Manual
WaveNet-Manager 2.6

12.2016

Manual
WaveNet-Manager 2.6

1 Introduction

You can use the SimonsVoss WaveNet Manager to set up radio and/or cable networks on your own accord. You must have extensive knowledge of the application software (LSM), WaveNet technology and the SV hardware components to do so. Knowledge of IT administration (TCP/IP, LAN / WAN and COM ports) is required.

WaveNet Manager provides automatic address assignation (hex addresses) for all network nodes – Central-, Router- and LockNodes – in a SimonsVoss radio/cable network. A scan will detect any network nodes already installed. Each component sends a feedback signal with its chip ID to WaveNet Manager. A network structure is then formed in WaveNet Manager and the automatically generated Hex addresses and chip IDs are displayed. When WaveNet Manager is closed, this structure (= topology [Hex address]) is then transferred to LSM.

It is possible to import the topology (LSMWNNet_XXYY_NetID.csv) manually for LSM, Version earlier than 3.1. 'Automatic configuration' within LSM enables the selected locking devices to be 'networked' and to be managed by the application software (LSM).

A WaveNet which has been configured with WaveNet Manager can be changed, extended or reset at any time.

The radio frequency for Europe and Asia is 868 MHz and 915 MHz for the US. Two special frequencies are supported for Hong Kong and Malaysia.

Existing WaveNet installations which were not created with WaveNet Manager **cannot** be managed using WaveNet Manager. **Prior approval** is required from SimonsVoss for hybrid operation between conventional WaveNet installations and WaveNet Manager. Contact your SV field sales representative and/or the Service Department for more information.

Note down the associated chip ID for the installation location, so that you can identify where the different network nodes are located. Remember that precise documentation and a data backup need to be maintained on a continuous basis to ensure stable operation.

2 Safety instructions

SimonsVoss Technologies GmbH reserves the right to make changes to the product without prior notification. For this reason, descriptions and illustrations in these documents may differ from the latest versions of products and software. The original German version should be taken as a reference in cases of doubt. Errors and spelling mistakes excepted.

You can obtain more information about SimonsVoss Technologies GmbH products online at: www.simons-voss.com

⚠ CAUTION

Access through a door may be blocked due to incorrectly fitted or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of incorrect installation, such as blocked access to injured persons or those at risk, physical damage or any other losses.

⚠ CAUTION

People who have electronic, medical implants, such as pacemakers and hearing aids, must maintain a minimum distance of 30 cm between the implant and network components and should be specially briefed about this requirement. As a precaution, people who have implants should consult their doctor regarding any possible hazards caused by radio component assemblies (868/915 MHz).

NOTICE

If you use the safety functions in the ordered product with IO functions, such as WNM.RN.ER.IO with anti-gunman attack, block lock, emergency release and remote opening, external interferences over which neither SimonsVoss Technologies GmbH or the product have control may affect the selected safety functions or cause a complete failure in the network. Such interferences include disruption in the WaveNet frequency range, an unstable power supply or defective cabling. SimonsVoss Technologies GmbH accepts no liability for such external interferences. SimonsVoss Technologies GmbH therefore recommends triggering the selected safety functions at least once a month to test all product components and their correct operation, i.e. all IO routers used (e.g. WNM.RN.ER.IO), all lock nodes used (e.g. WNM.LN.I), all lock devices used, such as cylinders, SmartHandles and SmartRelays.

3 System requirements

General information

- Local administrator rights for installation
- Communication TCP/IP (NetBios active), LAN (recommended: 100 MBit)
- Windows domain
- Acrobat Reader (for help function)

Client (minimum requirements for hardware)

- Monitor at least 19" (or larger for displaying the matrix screen)
- Processor 2.66 GHz (or faster)
- 2 GB RAM (or more)
- Client's operating system (static IP address, name resolution for LSM)
- Windows OS (XP Prof. SP3 / Vista Business / 7, 8, 8.1 Professional)
- NET Framework 2.0 (for LSM)
- USB interface / LAN connection
- Resolution min. 1024 x 768

4 Possible network structures WaveNet

TCP/IP with WNM.RN.E(X) and RN2, WLAN with WNM.RN.W(X), USB with WNM.CN.U(X) or serial with WNM.CN.S(X). Within WaveNet: by radio, 868 MHz (915 MHz in the US) and/or wired via a RS485.

5 Components

Central-, router- And LockNodes must be WNM components. Only components that start with "WNM" (order code) are suitable for autoconfiguration.

WaveNet Manager: Free download at www.simons-voss.com Make sure that only WNM components are in the radio range that are to be configured and/or programmed.

Locking System Management (LSM)

6 Procedure

All locking devices (cylinders, SmartRelays and similar) must be programmed correctly and thus form an integral part of the locking system.

The CommNode server and the communication node(s) must be set up correctly (if required) if LSM is used. WNM.RN.E(X) / WNM.RN.W(X) / RN2 must be configured with the necessary network parameters (IP address, Gateway, SSID and similar). All necessary drivers **must** be installed beforehand. VPN must be set up for LAN/WAN if necessary.

7 Installation of the WaveNet Manager

Install WaveNet Manager; *e.g. in the installation directory of the previously installed LSM software.*

8 WaveNet Manager update

If WaveNet Manager has already been installed, only the following files need to be replaced in the WaveNet installation folder:

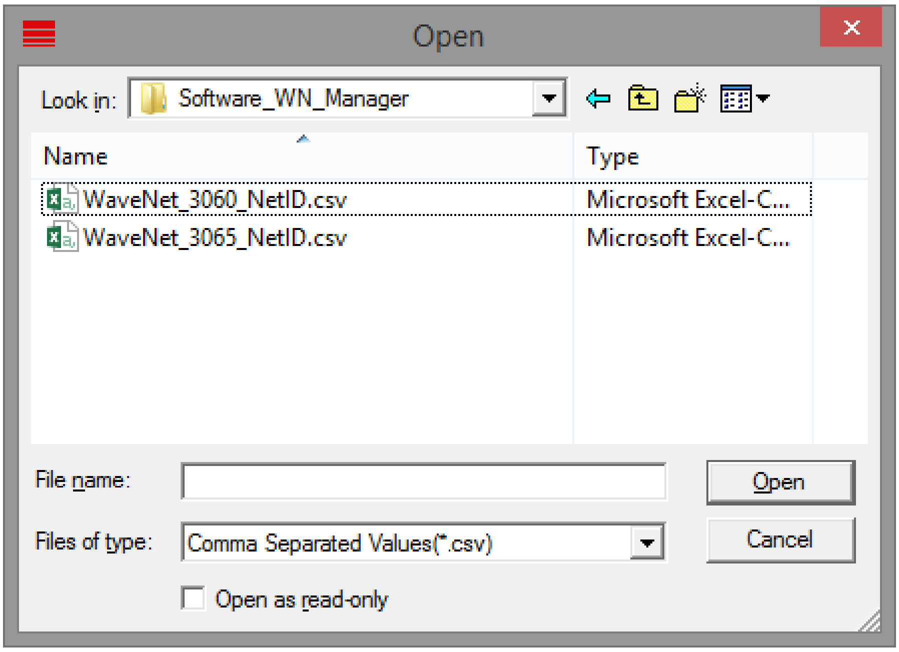
- boost_threadmon.dll
- WaveNetManager.exe
- WNIPDiscoveryLib.dll
- WNManager.ini

You will find the latest version of WaveNet Manager Infocenter/Downloads/ WaveNet Manager at www.simons-voss.com.

9 Start the WaveNet Manager

9.1 Manually

1. Execute the "WaveNetManager.exe" in the installation directory.
2. Select a topology or create a new one by pressing a new network.



Look in: Software_WN_Manager

Name	Type
WaveNet_3060_NetID.csv	Microsoft Excel-C...
WaveNet_3065_NetID.csv	Microsoft Excel-C...

File name:

Files of type: Comma Separated Values(*.csv)

☐ Open as read-only

⇨

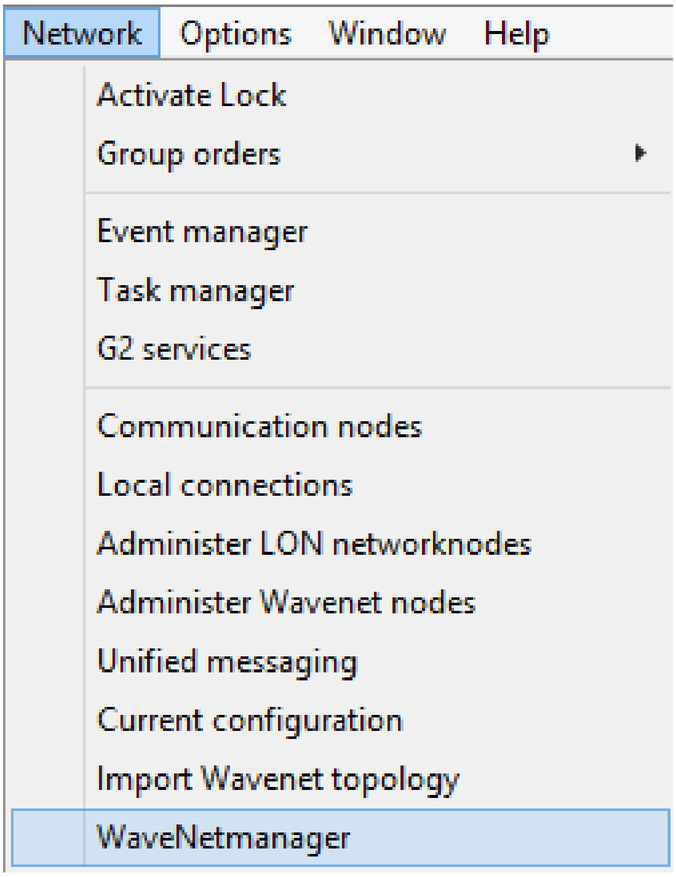
NOTICE

If there is more than one WaveNet topology, a dialogue box appears to select the respective network. If no topology is selected (cancel), the WaveNet Manager starts and a new network can be created.

9.2

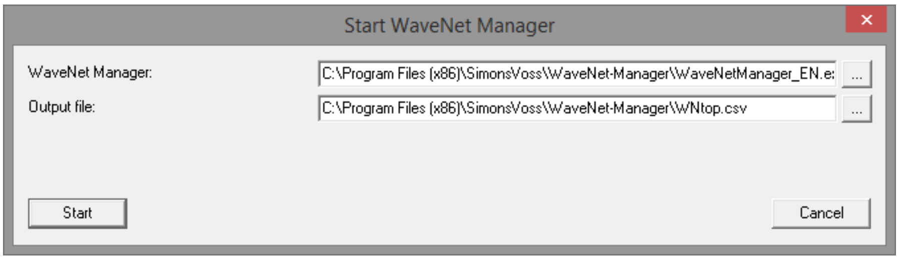
From the LSM software

1. Open WaveNet Manager via the network menu / WaveNet Manager.



⇨

2. Check file paths and execute the WaveNet Manager by clicking on "Start".



WaveNet Manager: C:\Program Files (x86)\SimonsVoss\WaveNet-Manager\WaveNetManager_EN.e:

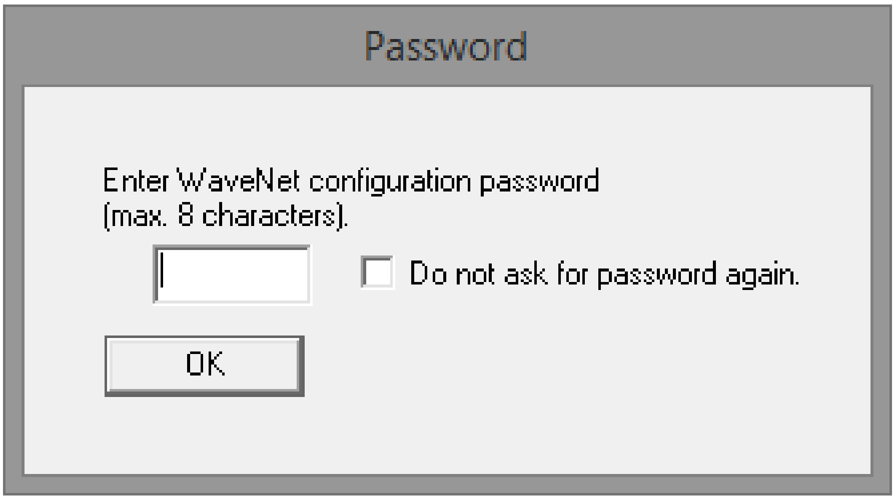
Output file: C:\Program Files (x86)\SimonsVoss\WaveNet-Manager\WNtop.csv

⇨

10 Password

The password is freely selectable and must consist of 1 to 8 characters. This password is programmed in all WaveNet components. The password cannot be changed at a later time!

The password is required to prevent accidental reprogramming of existing/ third-party networks. Only one password per WaveNet or LSM database may be used.



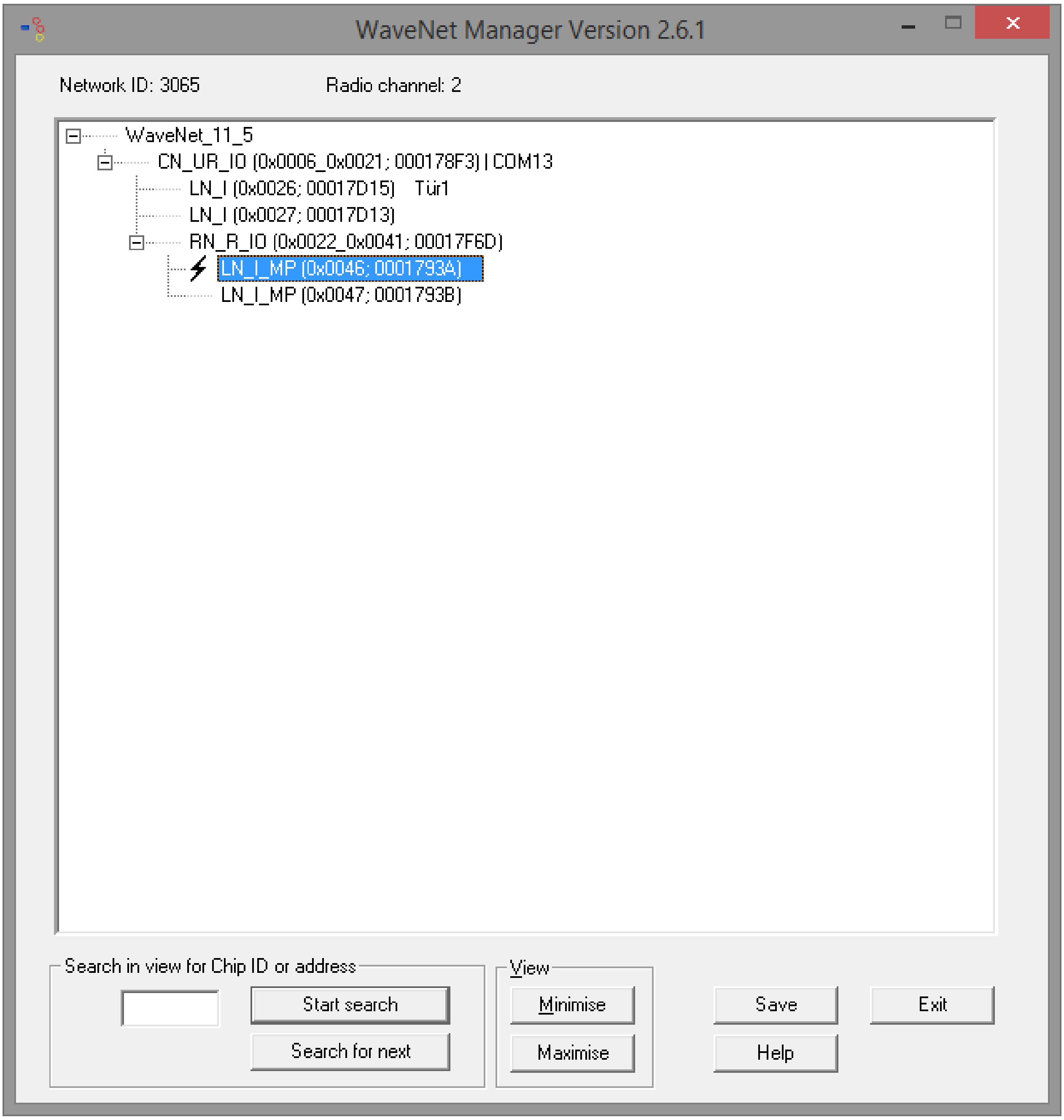
Password

Enter WaveNet configuration password
(max. 8 characters).

☐ Do not ask for password again.

11 WaveNet Manager

11.1 Network ID


WaveNet Manager Version 2.6.1

Network ID: 3065 Radio channel: 2

WaveNet_11_5
CN_UR_IO (0x0006_0x0021; 000178F3) | COM13
LN_I (0x0026; 00017D15) Tür1
LN_I (0x0027; 00017D13)
RN_R_IO (0x0022_0x0041; 00017F6D)
LN_I_MP (0x0046; 0001793A)
LN_I_MP (0x0047; 0001793B)

The default network ID is: DDDD (default). All non-programmed WaveNet components have this network ID. A new network ID must be issued manually at a later stage.

A flash (grey programming flash) indicates that the configuration could not be completed in this segment for this component.

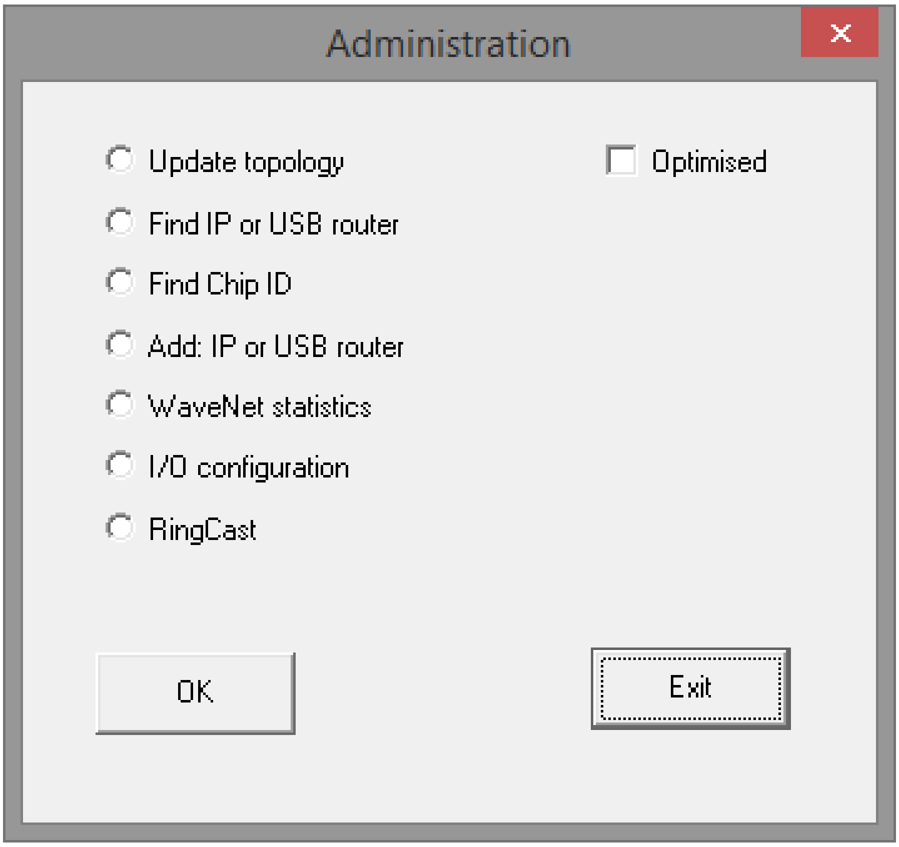
11.2 Radio channel

All unprogrammed WaveNet components have a standard frequency (default radio channel). At a later time, a different radio channel has to be assigned.

The default radio channel is always used in addition to the manually selected one. In this manner, new components can be added to existing radio networks. At some times, transmission takes place on two different frequencies. During normal operation only one frequency is used.

11.3 WaveNet

1. Administration can be launched using the right-hand mouse button on "WaveNet_11_5", "WaveNet_12_4" or "WaveNet_8_8" (in WaveNet Manager).

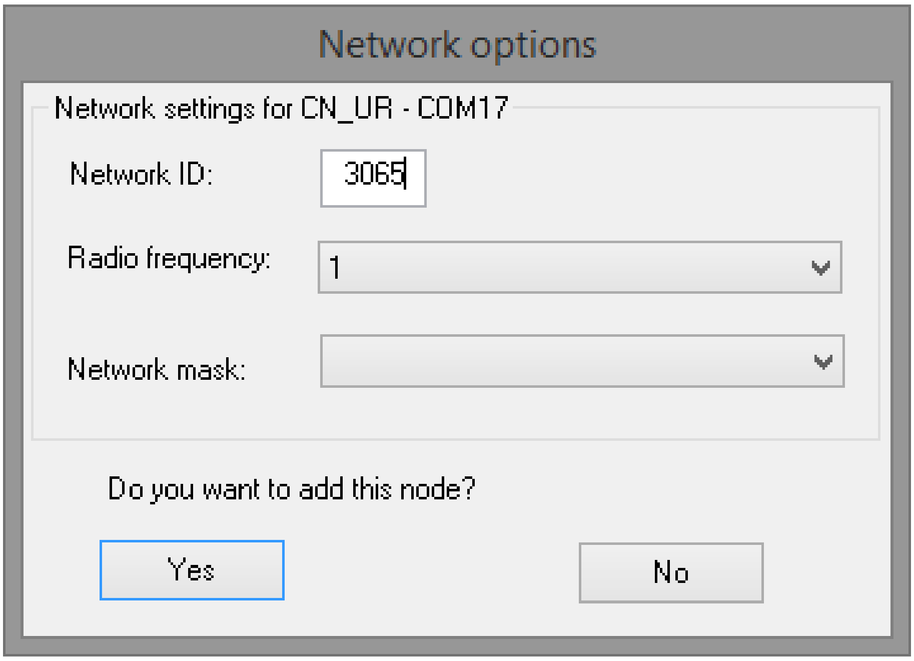


⇨

New network A network ID must be entered if a new network needs to be detected or created. Possible characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F – max. four characters. The addresses 0000, 0001, DDDD and FFFF are not permitted as a network ID. You also need to select a radio frequency manually. Channels 1-9 and 11-12 are available for this purpose. 11 and 12 are special frequencies which may be used for Hong Kong or Malaysia. Channels 11 and 12 may also be used in Europe. The network mask can also be set. This determines the number of segments.

- WaveNet_8_8
  - Max. 249 routers and 249 LockNodes can be addressed per router.
- WaveNet_11_5
  - Max. 1790 routers and 25 LockNodes can be addressed per router. 249 routers plus 249 LockNodes per router can be addressed in a wired segment.
- WaveNet_12_4
  - Max. 3,200 routers and 9 LockNodes can be addressed per router. 249 routers plus 249 LockNodes per router can be addressed in a wired segment.

If the dialogue box is checked "Yes" when closed, the network ID and radio frequency are programmed into the new components. This dialogue box does not appear in existing networks. The network mask determines the future address (address and mask).



Network settings for CN_UR - COM17

Network ID: 3065

Radio frequency: 1

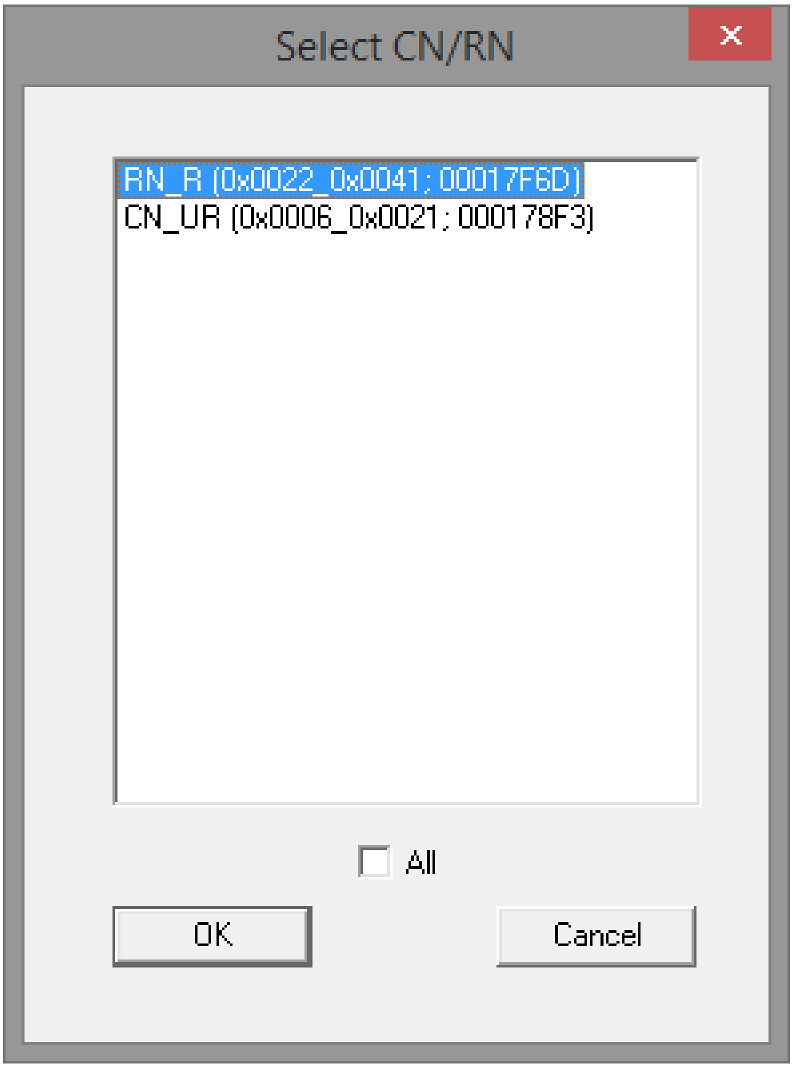
Network mask:

Do you want to add this node?

Update topology

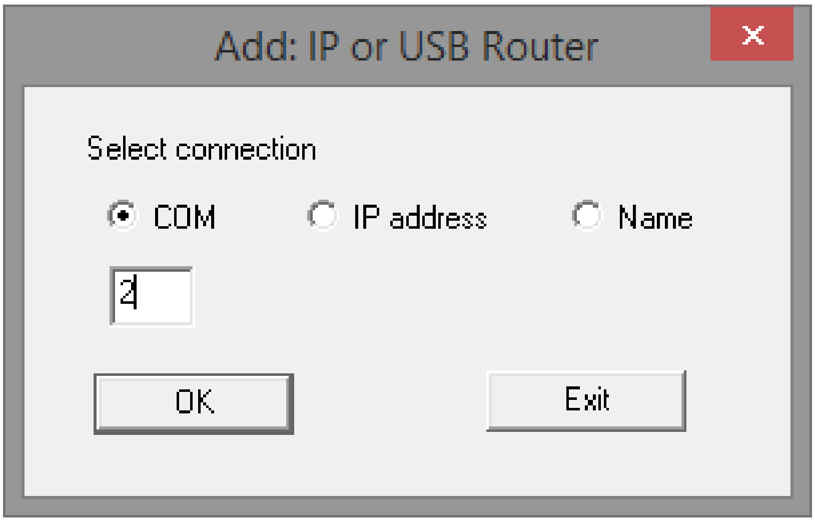
The whole network is updated automatically followed by messages in WaveNet Manager with hex address and chip ID for all network nodes/components reached. This may take a few minutes, depending on the size (calculated value --> about two minutes per router).

	Optimised: If the 'Optimised' setting is used, a search is initiated for both new nodes and previously configured nodes. During this process, configured nodes (from other segments) may be moved to another segment to provide enhanced availability. If this setting is not used, then the system will search for new nodes only.
Search by IP or USB router	The search is for these components only (see CN_U(X), CN_S(X), RN_E(X), RN_W(X), RN2 - maintenance [▸ 37] / "Search result").
Search by chip ID	search for a component in the entire network/topology using its chip ID.
Select CN/RN	If 'Update topology' or 'Search for chip ID' is selected, the function may be implemented in the master segment concerned by making a suitable selection (between CN / RN).

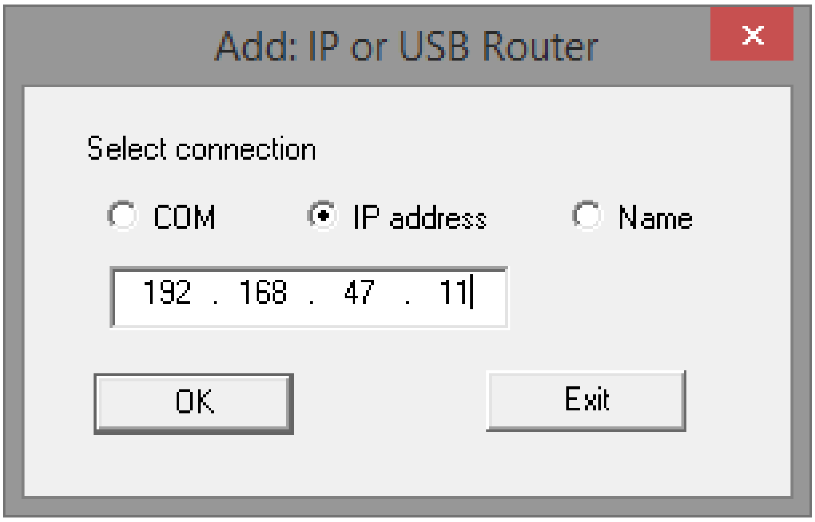


RN_R (0x0022_0x0041; 00017F6D)
CN_UR (0x0006_0x0021; 000178F3)

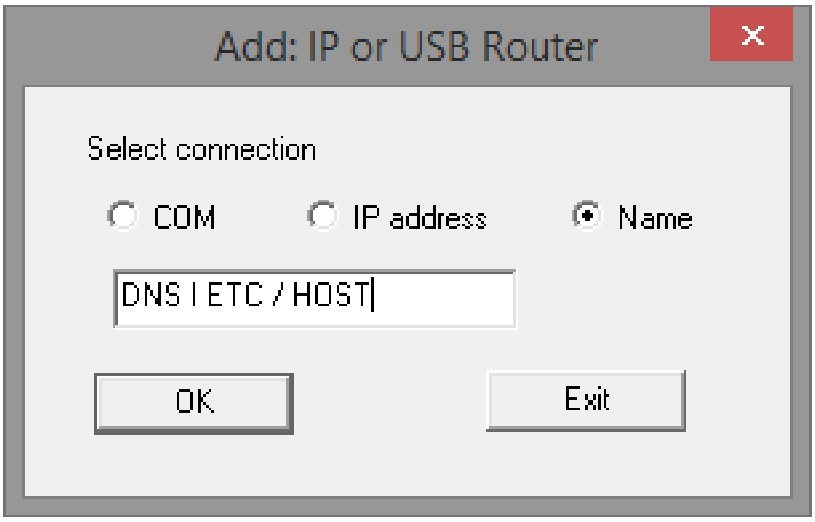
Add: IP or USB Router These components are added directly to the topology using a COM port, IP address, DNS or an ETC/HOST file.



2



192 . 168 . 47 . 11



Add: IP or USB Router

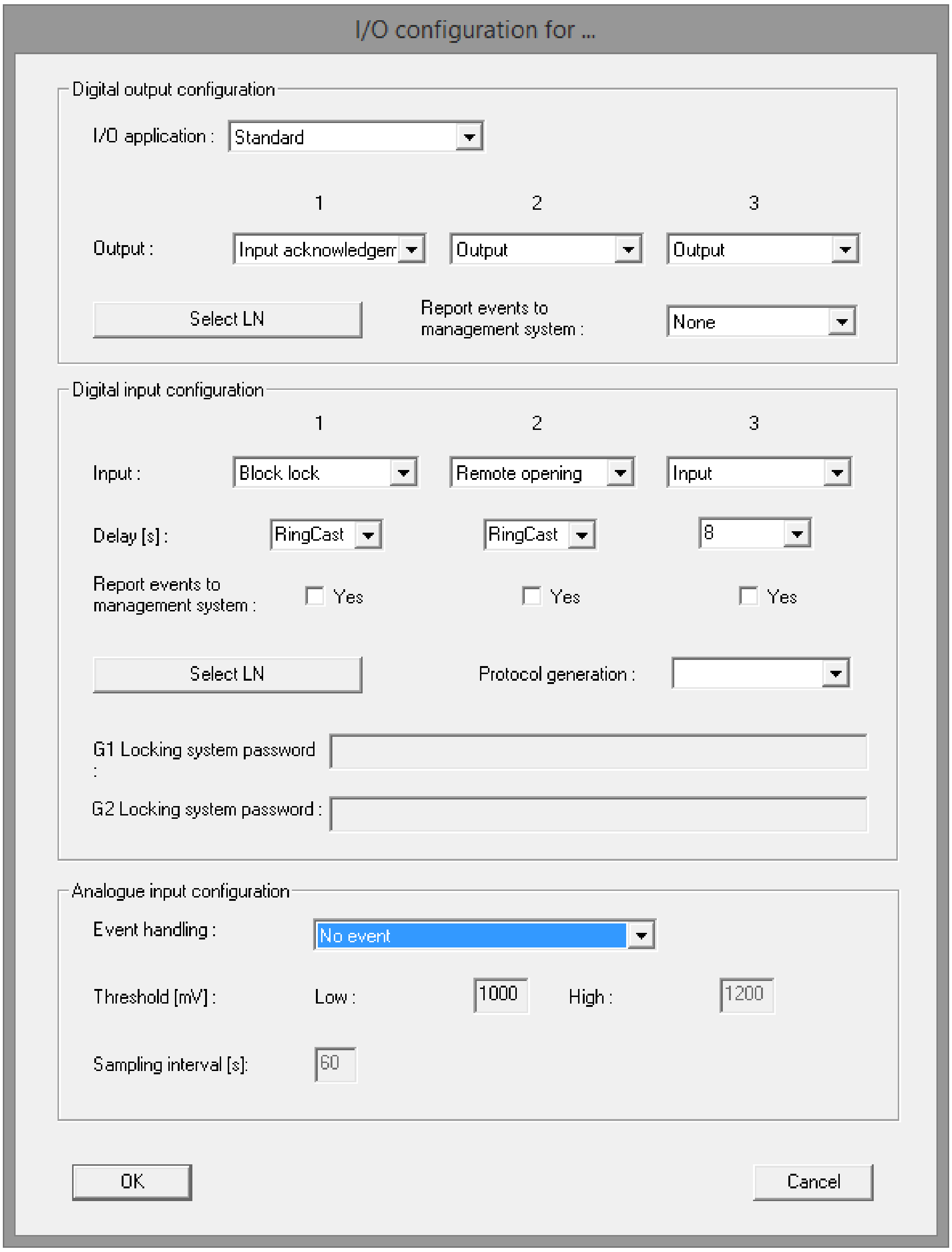
Select connection

○ COM ○ IP address ● Name

DNS I ETC / HOST

WaveNet statistics Displays all configured WNM components.

I/O configuration This is where the global settings can be configured for the inputs and outputs. Configuration(s) are thus made for all selected routers, such as the block lock (= input) and/or an input feedback (= output). Time delays between 0-32 seconds can also be configured per input, i.e. the router does not start the broadcast until after the pre-set time delay.



I/O configuration for ...

Digital output configuration

I/O application : Standard

	1	2	3
Output :	Input acknowledgem	Output	Output

Report events to management system : None

Digital input configuration

	1	2	3
Input :	Block lock	Remote opening	Input
Delay [s] :	RingCast	RingCast	8
Report events to management system :	☐ Yes	☐ Yes	☐ Yes

Protocol generation :

G1 Locking system password :

G2 Locking system password :

Analogue input configuration

Event handling : No event

Threshold [mV] : Low : 1000 High : 1200

Sampling interval [s]: 60

RingCast

This function allows input signals to be forwarded between radio routers via the transmission path or directly via the network (for RN2 deliveries from 2017 only). meaning that only one I/O router actually needs to be connected by cable. After the input has been changed, the I/O router starts with the pre-set broadcast, such as a block lock signal. The broadcast takes about 1 second in this segment. Once completed at the wireless interface, it is then transmitted to the next selected router. The next selected router then starts its broadcast for its respective segment. At least two routers must be able to communicate at the wireless interface for this process to take place. You thus **need to know** the routers' installation locations or the three-dimensional structure of the radio network. You must test all locking devices. You must ensure, **firstly**, that the router transmits the RingCast signal to the next respective router wirelessly and, **secondly**, that the locking devices carry out the right functions as a result.

Required firmware versions:

CN_XX and RN_XX	TM 30.11; FW 0.0
CN_XX_IO and RN_XX_IO	TM 30.11; FW 0.0
LN_C and LN_R	TM 30.8; FW 15.1
LN_I_XX	TM 30.8; FW 16.3
LN_I_ XX _SOC	TM 30.11; FW 16.3
LN_I_MP	TM 30.11; FW 17.3

If the global I/O configuration has been selected beforehand, Input 1, Input 2 or Input 3 appear in the radio domain. It is not possible to changed the "Name".

Select domain: new --> a new radio domain can be created.

Name: You can enter a name for the new radio domain.

Input: Selection of the input 1 | 2 | 3 for all routers in this radio domain.

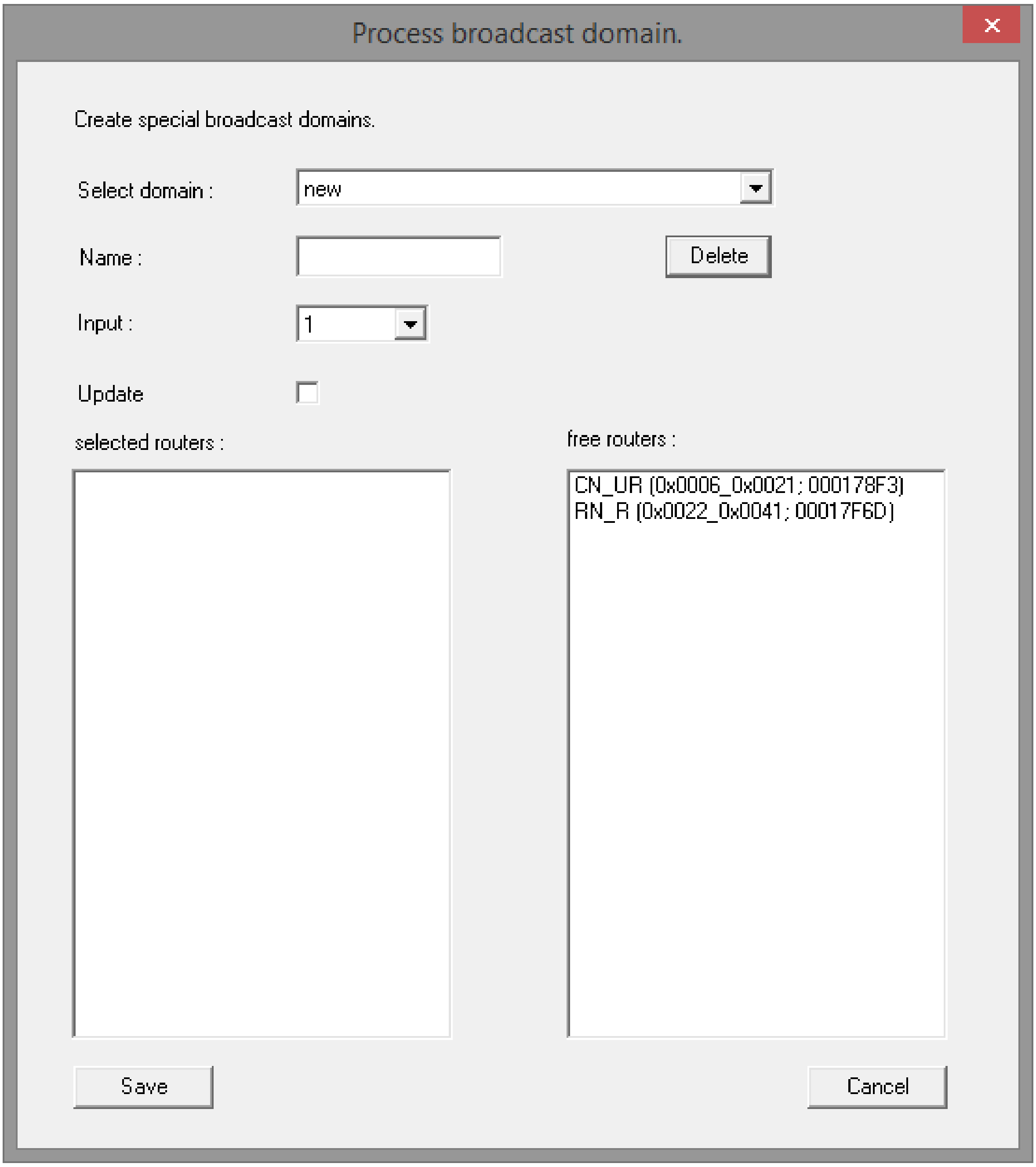
Update: an existing RingCast is re-established or updated --> within this radio domain.

Please note: There is no change to the surface which needs to be imported into LSM. A maximum of 10 routers are saved with a length of 15 characters. This means that nothing else needs to be observed if the IP address is used.

Delete: the selected radio domain is deleted.

Selected router: This is where all routers which are located within the radio domain are displayed --> for this RingCast.

Free routers: routers which are not assigned to a radio domain or RingCast.



Process broadcast domain.

Create special broadcast domains.

Select domain : new

Name :

Input : 1

Update ☐

selected routers :

free routers :

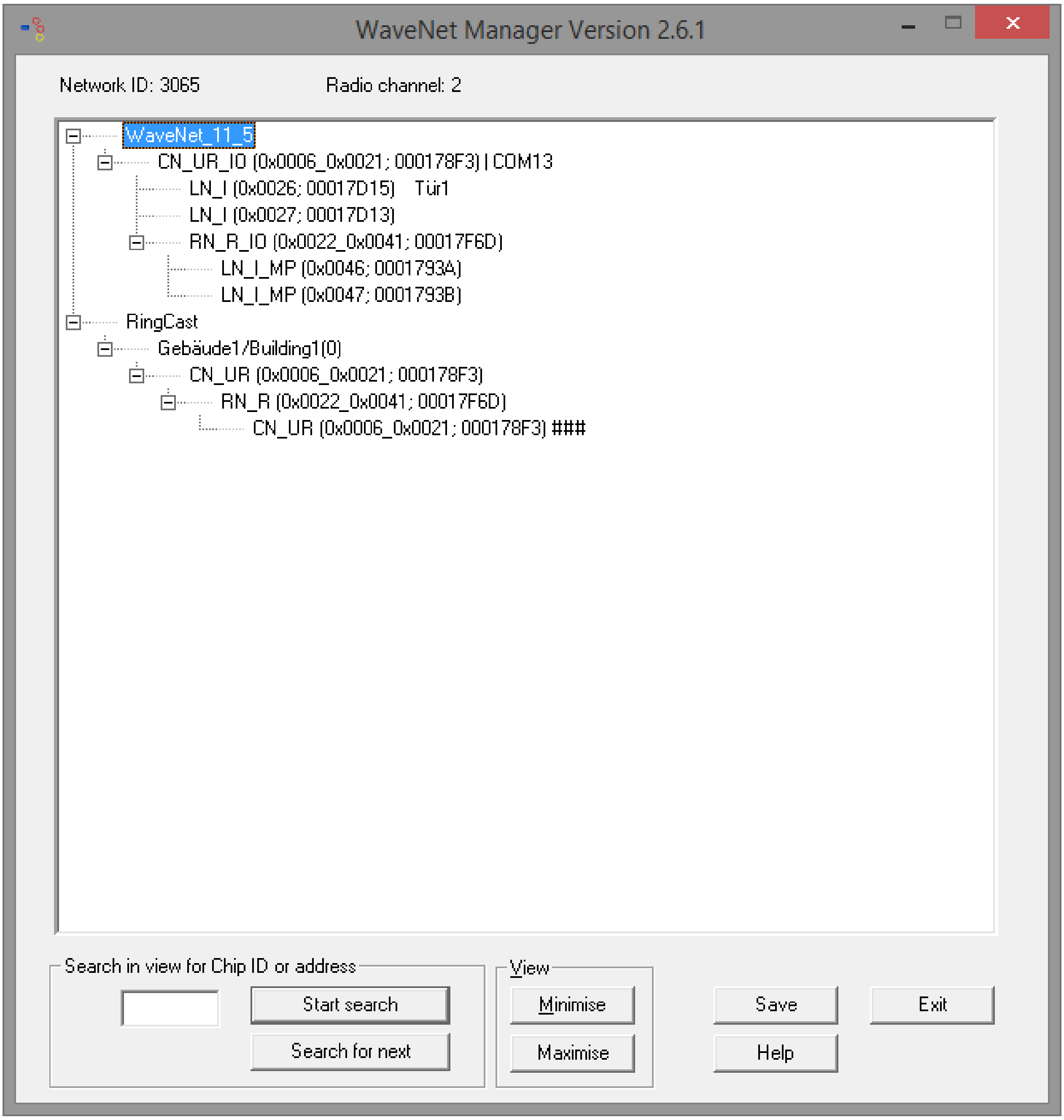
CN_UR (0x0006_0x0021; 000178F3)
RN_R (0x0022_0x0041; 00017F6D)

Double-click to add a free router to a created radio domain.

After saving, the created radio domain is then configured and displayed in WaveNet Manager.

RingCast: display of the radio domain created for the RingCast. It must be ensured that the wiring is connected to an input on an I/O router, so that the broadcast function can be triggered. "###" means that the RingCast is closed on the radio domain. This is for information purposes only and has no relevance on a technical level.

If you right-click on "RingCast", you can edit or modify it.



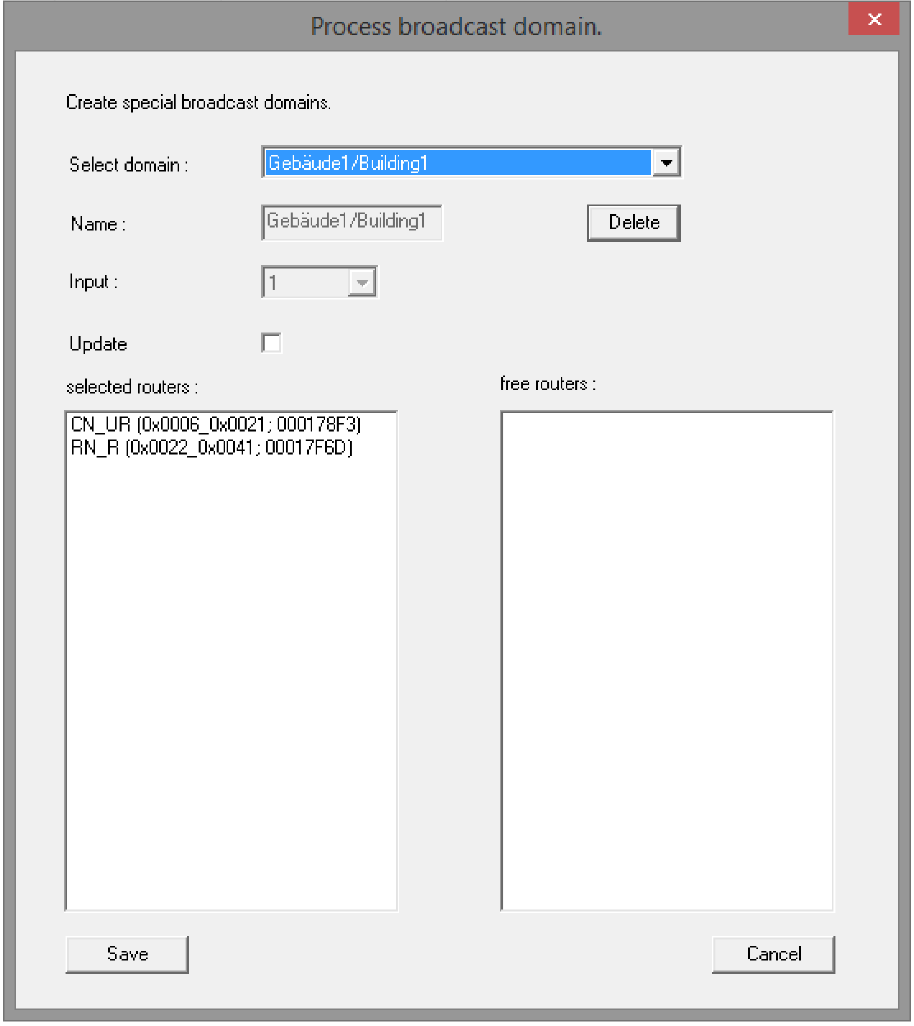
WaveNet Manager Version 2.6.1

Network ID: 3065
Radio channel: 2

```
WaveNet_11_5
    CN_UR_IO (0x0006_0x0021; 000178F3) | COM13
        LN_I (0x0026; 00017D15)    Tür1
        LN_I (0x0027; 00017D13)
        RN_R_IO (0x0022_0x0041; 00017F6D)
            LN_I_MP (0x0046; 0001793A)
            LN_I_MP (0x0047; 0001793B)
RingCast
    Gebäude1/Building1(0)
        CN_UR (0x0006_0x0021; 000178F3)
            RN_R (0x0022_0x0041; 00017F6D)
                CN_UR (0x0006_0x0021; 000178F3) ###
```

Search in view for Chip ID or address
Start search
Search for next
View
Minimise
Maximise
Save
Exit
Help

Diagram showing an installed RingCast



Process broadcast domain.

Create special broadcast domains.

Select domain : Gebäude1/Building1

Name : Gebäude1/Building1

Input : 1

Update ☐

selected routers :

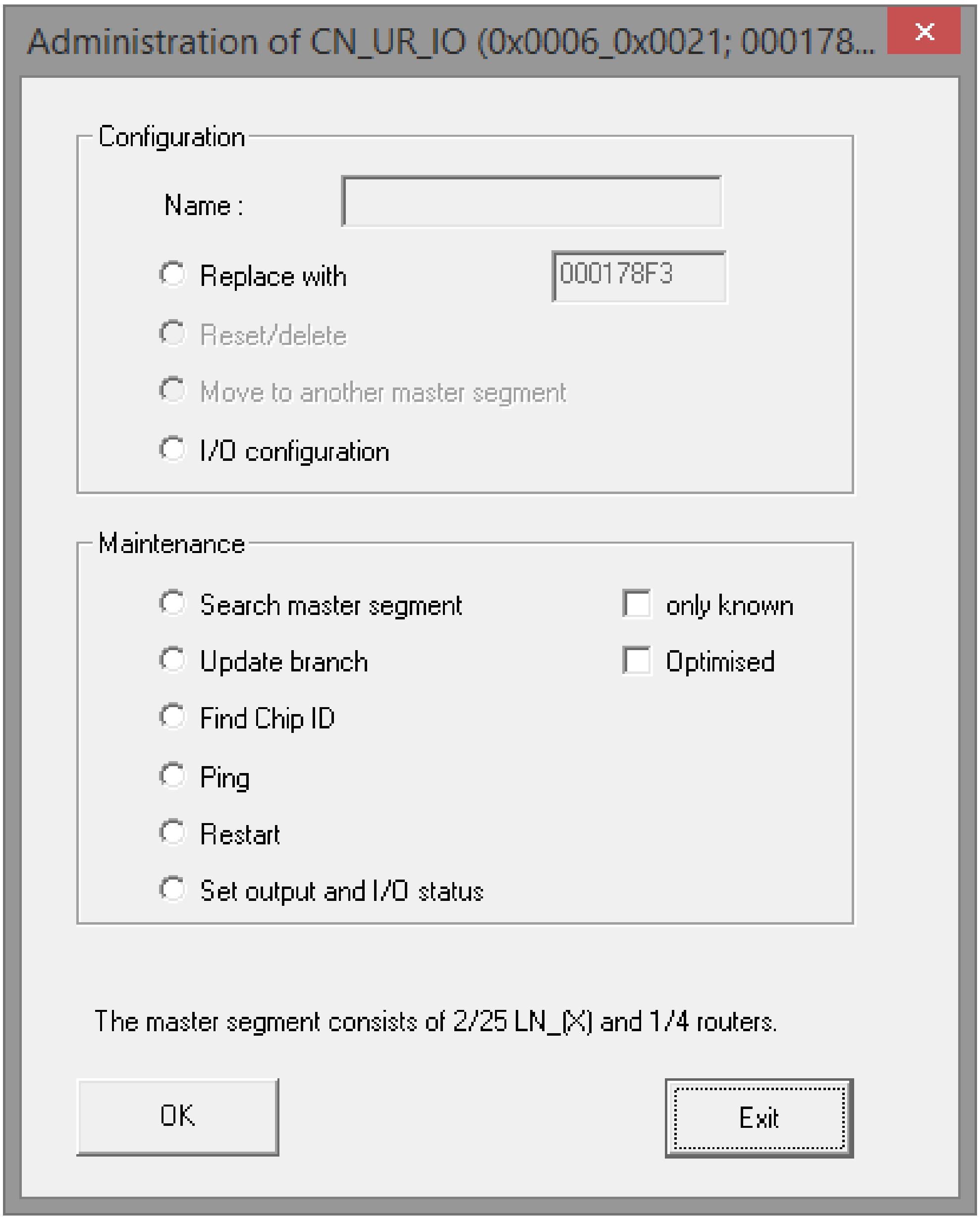
CN_UR (0x0006_0x0021; 000178F3)
RN_R (0x0022_0x0041; 00017F6D)

free routers :

12 Administration of Central- Router- und LockNodes

12.1 CN_U(X), CN_S(X), RN_E(X), RN_W(X), RN2 - configuration

You can open Administration by right-clicking on a central/router node (in WaveNet Manager).



Administration of CN_UR_IO (0x0006_0x0021; 000178...

Replace with: 000178F3

The master segment consists of 2/25 LN_(X) and 1/4 routers.

Replace with... when replacing a component, the new component can be added to the selected segment by entering its chip ID. The configuration is transmitted to the new network nodes.

Important notice:

- If the central/router node's IP address has been changed, the component can be replaced immediately.
- If the IP address remains the same, the IP address must be changed to a non-assigned IP address either under "Local connections" or "Communications nodes" in LSM. If a communication node or CommNode server (CNS) is used, the changed IP addresses must be "transmitted" to the CommNode server --> in LSM. First enter the IP address originally used in WaveNet Manager, then configure and import into LSM.
- If the COM port changes, it can be replaced, but the new COM port must be entered into LSM (local connection device)
- If the COM port remains the same, both segments (slave/master) must be deleted from LSM beforehand (manage WaveNet).

If the grey programming flash icon is visible on a component, you can attempt to re-programme the configuration without changing the chip ID, so that it can be added to the selected master segment.

Reset/delete

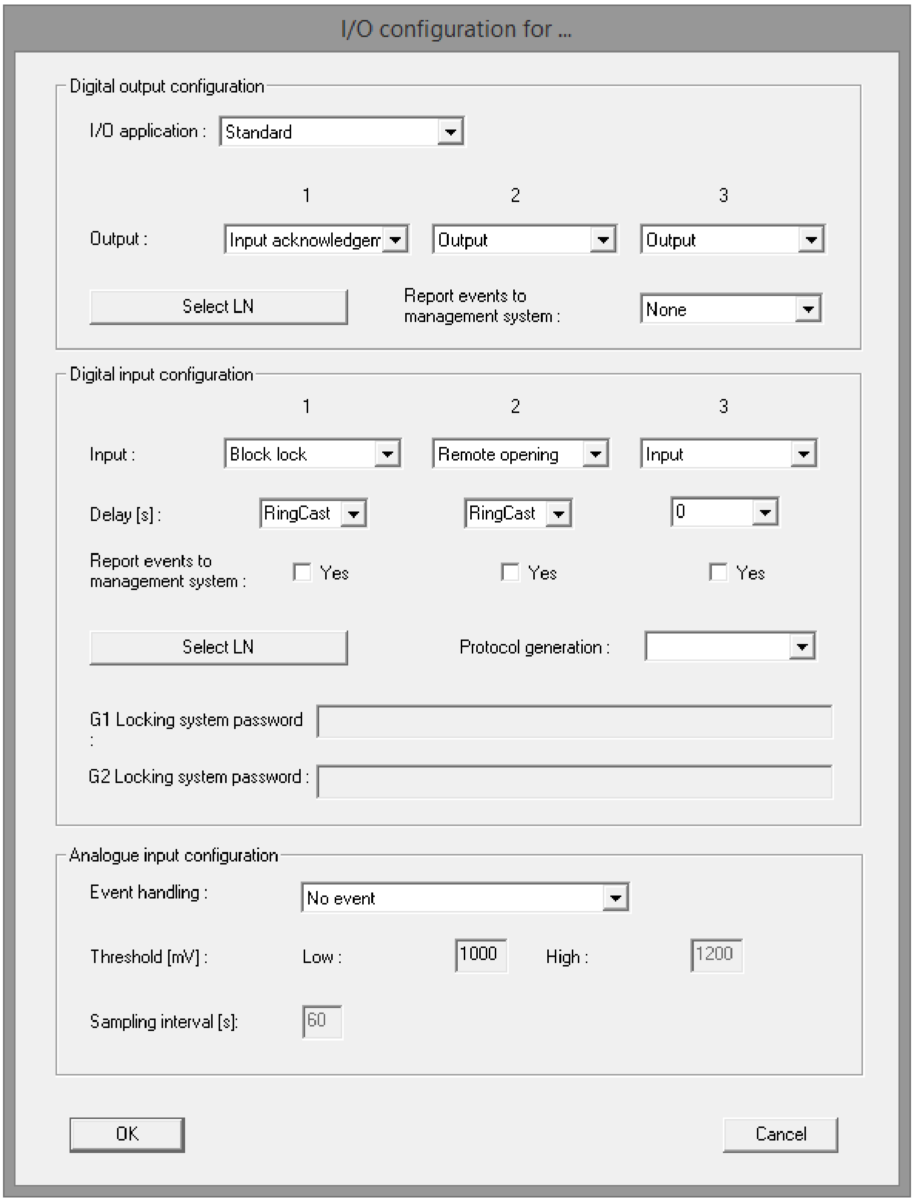
The selected components are reset and then deleted from the WaveNet Manager screen. These components then feature their default configuration again (default network ID: DDDD / radio channel: default).

Move to a different master segment:

Not possible for CNs.

I/O configuration

You can set the I/O configuration here.



I/O configuration for ...

Digital output configuration

I/O application : Standard

	1	2	3
Output :	Input acknowledgem	Output	Output

Report events to management system : None

Digital input configuration

	1	2	3
Input :	Block lock	Remote opening	Input
Delay [s] :	RingCast	RingCast	0
Report events to management system :	☐ Yes	☐ Yes	☐ Yes

Protocol generation :

G1 Locking system password :

G2 Locking system password :

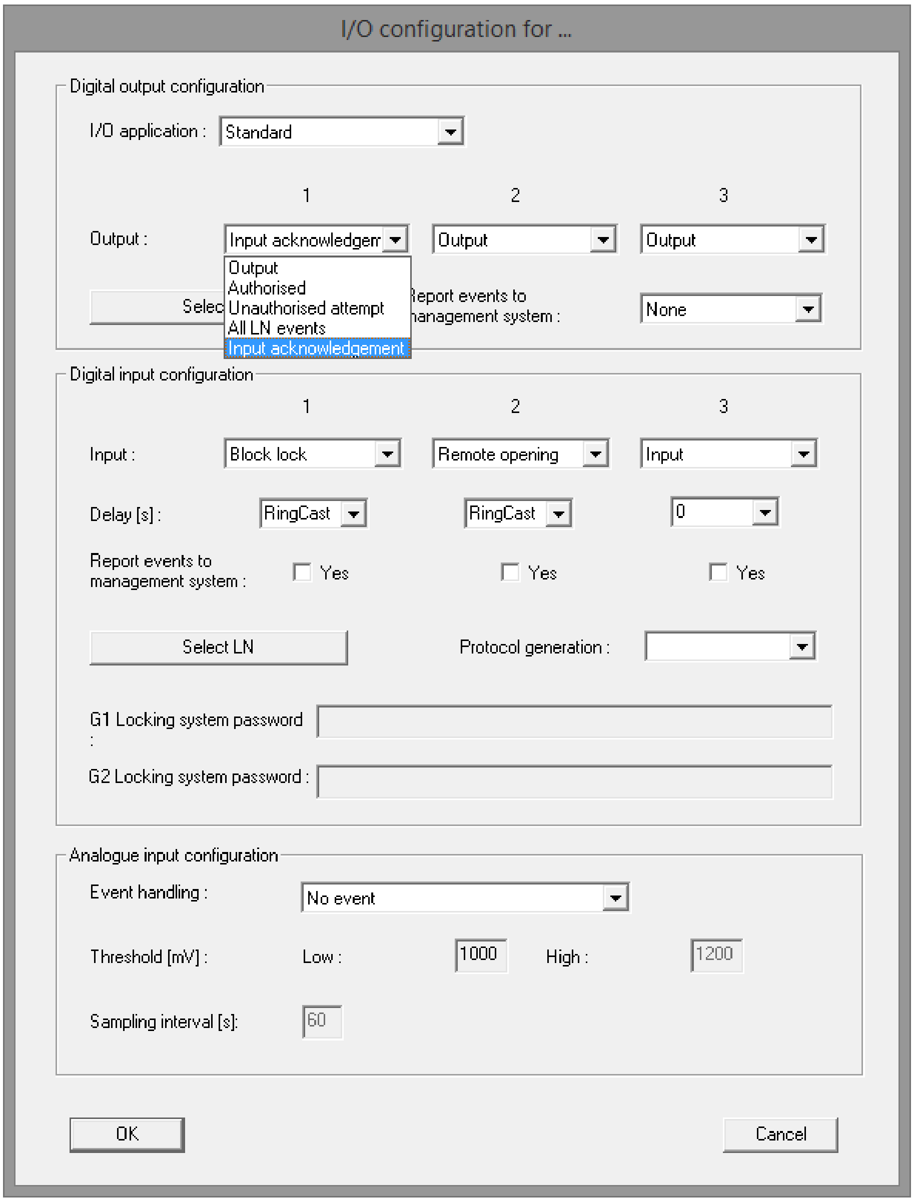
Analogue input configuration

Event handling : No event

Threshold [mV] : Low : 1000 High : 1200

Sampling interval [s]: 60

Digital output configuration: (function not available for WNM.LN.R / WNM.LN.C)



I/O configuration for ...

Digital output configuration

I/O application : Standard

	1	2	3
Output :	Input acknowledgem	Output	Output

Report events to management system : None

Digital input configuration

	1	2	3
Input :	Block lock	Remote opening	Input
Delay [s] :	RingCast	RingCast	0
Report events to management system :	☐ Yes	☐ Yes	☐ Yes

Protocol generation :

G1 Locking system password :

G2 Locking system password :

Analogue input configuration

Event handling : No event

Threshold [mV] : Low : 1000 High : 1200

Sampling interval [s]: 60

I/O application: only "standard" possible to date.

Output 1, 2, 3:

- **Output**

  The "Output" option means that the output is connected for about 0.2 seconds (open drain). Manual control using WaveNet Manager possible.
- **Authorised**

  Selecting 'Authorised' means that the output is set during an authorised access event at a locking device using a transponder or card --> OpenDrain
- **Unauthorised attempt**

Selecting 'Unauthorised attempt' means that the output is briefly connected (0.2 sec.) in the event of an unauthorised access attempt (transponder/card is not authorised for use on the locking device – does not apply to transponders/cards from external locking systems) --> OpenDrain. The locking devices must feature Access Control functionality and 'Log unauthorised access attempts' must be activated in the locking device's properties to ensure that authorised accesses and unauthorised access attempts are reported.

- **All LN events**

  The "All LN events" option means that the output always connects for a short interval (1, 2, 3)

- **Input feedback**

  The "Input feedback" option means that the broadcast function can be checked once the input signal has been transmitted. If the 'block lock' broadcast function is selected to deactivate locking devices, for example, the 'Input feedback' analysis at the output can determine whether all locking devices have actually been deactivated --> the output is then activated for about 0.2 seconds (open drain).

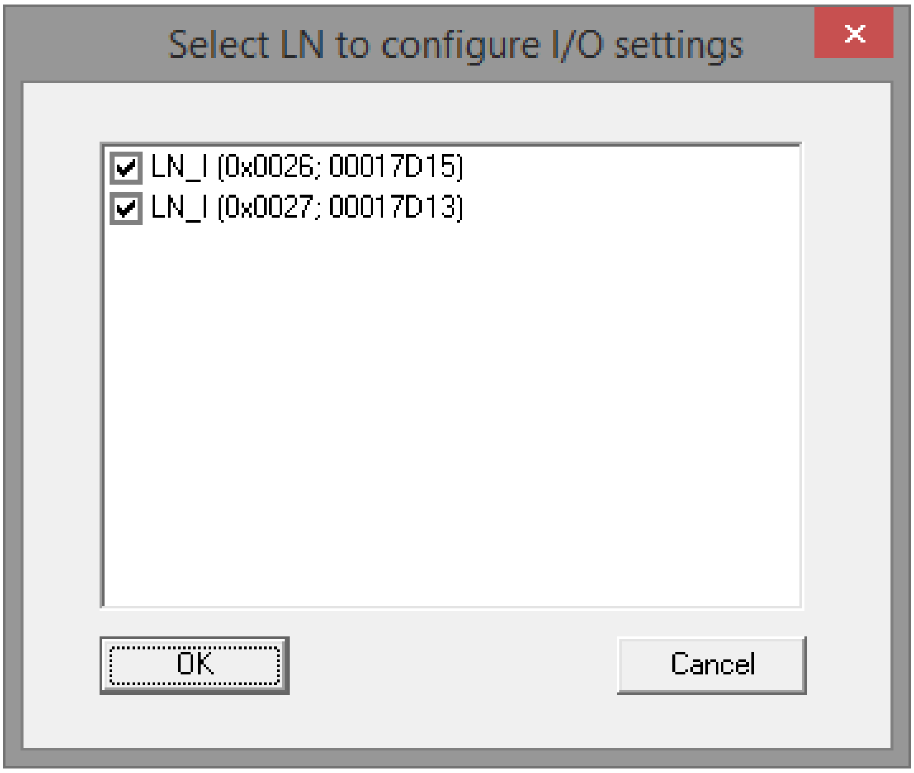
- **Short input feedback**

  The output is connected for a short interval.

- **Input receipt static**

  The output is connected while the status is active.

Select LN: This is where the lock nodes can be selected or deselected; select whether messages (events) are to be sent to the router or not. Selection (checking the box) and de-selection (unchecking the box) always applies to the whole segment and thus to all functions which have been selected



☑ LN_I (0x0026; 00017D15)
☑ LN_I (0x0027; 00017D13)

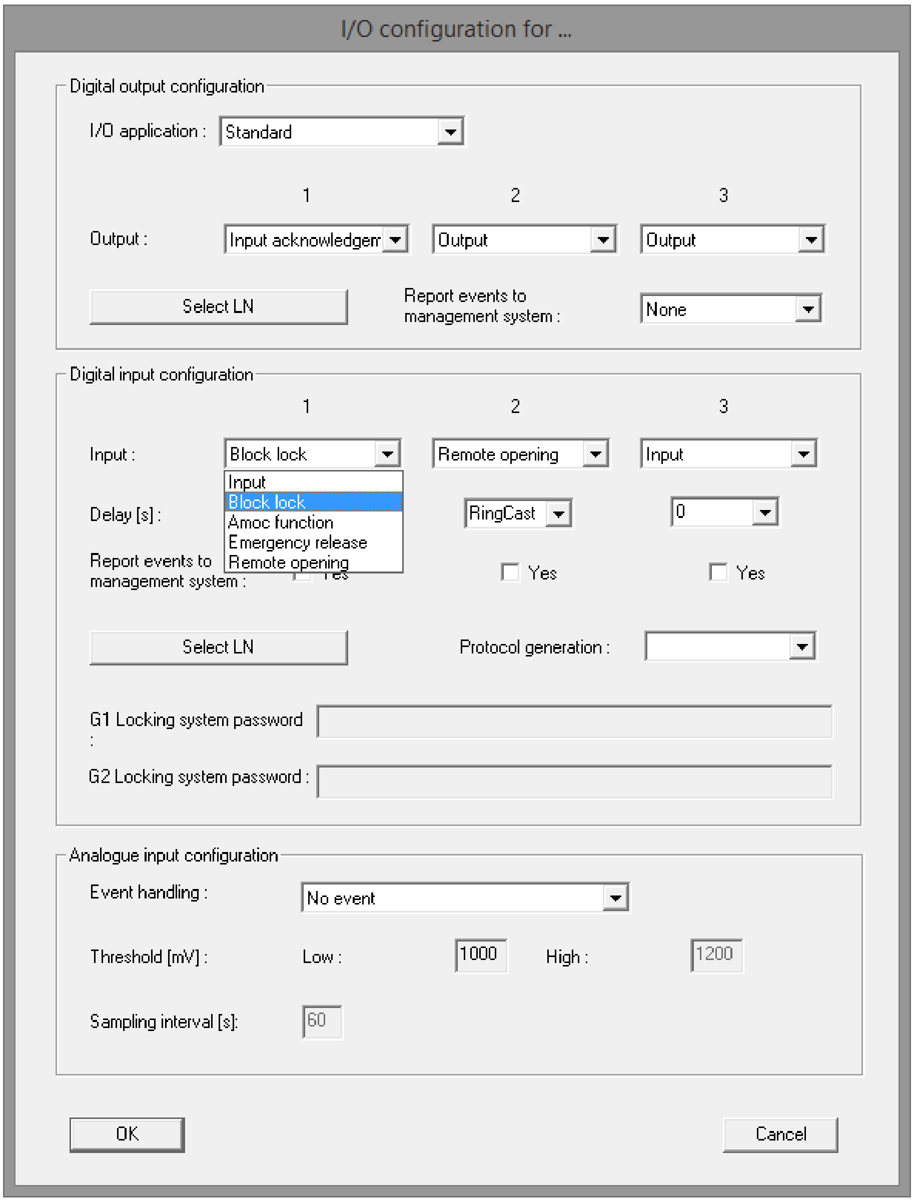
Report events to management system:

If you select 'None', no events are reported to the management system (LSM).

The "Authorised" option means that the access event is transmitted to LSM, where it can be used further as an "Access" event The "Unauthorised attempt" option means that the unauthorised access attempt event is transmitted to LSM, where it can be used further as an "Access" event

Selecting 'All LN events' means that an authorised access or unauthorised access attempt is reported.

Digital input configuration


I/O configuration for ...
Digital output configuration
1
2
3
Select LN
Digital input configuration
1
2
3
Input
Block lock
Amoc function
Emergency release
Remote opening
☐ Yes
☐ Yes
☐ Yes
Select LN
Protocol generation :
G1 Locking system password :
G2 Locking system password :
Analogue input configuration
OK
Cancel

I/O application : Standard

Output : Input acknowledgem | Output | Output

Report events to management system : None

Input : Block lock | Remote opening | Input

Delay [s] : RingCast | 0

Report events to management system :

Event handling : No event

Threshold [mV] : Low : 1000 High : 1200

Sampling interval [s]: 60

Input 1, 2, 3

- **Input**

  Selecting 'Input' means that control is provided from LSM (as with LN.R / LN.C). Pre-requisite for LSM 3.2

- **Block lock**

  Selecting 'Block lock': a relay output (NO, isolated), e.g. an intruder detection system (IDS), can be wired to the input. All selected LNs or locking devices are deactivated after the IDS is armed. It is no longer possible to open doors inadvertently. When the IDS is disabled, the IDS relay contact reopens, the locking devices are activated and can be opened again using a transponder or card. **NOT** VdS-compliant.

- **Gunman attack function**

  Selecting 'Gunman attack function': any contact (NO, isolated) can be wired to the input. After actuation, all selected locking devices are deactivated and remain so even if the contact is reset. The locking devices can only be re-activated using LSM or an activation transponder.
- **Emergency release**

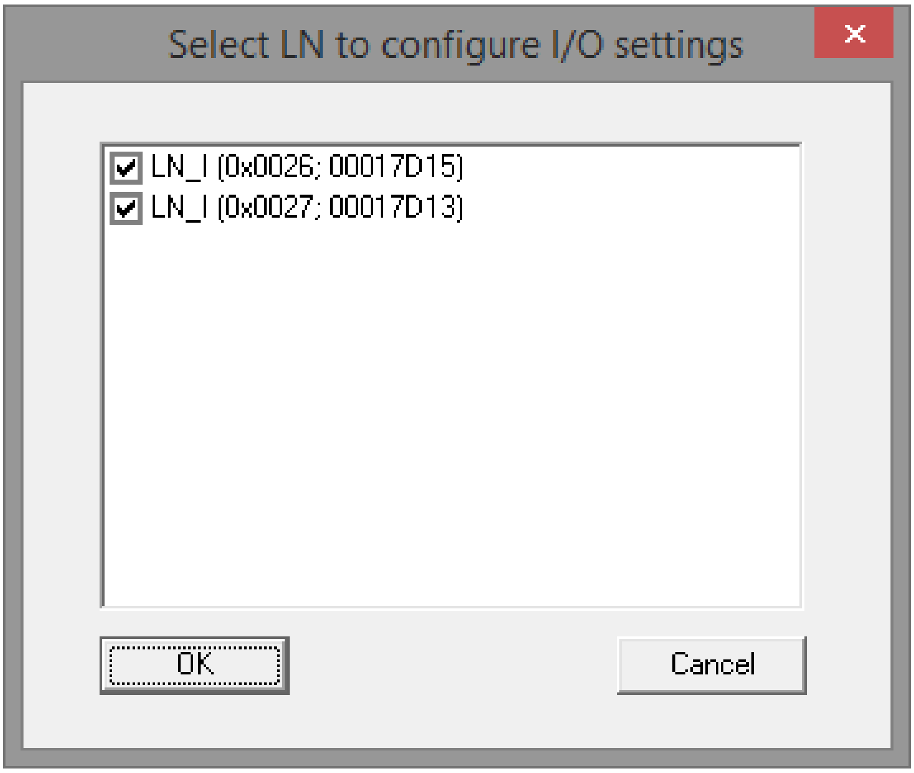
  Selecting 'Emergency release': a relay output (NO, isolated) in a fire alarm system can be wired to the input. If the fire alarm system is triggered, all selected locking devices are permanently enabled. The locking devices are returned to their normal mode by transmitting a remote opening signal in this segment.
- **Remote opening**

  Selecting 'Remote opening': a temporary release (NO, potential-free, e.g. button) enables the selected locking device for five seconds, for example.

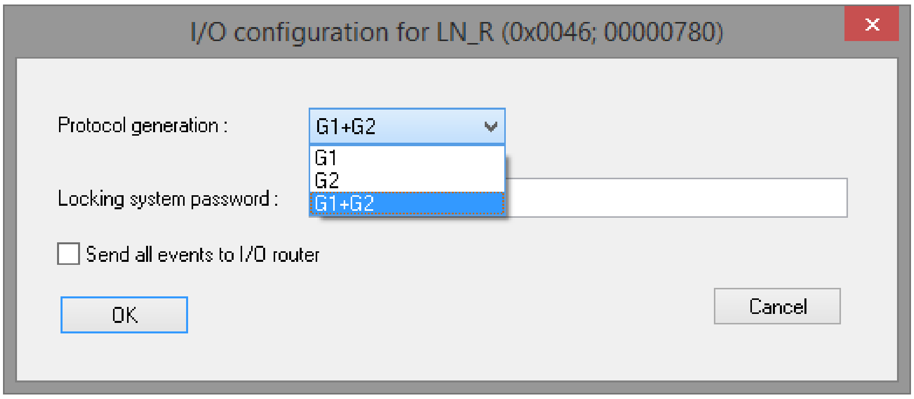
Reporting events to management system

If the 'Yes' box is checked, all changes to the input's status are transmitted to LSM and can then be used as an 'Input' event. --> "Input" configuration

Select LN: this is where the lock nodes can be selected or deselected to determine whether they are to be addressed via the segment broadcast function or not. Selection (checking the box) and de-selection (unchecking the box) always applies to the whole segment and thus to all functions which have been selected


Select LN to configure I/O settings
☑ LN_I (0x0026; 00017D15)
☑ LN_I (0x0027; 00017D13)
OK
Cancel

Protocol generation	This is where you must configure which protocol generation is to be used in the locking system (LSM). Possible settings: G1 | G1 + G2 | G2.
G1 + G2 locking system password	When using G1 protocol generation: enter G1 locking system password. When using G1 + G2 protocol generation: Enter G1 locking system password and G2 locking system password. When using G2 protocol generation: enter G2 locking system password. Whenever you make changes to the configuration, you must always select the protocol generation and enter the locking system password. If the configuration for an individual LN has been changed or a new lock node is added, the lock node in question can be configured without having to re-configure the whole segment by entering the password to use the mask below (LockNode administration). If a grey programming flash appears on one or more LockNodes, then there is a need to re-configure (LockNode administration).
Send all events to I/O router	This option must be selected to ensure that all events can be reported to the router and evaluated.



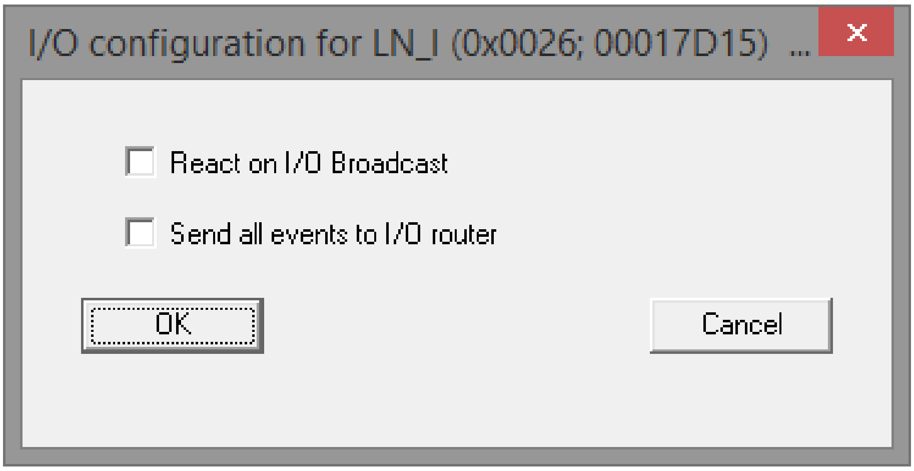
I/O configuration for LN_R (0x0046; 00000780)

Protocol generation : G1+G2

Locking system password :

☐ Send all events to I/O router

Following mask appears for firmware version 30.9 and higher for CN/RN and LN.

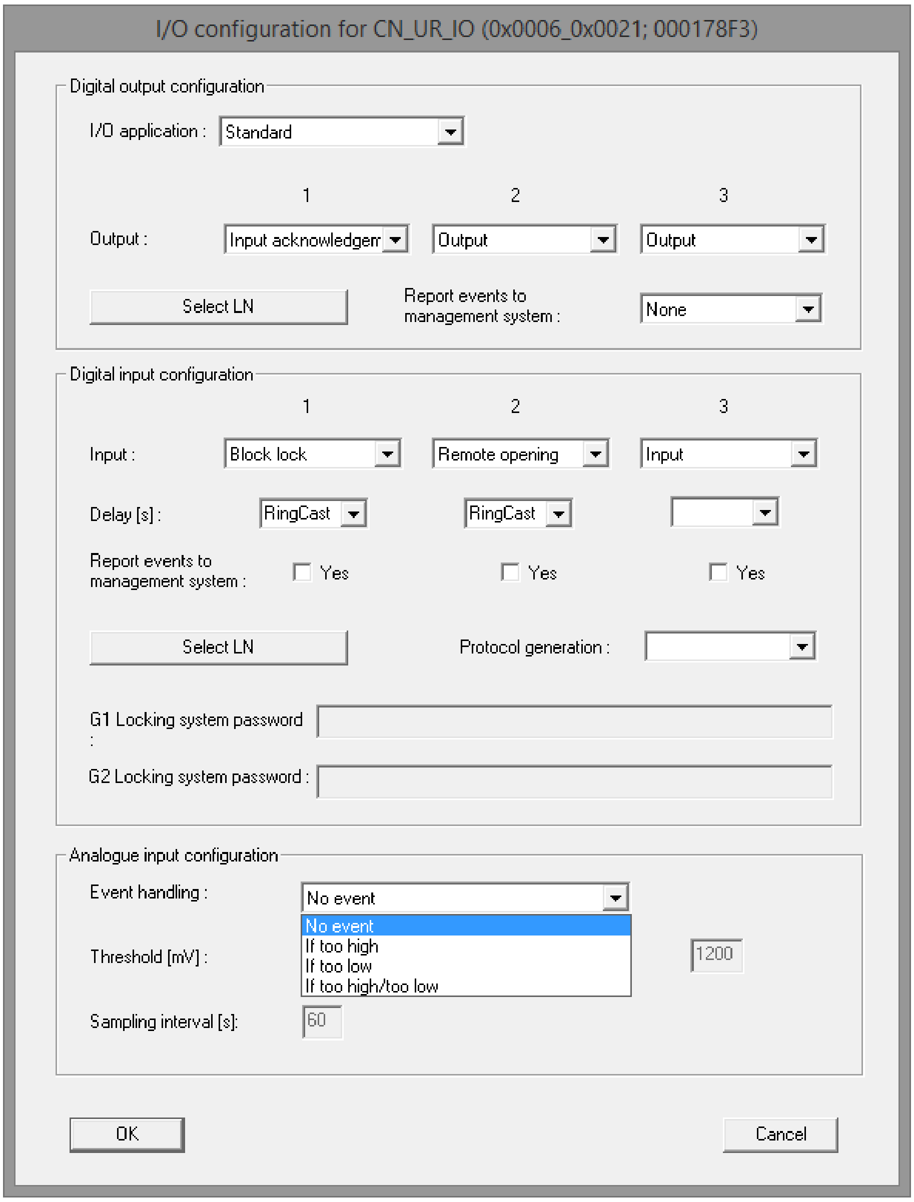


I/O configuration for LN_I (0x0026; 00017D15) ...

☐ React on I/O Broadcast

☐ Send all events to I/O router

Analogue input configuration



I/O configuration for CN_UR_IO (0x0006_0x0021; 000178F3)

Digital output configuration

I/O application : Standard

Output : 1 Input acknowledgem; 2 Output; 3 Output

Report events to management system : None

Digital input configuration

Input : 1 Block lock; 2 Remote opening; 3 Input

Delay [s] : 1 RingCast; 2 RingCast; 3

Report events to management system : 1 ☐ Yes; 2 ☐ Yes; 3 ☐ Yes

Protocol generation :

G1 Locking system password :

G2 Locking system password :

Analogue input configuration

Event handling : No event

Threshold [mV] : 1200

Sampling interval [s]: 60

Event handling: Only in combination with LSM 3.2 (event: analogue input)

No event: No events are reported to the management system (LSM).

On exceeding a threshold value: An event is reported to the management system (LSM). Event: analogue input can be linked to a response, e.g. email notification. Maximum setting of 2,500 mV On falling short of a threshold value: An event is reported to the management system (LSM). Event: analogue input can be linked to a response, e.g. email notification. Minimum setting of 100 mV

On exceeding/falling short of a threshold value: An event is reported to the management system (LSM). Event: analogue input can be linked to a response, e.g. email notification. The pre-defined interval of 200 mV causes hysteretic switching behaviour on exceeding/falling short of the required value Analogue input event transmitted to LSM. The same event is forwarded for both if the required value is exceeded/falls short.

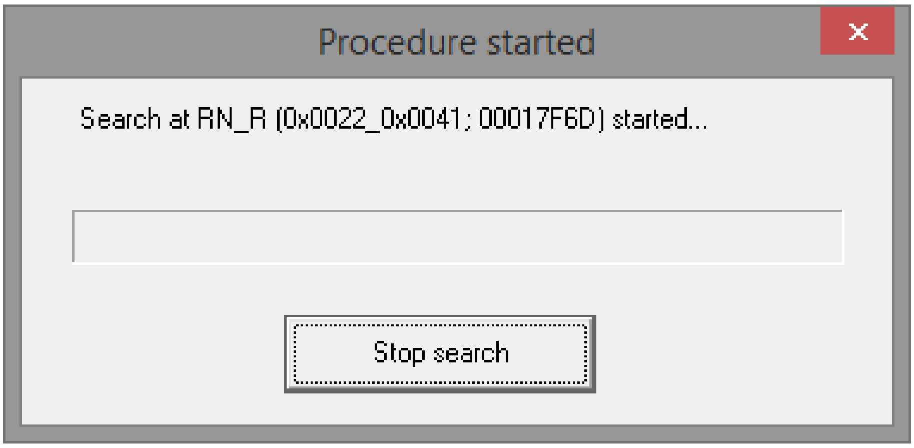
Threshold [mV]: Shortfall/exceedance: This is where threshold values can be set at intervals of 200 mV. Minimum value: 100 mV | maximum value: 2500 mV.

Sampling interval [s]: determines how often a check for a possible change (shortfall/exceedance) should be made. Minimum every 20 sec | Maximum 60 sec

12.2 CN_U(X), CN_S(X), RN_E(X), RN_W(X), RN2 - maintenance

Search by master segment

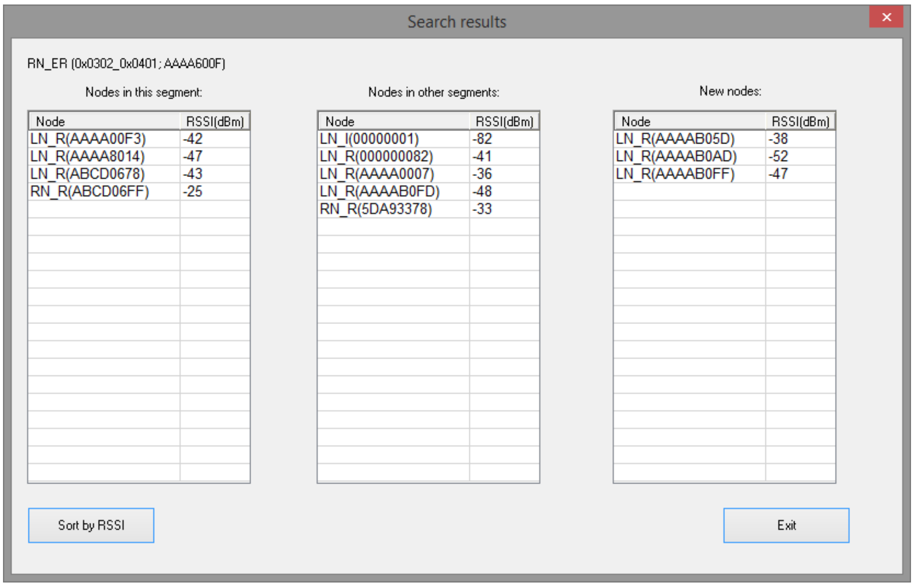
In router version 40 or higher, a query appears asking if a search should be initiated directly for new nodes.



Search at RN_R (0x0022_0x0041; 00017F6D) started...

Result of search

Provides an overview and possible configuration in this master segment.



RN_ER (0x0302_0x0401; AAAA600F)

Nodes in this segment:

Node	RSSI(dBm)
LN_R(AAAA00F3)	-42
LN_R(AAAA8014)	-47
LN_R(ABCD0678)	-43
RN_R(ABCD06FF)	-25

Nodes in other segments:

Node	RSSI(dBm)
LN_I(00000001)	-82
LN_R(000000082)	-41
LN_R(AAAA0007)	-36
LN_R(AAAAB0FD)	-48
RN_R(5DA93378)	-33

New nodes:

Node	RSSI(dBm)
LN_R(AAAAB05D)	-38
LN_R(AAAAB0AD)	-52
LN_R(AAAAB0FF)	-47

The three columns describe and evaluate (RSSI) the components/ nodes reached in the selected master segment. The RSSI value is always 0 (zero) for wired components.

Nodes in this segment: this column displays all components/nodes which are managed by the selected master segment.

Nodes from other segments: this column displays all nodes which can be reached by this master segment via a radio link but do not belong to this master segment. The nodes in this master segment can be assigned by highlighting and dragging them into the first column (nodes in this segment). Assignment may take a few seconds or minutes as the routing table needs to be updated.

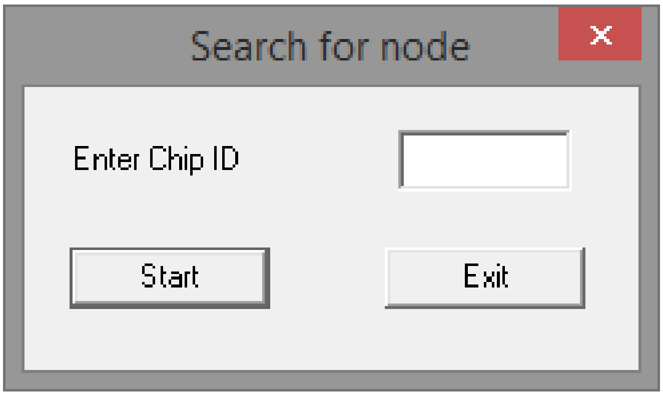
New nodes: this column displays all nodes which are not yet assigned to a master segment. The nodes in this master segment can be assigned either by double-clicking or highlighting them and dragging them into the first column (nodes in this segment). Assignment may take a few seconds or minutes as the routing table needs to be updated.

RSSI (dBm): Received Signal Strength Indication = strength of the received signal □ an indicator of the received field strength. The more negative the displayed dBm value is, the poorer the quality is that you can expect from the connection.

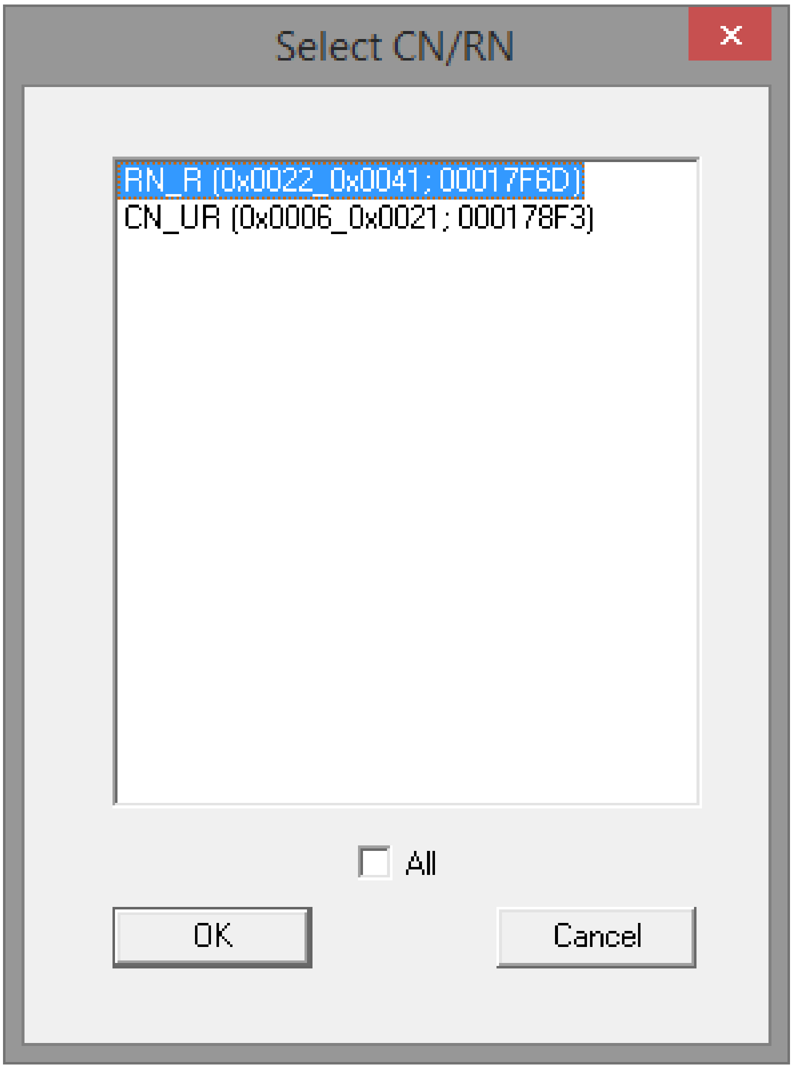
Update branch: non-programmed components are automatically incorporated into the branch based on the RSSI value. Optimised: If the 'Optimised' setting is used, a search is initiated for both new nodes and previously configured nodes. During this process, configured nodes (from other segments) may be moved to another segment to provide enhanced availability. If this setting is not used, then the system will search for new nodes only.

Only known ones: Only known or already configured LockNodes are updated.

Search by chip ID



This is where you can search for a chip ID. Another window will open once the chip ID is entered.



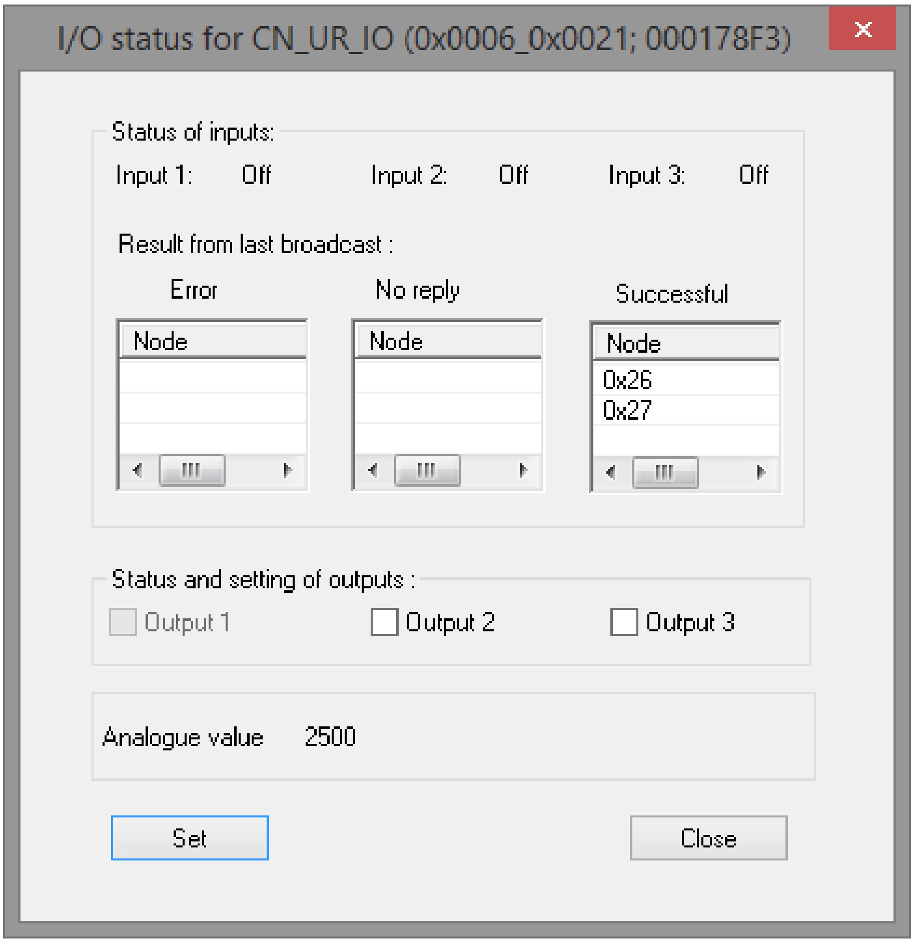
RN_R (0x0022_0x0041; 00017F6D)
CN_UR (0x0006_0x0021; 000178F3)

You can select which master segment is to be searched. Multiple segments can be selected. If you select 'All', the whole network is searched.

Ping an availability test is carried out for selected components.

Restart Re-starts the selected components.

Set output and I/O status



I/O status for CN_UR_IO (0x0006_0x0021; 000178F3)

Status of inputs:

Input 1: Off Input 2: Off Input 3: Off

Result from last broadcast :

Error	No reply	Successful
Node	Node	Node
		0x26 0x27

Status and setting of outputs :

☐ Output 1 ☐ Output 2 ☐ Output 3

Analogue value 2500

Status of inputs:

This is where you can see the status of inputs.

Result from last broadcast:

- Error: The LockNode(s) has/have received the broadcast, but the locking device was unable to process/transact the broadcast signal.
- No response: there is probably a radio range problem.
- Successful: the "Input feedback" output has been configured.

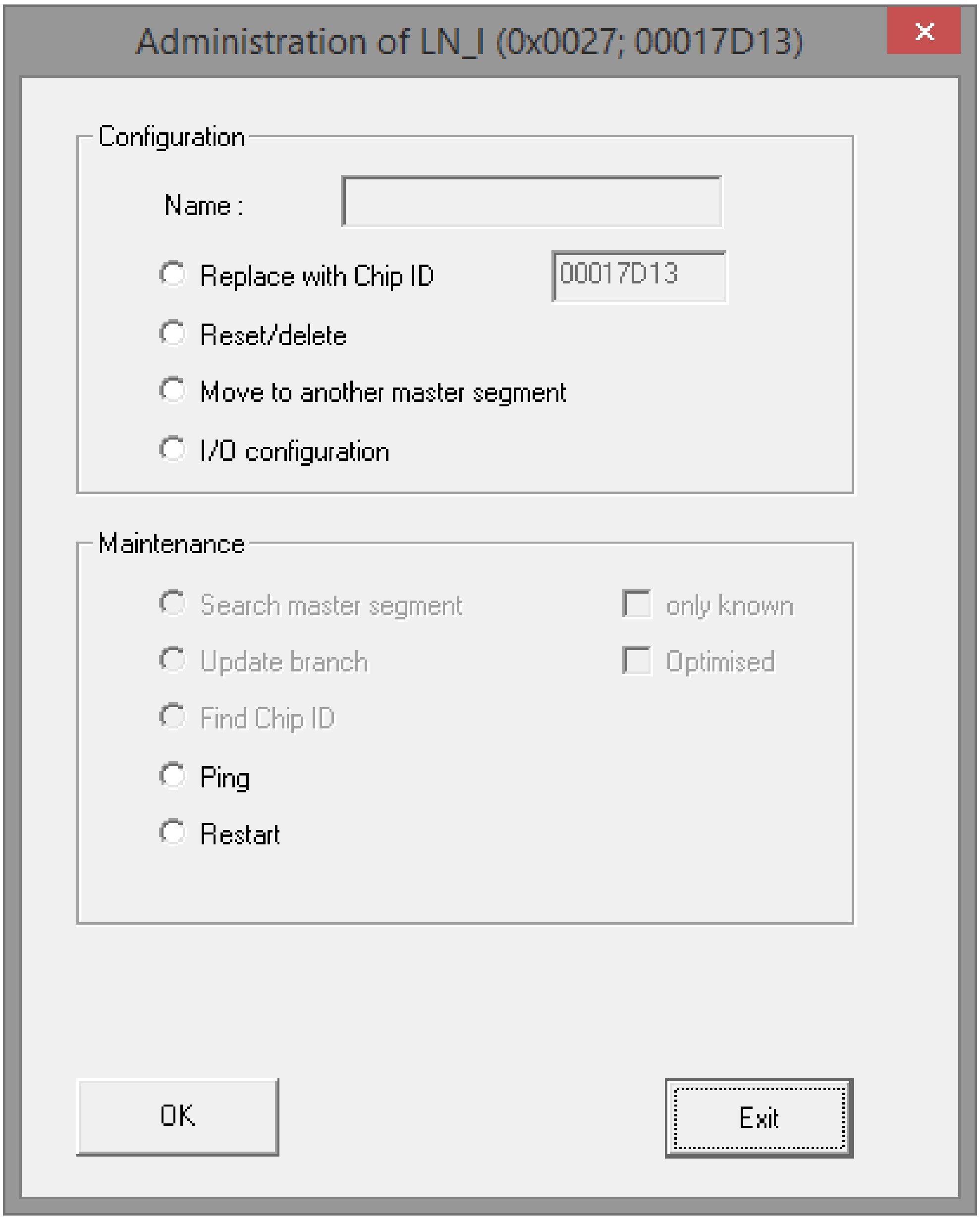
Status and setting of outputs:

This is where outputs can be set for test purposes or where their current status can be displayed.

- Analogue value [mV]: this displays the value from when it was last read.

12.3 LN_(X) Configuration

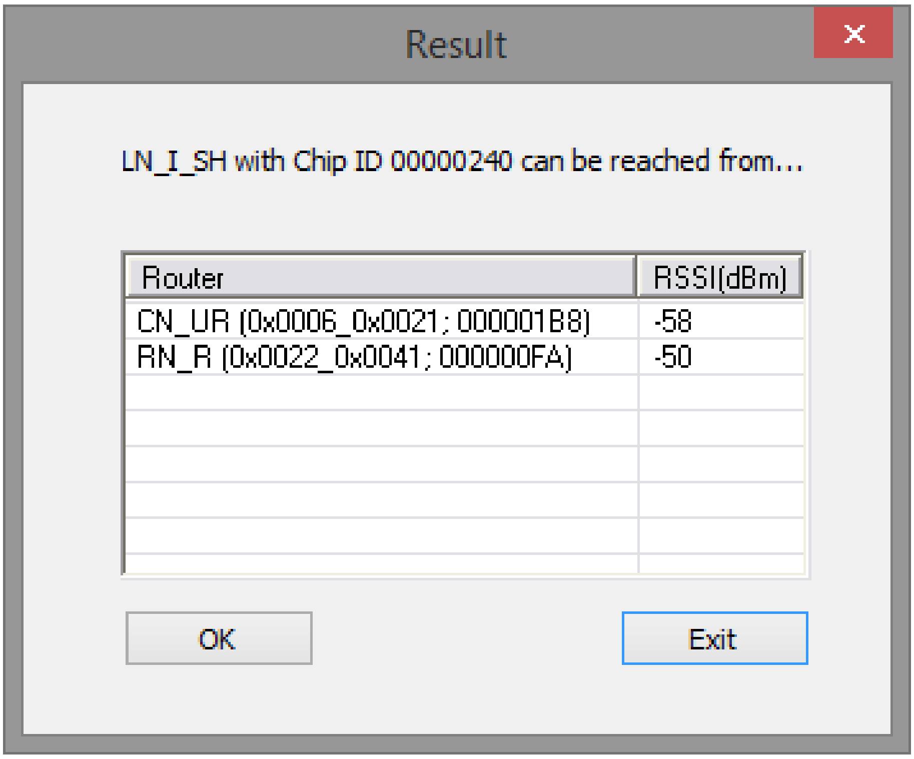
You can open Administration by right-clicking a LockNode (in the WaveNet Manager).



Replace with chip ID When replacing a component, the new component can be added to the selected segment by entering its chip ID. The configuration is transmitted to the new network nodes. If the grey lightning bolt icon is visible on a component, you can attempt to re-programme the configuration without changing the chip ID, so that it can be added to the selected master segment at a later time.

Reset/delete Selected components are reset and then deleted from the WaveNet Manager screen. Components feature the standard configuration again (default network ID: DDDD / radio channel: default).

Move to a different master segment: Option to check connection and move to another segment when required.



LN_I_SH with Chip ID 00000240 can be reached from...

Router	RSSI(dBm)
CN_UR (0x0006_0x0021; 000001B8)	-58
RN_R (0x0022_0x0041; 000000FA)	-50

The following applies: The more negative the RSSI value, the worse the connection quality By double clicking or selecting and pressing OK, LN_(X) / RN_(X) can be moved to another. The routing table is updated automatically when adding routers.

When moving RN_(X), an exclamation mark (!) can be placed in front of a router, that cannot be used. The reason for this is the existing network structure. The display of such a router is only for the sake of completeness.

13 Resetting Central- Router- and LockNodes

13.1 Resetting the WaveNet configuration for central and routing nodes

1. Disconnect power supply (remove plug).
2. Wait 20 seconds.
3. Remove housing lid (4 screws).
4. Press down button on circuit board (near to power plug) and hold down.
5. Reconnect power (plug).
6. Release reset button when red LED lights up (after around two seconds).
7. WaveNet configuration has been reset (default).

13.2 Resetting the WaveNet configuration for RN2

1. Disconnect power supply *(remove plug)*.
2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the network plug)*.
5. Release reset button after 1 second.
6. The configuration has now been fully reset *(default)*.

13.3 WaveNet configuration for LN.R/C

1. Disconnect power supply (connecting cable from LN.C/ both batteries from LN.R)
2. Wait 20 seconds.
3. Remove housing lid (carefully lever off lid side with SimonsVoss lettering)
4. Press down button on circuit board and hold down.
5. Reconnect power (see point 1.)
6. Release button when red LED lights up permanently.
7. WaveNet configuration has been reset (default).

13.4 WaveNet Configuration WNM.LN.I.XX.YY

If a previously configured lock node is connected to another locking component with a different locking system ID, all WaveNet Manager settings are re-set to default. The locking device which is selected to be reset must be programmed and thus be part of another locking system. A non-programmed locking device (locking system ID = 0 [zero]) cannot be used.

13.5 Resetting TCP/IP configuration RN.E(X)/RN.W(X)

1. Disconnect power supply (remove plug).
2. Wait 20 seconds.
3. Remove housing lid (4 screws)
4. Press down button on circuit board (next to power plug) and hold down.
5. Reconnect power (plug).
6. Hold down button until red and green LEDs flash alternately.
7. Release button.
8. TCP/IP configuration has been deleted.

13.6 Resetting the TCP/IP configuration for RN2

1. Disconnect power supply *(remove plug)*.
2. Wait 20 seconds.
3. Press reset button and hold pressed down.
4. Reconnect to power supply *(connect the network plug)*.
5. Release reset button after 5 seconds.
6. The configuration has now been fully reset *(default)*.

14 Performing standard WaveNet-based tasks in LSM Business

This example shows the key steps in setting up and administrating a WaveNet radio network in LSM Business. The examples are based on specific installations and are meant to help you become familiar with topics related to WaveNet.

14.1 Creating a WaveNet radio network and incorporating a locking device

This example describes how you create a WaveNet radio network from scratch. The aim is to address a locking device via a current RouterNode2.

14.1.1 Preparing LSM software

Note that the LSM software **must** be correctly installed and a corresponding network module licensed to network SimonsVoss locking components.

1. Install the CommNode server and ensure that the service has been started.
2. Install the current version of WaveNet Manager. (See Installation of the WaveNet Manager [▸ 10])
3. Open the LSM software and select "Network/WaveNet Manager".
   - ⇨ Indicate the WaveNet Manager installation directory and select a directory for the output file.
   - ⇨ Use the "Start" button to launch WaveNet Manager.
4. Issue a password to increase security in your network.

⇨ WaveNet Manager will start up and the settings are then saved for the future. Exit WaveNet Manager to make more settings.

14.1.2 Initial programming of locking components

Locking devices need to be programmed before they can be incorporated into the network.

14.1.2.1 Add new locking device

✓ A locking system has already been added.

1. Select *Edit/New locking device*.
2. Fill out all attributes and use the "Configuration" button to make further settings if necessary.
3. Click on the "Save & next" button.
4. Click on the "Finish" button.

14.1.2.2 Programme locking device

✓ A locking device has been added to the locking system and is visible in the matrix.

1. Right-click on the locking device concerned.
2. Click on Programme.
3. Follow the instructions in the LSM software.

Ensure that you select the right programming device. In the case of active locking devices, only the locking device to be programmed may be in the immediate area surrounding the programming device!

14.1.3 Preparing hardware

The current RouterNode2 can be quickly and easily placed into operation. Close the RouterNode2 as per the accompanying quick guide. The RouterNode2 is configured in the factory, so that it acquires its IP address from a DHCP server. You can use the OAM tool *(available free of charge from the download center)* to detect this IP address quickly.

NOTICE

Default settings:

IP address: 192,168,100,100

User name: SimonsVoss | Password: SimonsVoss

If the locking device has not been fitted with a LockNode (LN.I) in the factory, you need to retrofit the device using corresponding accessories.

NOTICE

Note down the RouterNode2's IP address and the locking device's chip ID after you have prepared the hardware correctly.

14.1.4 Creating communication nodes

The communication node forms the interface between the CommNode server and the LSM software. You must execute the LSM software as the Administrator to create the configuration XMLs.

1. Open the LSM software.
2. Select "Network/Communication nodes".
3. Add "Name", "Computer name" and "Description".
   ⇨ *e.g. WaveNet-Netzwerk_123; Computer_BS21; communication node for the WaveNet radio network 123*
4. Click on the "Config files" button.
5. Ensure that the path specifies the CommNode server's installation directory and click on the "OK" button.

6. Press "No" to accept the prompt and confirm your selection by pressing "OK". *The three configuration XMLs (appcfg, msgcfg and netcfg) must be located directly in the CommNode server's installation directory.*
7. Click on the "Apply" button to save your settings.
8. Click on the "OK" button to close the query.
9. Click on the "OK" button to close the dialogue.

14.1.5 Setting up the network and importing into LSM

14.1.5.1 Add WaveNet configuration

You can start to configure the network if all requirements are met:

- ✓ LSM is installed correctly and a network module is licensed.
- ✓ The Comm Node server has been installed and the service launched.
- ✓ The CommNode server's configuration files have been created.
- ✓ WaveNet Manager has been installed in its current version.
- ✓ A communication node has been created in the LSM software.
- ✓ The initial programming of the locking device to be networked has been successful.
- ✓ The RouterNode2 can be reached via the network and you know its address.
- ✓ The programmed locking device features a fitted LockNode and you know its chip ID.

1. Select "Network/WaveNet Manager" and press the "Start" button to launch WaveNet Manager.
2. Enter the password.
3. Right-click on "WaveNet_xx_x".
4. Install the RouterNode2 first, using the "Add: IP or USB Router" option, for example.
    - ⇨ Follow the dialogue and use the RouterNode2's IP address to incorporate it into your WaveNet radio network.
5. Initialise the locking device's LockNode by right-clicking on the newly added RouterNode2 and selecting the "Search for chip ID" option.
    - ⇨ Follow the dialogue and use the locking device's chip ID to assign it or the associated LockNode to the RouterNode2.
6. Click on the buttons "Save", "Finish" and "Yes" one after another to close WaveNet Manager.
7. Import the new settings and assign them to the corresponding communication node.

14.1.5.2 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transfer" button.
3. Click on the "Apply" button to save your settings.
4. Click on the "OK" button to close the dialogue.

14.1.5.3 Assigning a LockNode to a locking device

The initialised LockNode must be linked to a locking device. The easiest way to do this is using a collective command, particularly if there are a number of LockNodes:

1. Select "Network/Collective tasks/WaveNet nodes".
2. Select all LockNodes *(WNNode_xxxx)* which have not yet been assigned. *There is no entry in the "Door" column for LockNodes which have not yet been assigned.*
3. Click on the "Configure automatically" button.
   ⇨ Auto-configuration launches immediately.
4. Click on the "OK" button to close the dialogue.

14.1.5.4 Testing the WaveNet configuration

You can reprogramme the locking device at any time by using "Right-click/ Programme" in the network to test the network quickly. If programming is successful, the network is working correctly.

14.2 Putting the DoorMonitoring locking cylinder into operation

This example shows which settings need to be made to set up a DoorMonitoring locking cylinder. You will find the requirements in the Section "Creating a WaveNet radio network and incorporating a locking device [▸ 45]".

14.2.1 Adding a DoorMonitoring locking cylinder

The DM locking cylinder first needs to be added and programmed correctly in LSM:

1. Select the "Add locking device" button to launch the dialogue for a new locking device.
2. Select "G2 DoorMonitoring cylinder" as a locking device type and add all other details as you wish.
3. Exit the dialogue to add the locking device to the matrix.

4. Double-click to open the locking device's properties and select the "Configuration/Data" tab.
5. Configure the settings in the locking device's "Target area".
6. Click on the "Monitoring configuration" button and complete the following settings as a minimum:
   - ⇨ Fastening screw sampling interval: e.g. 5 seconds. The door status will be queried every 5 seconds in this case.
   - ⇨ The number of turns in the lock: e.g. one turn. This setting is important to record the bolt status correctly.
7. Save the settings and return to the matrix.
8. Use a suitable programming device to carry out initial programming.

14.2.2 Integrating a DoorMonitoring locking cylinder into the network

This is how you incorporate the DM locking cylinder into the WaveNet network:

- ✓ WaveNet Manager is already set up.
- ✓ The router to which the new locking device is to be assigned is already set up and online.
- ✓ A LockNode is correctly fitted to the DM locking cylinder and you know the chip ID.

1. Launch WaveNet Manager.
2. Initialise the locking device's LockNode by right-clicking on the router and selecting the "Search for chip ID" option.
   - ⇨ Follow the dialogue and use the locking device's chip ID to assign it or the associated LockNode to the RouterNode2.
3. Right-click on the newly added DM LockNode.
4. Activate the "I/O configuration" checkbox and click on the "OK" button.
5. Activate the "Send all events to the I/O configuration" checkbox and click on the "OK" button.
6. Click on the buttons "Save", "Finish" and "Yes" one after another to close WaveNet Manager.
7. Import the new settings and assign them to the corresponding communication node.

14.2.3 Transmitting the WaveNet configuration

The new settings still need to be transmitted to the CommNode server:

1. Select "Network/Communication nodes".
2. Select the RouterNode2 from the list of connections and click on the "Transfer" button.
3. Click on the "Apply" button to save your settings.

4. Click on the "OK" button to close the dialogue.

14.2.4 Assigning a LockNode to a locking device

The initialised LockNode must be linked to a locking device. The easiest way to do this is using a collective command, particularly if there are a number of LockNodes:

1. Select "Network/Collective tasks/WaveNet nodes".
2. Select all LockNodes *(WNNode_xxxx)* which have not yet been assigned. *There is no entry in the "Door" column for LockNodes which have not yet been assigned.*
3. Click on the "Configure automatically" button.
   ⇨ Auto-configuration launches immediately.
4. Click on the "OK" button to close the dialogue.

14.2.5 Activating locking device input events

You need to make more settings to ensure that door statuses are displayed correctly in the LSM software:

1. Select "Network/Collective tasks/WaveNet nodes"
2. Select the DoorMonitoring cylinder *(or any locking cylinder which is to forward events)*.
3. Click on the "Activate input events" button.
   ⇨ Programming is started immediately.
4. Click on the "Finish" button as soon as all locking devices have been programmed.

14.3 Setting up RingCast

A RingCast configuration is described below. The RingCast can be used to forward a RouterNode2 input event to other RouterNode2s in the same WaveNet radio network at the same time. This example shows how an emergency release is activated for the locking devices. When a fire alarm system activates Input 1 on a RouterNode2, all linked locking devices should be opened. Each locking device remains open until it receives the explicit command of a remote opening.

Obviously, a RingCast can also be used to activate other tasks such as a block lock function, remote opening and anti-gunman attack function.

This example requires a configured WaveNet radio network with two RouterNode2s. Each RouterNode2 is linked to a locking device. All locking devices should be opened as soon as Input 1 has been connected to a RouterNode2 for a short interval. This allows people to gain access to all rooms, so that they can seek safety from fire or smoke.

Please note: The RingCast for RouterNode2s networked via Ethernet is first available for models which are supplied from 2017. If a RouterNode2 cannot reach another one via Ethernet, it will try to do so in a second attempt via radio. Communication by radio functions over a distance of about 30 m (this value depends heavily on the surrounding area and cannot be guaranteed).

14.3.1 Preparing the router for RingCast

First of all, the two RouterNode2s need to be pre-configured:

- ✓ Two different RouterNode2s are configured and online in the WaveNet radio network.
- ✓ Each RouterNode2 is assigned to a locking device. Both locking devices are online.

1. Launch WaveNet Manager.
2. Right-click on the first RouterNode2.
3. Activate the "I/O configuration" checkbox and click on the "OK" button.
4. Optional: Select "Input feedback static" for Input 1, for example, to activate a signalling device during deactivation.
5. Select the "Emergency release" entry for Input 1.
6. The "RingCast" entry is to be selected as a delay.
7. Use the "Select LN" button to ensure that all required LockNodes have been selected. *(All LockNodes are incorporated the first time that the router's I/O configuration is set up).*
8. Select your protocol generation and enter the locking system password.
9. Click on the "OK" button to complete the configuration.
10. Make the same settings on the second RouterNode2 as well.

14.3.2 Adding RingCast

The RingCast can be added when the RouterNode2s have been configured accordingly:

1. Right-click on the entry "WaveNet_xx_x" in WaveNet Manager.
2. Activate the "RingCast" checkbox and click on the "OK" button.
3. Select the entry "Input 1" in "Select domain".
   - ⇨ The two RouterNode2s where you have set the I/O configurations for the RingCast appear in the "Selected router" field.
4. Highlight the two RouterNode2s where you have set the I/O configurations for the RingCast.
5. Click on the "Save" button.
6. Click on the "Finish" button.

7. Click on the "Yes" button to update the changes.
   - ⇨ The RingCast is added and is visible in WaveNet Manager after a short interval.

The configured settings have already been written in the RouterNode2s. Save the new settings and quit WaveNet Manager.

14.3.3 Functions test

The configured settings come into effect immediately. As soon as an Input 1 is connected, the locking devices are deactivated and the Output 1 connected.

Since the input cables or other parts may have been damaged in a fire, all locking devices remain in "Emergency opening" mode. This mode is not eliminated until each locking device receives a remote opening command.

14.4 Setting up event management

Networking locking devices via RouterNode2 offers many advantages. A decisive advantage is constant communication between the RouterNode2 and the locking device.

In this example, a predefined email is to be sent by the LSM software as soon as a transponder is actuated on a specific locking device at night.

The following preconditions need to be established for this requirement:

- A WaveNet radio network is set up as in the example Creating a WaveNet radio network and incorporating a locking device [▸ 45].
- The forwarding of events to the locking device as in Activating locking device input events [▸ 50] has also been activated.

14.4.1 Setting up email server

A rudimentary email client for sending emails is implemented in the LSM software. An own email account which supports SMTP format is required to send emails.

1. Select "Network/Email notifications"
2. Click on the "Email" button.
3. Enter all your email provider's SMTP settings.
4. Click on the "OK" button.
5. Click on the "OK" button.

14.4.2 Setting task service

1. Select "Network/Task manager".
2. Select your communication node under "Task service".
3. Click on the "Apply" button.

4. Click on the "Finish" button.

14.4.3 Forward input events via RouterNode2

Forwarding needs to be activated in the router's I/O configuration as soon as events *(e.g. a transponder is activated on a networked locking device)* need to be forwarded to the CommNode server via the RouterNode2.

1. Launch WaveNet Manager.
2. Right-click on the transponder on the router and select "I/O configuration".
3. Use the drop-down bar in "Report events to management system" to stipulate the "All LN events" option.
4. Confirm by pressing the "OK" button and quit WaveNet Manager.

14.4.4 Creating a response

Create a response first. This response can be selected later if a specific scenario arises.

1. Select "Network/Event manager".
2. Click on the "New" button under "Responses" in the right-hand section.
3. Complete a name and a description for the response.
4. Select the type "Email".
5. Click on the "Configure response" button.
6. Click on the "New" button.
7. Enter the recipient's email address, a subject matter and a message text. *You can use the "Test" button to check the email configuration immediately.*
8. Exit the dialogue box by pressing on the "OK" button three times. Press the "Finish" button to return to the matrix.

14.4.5 Creating an event

Once the response is created, you can then create the event.

1. Select "Network/Event manager".
2. Click on the "New" button under "Events" in the left-hand section.
3. Complete a name and a description for the response.
4. Select the type "Access".
5. Click on the "Configure event" button.
6. Activate the "Respond on all transponders" checkbox. *The event needs to trigger every time a transponder is activated. Alternatively, you can restrict the event to an individual transponder.*
7. You can adjust the action even further in the "Time setting" section.

8. Click on the "OK" button.
9. Click on the "Select" button in the "Locking devices" section.
10. Add all locking devices which need to trigger when the transponder is activated and confirm your choice by pressing the "OK" button.
11. Click on the "Add" button in the "Associated actions" section.
12. Add the previously created response.
13. Click on the "Configure time" button.
14. Enter the times for night time curfew. The event is only active for the time frame defined here.
15. Exit the dialogue box by pressing on the "OK" button three times. Press the "Finish" button to return to the matrix.

14.5 Administering the virtual network (VN)

A virtual network (VN network) allows you to change and regulate authorisations quickly and conveniently without the need for a full network. The authorisation for locking devices (and block IDs for blocked ID media) is stored directly on the ID medium and forwarded each time the medium activates a locking device. That is why it is important to activate ID media on a gateway at regular intervals in a virtual network.

This example shows the main set-up for a virtual network.

14.5.1 Setting up a locking system

The "Virtual network" checkbox needs to be activated in a(n) (exclusively) G2 locking system. If this setting is applied to an existing locking system, it may create considerable programming requirements.

14.5.2 Setting up a VN service

1. Select "Network/VN service".
2. Select the VN server (e.g. the communication node).
3. Indicate the installation path to the VN server. *The VN server is installed in a separate folder in the main directory in an LSM Business installation.*
4. Click on the "Apply" button.
5. Click on the "Finish" button.

14.5.3 Adding components and setting up the LSM software.

Before starting with the set-up, you first need to make the key settings for operating a network in the LSM software and the RouterNode2 must be ready for use.

- Preparing LSM software [▸ 45]

- Preparing hardware [▸ 46]
- Creating communication nodes [▸ 46]
- Setting task service [▸ 52]

1. Add the different ID media (e.g. transponders) and locking devices (e.g. active locking cylinders).
2. Carry out initial programming for the added components.
3. Add a SmartRelay2 and authorise all ID media which are to receive new authorisations from it at a later stage.
   ⇨ The "Gateway" checkbox **must** be activated in the tab in the SREL2's locking device properties.
4. Carry out initial programming of the SREL2 and ensure that it features a correctly connected LockNode.
5. Use WaveNet Manager to set up the RouterNode2 and assign the gateway (or the SREL2) to it.
   ⇨ See Setting up the network and importing into LSM [▸ 47].

14.5.4 Exporting changes to authorisations

Exporting changes to authorisations will only work if there is at least one change. Withdraw authorisation for Locking Cylinder 1 from Transponder 1, for example, to test the export.

1. Select "Programming/Virtual network/Export to VN network".
2. Select all SREL2s to which the changes need to be sent/exported.
3. Check that you have selected the right locking system.
4. Click on the "Prepare" button
   ⇨ The "Persons" list contains all the changes which are being exported.
5. Click on the "Export" button
   ⇨ The export process will now start. The changes are transmitted to the gateway.

The authorisation change is now ready at the gateway. There are now two scenarios:

- Transponder 1 books on the gateway. Locking Device 1 then detects that Transponder 1 is no longer authorised and refuses entry.
- Another transponder (not Transponder 1) first books on the gateway and authorises itself on Locking Device 1. Locking Cylinder 1 is informed of the block ID for Transponder 1.

14.5.5 Importing changes to authorisations

When the changes have been exported to the gateway, you are not able to see which changes have already been collected from the gateway in LSM software at first. Only an import will reveal this.

1. Select "Programming/Virtual network/Import synchronisation".
   ⇨ The import process starts immediately.
2. Click on the "Finish" button

14.5.6 Tips on VN

- It is important to use all transponders in the system at short, regular intervals to distribute the changes quickly offline throughout the locking system. This is where you can use time budgets:

  The "Dynamic time frames" options in the locking system properties offer the option of imposing a time budget on transponders. This obliges a person to reload their ID medium at the gateway on a regular basis. If they do not, the ID medium is blocked for this locking system.
- You can automate the import and export of changes for a gateway. You can make the settings directly under "Network/VN service". *Note that importing and exporting many changes will take up the WaveNet's full capacity for a time.*

15 Help & Contact

Instruction manuals	You will find detailed information on operation and configuration online under INFOCENTER > DOWNLOADS on our homepage at www.simons-voss.de
Hotline	If you have any questions, the SimonsVoss Service Hotline will be happy to help you on +49 (0)89 99 228 333 (German fixed network; call charges vary, depending on the operator)
Email	Would you prefer to send us an email? hotline@simons-voss.com
FAQs	You will find information and help for SimonsVoss products in the FAQ section www.simons-voss.de in INFO CENTRE > FAQ SECTION

SimonsVoss Technologies GmbH, Feringastrasse 4, 85774
Unterföhring, Germany