and drivers

Software and drivers can be found on the website:

<https://www.simons-voss.com/en/service/software-downloads.html>

### Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

### Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

### Email

You may prefer to send us an email.

[support-simonsvoss@allegion.com](mailto:support-simonsvoss@allegion.com)

### FAQs

You will find information and help in the FAQ section:

<https://faq.simons-voss.com/otrs/public.pl>

### Address

SimonsVoss Technologies GmbH  
Feringastr. 4  
D-85774 Unterfoehring  
Germany



## This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide ([www.allegion.com](http://www.allegion.com)).

### Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2024, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

**SimonsVoss**  
technologies

Made in Germany

A BRAND OF

