Industrial Security Router / Firewall

IE-SR-4GT
IE-SR-4GT-LTE/4G-EU
IE-SR-4GT-LTE/4G-USEMEA
IE-SR-4GT-M
IE-SR-4GT-LTE/4G-USEMEA-M

Manual

Version 1.5

August 2025

Important notes:

This document will be updated continuously.

This version refers to Router firmware version 2.1.1 and above.

This document, a Security Data Sheet, new firmware or additional product information can be downloaded at the Weidmüller eShop using following link:
https://eshop.weidmueller.com/

► Type the article number into the search bar
→ Select “IE-SR-4GT-X” and download needed documentation and software

Industrial Security Router / Firewall
Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2025 Weidmüller Interface GmbH & Co. KG
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.

Weidmüller provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG
PO box 3030
32760 Detmold
Klingenbergstrasse 26
32758 Detmold
Germany

Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

1. Introduction

1.1 Proper and intended usage

The Router is intended for use in industrial (IP20) environments. It is equipped with Ethernet interface ports and is used solely for connecting components within a network.

By connecting network components, the Router enables network nodes to exchange data between the LAN and WAN port. The Router is responsible for routing IP packets between an industrial network and an external network (such as the Internet). The Router can be configured on-site using an IP network on both Ethernet ports (LAN or WAN).

A Security Data Sheet is available and should be consulted for detailed operational and security guidance. It provides essential information to ensure secure and reliable network operation supported by the router's built-in security standards.

Additionally, VPN (virtual private network) connections can be used to connect the Router as a VPN-Client or a VPN-Server with other VPN devices.

1.2 Package Checklist

Non-DNV models

1 x Industrial Security Router (IE-SR-4GT, IE-SR-4GT-LTE/4G-EU or IE-SR-4GT-LTE/4G-USEMEA)

1 x 3-pin connector

2 x 4-pin connectors for power supply and I/Os

2 x Antennas for mobile connection (only models with integrated 4G modem)

1 x Hardware Installation Guide

DNV models

1 x Industrial Security Router (IE-SR-4GT-M or IE-SR-4GT-LTE/4G-USEMEA-M)

1 x 4-pin connector for I/Os

1 x 8-pin connector for I/Os

1 x 3-pin connector

1 x 3-pin connector for power supply

1 x cover for pins

2 x Antennas for mobile connection (only models with integrated 4G modem)

1x Hardware Installation Guide

If any of these items are missing or damaged, please contact your customer service representative for assistance.

1.3 Safety instructions

	**Warning** - Using the selected device for purposes other than those specified or failure to observe the operating instructions and warning notes can lead to serious malfunctions that may result in personal injury or damage to property. - If this product malfunctions, it is no longer possible to predict the behavior of neighboring networked facilities and their connected devices. Personal injury and property damage can occur because of malfunctions. Only carry out changes to the settings when you are certain of the consequences such changes will have on all connected networks, facilities and devices. - Personal injury and property damage can occur if this product is used improperly. Adjustments and setting changes to this product should only be carried out by sufficiently qualified personnel.

Caution

- This device is designed only for an operating voltage range from 7 to 36 V DC. Do not use a higher voltage; this could destroy the Router and other devices.

- The Security Router does not have an on/off switch. The operating voltage must be switched on by the facility in which the device is integrated.

Caution

You should activate and synchronize the time server or set the system time manually if you are using certificates in virtual private networks (VPNs) or simple network management protocol (SNMP). An inaccuracy in the system time can cause the virtual private network (VPN) to malfunction.

You should synchronize the system time with a time server after each Router reboot and after you load the default settings. Or you can set the system time manually.

Caution

- The default system access information for the Security Router is included in this document. Unauthorized individuals can use this access data to gain access to the Router's web browser and cause damage. Be sure to change these system default access settings.

- Some services may be blocked by a firewall. You may need to deactivate the firewall. By deactivating the firewall, the PC is no longer protected against viruses or other attacks. Only deactivate the firewall when your PC is sufficiently protected by other measures.

- A single port can only properly execute one service. If multiple services are assigned to a port, the port can no longer execute any service. Be sure to assign only one service to any port.

Note

- The IP protocol reserves certain IP address ranges for special purposes (such as multicasting). Do not assign IP addresses in the range from 127.0.0.0 – 127.255.255.255 or 224.0.0.0 – 255.255.255.255.

- This device is intended for use in applications as described in the operating instructions only. Using this device in non-approved applications will lead immediately to the expiration of all guarantee and warranty claims on the part of the operator against the manufacturer.

1.4 Mounting the device

	**Caution** - This device is designed only for an operating voltage range from +19,2 to 28,8 VDC. Do not use a higher voltage; this could destroy the Router and other devices. - Connecting plugs should never be connected or disconnected from electrical devices if they are carrying a live load. Be sure to first disconnect all poles of the plug. Remember to disconnect all plugs from the Router before it is installed or removed. - Electrical devices should not be installed or removed during operations. Never install or remove the Router while it is running.

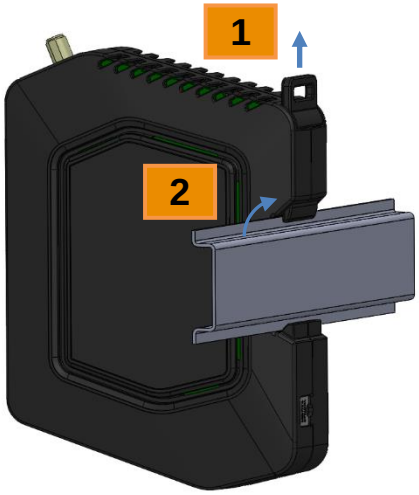
	**Caution** - It is important to provide sufficient clearance between devices which cause strong electromagnetic interference (such as frequency converters, transformers or motor regulators). The clearance gap between such devices and the Router should be as wide as possible. The Router can be further shielded by using a mu-metal partition. - The Router is designed to be mounted on a top-hat rail that is compliant with the EN 50022 standard. This Router will not have a secure mount if any other type of rail is used. Use a top-hat rail that complies with the EN 50022 standard. Be sure to observe the mounting information provided by the manufacturer.

	**Note** - A minimum of 2-inch (5 cm) gap should be kept between the Router and neighboring devices from the top and bottom. This will ensure that the Router is sufficiently ventilated. - The top-hat rail should be in a horizontal position along the vertical rear wall of the electrical cabinet. This ensures that the Router can be adequately ventilated from below to above.

DIN-rail mounting:

Insert the bottom of the DIN-rail clip behind the lower edge of the DIN-rail. Then open the latch at top of the device by using a flatbladed screwdriver (1) and fix the device on theDIN-rail by gently tilting the top towards the DIN-rail (2).

To remove the Router from the DIN-Rail, simply reverse the steps as described above.



1.5 Technical data

Operation mode

IP-Router	• IPv4-Routing between ports (group) and WWAN interface (optional). The LAN-Ports (ETH2…4) behave each as an unmanaged switch. • Static or dynamic routing according to RIPv2 or OSPF protocol.
IP-Router (extended)	• Each RJ45 port can be configured individually • IPv4-Routing between all available RJ45 ports (ETH1…4) and WWAN interface (optional). • A maximum of 4 individual subnets (using LAN/WAN ports) can be configured. • Static or dynamic routing according to RIPv2 or OSPF protocol.
Transparent Bridge	• Running as 4-Port-Switch with additional Layer-2 (MAC) or Layer-3 (IP-based) filter.
Network Services	• DHCP Server • DNS-Relay • NTP-Server/Client
Firewall	• IPv4 Stateful inspection Firewall • NAT-Masquerading, 1:1 NAT, Port forwarding • Layer-2/3-Filter (VLAN ID, VLAN QoS Tag, MAC address based, Ethertype Frame)

VPN

OpenVPN	• Configurable as OpenVPN server or client (Layer 2 and Layer 3) • Authentication with X.509 Certificates • Tunnel support via HTTP-Proxy • A maximum of 10 different server configurations • Unlimited number of client connections in server mode
IPsec	• Can be configured as an IPsec server or client. • Authentication with PSK (user ID, password) or X.509 certificates. • Hardware encryption for faster data flow rate. • A maximum of 64 simultaneous connections (subnet with subnet or as IPsec server) • Encryption algorithms such as SHA512, AES256, DH24, 3DES
u-link	• Based on certificate-secured OpenVPN technology • To be used with the Weidmüller Remote Access Service • Simplifies VPN connections and management • Fast and easy connections • Free of charge for a limited time • Visit https://u-link.weidmueller.com for further information.

Configuration

Management	• Configuration with web interface (HTTP/HTTPS) • Web interface selectable in English or German language • Configuration support through wizard • Configuration support through detailed help information (tooltip) • Configurable Multi-user access with definable rights • Support for SNMP v3 • Event log / audit log / syslog

Other features

Modbus/TCP (Slave mode)	The integrated Modbus/TCP Slave provides control functions sent by a Modbus/TCP master. Following functions are imaged in the registers: • Cut & Alarm: Get status / Set acknowledgment • IPsec /OpenVPN/u-link: Switch configured VPN connections on or off
Diagnosis	• „Remote Capture“ - feature for network diagnostics via a connected PC (Wireshark)
Monitoring	• WWAN connection monitoring via ICMP protocol (ping request)

Interfaces

RJ45-Ports	• 4 x 10/100/1000BaseT(X)
USB-Port	• Useable for automatic configuration restore from backup file (*.cf2) or firmware upgrade via USB stick at boot process • USBIP Server for remote access to the USB stick
SCM card reader	• Save and restore the configuration using a Weidmüller smart card (SIM card without mobile provider data, only the storage capacity of the chip will be used)
SIM card slot*1	• Insert SIM card for mobile communication
Micro-SD card slot	• For future use
LED displays	• Signaling the status for power, device status, active VPN connection, Wireless WAN*2, Application 1 and Application 2 (both for future use)
Digital Inputs	• "DI” can be used e.g. to initiate VPN connection for u-link, OpenVPN via external input (19,2…28,8 V DC, max 10mA), “DI2” can be used e.g. for I/O cut, … • Note that the digital inputs require power to be used
Digital Outputs	• "DO” can be used e.g. to monitor VPN connection or be triggered by firewall rules (19,2…28,8 V DC, max 10mA) • Note that the digital outputs require power to be used
Reset-Button	• Restore to the factory settings

*1 for the IE-SR-4GT-LAN device no function

*2 for LTE/4G models only

Power

Input Voltage	• 1* 24 VDC (19,2 to 28,8 Volt) Use a power supply according to NEC Class 2 for use according to UL certification
Current consumption	• Theoretical max. 1600 mA @ 24 VDC

Technical data (housing)

Housing	• Metal, protection IP20
Mounting	• TS35 (DIN rail)

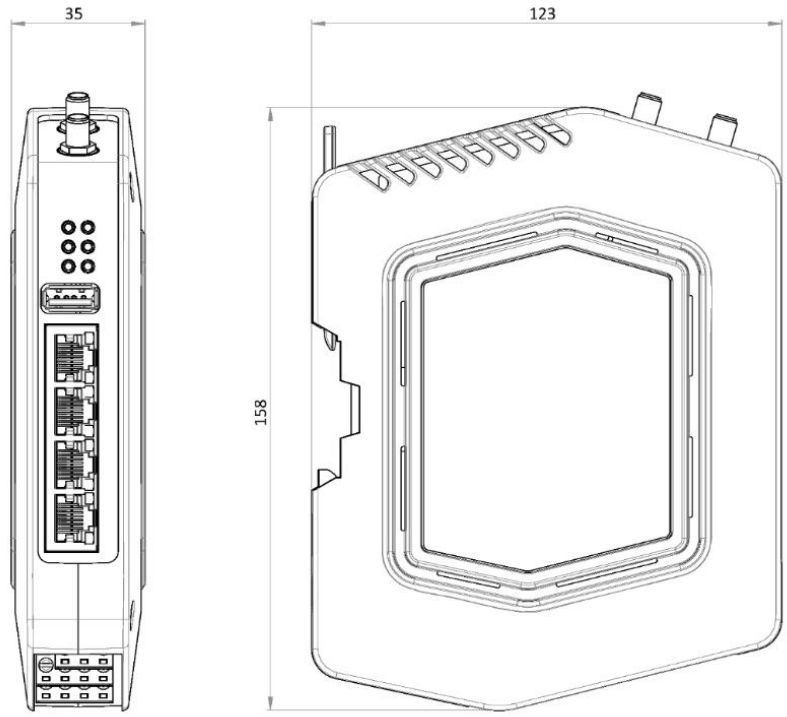


Figure 1: Non-DNV Router

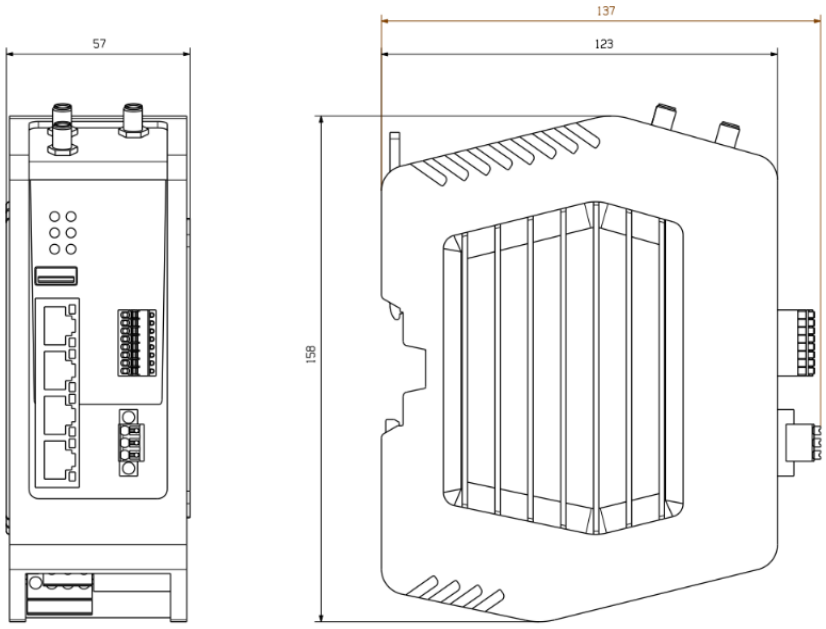
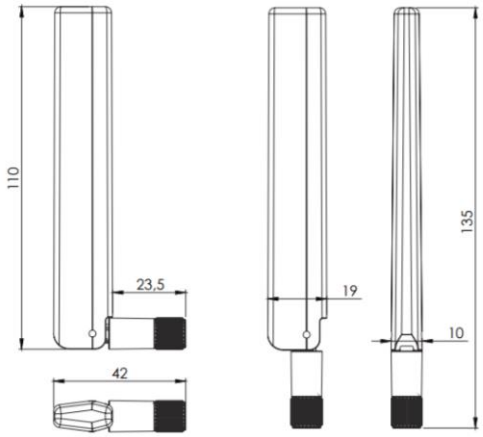


Figure 2: DNV Router

Environmental conditions

Operating Temperature	• -25°C to +70°C
Storage Temperature	• -40°C to + 85°C
Ambient Humidity	• 5 to 90% non-condensing

WWAN

LTE/4G*	• Built-in 4G/LTE modem with 300 Mbps peak downlink and 50 Mbps peak uplink • FCC, CE, IC, NCC, PTCRB, Bell, AT&T
Standards*	• LTE: 3GPP Release 11 • UMTS: 3GPP Releases 9
Frequency bands EU*	• **LTE:** B1, B3, B5, B7, B8, B20, B28, B38, B40, B41 • **UMTS:** B1, B5, B8 • **GSM:** B3, B5, B8
Frequency bands US, EMEA and Australia*	• **LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B20, B25, B26, B29, B30, B41 • **3G UMTS/HSPA+:** B1, B2, B4, B5, B6, B8, B9, B19
Antennas*	Antenna gain and frequencies: • -1,1 dBi @ 617-960 MHz • 0,5 dBi @ 1427-2690 MHz • 0,3 dBi @ 3300-5000 MHz • 1,6 dBi @ 5150-5925 MH 

* Only models IE-SR-4GT-LTE/4G-EU, IE-SR-4GT-LTE/4G-USEMEA, IE-SR-4GT-LTE/4G-USEMEA-M

Approvals

Non-DNV models

Safety	• cULus (UL508)
EMC	• FCC Part 15 Class A • EN61000-6-2 Immunity for industrial environments • EN61000-6-4 Emission Standard for industrial environments
Shock	• DIN EN 60068-2-27
Vibration	• DIN EN 60068-2-6

DNV models

EMC	• FCC Part 15 Class A • EN61000-6-2 Immunity for industrial environments EN61000-6-4 Emission Standard for industrial environments
Shock	1. DIN EN 60068-2-27
Vibration	2. DIN EN 60068-2-6
Ship use	DNV

Order Information

	Model name	Order number
4-Port LAN/WAN Router **with** VPN features	IE-SR-4GT-LAN	2873910000
4-Port LAN / WAN Router **with** VPN features and additional integrated LTE/4G modem	EU: IE-SR-4GT-LTE/4G-EU USEMEA: IE-SR-4GT-LTE/4G-USEMEA	2873920000 2873930000
4-Port LAN/WAN Router **with** VPN features and DNV approval	IE-SR-4GT-M	2990450000
4-Port LAN/WAN Router **with** VPN features, additional integrated LTE/4G modem and DNV approval	IE-SR-4GT-LTE/4G-USEMEA-M	2990440000

2. Hardware related functional descriptions

2.1 Description of LED status indicators

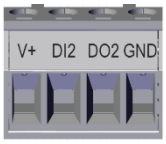
Description of LED status indicators

LED	Signal	Meaning
PWR	Off	The device is not powered
	Flashing green (1Hz)	Device is turned on; the boot process is running
	Flashing Green (5Hz)	Firmware update is processing
	Green	Device is turned on and ready to run
STAT	Off	The device is not powered or runs a working firmware
	Red	Error after boot process or recovering an image
VPN	Off	No activated VPN tunnel
	Green	The tunnel activated via VPN key is active
AP1	Off/Red/Green	Different Cut & Alarm features can be mapped here by using the physical in-/ouputs and software functions (see **4.2.4 Configuration → I/Os**)
AP2	Off/Red/Green	Different Cut & Alarm features can be mapped here by using the physical in-/ouputs and software functions (see **4.2.4 Configuration → I/Os**)
Only LTE/4G models		
WWAN	Off	No active 4G / LTE connection
	Flashing yellow (1Hz)	Searching wireless network
	Flashing yellow (2Hz)	Log-In declined
	Flashing yellow (5Hz)	Firmware update of cellular module
	Yellow	Connected to a network provider but no active data connection (Offline)
	Flashing green	Connected to a network provider. Router activates the connection on data flow (Standby)
	Green	Logged in, online

2.2 Interfaces

Non-DNV models:

Description of device interfaces at top, bottom and front side

Connectors for LTE/4G antennas at top side; Connector type: **SMA female** (Only model IE-SR-4GT-LTE/4G-EU and IE-SR-4GT-LTE/4G-USEMEA)	
USB 2.0 connector	
3 x RJ45-Connector LAN ETH2…ETH4(10/100/1000BaseTX)	
1 x RJ45-Connector WAN ETH1 (10/100/1000BaseTX)	
	4-pin connector for digital input and output
	4-pin connector for 24 V DC power supply and digital input

Description of device interfaces at rear side

SIM1 slot / socket

Slot for mobile SIM card (only 4G/LTE models)

SCM/SIM2 slot / socket

SIM memory card reader for external backup and restore of the Router configuration. A second SIM-card currently is not supported. **Only SCM cards** are supported!

See picture above for correct insertion of the cards

Note: No snapping when inserting the SIM/SCM card

Factory Default Button

Resetting the router

Connectors for LTE/4G antenna of type **SMA female** (only 4G/LTE models).

2 x SMA connectors, MAIN and AUX (AUX = Diversity / MIMO)

External antennas:

EMEA/Australia - Operating bands - Ant. 1: 791–960 MHz; 1710–1990 MHz; 2110–2170 MHz; 2500–2690 MHz

Americas - Operating bands - Ant. 1: 704–960 MHz; 1710–1995 MHz; 2110–2170 MHz

Use coaxial cable with nominal impedance of 50 ohms.

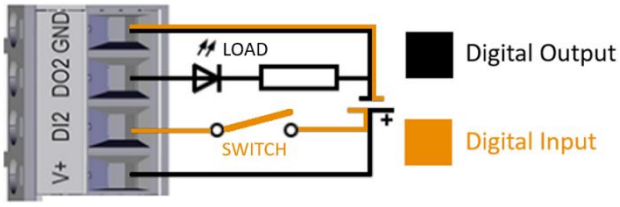
2.3 Pin assignments

Pin assignment of 4-pin connector for „24 V DC power supply and digital input“

Pin number	Description
DI	Digital Input for allowing u-link and OpenVPN
FE	Functional Earth
0V	GND
V+	24 V DC ± 20 %

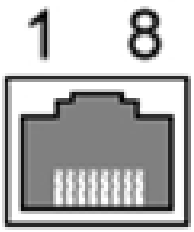
Pin assignment of 4-pin connector for „Digital input and output“

Pin number	Description
V+	24 V DC ± 20 %
DI2	Digital Input 2 0-Signal: 0…4,5V 1-Signal: 10…30V max. 6mA
DO2	Digital Output 2 0-Signal: 0V 1-Signal: Outputs the voltage supplied between V+ and GND max 0,5A
GND	Reference Potential



Pin assignment of RJ45 Ethernet ports (LAN and WAN)

Pin number	SIGNAL NAME (MDI)	
	10/100Base T(x)	1000Base T
1	TX +	BI_DA+
2	TX -	BI_DA-
3	RX +	BI_DB+
4	NC	BI_DC+
5	NC	BI_DC-
6	RX -	BI_DB-
7	NC	BI_DD+-
8	NC	BI_DD-



Pin assignment of USB 2.0 connector

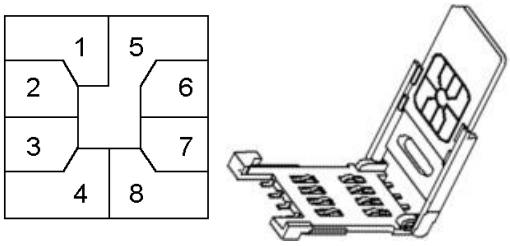
The USB interface is intended for connecting peripheral devices (USB 2.0). The connector is without function in the current firmware version, but is optional for future planned applications.

Pin number	SIGNAL NAME
1	VDC
2	D -
3	D +
4	GND

Pin assignment of Smartcard Reader (ISO 7816 Standard)

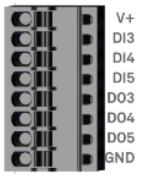
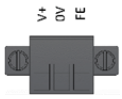
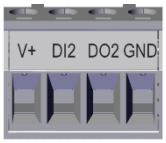
The integrated SIM card reader is intended for saving and restoring the configuration data.

Pin number	SIGNAL NAME
1	VCC 5 Volt
2	RESET
3	CLOCK
4	n/c
5	GND
6	n/c
7	I/O
8	n/c



DNV-models:

Description of device interfaces at top, bottom and front side

Connectors for LTE/4G antennas at top side; Connector type: **SMA female** (Only model IE-SR-4GT-LTE/4G-USEMEA-M)	
USB 2.0 connector	
3 x RJ45-Connector LAN ETH2…ETH4(10/100/1000BaseTX)	
1 x RJ45-Connector WAN ETH1 (10/100/1000BaseTX)	
	8-pin connector for I/O interface
	3-pin connector for 24 V DC power supply
	4-pin connector for digital input and output
	3-pin connector for RS485 interface

Description of device interfaces at rear side

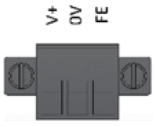
<table>
<tr>
<td rowspan="3">  </td>
<td>SIM1 slot / socket
Slot for mobile SIM card (only 4G/LTE models)</td>
<td rowspan="3">  </td>
<td rowspan="3">Connectors for LTE/4G antenna of type SMA female (only 4G/LTE models).
2 x SMA connectors, MAIN and AUX (AUX = Diversity / MIMO)

External antennas:
EMEA/Australia - Operating bands - Ant. 1: 791–960 MHz; 1710–1990 MHz; 2110–2170 MHz; 2500–2690 MHz
Americas - Operating bands - Ant. 1: 704–960 MHz; 1710–1995 MHz; 2110–2170 MHz
Use coaxial cable with nominal impedance of 50 ohms.</td>
</tr>
<tr>
<td>SCM/SIM2 slot / socket
SIM memory card reader for external backup and restore of the Router configuration. A second SIM-card currently is not supported. Only SCM cards are supported!
 
See picture above for correct insertion of the cards
Note: No snapping when inserting the SIM/SCM card</td>
</tr>
<tr>
<td>Factory Default Button
Resetting the router</td>
</tr>
</table>

2.3 Pin assignments

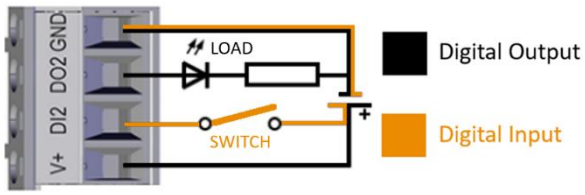
Pin assignment of 3-pin connector for „24 V DC power supply“

Pin number	Description
FE	Functional Earth
0V	Reference Potential
V+	24 V DC ± 20 %



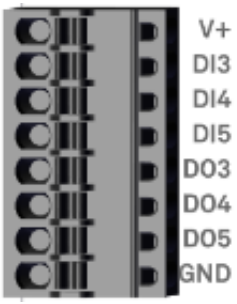
Pin assignment of 4-pin connector for „Digital input and output“

Pin number	Description
V+	24 V DC ± 20 %
DI2	Digital Input 2
DO2	Digital Output 2
GND	Reference Potential



Pin assignment of 8-pin connector “I/O interface”

Pin number	Description
V+	24 V DC ± 20 %
DI3	Digital Input 3
DI4	Digital Input 4
DI5	Digital Input 5
DO3	Digital Output 3
DO4	Digital Output 4
DO5	Digital Output 5
GND	Reference Potential



Power needed for every Digital Input:

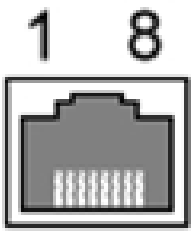
0-Signal: 0…4,5V / 1-Signal: 10…30V, max. 6mA

Power output from every Digital Output:

0-Signal: 0V / 1-Signal: Outputs the supplied voltage between V+ and GND, max 0,5A

Pin assignment of RJ45 Ethernet ports (LAN and WAN)

Pin number	SIGNAL NAME (MDI)	
	10/100Base T(x)	1000Base T
1	TX +	BI_DA+
2	TX -	BI_DA-
3	RX +	BI_DB+
4	NC	BI_DC+
5	NC	BI_DC-
6	RX -	BI_DB-
7	NC	BI_DD+-
8	NC	BI_DD-



Pin assignment of USB 2.0 connector

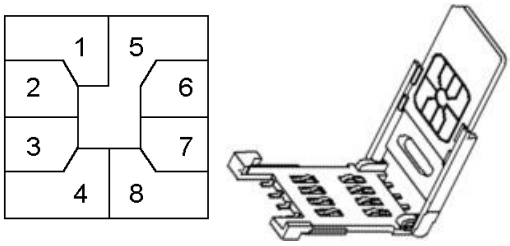
The USB interface is intended for connecting peripheral devices (USB 2.0). The connector is without function in the current firmware version but is optional for future planned applications.

Pin number	SIGNAL NAME
1	VDC
2	D -
3	D +
4	GND

Pin assignment of Smartcard Reader (ISO 7816 Standard)

The integrated SIM card reader is intended for saving and restoring the configuration data.

Pin number	SIGNAL NAME
1	VCC 5 Volt
2	RESET
3	CLOCK
4	n/c
5	GND
6	n/c
7	I/O
8	n/c



3. Initial start-up / Getting Started

3.1 Configuration of the Router by using an Internet browser

	Note
	The configuration of the device can be done either via LAN or WAN RJ45 ports.

Connect the unit to a 24V DC (4-pin plug) power source. The corresponding plug is included.

During the initial boot phase, the PWR LED is flashing. The Router is ready when the PWR LED is lit constantly (after about 30 seconds).

Connect the Router to the Ethernet interface of a configuration PC using a RJ45 network cable.

It is possible to use a standard Ethernet patch cable or a crossed network cable. By default, all Ethernet ports are configured with auto negotiation.

The configuration and control of the Router is to be done via the integrated Web server. Any common Internet browser can be used.

When delivered, the Web interface of the Router can be accessed from both LAN and WAN port.

To access the Web interface of the Router the IP address of the connected PC must be in the same logical network (IP address range) as the Router.

Factory default IP addresses and net masks:

ETH 2-4 ports: **192.168.1.110 / 255.255.255.0**

ETH 1 port: **DHCP**

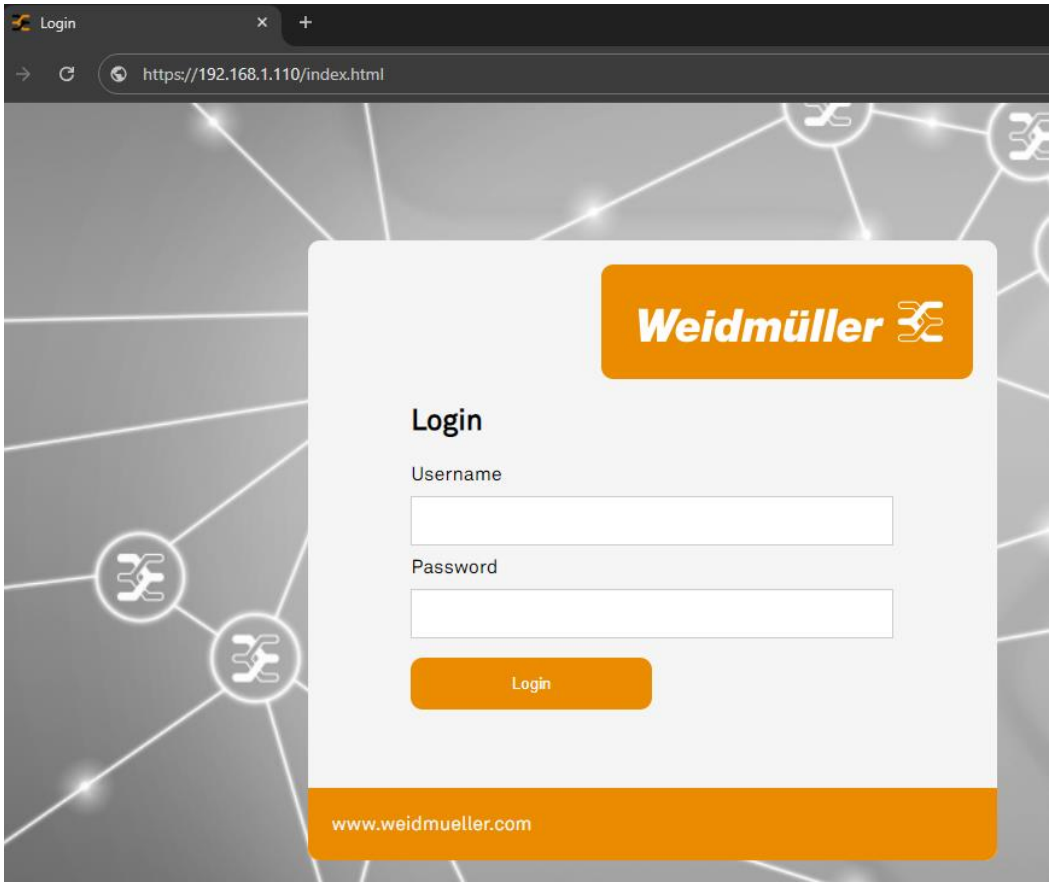
3.2 Starting the Web interface

	Important note
	The Router's Web server **partly** is using **Java script** for parameter settings (e.g. if you want to apply or delete a configured Open VPN session). **Please ensure that the Web browser you are using can run Java script. For Router configuration. You do NOT need to install Java runtime software (for executable Java applets) because only Java script will be used. Standard Web browsers by default can run Java script code.**

1. Start your Web browser and enter the IP address of the connected Router port into the browser's address line. (i.e., when connected to a LAN-Port 192.168.1.110). Now the login prompt of the Router should appear for input Username and Password.

   Default values (factory settings) for Login:

   Username: admin
   Password: Detmold



   Confirm your input by pressing the Log in button.

Now the Router needs to be configured with the Config Wizard. This page corresponds to the menu item "4.2.1 Configuration → Config Wizard". On this page, the most important configuration and status option are displayed.

	Note
	If the login prompt does not appear, please check the network LED's, if the devices are connected to the network correctly. If problems still persist, please check the proxy and firewall settings of the local PC

3.3 Default factory settings of the Router:

	Note
	Some fields are linked with a hyperlink to jump directly into the corresponding menu item.

Language	English
Operation Mode	IP Router
IP address LAN Port(s)	192.168.1.110 (static value)
Subnet Mask	255.255.255.0
NAT (Masquerading) on LAN Port	Not activated
IP address WAN Port	DHCP
Subnet Mask	255.255.255.0
NAT (Masquerading) on WAN Port	Not activated
Default gateway	No entry
DNS	Activated
Firewall (Packet filter)	By default, data traffic in both directions between LAN and WAN is allowed on Layer 2 but blocked on Layer 3. For this purpose, the packet filter contains two default rules: “Allow_L2” (which allows all network traffic at Layer 2) and “Block_L3” (which blocks all network traffic at Layer 3). Please note that the devices will no longer forward IP traffic between the different network interfaces LAN/WAN or ETH1/ETH2-4 if it is not yet configured and running in commissioning mode.
IP routing	No static routes, Dynamic routing disabled (OSPF, RIP)
SNMP / DHCP / DNS	Disabled
VPN	Disabled
4G Modem (for LTE/4G models only)	Disabled

3.4 Reset to factory default settings by external push button

By pressing the push button "Factory Default" the security Router can be reset at any time and regardless of the configuration to the default settings (factory settings).

How to set the factory settings:

1. Power off the Router.
2. Press the button „Factory Default“ and keep it hold down.
3. Power on the Router and keeping button „Factory Default“ pressed while Router is booting.
4. Release button „Factory Default“ when Power LED starts flashing fast (~ 10 seconds after power on).
5. Wait until Power LED is glowing constantly green.

→ Now the Router is ready to run with factory default settings.

3.5 Using the Weidmüller Router-Search-Utility

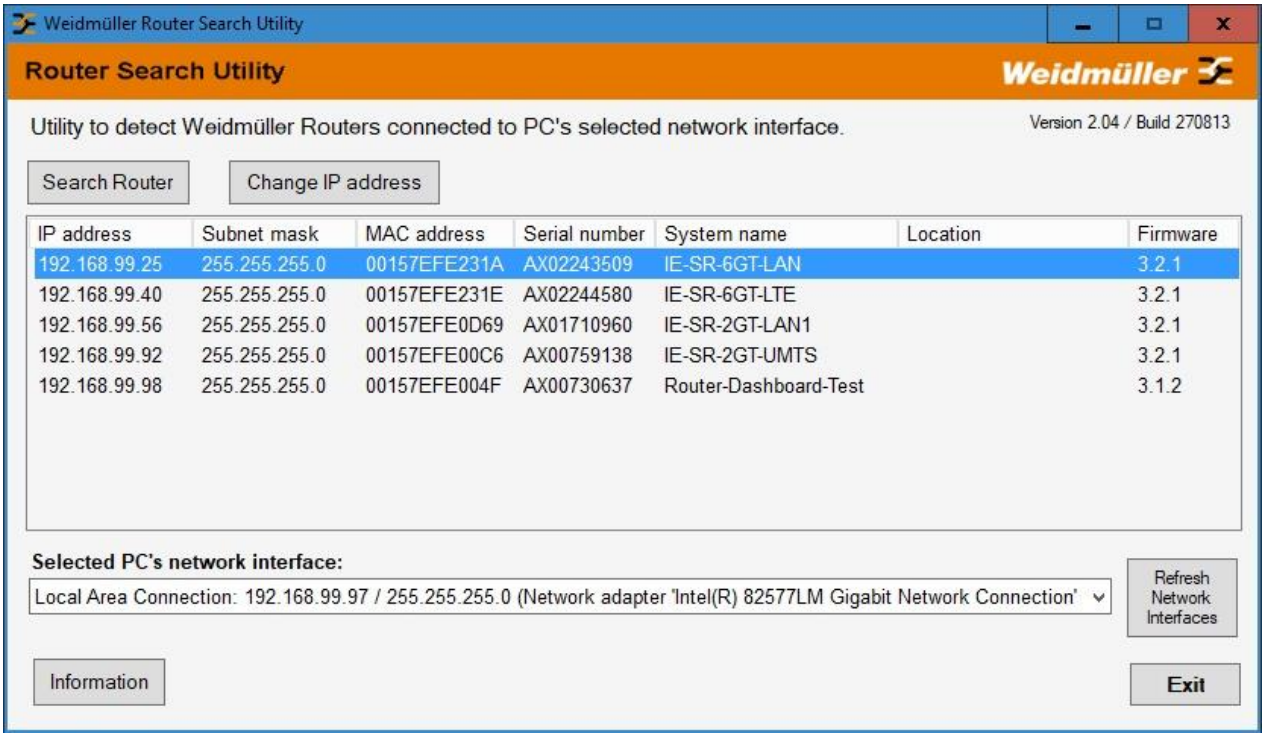
The software tool Weidmüller Router-Search-Utility can be used to find Weidmüller Routers and detect their IP addresses within a switched network. This software is very helpful if you don't know the current IP address of a Router. This can e.g. happen in cases that you have forgotten the current IP configuration, or you have lost the Router access in case of configuring an unintended IP address.

The main features of the software are

- Detecting a Router and displaying the parameters IP address, Subnet mask and MAC address. If the PC and the Router are in the same network range then additionally the values of parameters Device name, Location and Firmware version are displayed.
- Change the IP address of a detected Router
- Open the web interface of a detected Router

You may download the Weidmüller Router-Search-Utility from the Weidmüller web site using the following path:

1. Open catalog.weidmueller.com
2. Search for the article number or product name
3. When the product is selected, find the files in section "*Downloads*"



3.6 Basic description of Router’s configuration interface (menu items)

The menu structure of the web Interface is divided into 4 main sections:

Section Diagnostics

- Displays system status data
- Display of logging information such as Eventlog, Audit
- Displays current interface parameters (Ethernet/WWAN)
- Feature for testing the data communication between the Router and other Ethernet devices (Ping test)
- Remote capture and download of current settings

Section Configuration

- Setting the major functions with the Config Wizard
- Setting of operation mode (*IP Router*, *IP Router (extended)* or *Transparent Bridge*) and basic network parameters (IP addresses, Default gateway)
- Setting of firewall rules (Packet filter)
- I/Os Cut & Alarm
- Configuration of general system data (name, location, contact person, date / time, language interface, etc.)
- Certificate Management for VPN connections
- Access control for users and permission control
- Web Access and Custom Menu settings
- IP-Routing (static, dynamic) and IP address management (Masquerading, 1:1 NAT, Port forwarding)
- Configuration of u-link Remote Access Service / OpenVPN / IPsec connections
- Configuration of general network services (e.g. DHCP, DNS, SNMP)

Section system

- Backup and restore of device configuration
- Factory default, Save settings
- Update firmware, Reboot

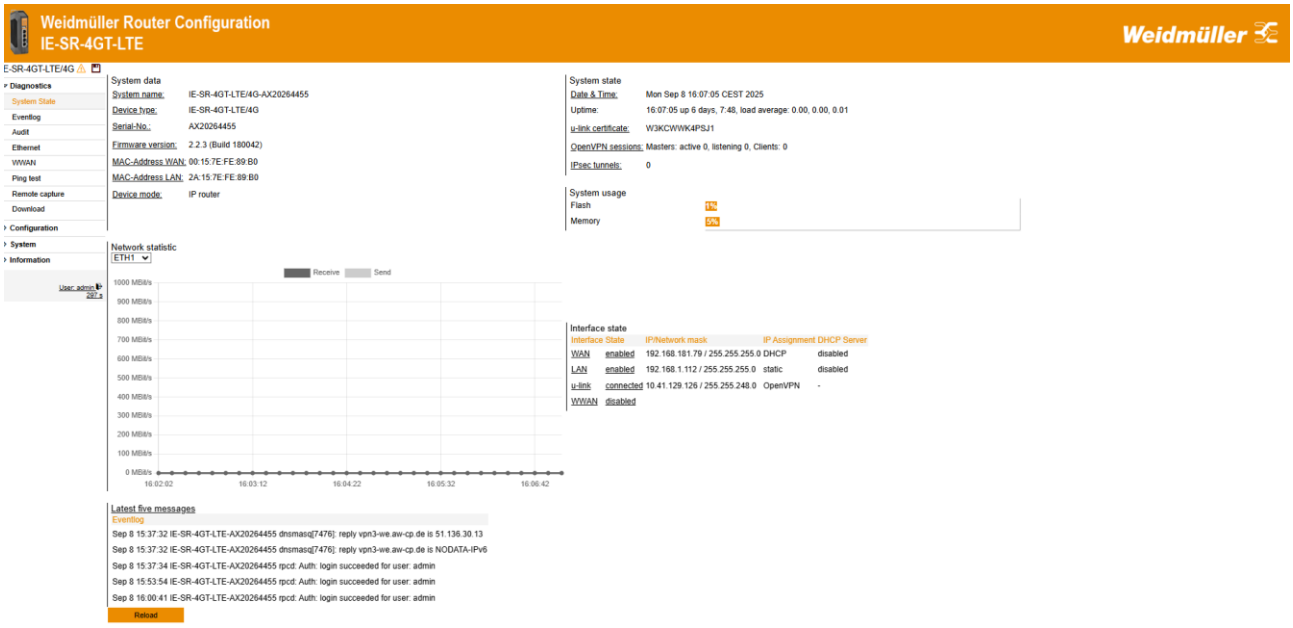
Section Information

- Display of technical data and hardware information (e.g. serial number and MAC address)
- License Information

4. Web Configuration

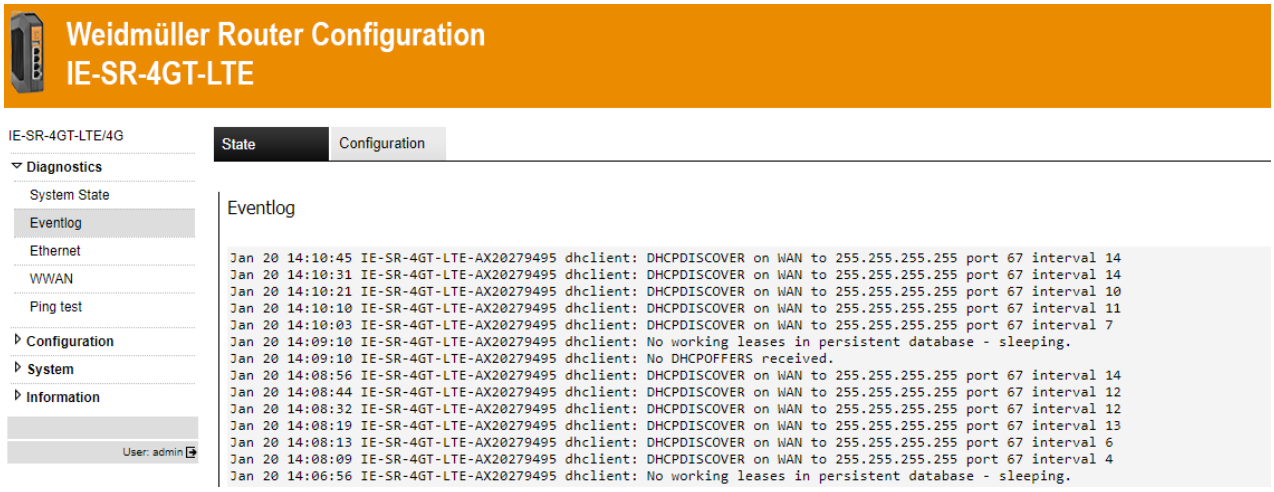
4.1 Section Diagnostics

4.1.1 Diagnostics → System State



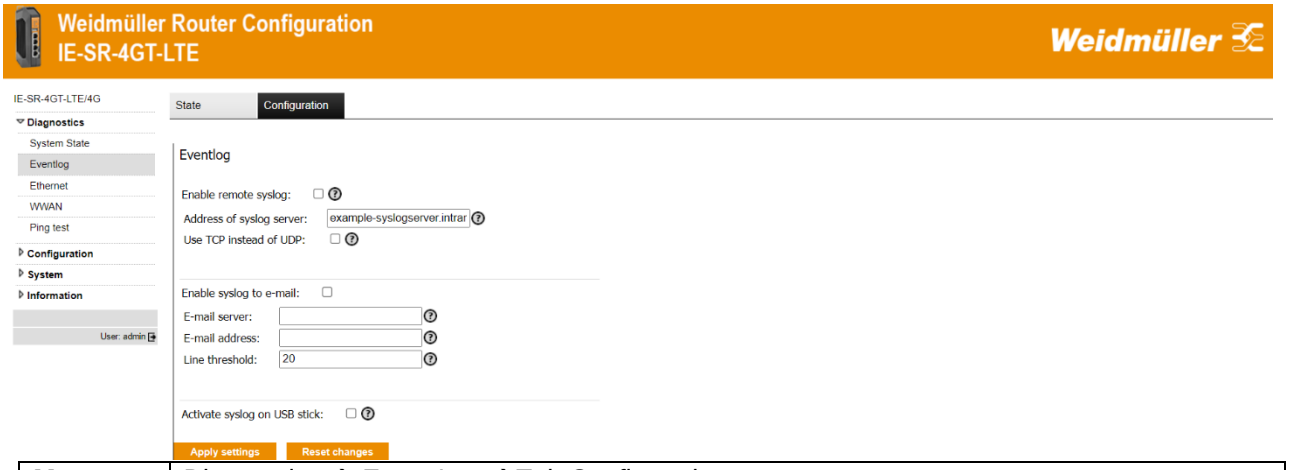
Menu	Diagnostics → System State	
Function	**Startup screen of the web interface after login**. Displays current configuration and status data.	
	System name	Name of the device, default “<Device Type>-<Serial No.>”
	Device type	Article Name
	Serial No.	Unique Number of this product
	Firmware version	Actual used Firmware and Build
	MAC-Address WAN	Registered MAC-address of the WAN-Ports
	MAC-Address LAN	Registered MAC-address of the LAN-Ports
	Device mode	Displays actual device mode
	Network statistics	Displays current network traffic on selected interface
	Date & Time	Date and time of the router
	Uptime (see screenshot)	Actual time (14:05:19) followed by Time the router is running continuously (1 min) followed by average system usage in order Memory (0,24) and Flash (0,08), whereby 1 is 100 %
	u-link certificate	Shows the u-link registration code of the router, if used
	OpenVPN sessions	Number of master, clients or listening channels
	IPsec tunnels	Number of IPsec tunnels
	System usage	Actual usage of Flash and Memory
	Interface state	Overview of all interfaces, providing: State (enabled, disabled, active, inactive) IP address and Subnet mask (xxx.xxx.xxx.xxx / yyy.yyy.yyy.yyy) IP assignment (static or DHCP) DHCP server (disabled or enabled)
	Latest 5 messages	Latest messages of the Event Log

4.1.2 Diagnostics → Event Log (Tab State)



Menu	Diagnostics → Event Log →Tab State
Function	Display events and error messages that have occurred in chronological order. Message syntax: <Month> <Day> <hh:mm:ss> <System name> <Service>: Message The buffer for the event log is set to 1 MB. When the buffer is full, events will be overwritten. After a reboot, all logs on the device will be deleted and new device logs start on.

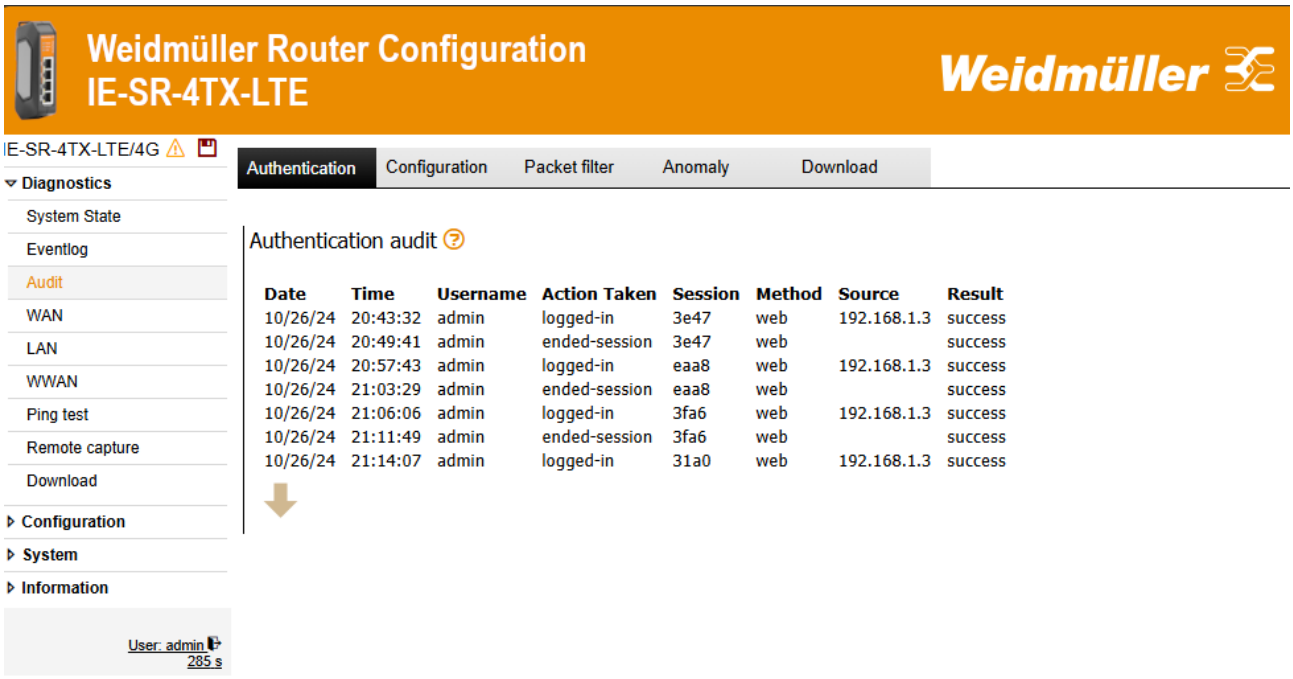
4.1.3 Diagnostics → Event Log (Tab Configuration)



Menu	Diagnostics → Event Log →Tab Configuration	
Function	Event and error messages can be sent to a syslog server (PC on the network) or sent as emails. Furthermore, it can be stored on a USB stick.	
	Enable remote syslog	Write log messages to a remote machine
	Address of syslog server	Local syslog server address
	Use TCP instead of UDP	Syslog is using 514 for UDP as standard port and when activated it will use TCP port 514
	Enable syslog to e-mail	Send syslog files to an e-mail address
	E-mail server	Local syslog-server address
	E-mail address	E-mail address of the syslog-receiver
	Line threshold	Amount of code lines in an email

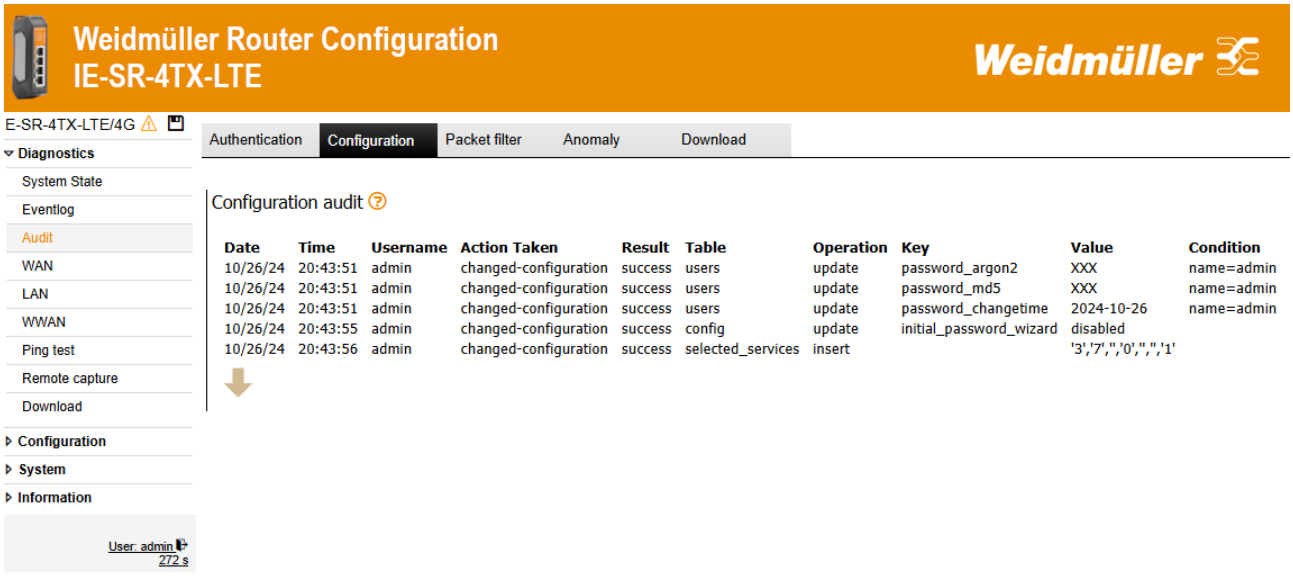
4.1.4 Diagnostics → Audit

Diagnostics → Audit (Tab Authentication)



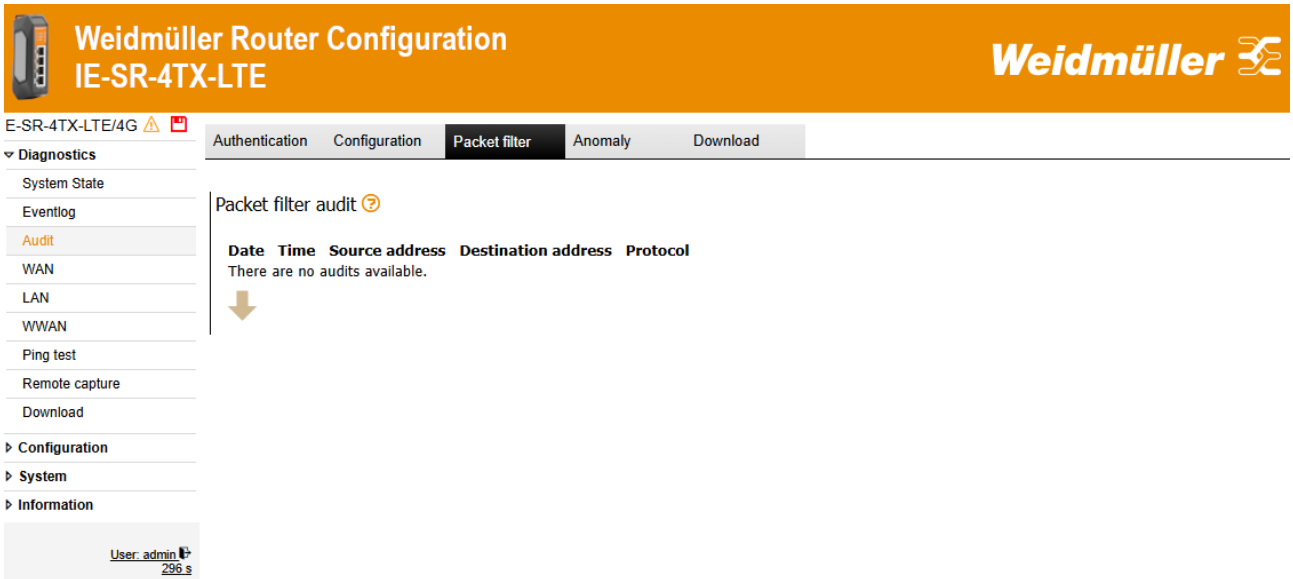
Menu	Diagnostics → Audit →Tab Authentication
Function	This audit log view shows all successful and failed login attempts. Failed logins during an active login ban period are not logged. Configure a sufficiently large login ban timeout to prevent flooding with failed login attempts. The audit.log is implemented as a 40 MB ring buffer. Once the buffer is full, the oldest entries get overwritten! This buffer is shared among all audit message types. Please note that date and time entries may appear inconsistent due to NTP updates or manual time changes

Diagnostics → Audit (Tab Configuration)



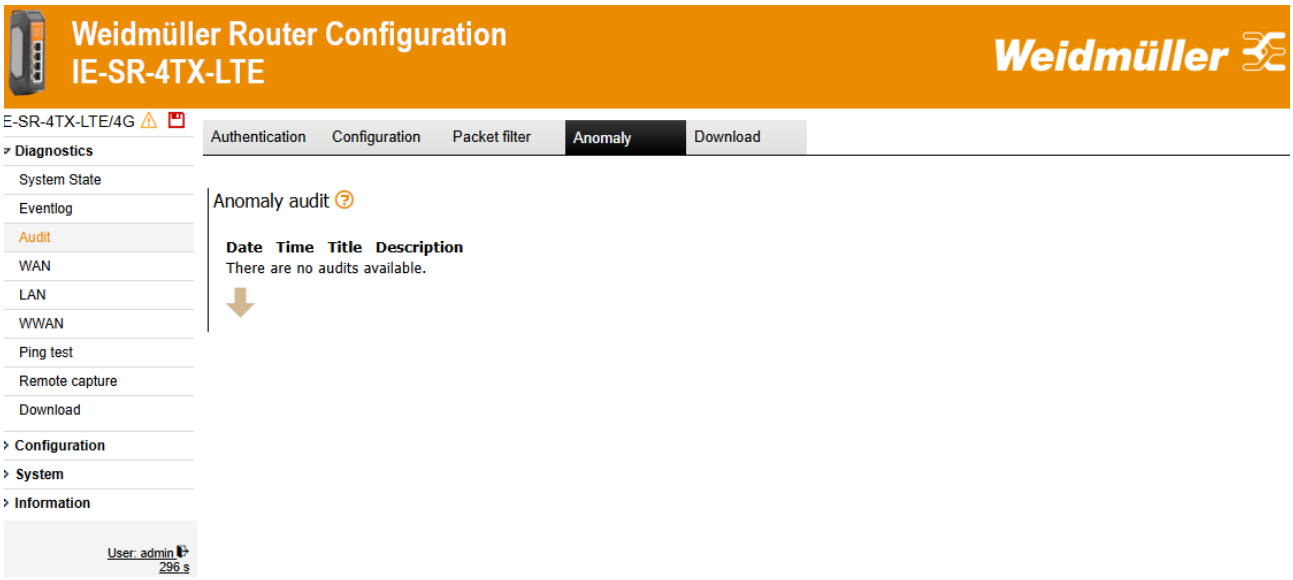
Menu	Diagnostics → Audit →Tab Configuration
Function	This audit log view shows all configuration changes to the main configuration database. Passwords will be shown as XXX. The audit.log is implemented as a 40 MB ring buffer. Once the buffer is full, the oldest entries get overwritten! This buffer is shared among all audit message types. Please note that date and time entries may appear inconsistent due to NTP updates or manual time changes.

Diagnostics → Audit (Tab Packet filter)



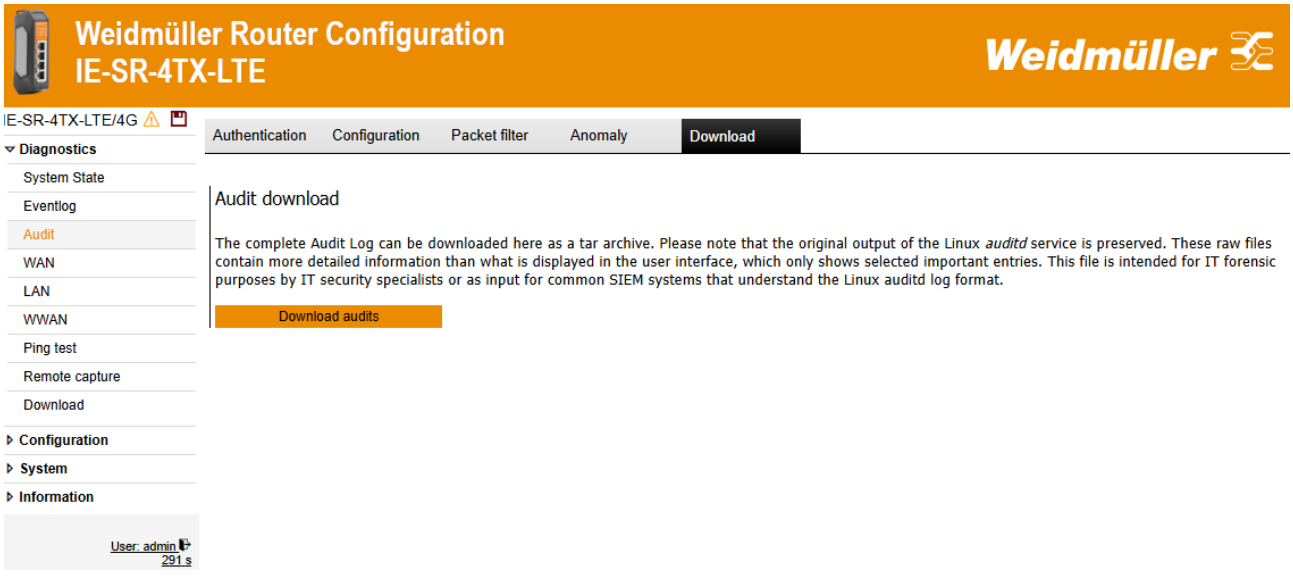
Menu	Diagnostics → Audit →Tab Packet filter
Function	This audit log view shows alerts from the Packet Filter. Each Packet Filter rule can be configured to log to the Audit Log, but only IPv4 source, target and protocol are logged, no rule names are logged. Only one audit.log entry per minute for each rule will be created. The audit.log is implemented as a 40 MB ring buffer. Once the buffer is full, the oldest entries get overwritten! This buffer is shared among all audit message types. Please note that date and time entries may appear inconsistent due to NTP updates or manual time changes.

Diagnostics → Audit (Tab Anomaly)



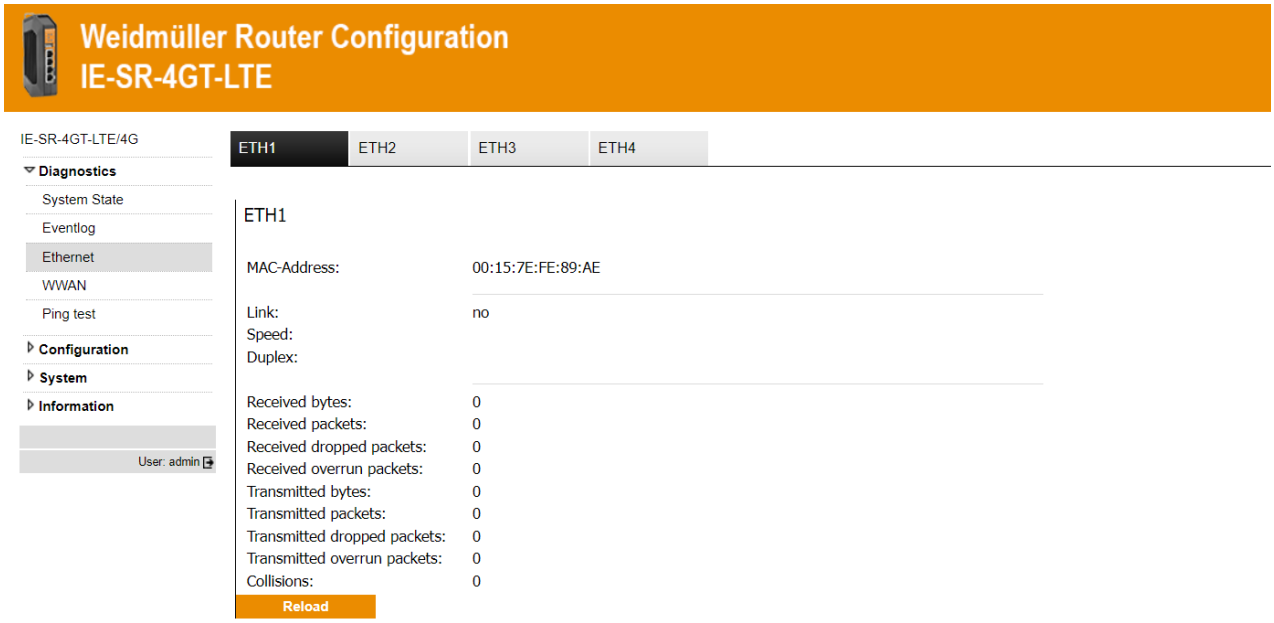
Menu	Diagnostics → Audit →Tab Anomaly
Function	This audit log view displays alerts from the integrated network monitoring system. It reports potential security threats such as ARP spoofing attacks or duplicate IP addresses that conflict with the device's own IP address. The audit.log is implemented as a 40 MB ring buffer. Once the buffer is full, the oldest entries get overwritten! This buffer is shared among all audit message types. Please note that date and time entries may appear inconsistent due to NTP updates or manual time changes.

Diagnostics → Audit (Tab Download)



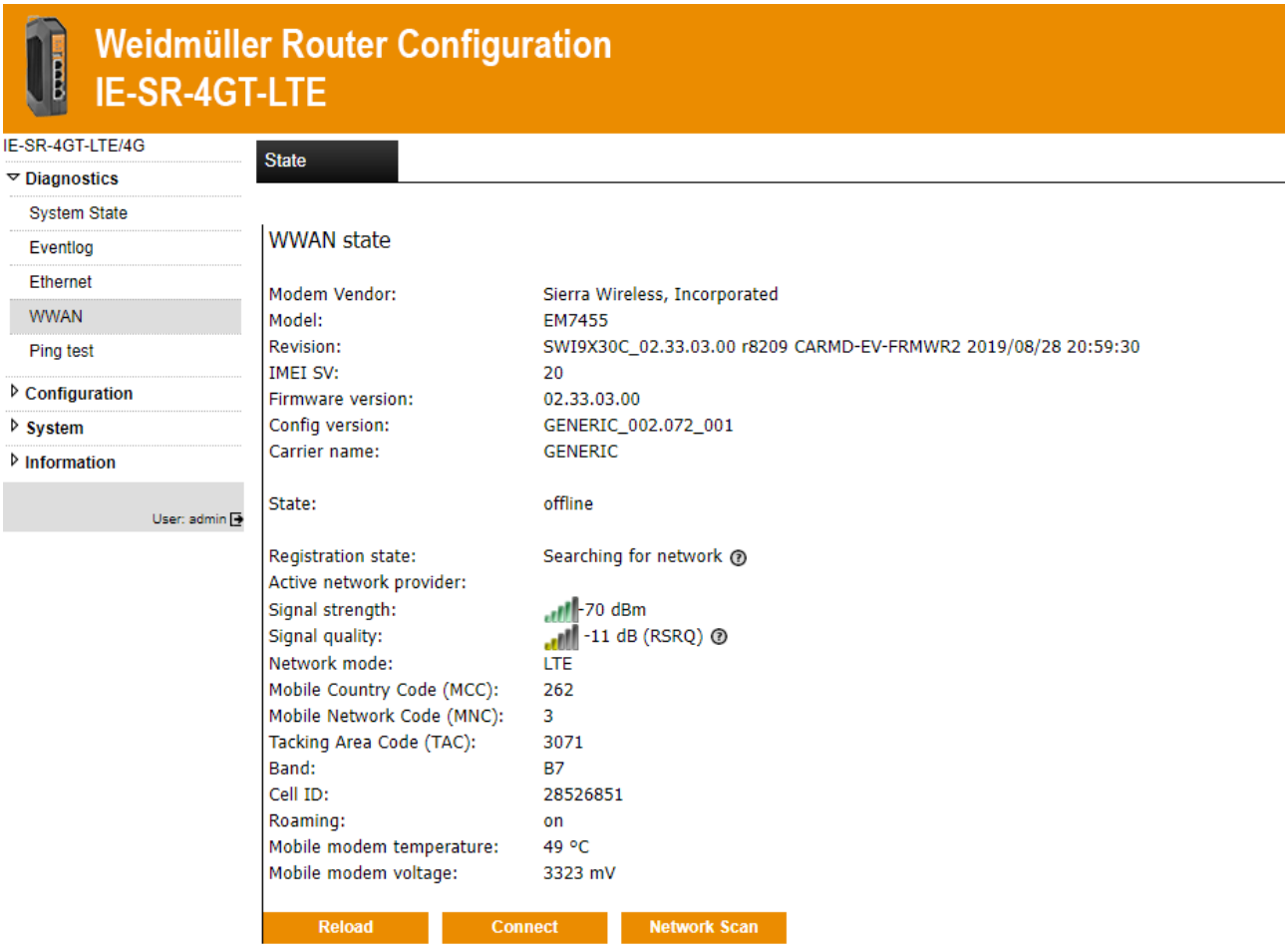
Menu	Diagnostics → Audit →Tab Download
Function	The complete Audit Log can be downloaded here as a tar archive. Please note that the original output of the Linux *auditd* service is preserved. These raw files contain more detailed information than what is displayed in the user interface, which only shows selected important entries. This file is intended for IT forensic purposes by IT security specialists or as input for common SIEM systems that understand the Linux auditd log format.

4.1.5 Diagnostics → Ethernet



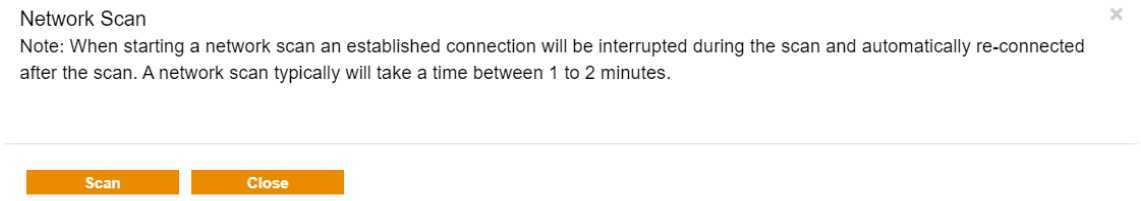
Menu	Diagnostics → Ethernet
Function	Displays the current status of the 4 Ethernet ports. Diagnose the LAN- or WAN-port.

4.1.6 Diagnostics → WWAN

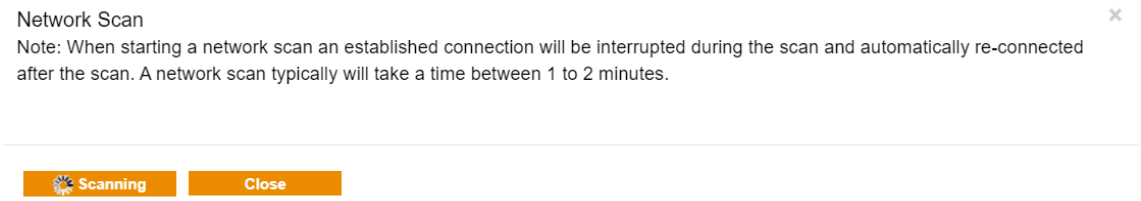


Menu	Diagnostics → WWAN	
Function	Displays the current status of the 4G mobile connection. Menu available for cellular models only.	
	Reload	Refreshes the page with actual values
	Connect	Connects the 4G connection.

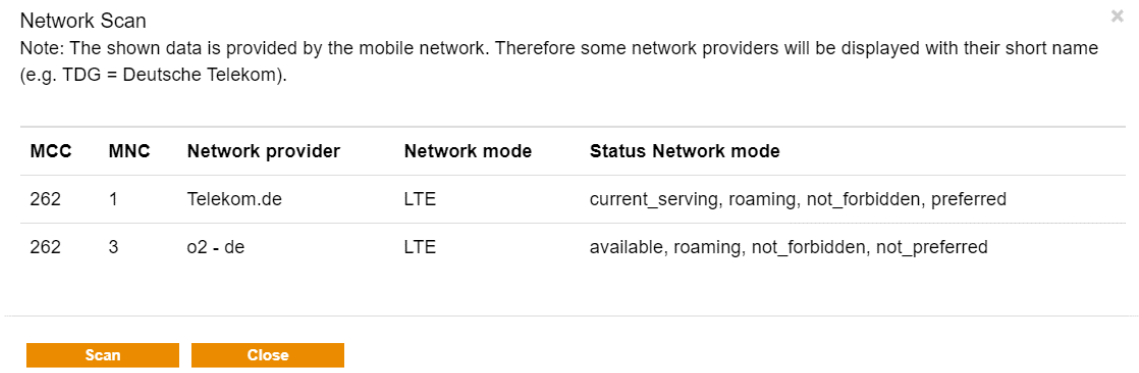
Network Scan
A network scan shows available networks. It can be used to determine a fitting network for the place of installation.



Click “Scan”:



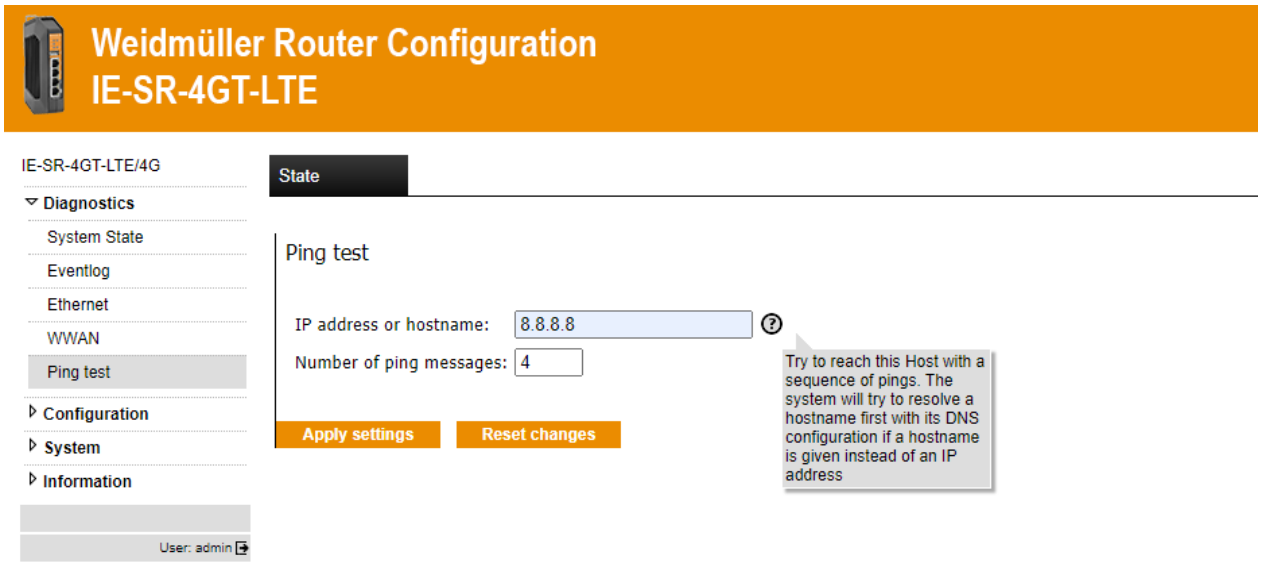
Scan result:



The result of the network scan is a table with all Networks including information about:

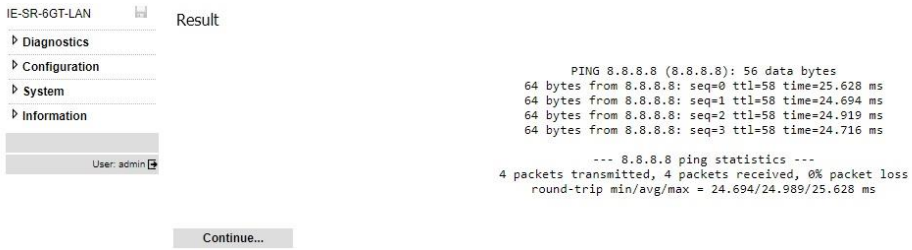
Mobile Country Code MCC	County of network provider	
Mobile Network Code MNC	Network provider Code	
Network Provider	Name or short Name of Provider	
Network Mode	Network mode provided 2G GSM, 3G UMTS or 4G LTE	
Status	Availability	Not available networks will not be displayed (e.g. locking to Frequency Bands enabled)
	Roaming	Shows home (provider) network and roaming network
	Forbidden	SIM card has the not the right to log in into the network
	Preferred	Network that will be selected by the router when signal is good enough.

4.1.7 Diagnostics → Ping test

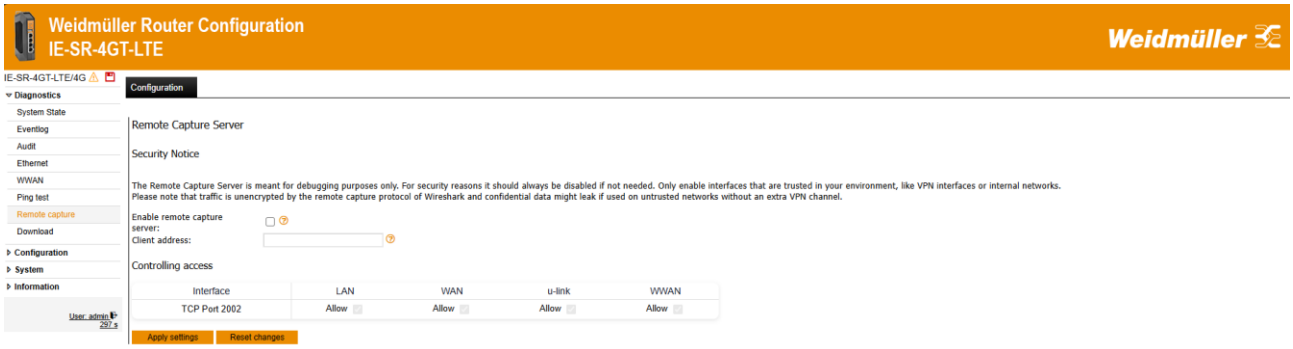


Menu	Diagnostics → Ping test
Function	Allows sending of ICMP packets (ping) to test network connections between the Router and other Ethernet devices. To test internet connection, to use u-link Remote Access Service for example, try to ping a well-known internet IP address like 8.8.8.8, the DNS server of google. To test if your DNS-server is working use a hostname such as www.google.com

Example of result of a ping test:

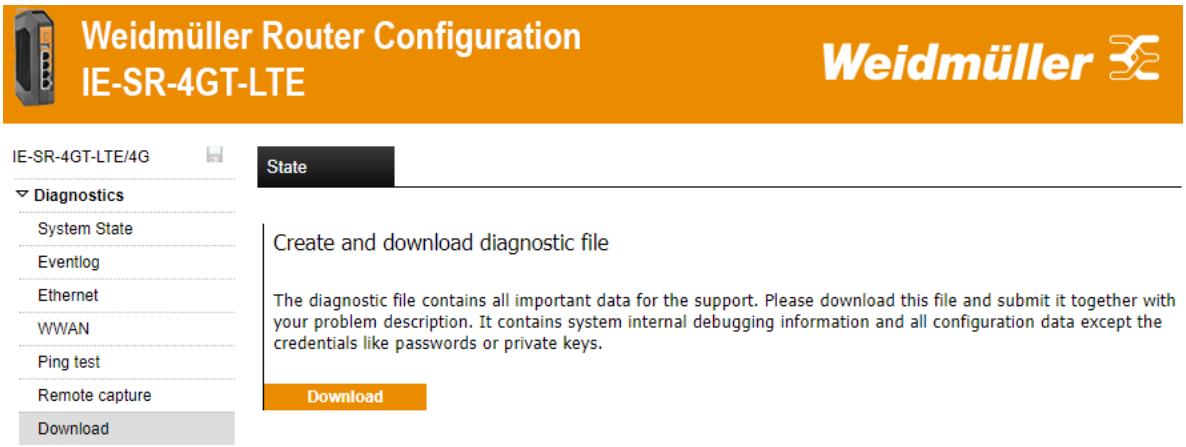


4.1.8 Diagnostics → Remote capture



Menu	Diagnostics → Remote capture	
Function	Enable this service to capture network traffic of any interface remotely, e.g., with Wireshark. The server's listening port is 2002. **Note: Authentication is not possible. Therefore, this feature should only be activated shortly for diagnostics.**	
	Client address	IP address of permitted client. Must be specified. Only one capture session allowed at a time.

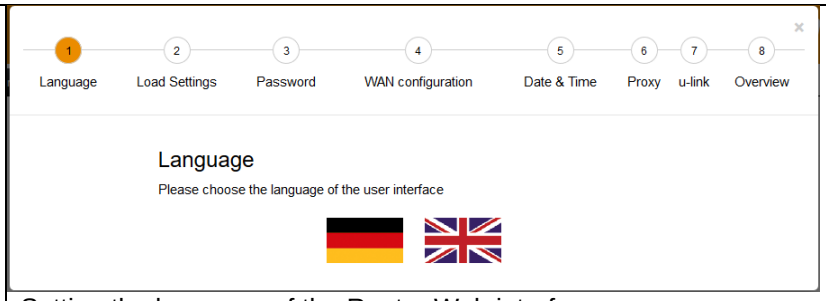
4.1.9 Diagnostics → Download

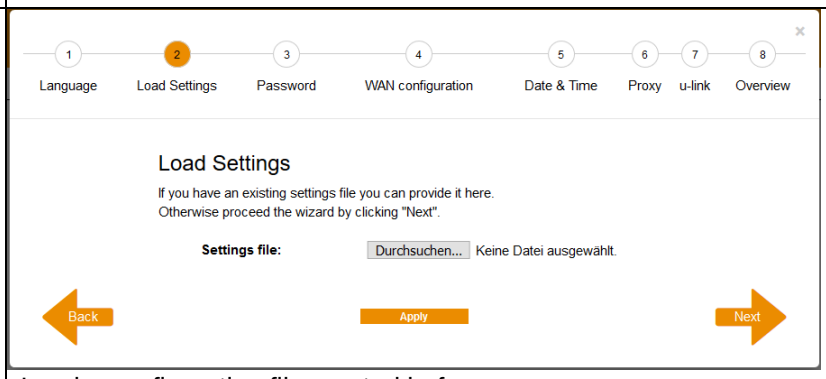


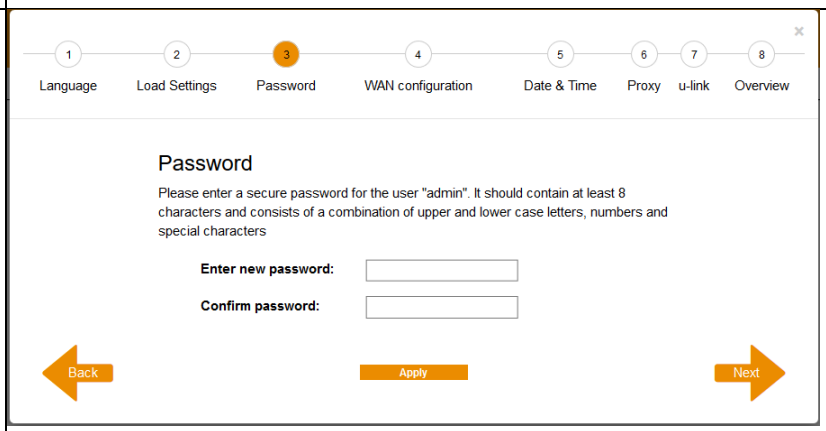
Menu	Diagnostics → Download
Function	Allows to create and download a diagnostic file with internal debugging information for the support. When downloaded, you get a GZ File that can be sent to the support with a problem description.

4.2 Section Configuration

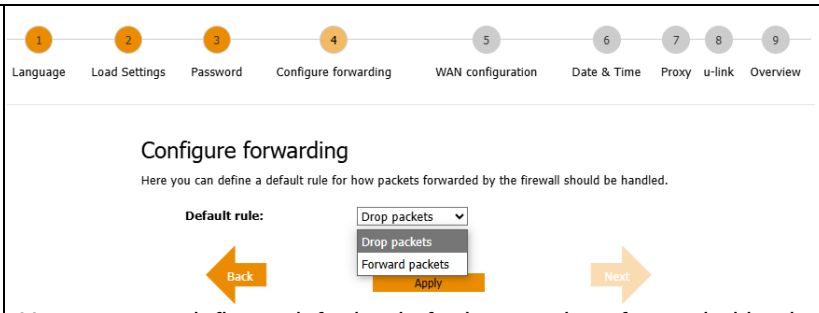
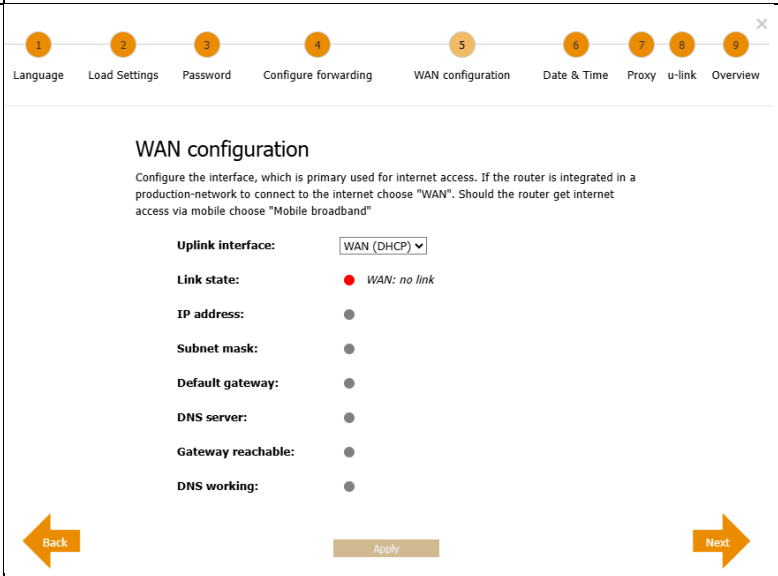
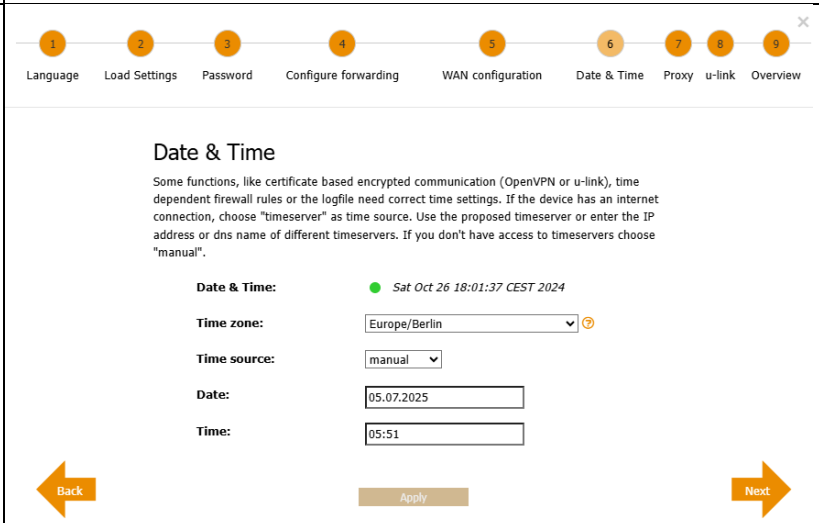
4.2.1 Configuration → Config Wizard

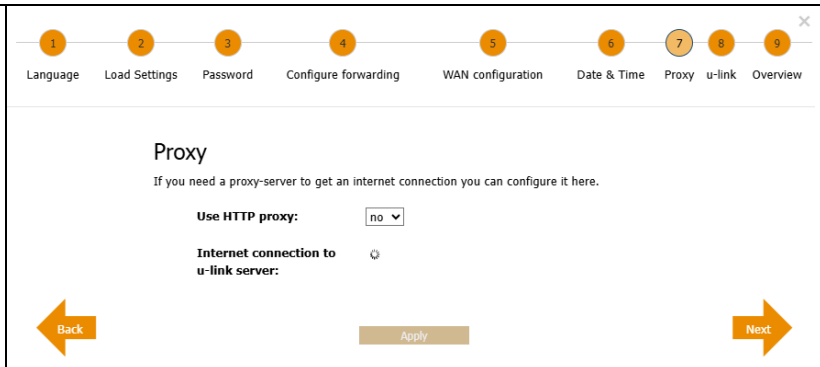
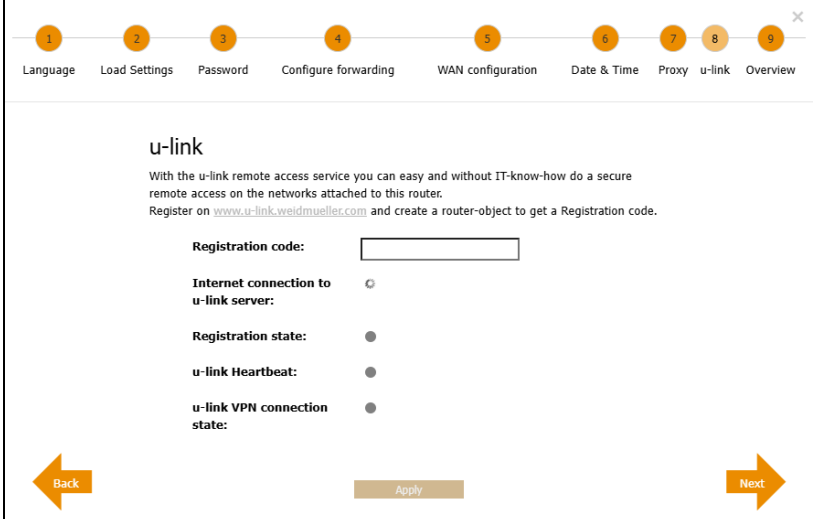
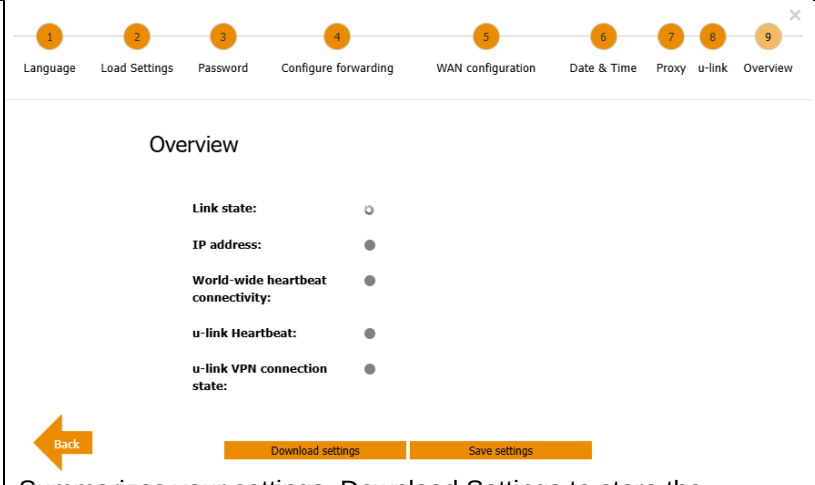
<table>
<tr><td>Menu</td><td colspan="2">Configuration → Config Wizard</td></tr>
<tr><td rowspan="3">Function</td><td colspan="2">The Config Wizard is a tool which helps setting up the major functions of the router. It will be displayed automatically at the initial configuration but may be used later for configuration change as well.</td></tr>
<tr><td>Language</td><td> 

Setting the language of the Router Web interface</td></tr>
<tr><td>Load settings</td><td> 

Load a configuration file created before.</td></tr>
<tr><td>Password</td><td> 

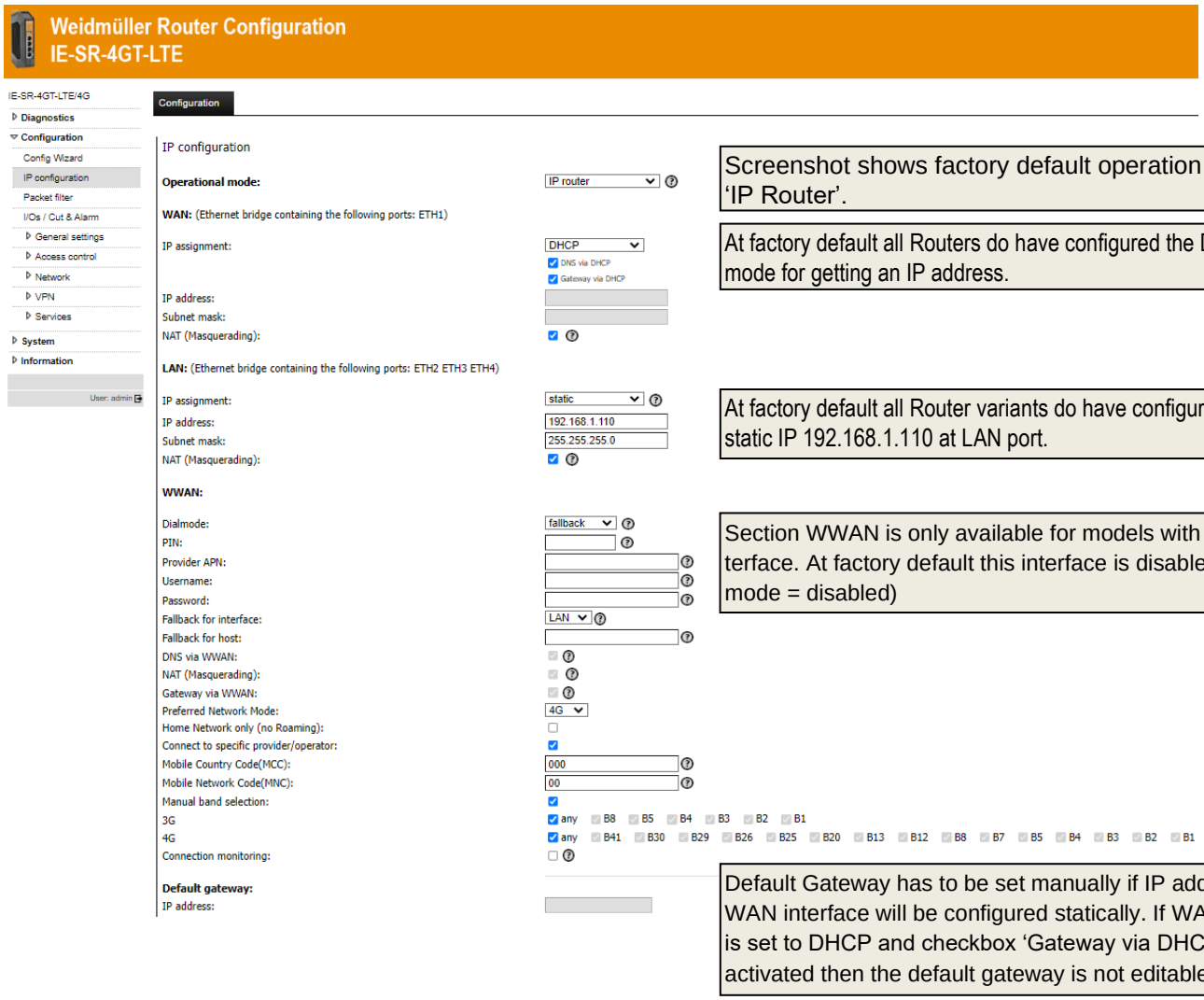
Change the default password to a new one. The new password cannot be the default password!</td></tr>
</table>

	Configure Forwarding	 Here you can define a default rule for how packets forwarded by the firewall should be handled. • Drop packets: Network traffic is blocked • Forward packets: Network traffic is allowed
	WAN configuration	 Configure the WAN-Interface of the router. This can be done via DHCP client (factory default), static IP and Mobile Broadband. The status LED's will turn green, if settings work. For more information on the settings please refer to the respective chapter.
	Date & Time	 Setting the router system time via a time server or manually. When choosing manually please consider that the router will loose time settings after 15 minutes without power.

	Proxy	 If you need to pass a Proxy you can set a system wide Proxy here. The router will test it's https connection to the u-link server. The status LED's will turn green, if settings work.
	u-link	 With the u-link remote access service you can easy and without IT-know-how do a secure remote access on the networks attached to this router. Register on www.u-link.weidmueller.com and create a router-object to get a Registration code. The status LED's will turn green, if settings work.
	Overview	 Summarizes your settings. Download Settings to store the configuration or to load this configuration into another router. Save settings to activate the settings on this router. The status LED's will turn green, if settings work.

4.2.2 Configuration → IP Configuration

IP Configuration → Operational mode “IP Router”



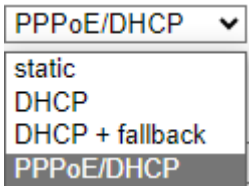
Screenshot shows factory default operation mode ‘IP Router’.

At factory default all Routers do have configured the DHCP mode for getting an IP address.

At factory default all Router variants do have configured static IP 192.168.1.110 at LAN port.

Section WWAN is only available for models with 4G interface. At factory default this interface is disabled (Dial mode = disabled)

Default Gateway has to be set manually if IP address of WAN interface will be configured statically. If WAN port is set to DHCP and checkbox ‘Gateway via DHCP’ is activated then the default gateway is not editable.

Menu	Configuration → IP configuration	
Function	This is the main configuration window for setting the operating mode and the network configuration (Assignment of IP data on LAN / WAN ports and optional 4G interface).	
	Operational mode	Transparent bridge: The device is acting like a layer 2 bridge and is transparent within a switched network. All Ethernet ports (LAN and WAN) behave like a common unmanaged Ethernet Switch. Only 1 IP address will be configured for accessing the web interface. This mode typically will be used for Layer 2 firewall application based on Ethernet frames (including IP packet control). IP Router: Supports routing functions (Layer 3) between WAN and LAN port(s). The ETH2-4 ports act as unmanaged switch. The IP address ranges of WAN and LAN side must not be the same. IP router (extended): Supports flexible routing functions between WAN and LAN ports. In this mode each port ETH 1…4 can be configured as an individual subnet with its own IP address range. The IP address ranges must not be the same for the ports.
	LAN / WAN IP assignment 	All interfaces can be configured with static or dynamic (DHCP) IP addresses. Static: Assign a static IP address and subnet mask to the interface. DHCP: Request an IP address from a DHCP (Dynamic Host Configuration Protocol) server. DHCP + fallback: First, try to request an IP address by DHCP and if it fails use the static one. PPoE/DHCP: The IP Address will be assigned by the provider.
	WWAN (optional)	Configuration of 4G network connection
	Dialmode	Disabled: Do not use 4G modem. Manual: Dialing can be triggered manually from 4G status page. Permanent: The 4G link will be established automatically on system boot. Fallback: The 4G link will go online if the monitoring on the given interface “Fallback for interface” fails. The system will actively monitor the given IP addresses on the given interface. After a failure of at least 30 seconds the 4G link will be established.
	PIN	The Pin of your SIM-Card.
	Provider APN	Access point name (APN) of your provider for packet based services.
	Username	Username needed to authenticate at the APN (Access Point Name).
	Password	Password needed to authenticate at the APN (Access Point Name).
	Fallback for interface	Selection of the interface (LAN/WAN/u-link) for which the 4G interface shall be used as fallback.
	Fallback for host	Enter IP address which shall be monitored by ICMP pings over the selected interface for fallback. Monitoring interval: 3 ICMP ping requests each 10 seconds.
	DNS via WWAN	DNS server settings will be obtained from 4G provider.

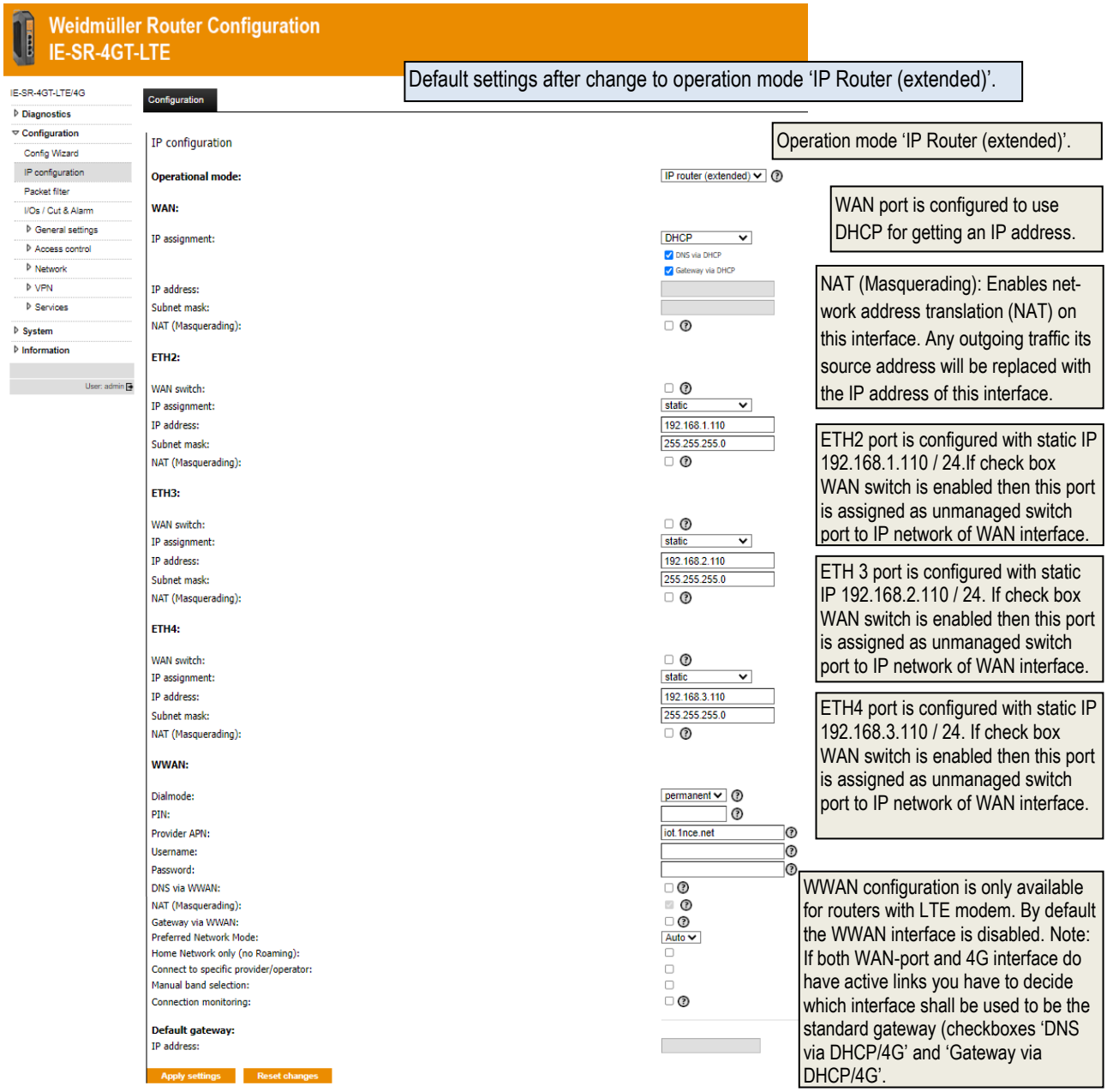
NAT (Masquerading)	Enable network address translation (NAT) on this interface. Any outgoing traffic, it's source address will be replaced with the IP address of this interface. **NAT is always activated for 4G modem**.
Gateway via WWAN	If activated as soon as mobile connection is active (Online) it will be used as the Router's **default** gateway.
Preferred Network Mode	Select a network mode which will be used automatically when connection is sufficient.
Home Network only (no Roaming)	If selected the Router will only connect to the provider Network and is unable to connect to other networks.
Connect to specific provider/operator	When selected, a fixed MCC and MNC can be typed in, so the router will only connect to this provider.
MCC	Type in the Mobile Country Code of the respective country. The code is a 3-digit code. 262 stands for Germany, 000 is auto select
MNC	The Mobile Network Code consists of a 2 digit code and identifies the provider in combination with the MCC. 00 is auto select.
Manual band selection	Enable or disable specific bands of operation in 3G and 4G network.
Default gateway	Assign the IP address of the Routers default gateway. If IP assignment (LAN / WAN or optional 4G interface) is set to DHCP and if one of the checkboxes "Gateway via DHCP" or "Gateway via WWAN" is enabled then the default gateway IP address will be set automatically and cannot be edited manually.

Additionally, the IE-SR-4GT-4G-USEMEA router can activate the manual band selection when the WWAN mode is set to manual.

IP Configuration → Operational mode "IP Router (Extended)"

Each interface (WAN, ETH 2…4, WWAN modem) can be configured as an individual IP network (Static, DHCP, DHCP + fallback or PPPoE). When using this mode then generally each router function (Firewall, Forwarding, NAT, etc.) can be applied to each interface.

Alternatively to an individual IP configuration of a LAN port, each LAN port can be set as an unmanaged switch port assigned to the IP address of the main WAN port.

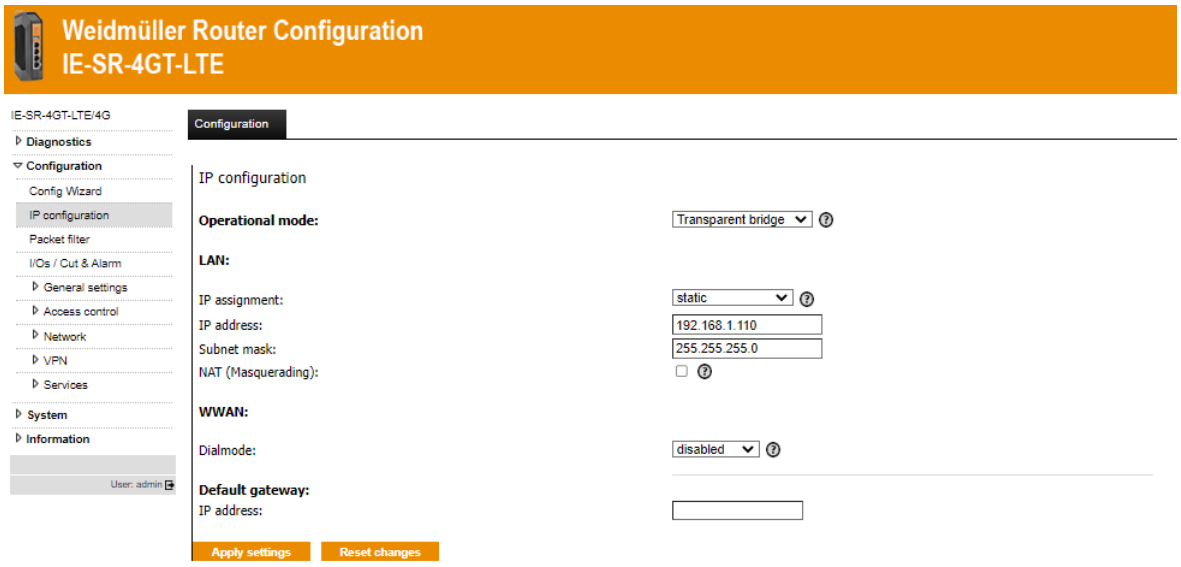


IP Configuration → Operational mode “Transparent bridge”

In operation mode ‘Transparent bridge’ the device is acting like a layer 2 bridge and is invisible to clients. All Ethernet ports (LAN and WAN) behave like a common unmanaged Ethernet Switch.

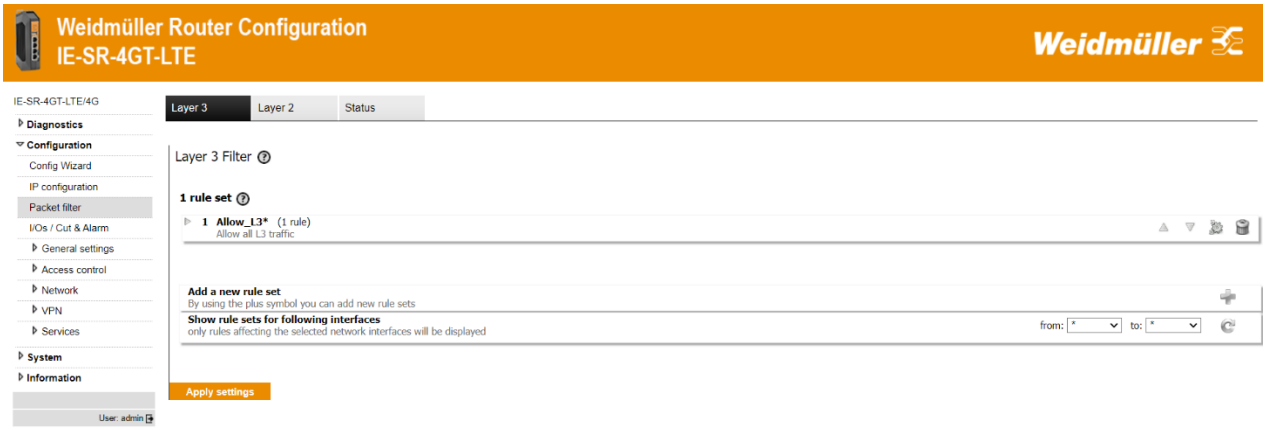
Only 1 IP address will be configured for accessing the web interface independent of the Ethernet port to which the configuration PC is connected.

This mode typically will be used for Layer 2 based firewall applications (checking MAC-based Ethernet frames including IP based packet control).



4.2.3 Configuration → Packet filter (Firewall)

Packet filter → Tab Layer 3

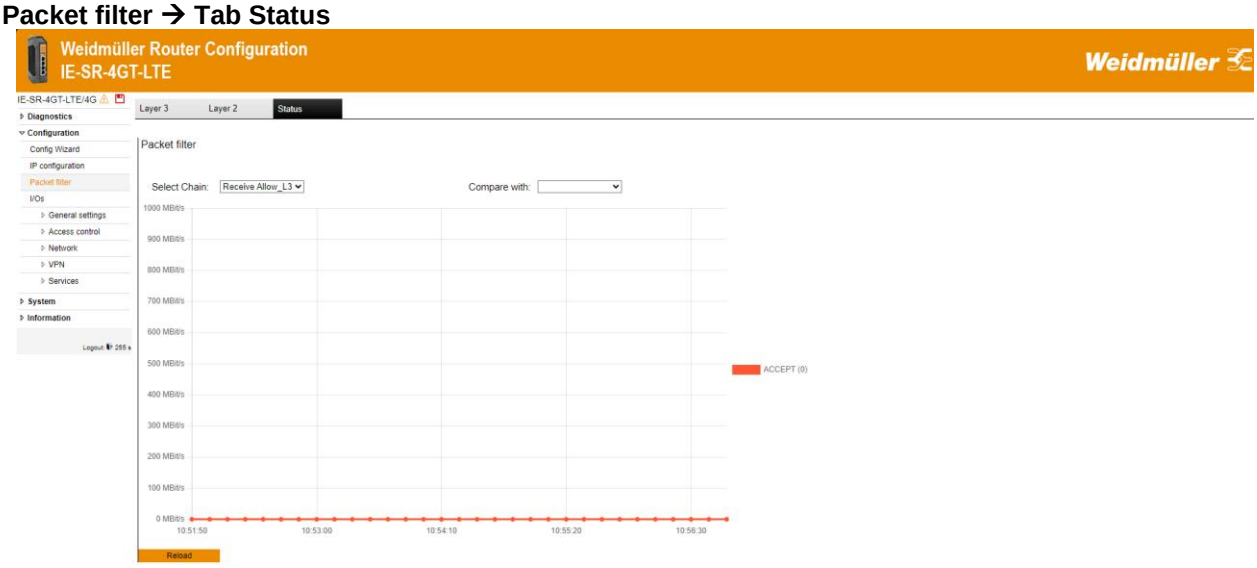


Menu	Configuration → Packet filter → Tab „Layer 3”
Function	This is the window for the manual configuration of firewall filter rules based on Layer 3 (IP layer). The screenshot shows the firewall settings as already configured in the Config Wizard (Default Block_L3* or optionally Allow_L3*). This rule says that any IP protocol (*) and any traffic regardless the direction (source and destination=*) is allowed. The result is that - on delivery - the firewall is "open" on layer 3. For more detailed information about using the packet filter please refer to firewall-related application notes in appendix A.

Packet filter → Tab Layer 2

Menu	Configuration → Packet filter → Tab „Layer 2“
Function	This is the window for the manual configuration of firewall filter rules based on Layer 2 (MAC layer). The screenshot shows the firewall settings as delivered with the 2 default rules "Allow_L2*" and „ARP*“ (Address resolution protocol). The rule Allow_L2* allows transmitting any Ethernet frame type (*) and any traffic regardless the direction (source and destination mac address =*). The result is that - on delivery - the firewall is "open" for layer 2.

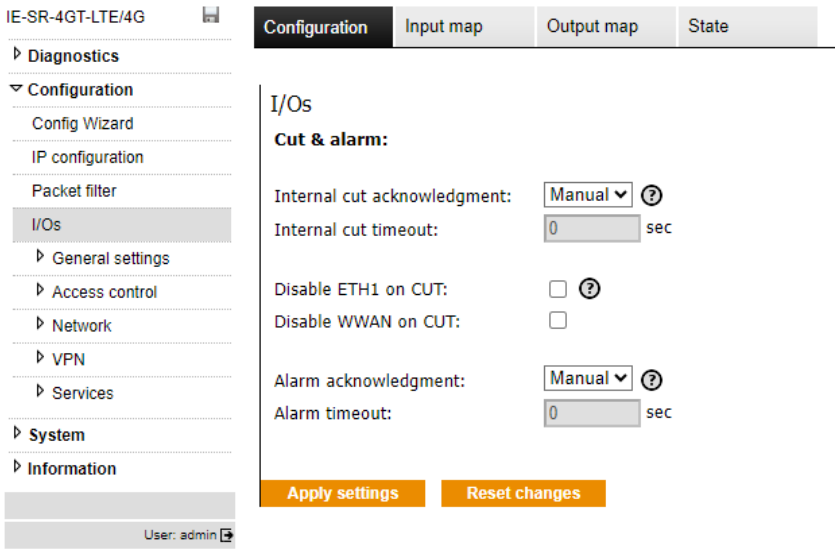
Packet filter → Tab Status



Menu	Configuration → Packet filter → Tab „Status“
Function	Overview of transmit and receive activities of the physical and virtual interfaces. You can also compare the activities between the interfaces.

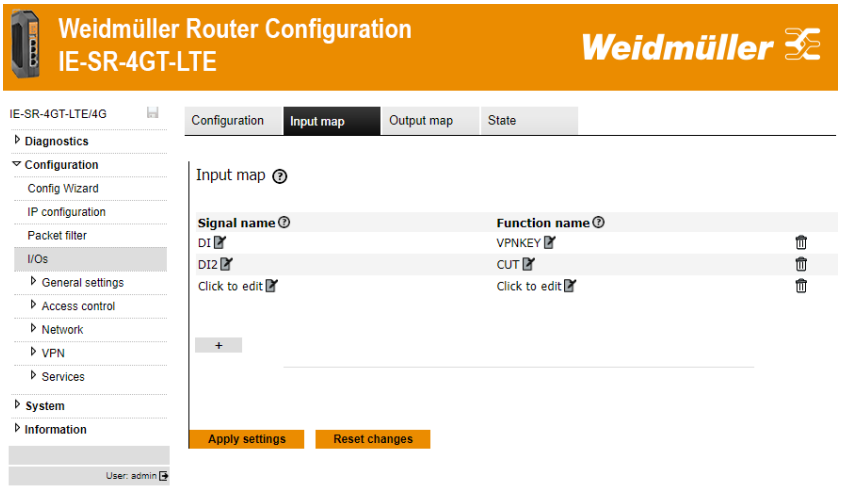
4.2.4 Configuration → I/Os

I/Os→ Tab Configuration



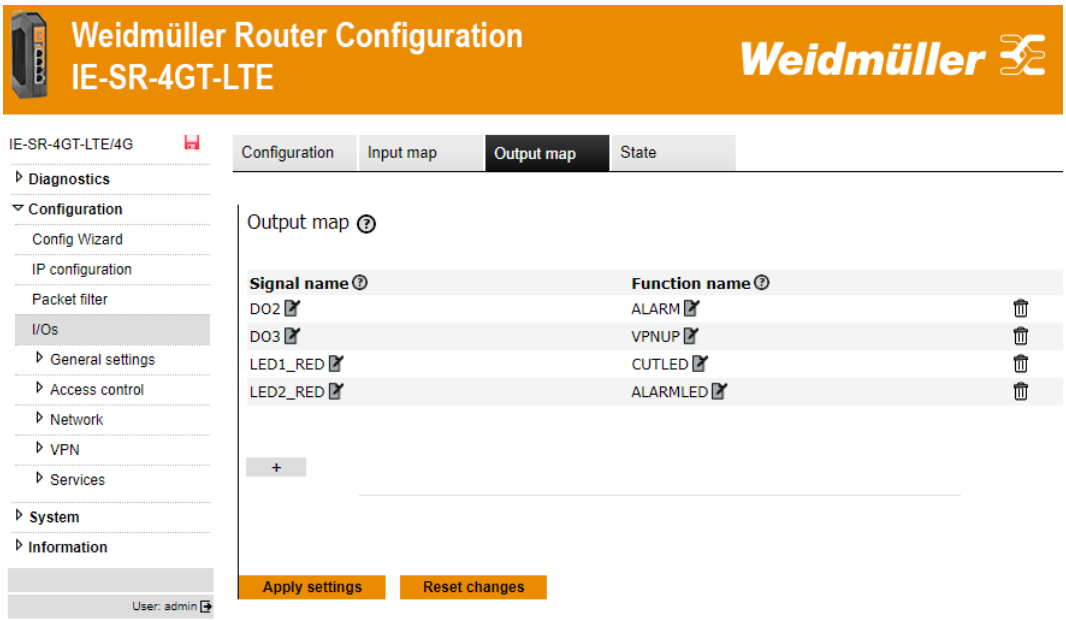
Menu	Configuration → I/Os→ Tab „Configuration“	
Function	In this menu, it can be configured how the events "Cut" and "Alarm" - after they have been triggered will be reset.	
	Acknowledgements	Manual: Cut must be reset manually by button on the tab “State” Auto: Cut will be reset automatically after the given timeout in seconds
	Disable WAN port WWAN on external cut	By default, an external CUT signal will disable the WAN Ethernet ports or the WWAN connection. You can disable the feature if you like to use CUT signal for switching packet filter rules only. The behavior of the internal CUT signal is not affected by this option

I/O s→ Tab Input Map



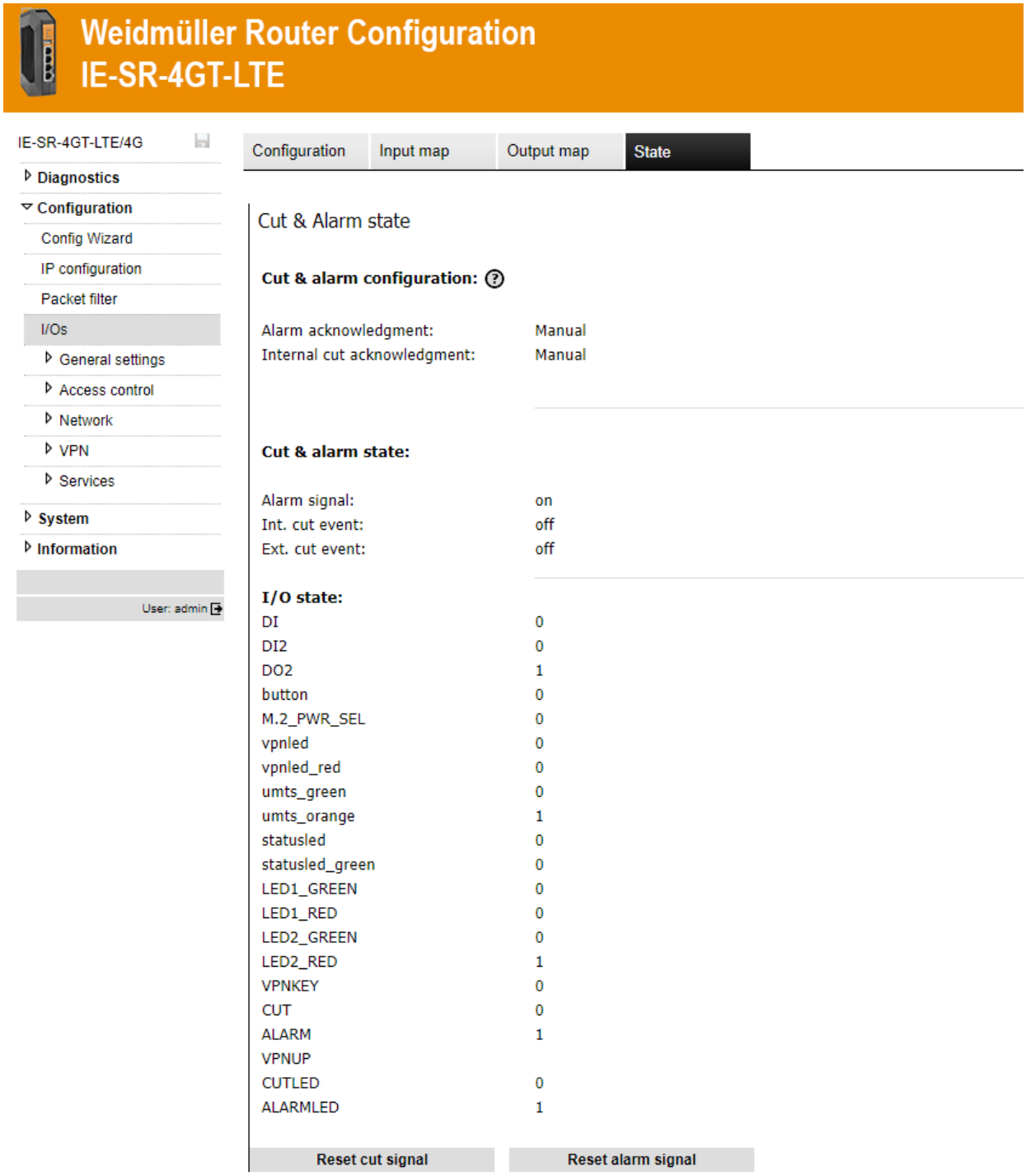
Menu	Configuration → I/Os→ Tab Input Map	
Function	In this mapping the available physical input signals can be configured to trigger certain software functions.	
	Signal name	I/O signal name of the connector. Select between the digital inputs. Non-DNV models: • DI • DI2 DNV models: • DI2 • DI3 • DI4 • DI5
	Function name	Name of the software function which the I/O signal shall trigger. CUT: Disables the corresponding Ethernet 1 port. VPNKEY: Activates the digital VPN key of the router. VPNKEY & CUT: Disables the Ethernet port and activates the digital VPN Key.

I/Os → Tab Output map



Menu	Configuration → I/Os→ Tab Output Map	
Function	The available physical output signals can be configured to get activated by different software functions. This can be mapped here.	
	Signal name	I/O signal name that gets activated by the internal software function. You have the option to select either the digital outputs, the front LEDs, or both. <u>Non-DNV models:</u> • DO • LED1_RED/GREEN • LED2_RED/GREEN <u>DNV models:</u> • DO2 • DO3 • DO4 • DO5 • LED1_RED/GREEN • LED2_RED/GREEN
	Function name	Internal software function that triggers a physical output, e.g., a VPN connection can activate DO2.

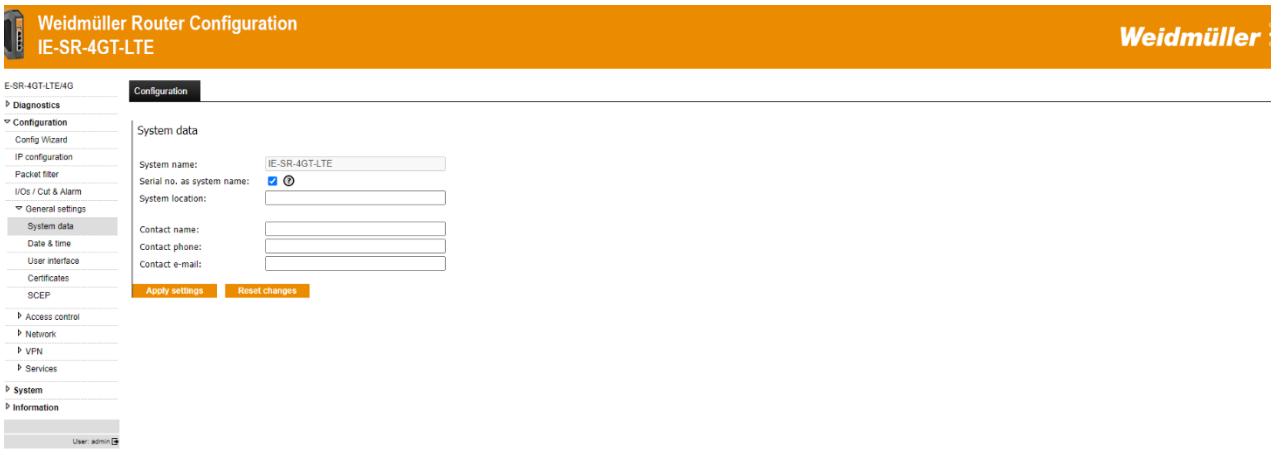
I/Os→ Tab State



Menu	Configuration → I/Os / Cut & Alarm → Tab State
Function	Displays the current status of the events "Internal Cut" → triggered by a special firewall rule "External Cut" → Input of 24 VDC at 4-pin connector (DI2) "Alarm" → triggered by a special firewall rule or by the function „Client monitoring“ With „Reset Cut Signal“ and „Reset Alarm Signal“ you can manually reset the events „Internal Cut“ and „Alarm“. The "External Cut" will automatically be reset if the 24 VDC CUT signal at the 4-pin connector will be released.

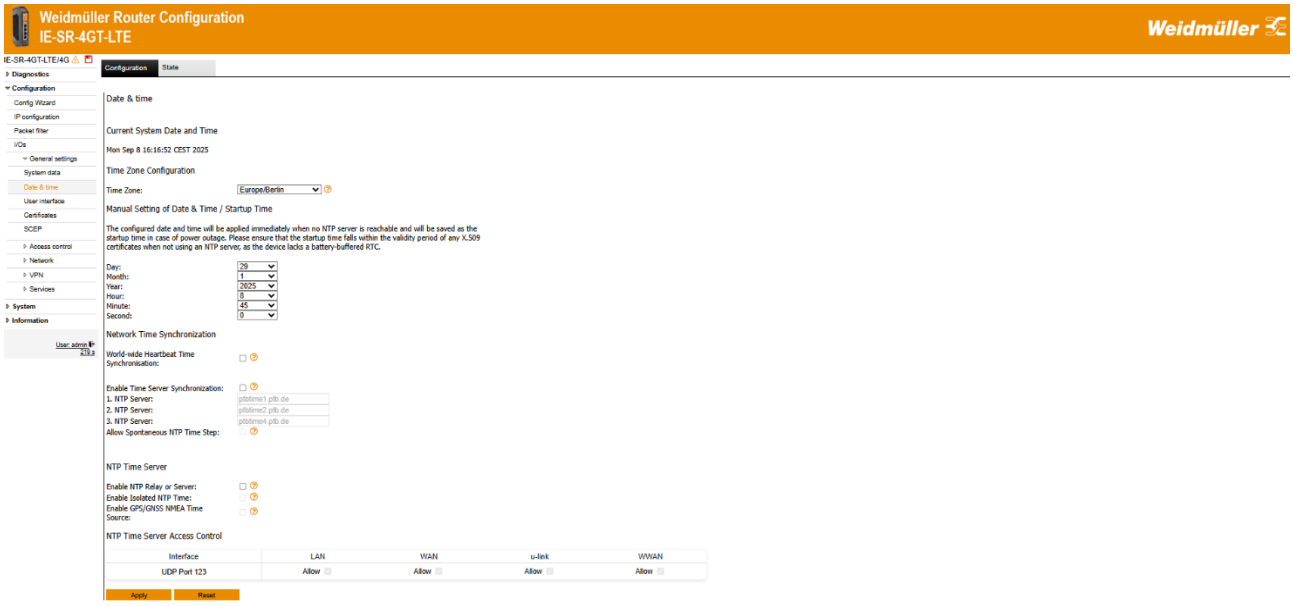
4.2.5 Configuration → General settings

General settings → System data



Menu	Configuration → General settings → System data	
Function	Configuring application-related data of the Router (free text).	
	System name	Name of the router (by default the Router model name). Can be edited if checkbox 'Serial no. as system name' is disabled. Note: When doing a backup of the configuration (file of type *.cf2) the name of the backup file will be <system name>.cf2.
	Serial no. as system name	If this checkbox is enabled then the system name consists of device type and serial number (e.g. IE-SR-4GT-LTE-AX20279495).

General settings → Date & Time



Menu	Configuration → General settings → Date & time
Function	Setting of date, time and time zone. Alternatively, the date/time setting can be configured using the "Network Time Protocol" NTP and accessing an external NTP server. When NTP time server relay is activated, the device will be act as a NTP time server for other services.

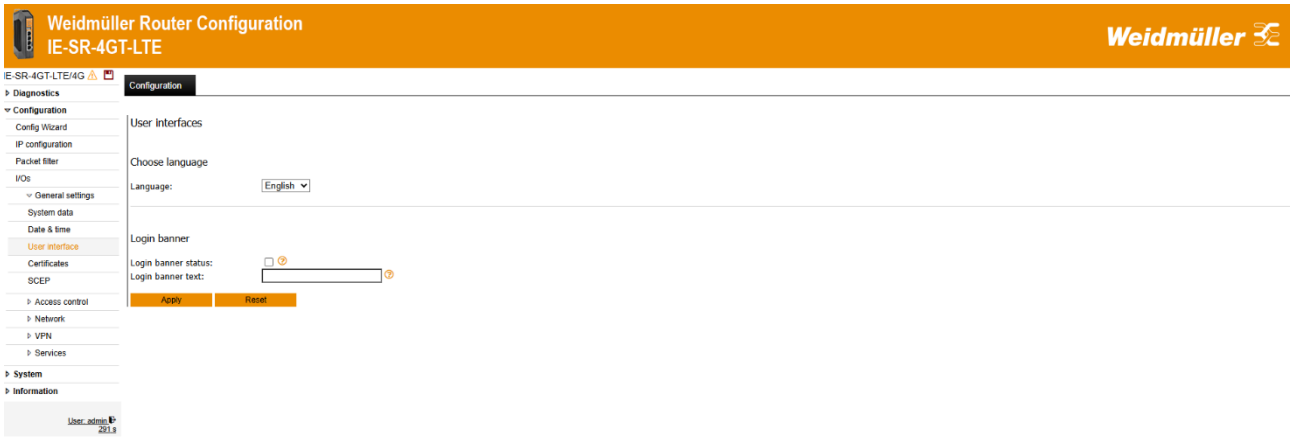
	Time Zone	Setting of time zone. Alternatively, the time zone setting can be configured using the "Network Time Protocol" NTP and accessing an external NTP server.
	Manual Setting of Date & Time / Startup Time	The configured date and time will be applied immediately when no NTP server is reachable and will be saved as the startup time in case of power outage. Please ensure that the startup time falls within the validity period of any X.509 certificates when not using an NTP server, as the device lacks a battery-buffered RTC.
	World-wide Heartbeat Time Synchronisation	Sets the local time if it differs from the u-link server time by more than 60 seconds.
	Enable Time Server	Via the Network Time Protocol (NTP) the local clock gets synchronized to the clock of the first reachable NTP server. Alternatively, the date and time may be set manually.
	Allow Spontaneous NTP Time Step	Allows large spontaneous time steps of an NTP time source during the runtime of the device. If the option is switched off, this is only carried out immediately after the device has been started, in order to initially synchronize the time and date. Connected NTP clients or other software can be disrupted in their function by such time jumps.
	Enable NTP Relay or Server	If this function is enabled, an NTPv4 time server service is activated on the device. The time source used for this depends on the other options
	Enable Isolated NTP Time	This option can be enabled if the device time is to be provided as NTP time in a local network without a time source. It activates a stratum value of 10 so that clients will only use the time if no other server is available. Please note that the devices have no battery buffer for the time, so it is possible that the time stops if the devices have no power supply for a longer time!

	Note
	The Router has no battery-buffered, but a capacity-buffered system clock. General behavior of date/time settings: During operation the Router will save its current date/time (either based on manual input or by NTP update) each hour into the flash memory. After next power-up the Router will restore the internal system clock with the date/time value last saved into the flash memory. If no NTP update is enabled then the system clock will run based on the last stored date/time.

Date & Time → Tab State

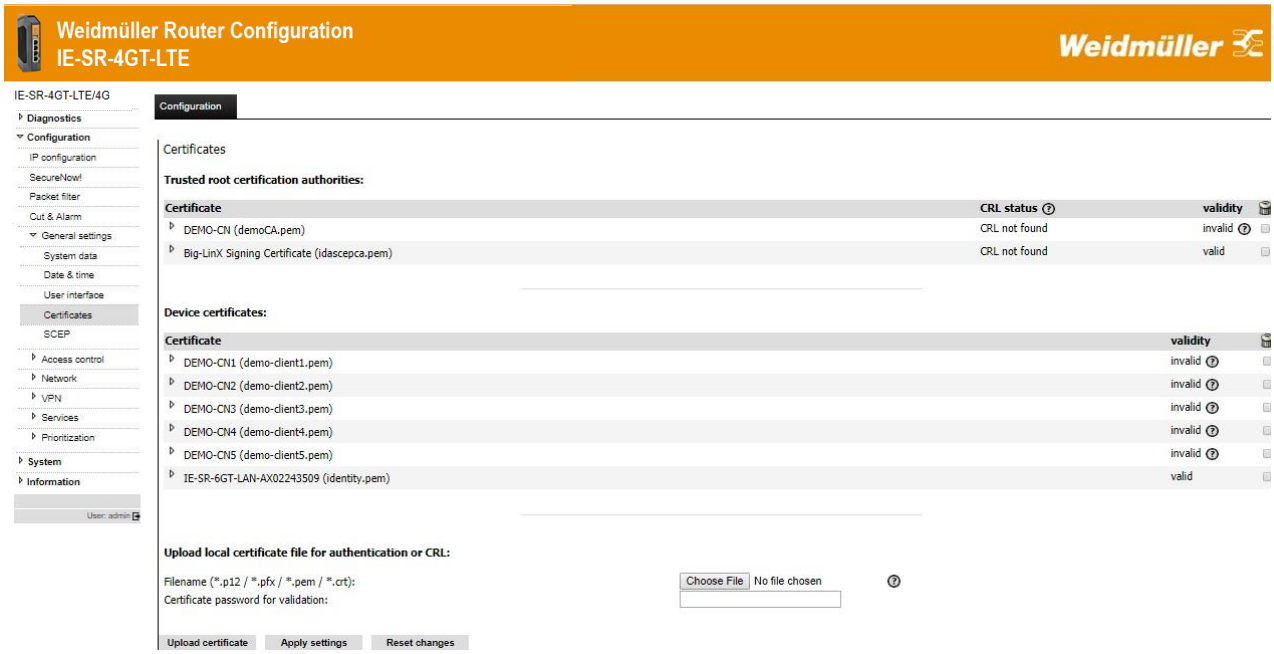
Menu	Configuration → General settings → Date & time → Tab “State”
Function	Shows the states of the used NTP servers. Please use tooltips for further information.

General settings → User Interface



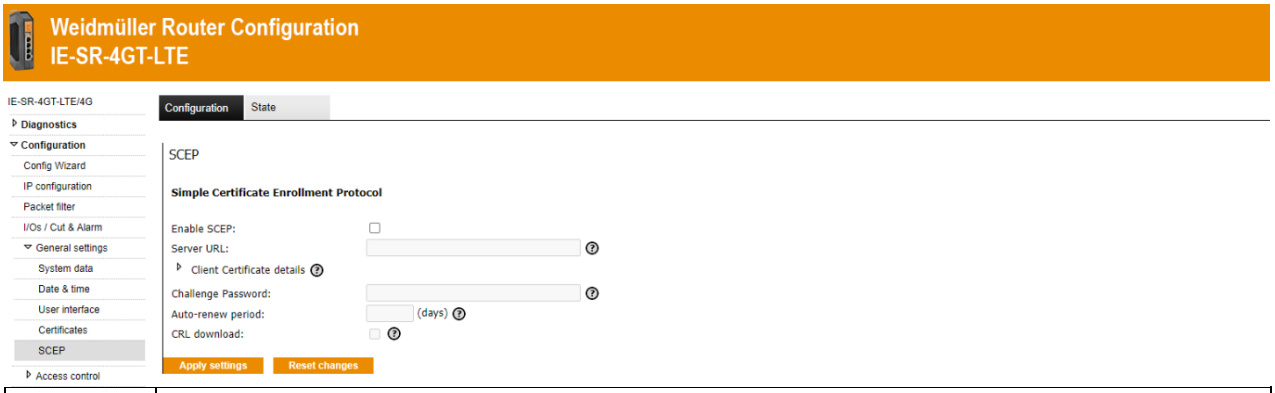
Menu		Configuration → General settings → User interface
Function	• Language	Setting the language (German or English) of the Web interface.

General settings → Certificates



Menu	Configuration → General settings → Certificates
Function	Adding or deleting of certificates for VPN applications (used for both IPsec and OpenVPN).

General settings → SCEP (Tab Configuration)



Menu	Configuration → General settings → SCEP		
Function	Configuration of the Router for online access to certificates which are stored on a centralized online certificate server (SCEP Simple Certification Enrollment Protocol). When setting up certificate-based VPN connections, the necessary certificates can be obtained directly from a SCEP server.		
	Server URL	e.g. http://192.168.1.1/certsrv/mscep.dll	
	Client Certificate details	Common Name (CN)	
		Device serial no. as CN	Auto setting of CN if activated
		Country	Free text
		State	Free text
		Locality	Free text
		Organization	Free text
		Organizational Unit	Free text
		RSA key length (bits)	1024, 2048, 3072 or 4096-bit keylength
	Challenge Password	If the SCEP-Server requires a one-time challenge password, it must be given here. In this case, it is not possible to auto-renew the certificate	
	Auto-renew period	Define a number of days. The corresponding number of dates before the certificate expire, it will be automatically renewed. This option is disabled if a one-time password (challenge) is required.	
	CRL download	If activated, the device will try to obtain an up-to-date certificate revocation list from the server every hour.	

General settings → SCEP (Tab State)

Menu	Configuration → General settings → SCEP
Function	Shows the actual status of SCEP process

4.2.6 Configuration → Access Control

Password Complexity Guideline

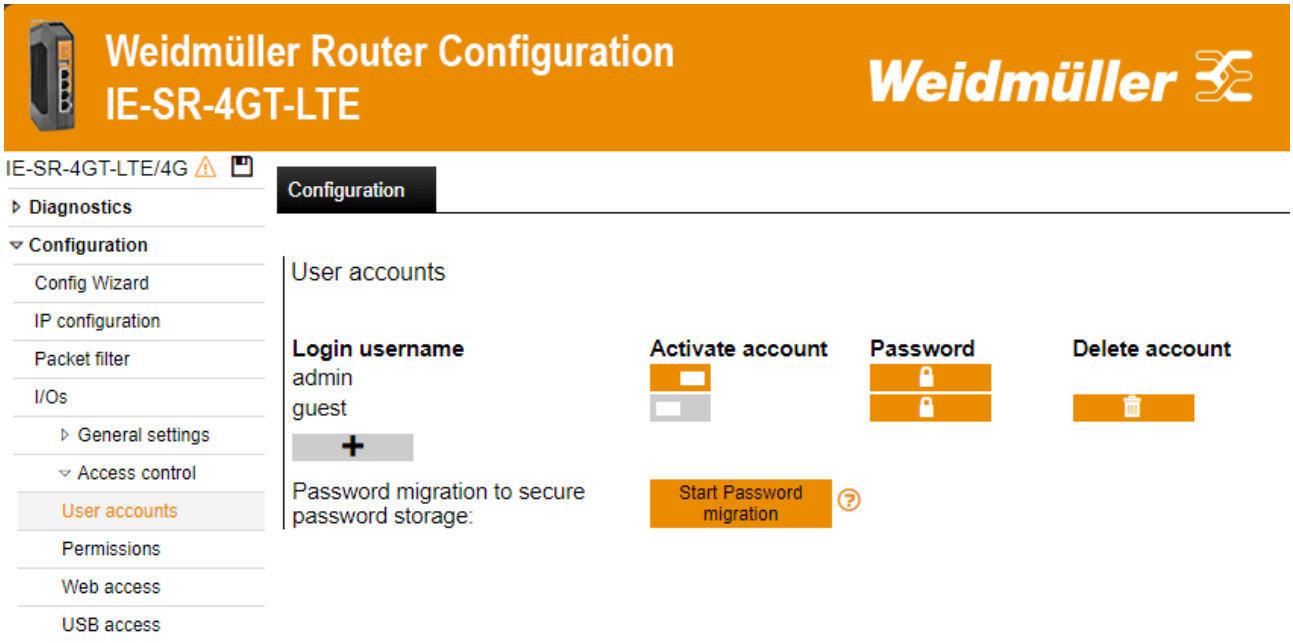
All user passwords must meet the following requirements:

- Length:
  - Minimum: 8 characters
  - Maximum: 64 characters
- Complexity:
  - Must not contain common dictionary words
  - Must not include sequential or repetitive characters (e.g., "123456", "aaaaaa")
  - Must not be found in known data breaches
- Content Restrictions:
  - Must not contain personal information (e.g., username, first/last name)
  - Must not include company or product names

Access Control → User accounts (Tab Configuration)

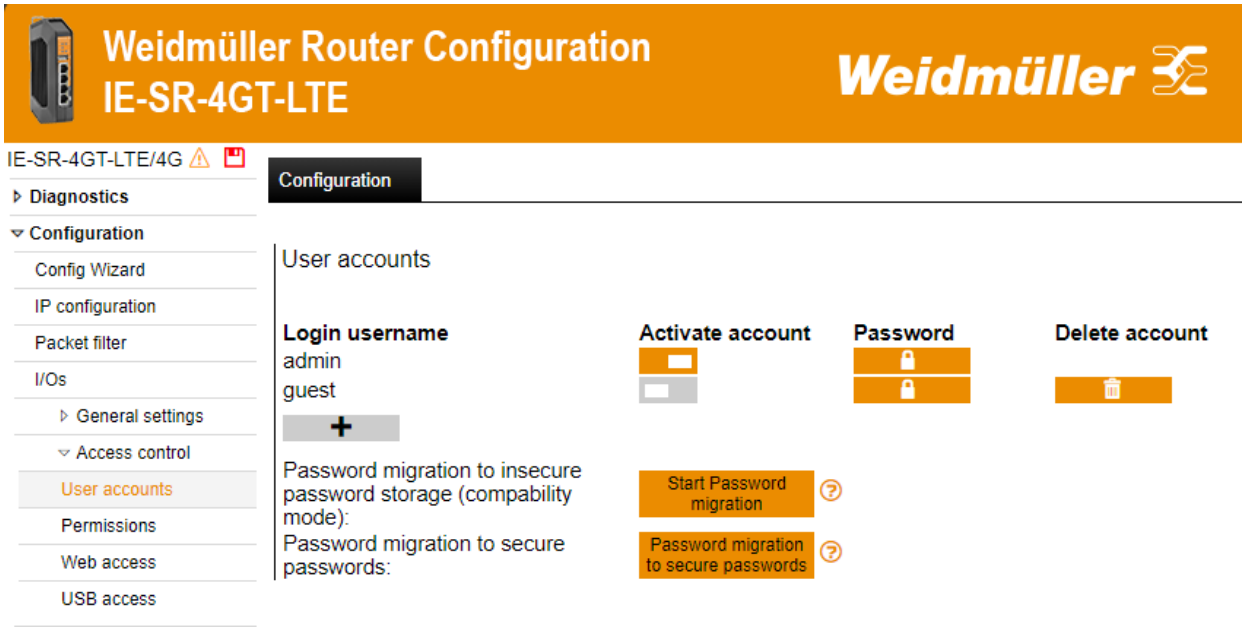
The following section only applies to firmware versions 2.1.x and below!

Menu	Configuration → Access control→ User accounts (Tab Configuration)
Function	Create, manage and delete all the user accounts Note: The Administrator account always has full access. It cannot be deleted.



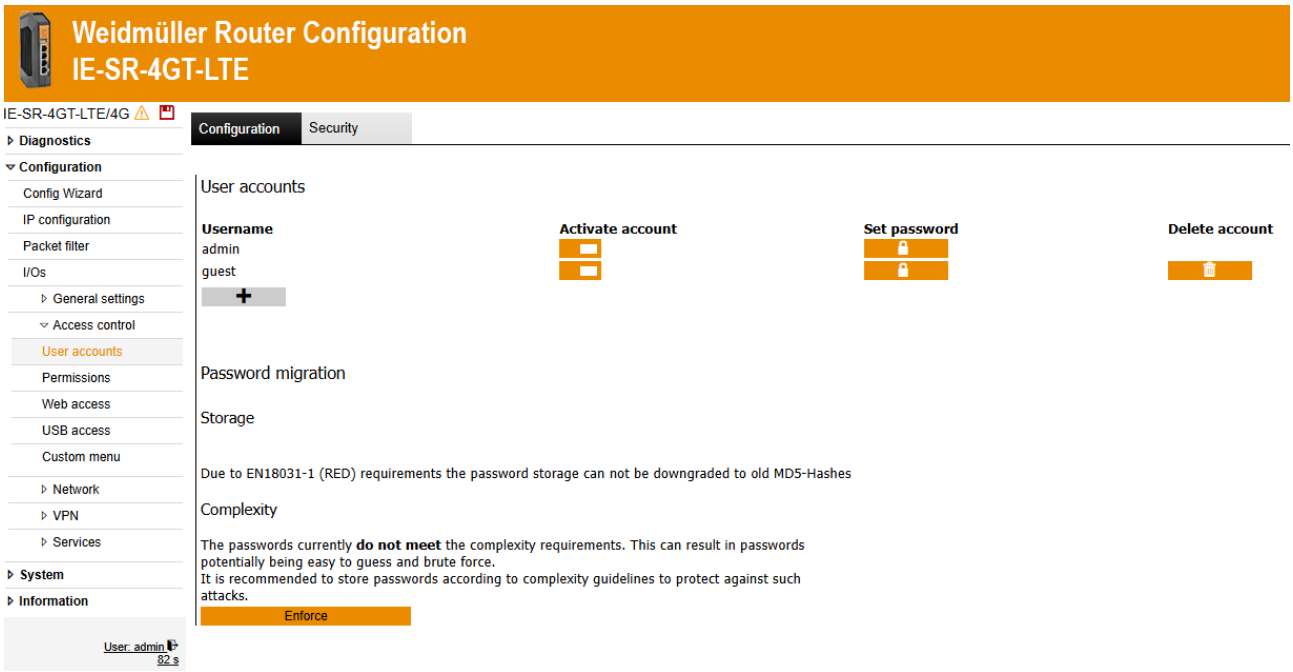
Function	In this state, your password is currently stored as a Message Digest 5 hash, which is considered broken. You can migrate your password to be stored using the secure Argon2 hashing algorithm.

	Start password migration	Press this button to start the migration to a secure password storage using Argon2. In this process, you are required to replace the current password with a password that meets the password policy's complexity requirements. You can also choose to allow passwords that do not meet the complexity requirements from the password policy.



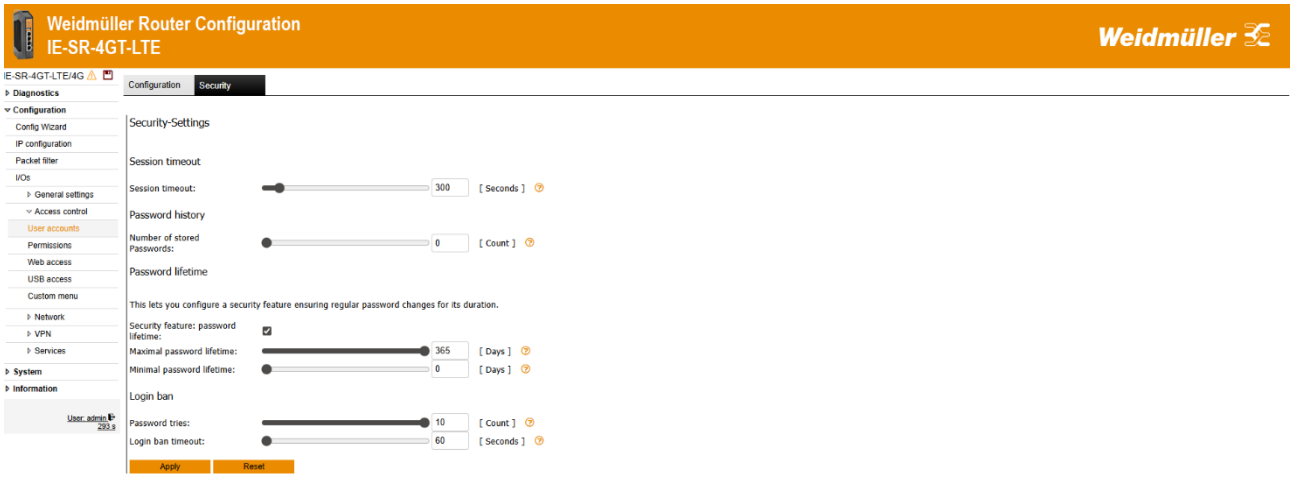
Function	Your password is currently stored securely with the Argon2 algorithm, and depending on your previous selection, it either meets the required complexity standards or does not.	
	Password migration to insecure password storage (**compability mode**)	You can migrate back to the old password storage algorithm with this button. This is not recommended since the Message Digest 5 algorithm is considered broken. Compatibility mode should only be used if you are downgrading to firmware below 2.0.0 or if you want to use the HTTP API.
	Password migration to secure/insecure pass-words	This button can be used to switch the preset password policy on and off. The default policy states that a password must be at least 8 characters long and contain at least one upper and lower case letter, one number and one special character. If you enable the policy, you must meet the complexity requirements, if you disable it, you can use passwords that do not meet those requirements.

The following section only applies to firmware version 2.2.x and above!



Menu	Configuration → Access Control → User Accounts (Tab Configuration)	
Function	Create, manage and delete all the user accounts Note: The Administrator account always has full access. It cannot be deleted.	
	Storage	Due to security requirements the password storage cannot be downgraded to old MD5-Hashes as in previous firmware versions 2.1.x and below and is stored in Argon2-Hashes.
	Enforce Password Complexity	The passwords currently do not meet the complexity requirements. This can result in passwords potentially being easy to guess and brute force. It is recommended to store passwords according to complexity guidelines to protect against such attacks.
	Abolish Password Complexity	The passwords currently meet the complexity requirements. This ensures that the passwords are not easy to guess or brute force. It is not recommended to generate passwords without complexity guidelines.

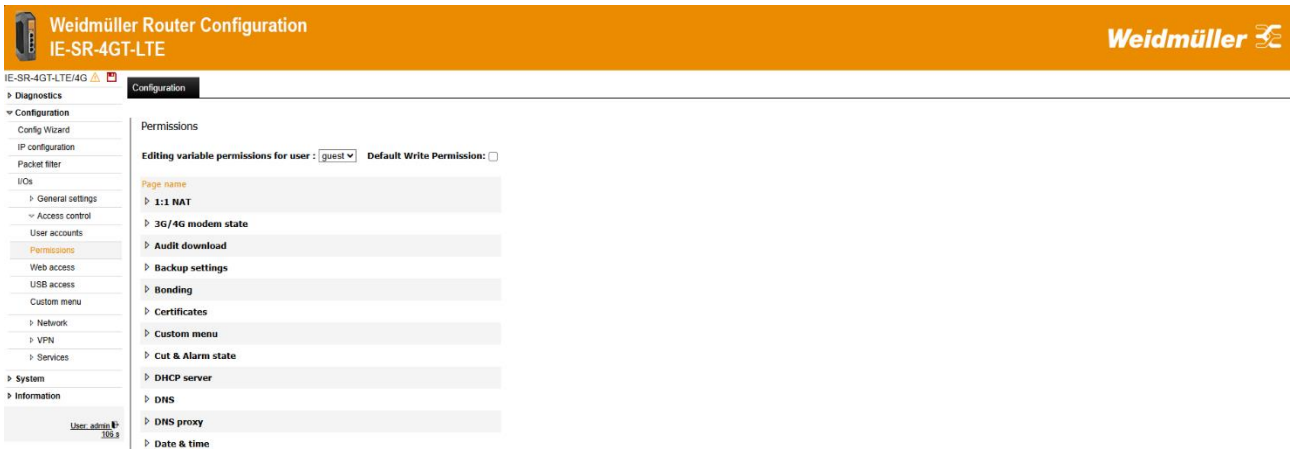
Access Control → User accounts (Tab Security)



Menu	Configuration → Access control→ User accounts (Tab Security)	
Function	Configuration of the router's security settings such as the Session timeout after inactivity, a password expiry feature and login ban after a certain amount of times.	
	Session timeout	Here you can globally set how long a session takes until it expires when inactive.
	Password history	This setting controls how many of your previous passwords the system remembers (only the hash not clear password) so you cannot reuse them when setting a new password.
	Password lifetime feature	This lets you configure a security feature ensuring regular password changes for its duration.
	Maximal password lifetime:	Number in days that can be configured as the maximum lifetime of passwords.
	Minimal password lifetime:	Number of days that can be configured as the minimum lifetime of passwords.
	Password tries:	Password tries after user is banned. The value 0 disables the login ban functionality.
	Login ban timeout:	Timeout in seconds until user can try logging in again.

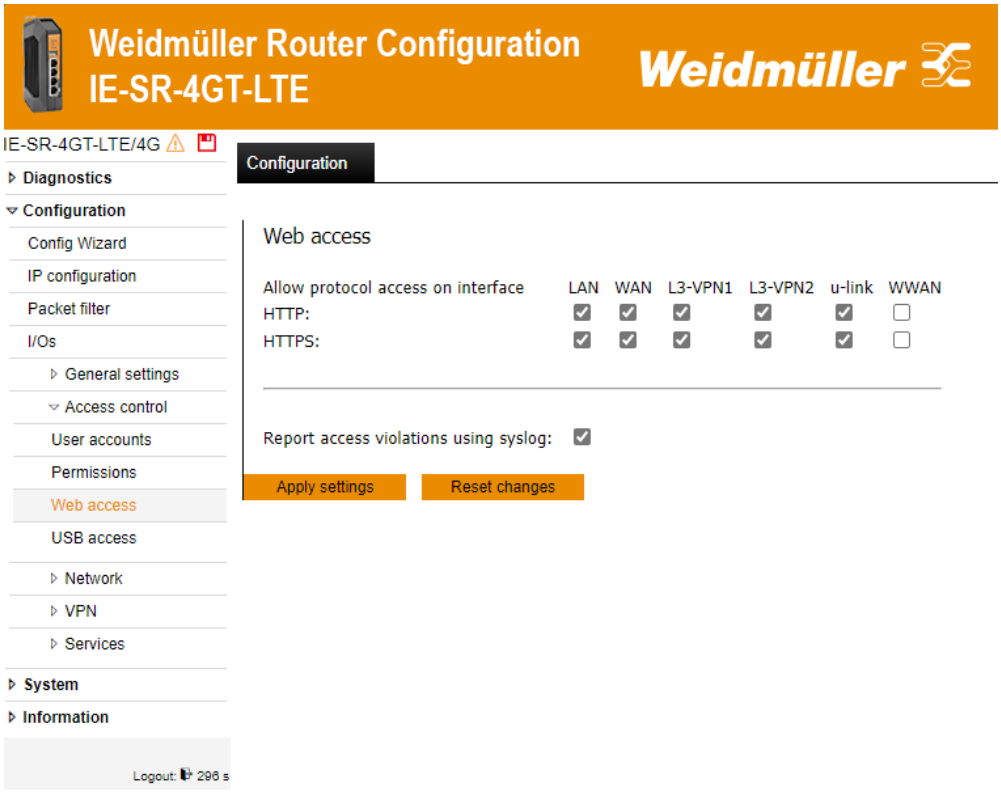
Note:
Regular password rotation is required to meet important security regulations. Since the device does not have a real-time clock, it relies on a secure NTP connection to track password age. Without NTP, the device cannot enforce password expiration accurately. Password expiration is only checked at login, so users will be prompted to change their password the next time they log in after expiration. Administrators should regularly review all user accounts to ensure expired passwords are updated promptly.

Access Control → Permissions



Menu	Configuration → Access control → Permissions
Function	Detailed assignment of individual rights for each created user account. Note: The Administrator account always has full access. It cannot be changed or deleted.

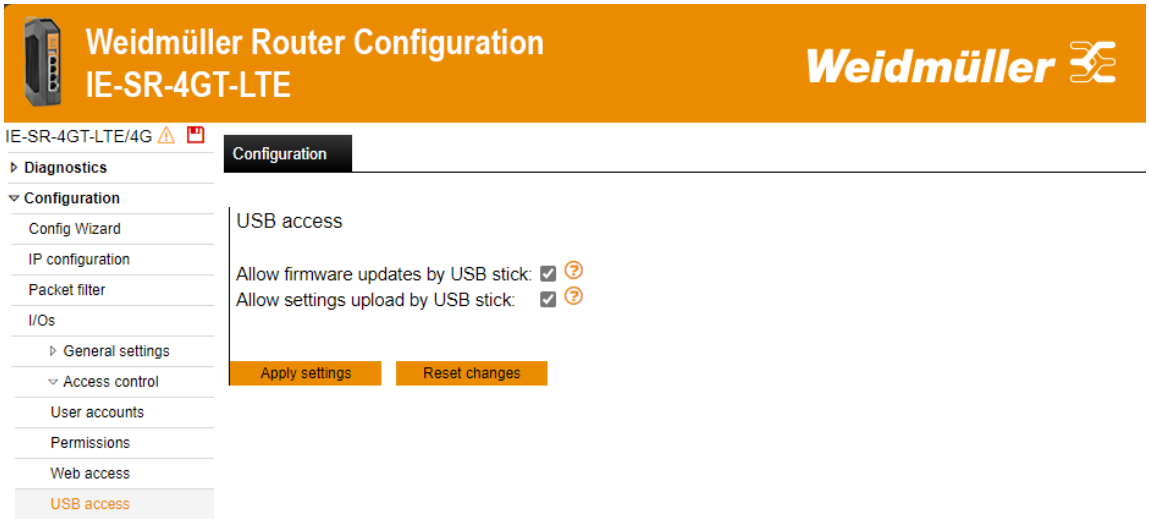
Access Control → Web access



Menu	Configuration → Access control → Web access

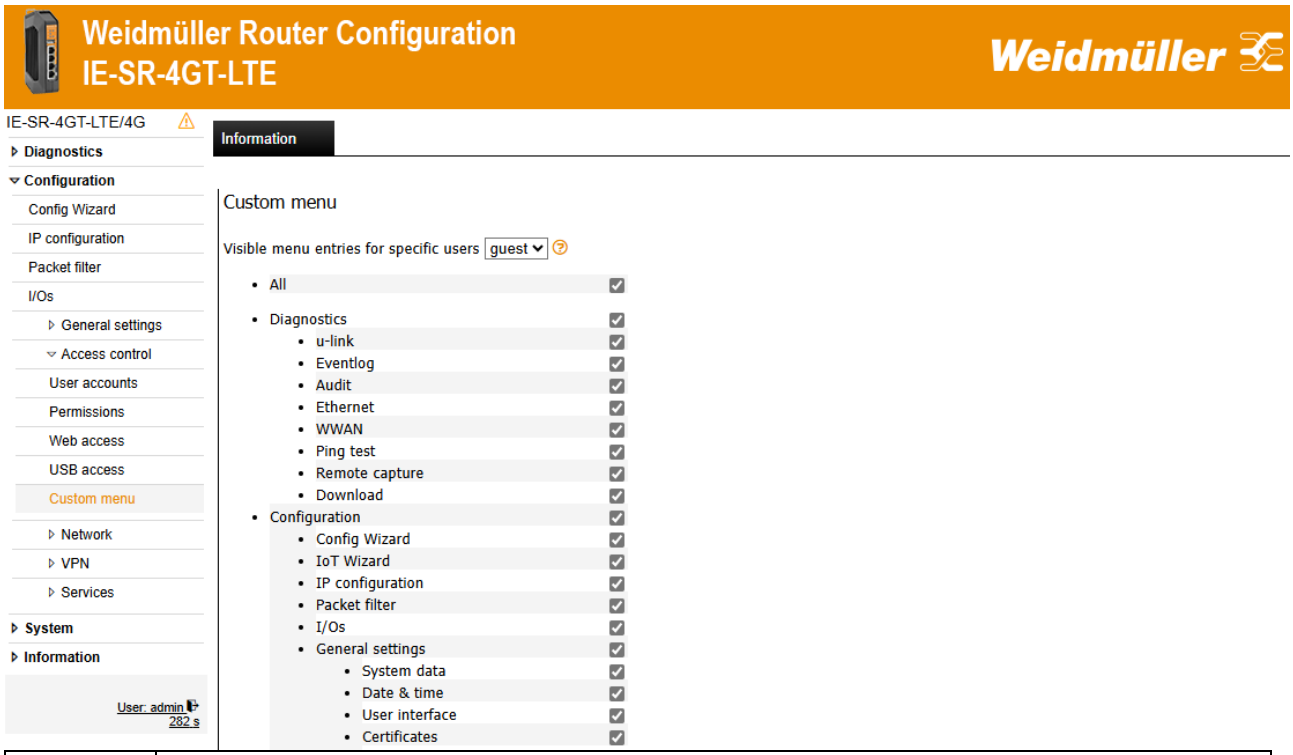
Function	Select the possible access modes of the web interface (via http and / or https) for the different interfaces. For cellular models additional checkboxes named „WWAN“ will be displayed to control access to the Web interface via 4G connection. In extended routing mode or if VPN is used, all interfaces will be displayed if they represent different subnets. *Note: The web interface is only accessible with HTTPS. Activating the HTTP check box enables the automatic redirect from HTTP to HTTPS. Otherwise the web interface will not be accessible with the HTTP link.*

Access Control → USB Access



Menu	Configuration → Access Control → USB Access	
Function	Menu to enable or disable USB access for the settings and firmware of the router.	
	Allow firmware updates by USB stick	Allow firmware updates from USB sticks, if they are inserted when the device starts.
	Allow setting upload by USB stick	Allow the import of settings via USB sticks, if they are inserted when the device starts. In this case, it is also permissible to activate the factory settings via control files on the USB stick.

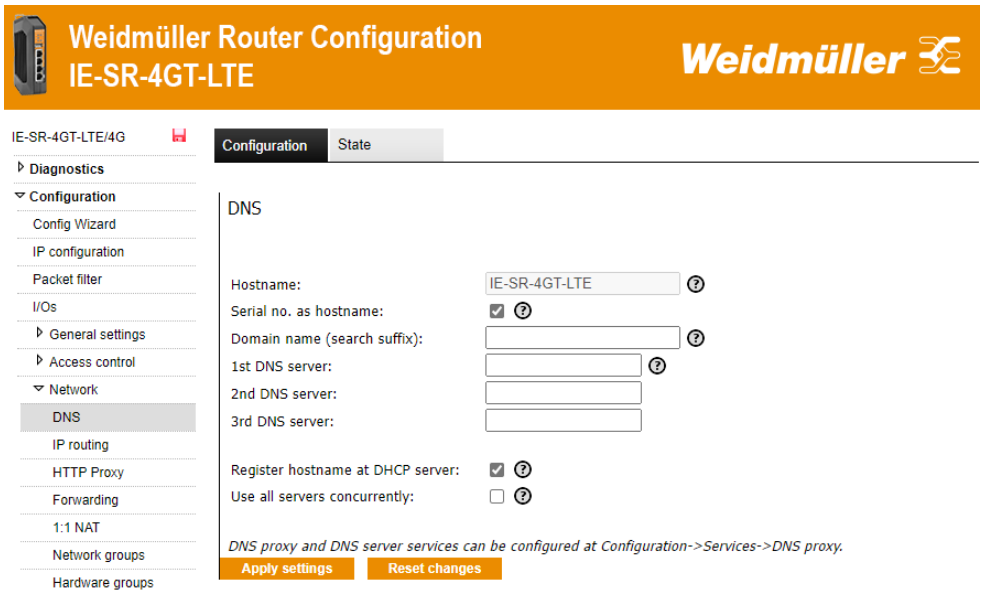
Access Control → Custom menu



Menu	Configuration → Access control → Custom menu
Function	Only menu items that are marked are displayed for the selected user. The selection only has a visual impact and does not affect the permissions of the page. Deep links will continue to work and the API will not be affected.

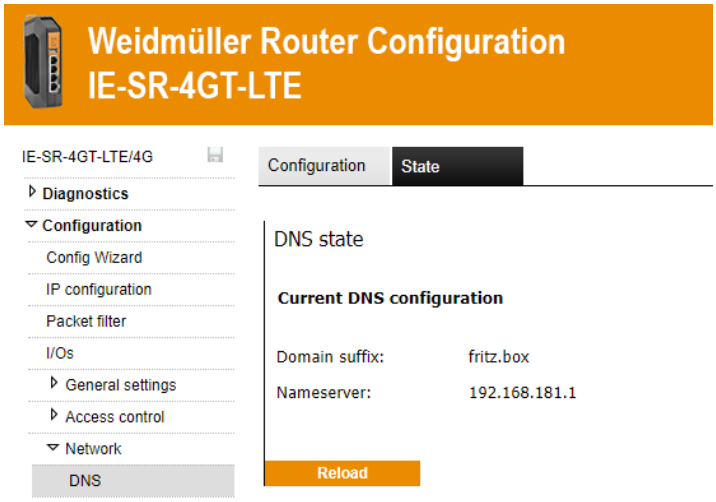
4.2.7 Configuration → Network

Network → DNS (Tab Configuration)



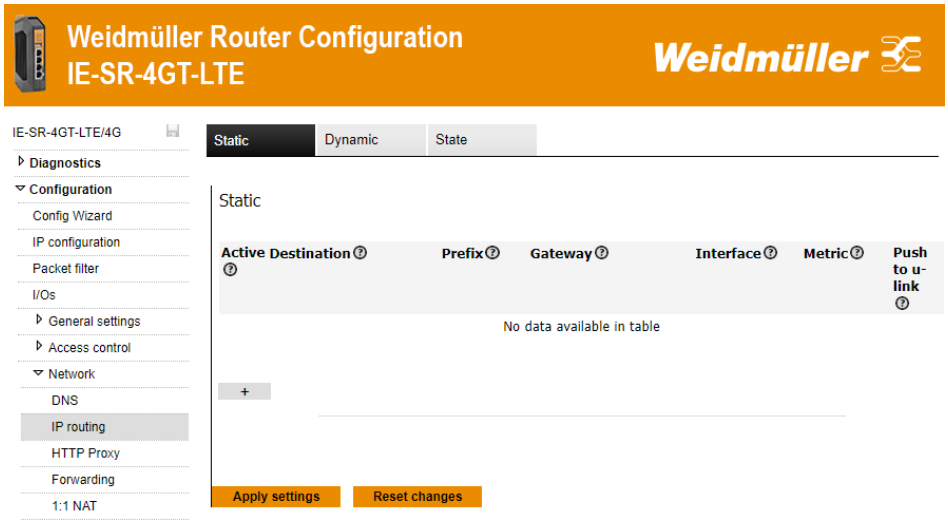
Menu	Configuration → Network → DNS → Tab „Configuration“	
Function	Registration of up to 3 DNS servers for name resolution. The Router acts as a DNS relay server.	
	Hostname	The DNS hostname of the device itself is used in Event Log messages for example.
	Serial no. as hostname	If checkbox is enabled then the device type and serial number will be used as hostname.
	Domain name (search suffix)	The domain name search suffix will be given to DHCP clients if DHCP service is enabled. DNS requests for names with this suffix will not be forwarded to any uplink DNS-Server
	1st, 2nd, 3rd DNS server	If the interface for accessing the Internet (e.g. WAN port) is configured statically then you must configure at least one accessible DNS server for resolving DNS names (e.g Google’s name server with IP 8.8.8.8). If the Interface for Internet access is set to DHCP then typically the DNS server will be retrieved from DHCP server. In this case you do not need to enter the IP address of a DNS server. Generally at least one DNS server must be configured for resolving hostnames to IP addresses. A DNS server is mandatory if the Router is configured for using the u-link Remote Access Service. Note: See Tab „State“ to check the currently configured name server(s).
	Register host name at DHCP server	If enabled all DHCP requests by the device will register the specified hostname at the DHCP server. If the DHCP server is running dynamic DNS updates according to RFC2136 this will result in a valid DNS record on the DNS server with the specified Hostname
	Use all servers concurrently	If set active, incoming queries will be forwarded to all configured DNS servers. The fastest reply will be sent back to the requester. Otherwise, only one DHCP server will be used.

Network → DNS (Tab State)



Menu	Configuration → Network → DNS → Tab „State“
Function	Displays the currently active DNS server

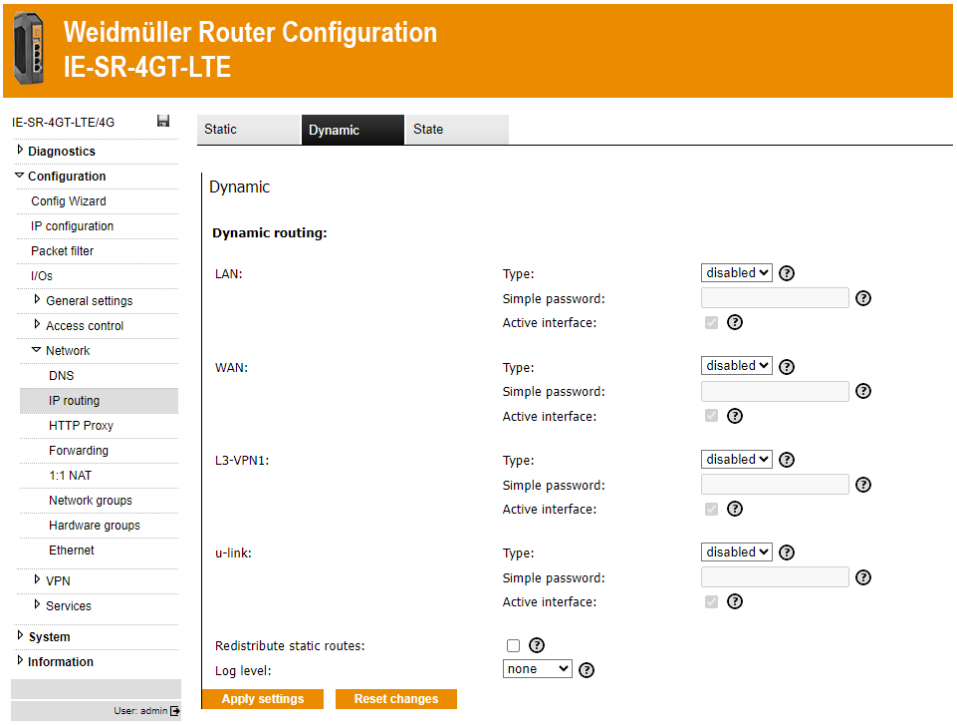
Network → IP Routing (Tab Static)



Menu	Configuration → Network → IP Routing → Tab „Static“	
Function	Registration of static IP routes and activating/deactivating of dynamic routing. For dynamic routing, both can be selected the RIP and the OSPF protocol. Please note that dynamic routing can be set per interface. Cellular routers, or routers in extended routing mode, will have more interfaces to define dynamic routing. Up to 20 static IP routes can be configured.	
	Static Routing Routing Table	Displays all configured static routes Static routing forwards IP packets belonging to the specified network to the given gateway. The network is defined by an IP address and a subnet mask, which tells how many bits counted from the left are fixed. For example, IP 192.168.5.0 and subnet mask 24 means, that any IP of the format 192.168.5.xxx belongs to the network (3 bytes = 3 * 8 bit = 24 bits). Another example is 192.168.0.0 and subnet mask 16. Any IP of the format 192.168.xxx.xxx belongs to this network.

	Static Routing Destination	Network address of the destination network, i.e. 192.168.0.0
	Static Routing Prefix	Network mask of the destination network, i.e. 8, 16 or 24. Without leading /
	Static Routing Gateway	IP address of the gateway for this entry. In case of a device route you can use 0.0.0.0
	Static Routing Metric	Metric for this entry. Allowed values are 0-100. Normally this is used in conjunctions with dynamic routing. This field is optional and can be left empty.
	Static Routing Interface	Network device for this entry. Select * for static routes with a valid gateway IP address. Select a specific device for a device route with the IP 0.0.0.0 as a gateway.
	Static Routing Push to u-link	Push the route also to u-link and its clients. Probably you also need to adopt the routing tables of the devices in the specified subnet.
	Static Routing Add entry	Adds the static route to the table
	Static Routing Apply settings	Apply settings for the whole site (dynamic AND static routing)
	Static Routing Reset changes	Reset all changes made on this web page to initial values of currently applied/saved settings. It has no effect after clicking button “Apply settings”.

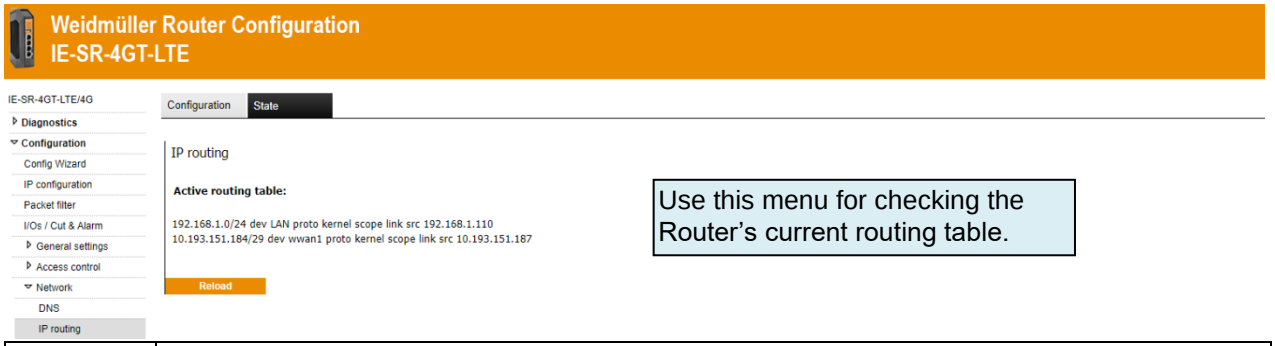
Network → IP Routing (Tab Dynamic)



Menu	Configuration → Network → IP Routing → Tab „Configuration“
Function	Registration of static IP routes and activating/deactivating of dynamic routing. For dynamic routing, both can be selected the RIP and the OSPF protocol. Please note that dynamic routing can be set per interface. Cellular routers, or routers in extended routing mode, will have more interfaces to define dynamic routing. Up to 20 static IP routes can be configured.

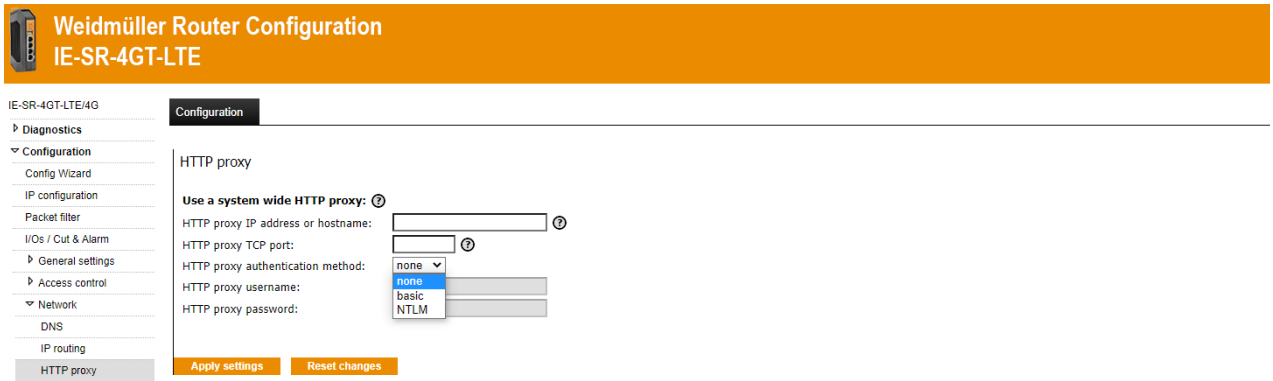
	Dynamic Routing Type:	Which routing protocol should be used on this interface. - RIP the Routing Information Protocol is frequently used and helps routers to dynamically adapt to changes - OSPF Open Shortest Path First is newer and mage RIP obsolete - Both Select this if you want to use both protocols at a time	
	Dynamic Routing Simple Pass-word	This field is optional. The OSPF/RIP simple password authentication will protect all packets with this password. **Note that this password will be send as clear text!** It is only meant to prevent misconfigured routers to be placed on the network.	
	Dynamic Routing Active inter-face	RIP: Mark the checkbox to send advertisements on this interface. If the checkbox is left empty, the interface will only listen for incoming advertise-ment and it will be included in advertisement on other active interfaces. OSPF: Enable OSPF on this interface. IF the checkbox is not marked the interface will be included in advertisements on other active interfaces. Other than RIP it will not even listen for incoming advertisements.	
	Dynamic Routing Redistribute static routes	When enabled: redistribute all static routes with OSPF and RIP. Note: the metric of the static table will not be used.	
	Dynamic Routing Log level	None	Will log no messages through the Event Log.
		Info	Log only some information and critical errors.
		Debug	Log state information too.
		Verbose	Log all possible messages

Network → IP Routing (Tab State)



Menu	Configuration → Network → IP Routing → Tab „State“
Function	Displays currently valid routing table. The line with text “default via….” shows the default gateway IP and the gateway interface Format of other routes: <Target Network> dev <interface> proto kernel scope link src <interface IP address > Means: <Target Network> is accessible via <IP address> of device <interface>

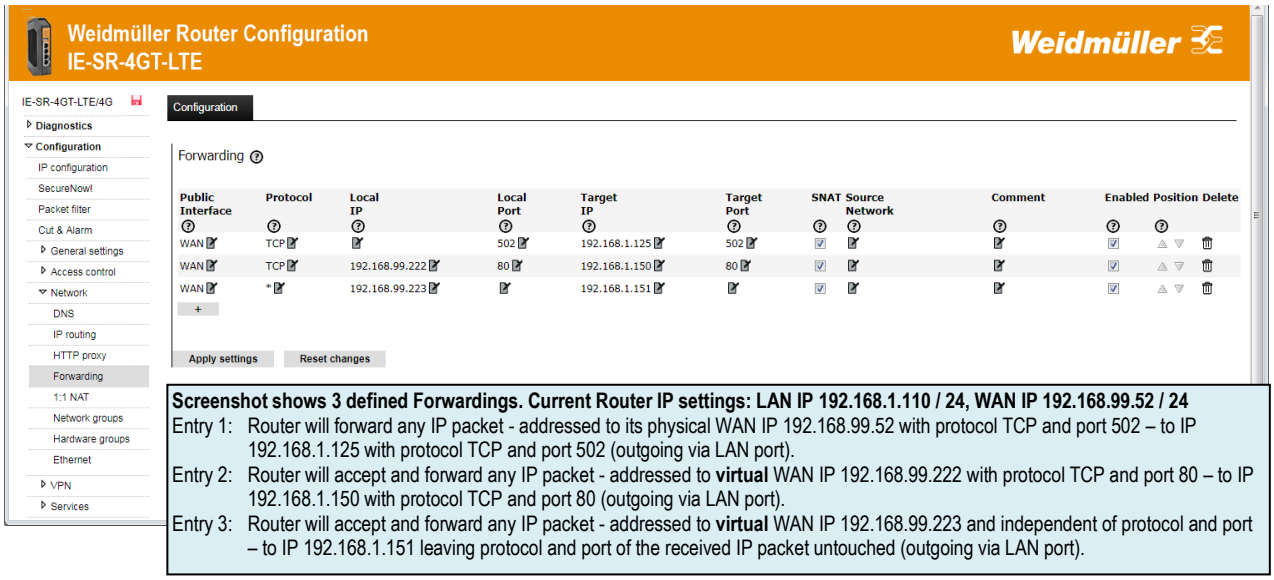
Network → HTTP proxy



Menu	Configuration → Network → HTTP proxy		
Function	Configuration of a system wide HTTP proxy. This will be used for several services depending on the features of the device. You must enable the usage of this proxy for most services separately.		
	HTTP proxy IP address or hostname	IP address or hostname of the proxy. You must configure a valid DNS configuration to use a hostname	
	HTTP proxy TCP port	The TCP port of the proxy. In many cases 8080 is used.	
	HTTP proxy authentication method	None	No authentication required
		Basic	HTTP standard authentication, username and password required
		NTLM	Microsoft Windows ISA server authentication style, username and password required.
	HTTP proxy username	Username	
	HTTP proxy password	Password	

Note: If the Router - for Internet access - has to pass the corporate Router/Firewall and Security systems (controlled by company IT) then often the configuration of a HTTP proxy is necessary. In those cases, please ask the responsible IT department for parameters and credentials for proxy settings.

Network → Forwarding



Screenshot shows 3 defined Forwardings. Current Router IP settings: LAN IP 192.168.1.110 / 24, WAN IP 192.168.99.52 / 24

Entry 1: Router will forward any IP packet - addressed to its physical WAN IP 192.168.99.52 with protocol TCP and port 502 – to IP 192.168.1.125 with protocol TCP and port 502 (outgoing via LAN port).

Entry 2: Router will accept and forward any IP packet - addressed to **virtual** WAN IP 192.168.99.222 with protocol TCP and port 80 – to IP 192.168.1.150 with protocol TCP and port 80 (outgoing via LAN port).

Entry 3: Router will accept and forward any IP packet - addressed to **virtual** WAN IP 192.168.99.223 and independent of protocol and port – to IP 192.168.1.151 leaving protocol and port of the received IP packet untouched (outgoing via LAN port).

Menu	Configuration → Network → Forwarding

<table>
<tr><td>Function</td><td colspan="2">Configuring of forwardings based on IP address, protocol and port number.

The forwarding can be used to forward IP packets incoming at selected “Public Interface” (e.g. WAN) and having as original target IP the Routers WAN IP to a defined Target IP e.g. behind LAN port.

This can either be done on special TCP/UDP ports or on a whole IP address. The table supports IP aliases on the Public interface, source NAT of the request and conditional matching by filtering on the source address. Please take care of the position of each row, as the table is progressed from the top to the bottom for each packet until a match is found. If you run a restricting packet filter you must open the data paths there too. The packet filter will see the forwarding target as destination and always the original source independent of the SNAT checkbox.

The feature „IP address forwarding“ (also called Virtual Mapping) can be used to forward an IP packet - addressed to “Local IP” – independent of protocol and port number – to a defined “Target IP”.</td></tr>
<tr><td></td><td>Public interface</td><td>Incoming interface on which the IP packet - which shall be forwarded - will arrive.</td></tr>
<tr><td></td><td>Protocol</td><td>Select protocol TCP or UDP if you want to forward a special port.

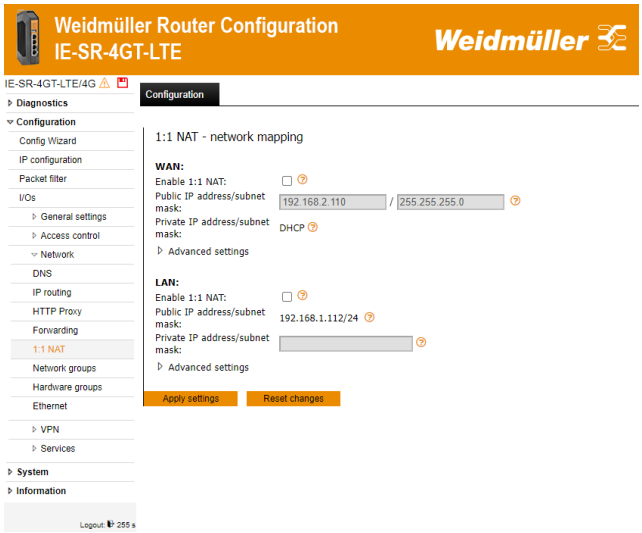
Use “*” if you want to forward all IP packets (ICMP, TCP, UDP) independent from protocol and port.</td></tr>
<tr><td></td><td>Local IP</td><td>Enter a free available IP address which will behave as an additional (virtual) IP address of the selected “Public Interface” (mostly WAN). In case of physical interfaces this address is most likely one of the public interface range. In case of OpenVPN or IPsec interfaces it should be one of the VPN address range. The device will take this additional IP address as its own and will forward the traffic - addressed to this IP – to defined Target IP. This option cannot be used on 4G or DSL links.

If you leave it empty then the current IP address of the defined (incoming) interface will be used as ‘Local IP’.</td></tr>
<tr><td></td><td>Local port</td><td>The addressed port belonging to “Local IP” if protocol TCP or UDP is selected. Leave empty if entry ‘*’ is selected for protocol.</td></tr>
<tr><td></td><td>Target IP</td><td>The target IP to which the IP packet – addressed to “Local IP” will be forwarded. This can be any reachable IP address.</td></tr>
<tr><td></td><td>Target Port</td><td>The addressed port belonging to “Target IP” if protocol TCP or UDP is selected. Leave empty if entry ‘*’ is selected for protocol.</td></tr>
<tr><td></td><td>SNAT</td><td>In enabled the source of the connection will be hidden behind the local address of the device on the outgoing interface (i.e. LAN). This is helpful if the target does not know an IP route to the original source (e.g. a S7 PLC with no default gateway or a default gateway to a different router). The target will only see the local address and therefore will not need an IP route to the original source.</td></tr>
<tr><td></td><td>Source Network</td><td>Will only enable the forward if the original source of the request is within the given IP subnet. The syntax is IP/mask (i.e. 192.168.0.0/24)- Leave empty if unsure.</td></tr>
<tr><td></td><td>Comment</td><td>An optional comment</td></tr>
<tr><td></td><td>Enabled</td><td>Enables or disables the entry.</td></tr>
<tr><td></td><td>Position</td><td>Move the entries to the correct position in the table. The Router is checking the defined Forwardings from Top to Down until an entry is matching.

Example: You can configure a forward of TCP port 80 to an internal address of the device itself (i.e. the LAN IP address) as the first row. Then a second row insert a forward with protocol “*” to a target IP.
The effect will be that you can reach the device on its web interface TCP port 80 but all other ports and protocols including ICMP pings will be forwarded to the target.</td></tr>
</table>

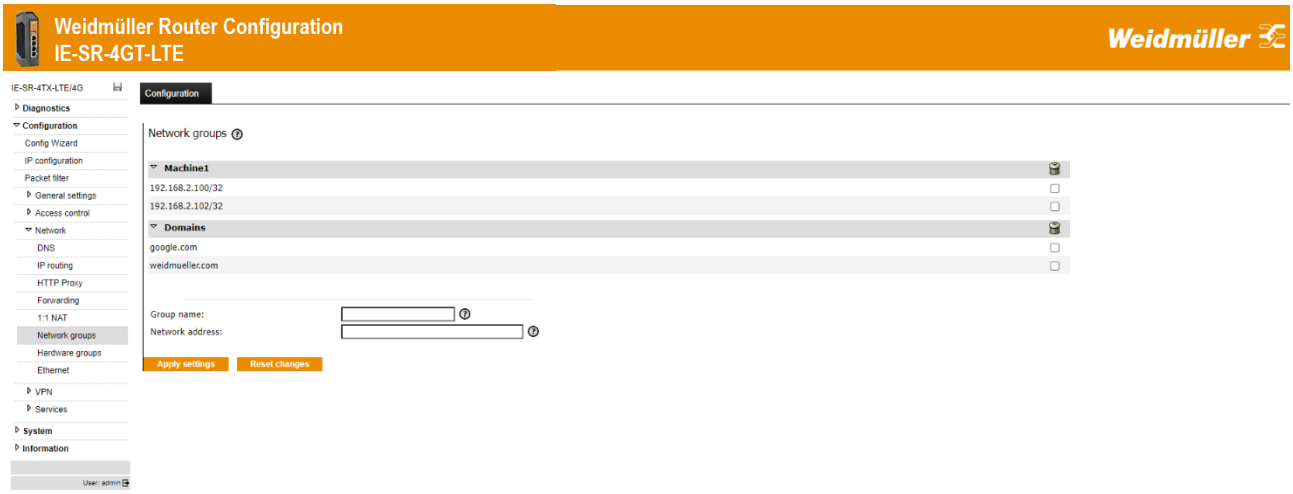
	Reverse SNAT	On connections being initiated from the target IP and leaving the system via the public interface the sender address will be mapped to the local IP. Only active if the protocol is “*”
	Note after editing a value, press accept ✔ or delete x, otherwise the message “Syntax error applying data” will appear.	

Network → 1:1 NAT



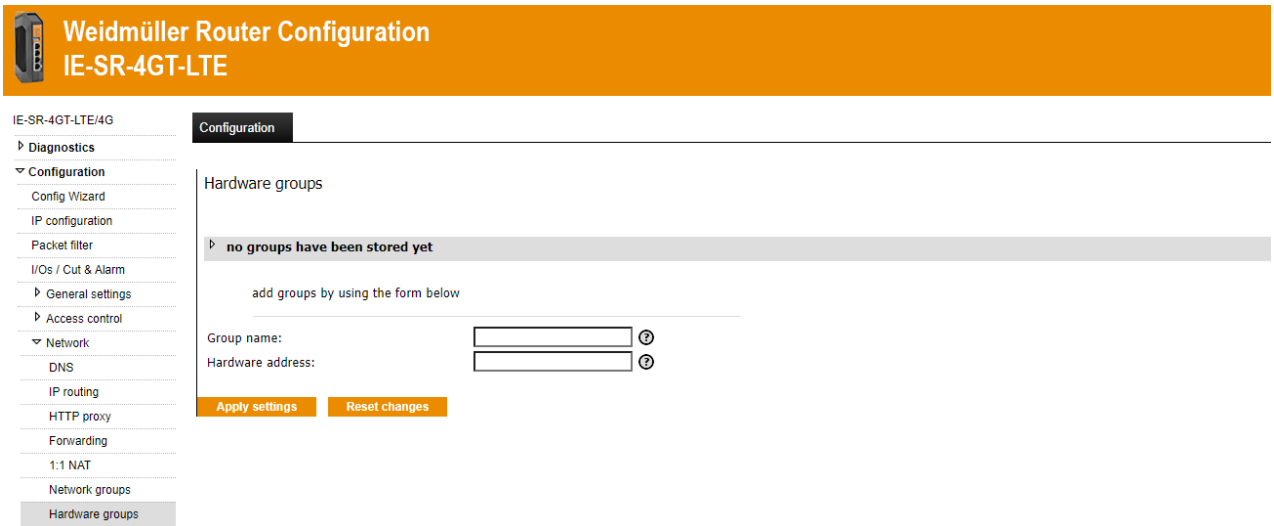
Menu	Configuration → Network → 1:1 NAT	
Function	With 1:1 NAT you can map a private subnet to the public subnet defined in the IP configuration. This allows you to resolve conflicts between identical networks. E.g. if all LAN ports in extended IP routing mode are connected to equal subnets, they can be accessed uniquely via the public subnet without the need for changing any configuration of the private subnets. 1:1 NAT can be configured for all active (physical and virtual) interfaces. Note: While the private subnets may be equal they must not conflict with the public IP subnets. **For more detailed information about using 1:1 NAT please refer to application notes in appendix A.**	
	Enable 1:1 NAT	Enable 1:1 NAT for this interface. Note: 1:1 NAT only can be activated if NAT (masquerading) is **not** enabled for this interface
	Public IP address	This is the public interface IP address and subnet mask as defined in menu 'IP Configuration', e.g. 192.168.1.110/24. If DHCP is enabled, you must define a network to which the IP addresses received via DHCP will be mapped.
	Private IP address	The definition of the private subnet is the private device IP with the subnet mask appended. E.g. 192.168.0.110/24 means, that the device itself is reachable as 192.168.0.110 from the private subnet 192.168.0.0/24
	Enable double sided network mapping	With this extension, (private) IP address conflicts can be solved if public hosts use IP addresses from the same subnet as the 1:1 NAT private subnet. Where possible, you should not use such a subnet for 1:1 NAT private subnet, but sometimes the private subnet is already defined through the according network components. This conflict will be solved by using a further subnet that is not used anywhere else, neither on public nor on private subnets.
	Substitute with IP address/subnet mask	A subnet, preferably of the same size as the according private 1:1 NAT subnet. Will be used for translating private IP addresses on public interfaces to a subnet of IP addresses that is otherwise not used. Therefore, only IP source address for packets going to the according private subnet will be changed. This option is not necessary if the private subnet is not used on public interfaces.

Network → Network Groups



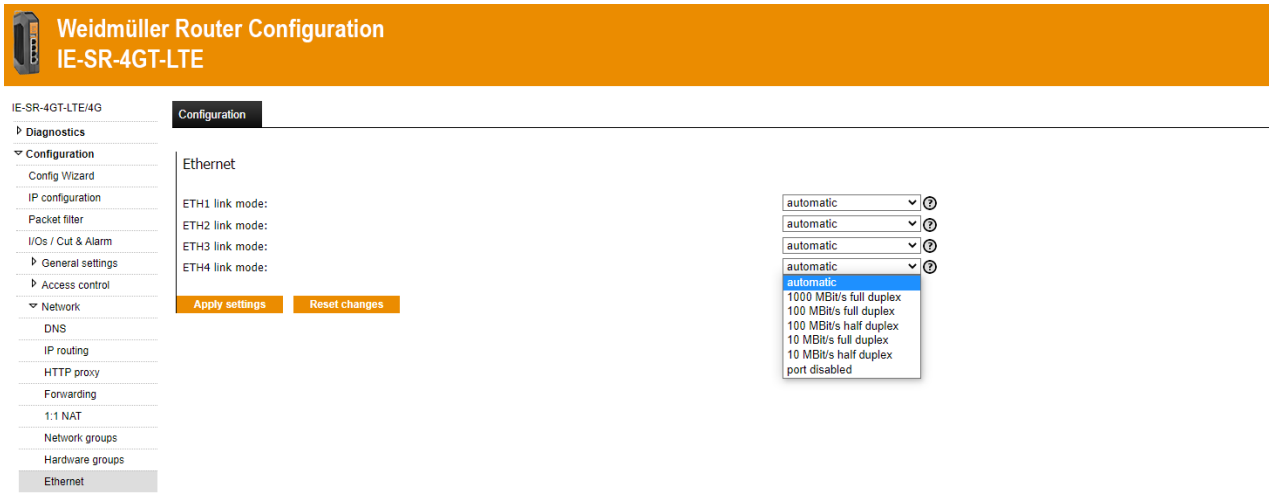
Menu	Configuration → Network → Network groups	
Function	Network groups are used to group individual IP addresses, IP subnets, or DNS Host and domain names. These groups can be used in the firewall packet filter as source or destination criteria. Note, that DNS Host and domain names do not work on Layer 2 packet filter rules and will be discarded without an error message. To add several IP address (ranges) or DNS host and domain names to a group, insert the same group name for each rule.	
	Group name	The group name for which a network should be added. It may contain letters and digits. If the given group does not exist, it will be created automatically. Hint: Click on an existing group name will fill the empty text field.
	Network address	In this field, an IP network is specified in the format IP address/subnet (CIDR), e.g., 192.168.0.0/24. Alternatively, DNS host – and domain names or domain extensions are used for the layer 3 packet filter. There can be many entries in each group. Caution: Filter rules, that use a rule with a recently modified group, will not be updated until <Apply settings> is triggered (or <Save settings> respectively)

Network → Hardware Groups



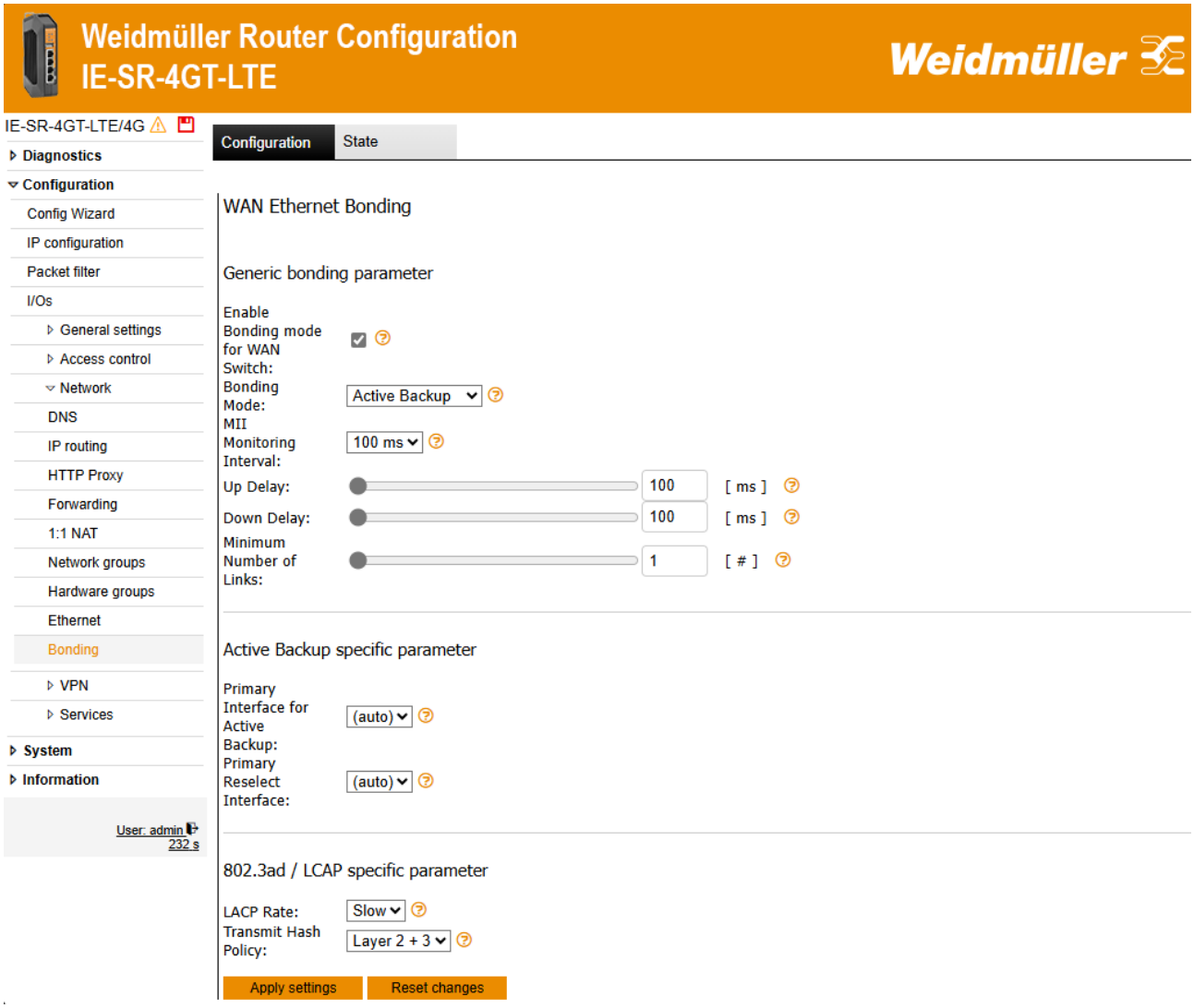
Menu	Configuration → Network → Hardware groups	
Function	Creating groups with "speaking" names based on MAC addresses (layer 2). A hardware group can contain any number of MAC addresses (for example, 00:15:7E:D9:09:00). Hardware groups can be used for better readability than individual MAC addresses if you will create firewall filtering rules (See menu Configuration → 4.2.3 Configuration → Packet filter (Firewall→ Layer 2).	
	Group name	The group name for which a hardware address should be added. It may contain letters and digits. If the given group does not exist, it will be created automatically. Hint: Click on an existing group name will fill the empty text field.
	Hardware address	Hardware Address (also known as physical address or MAC) to be added to a given group. These groups can be referred to by other services like filter rules e.g. Caution: Filter rules, that use a rule with a recently modified group, will not be updated until <Apply settings> is triggered (or <Save settings> respectively)

Network → Ethernet



Menu	Configuration → Network → Ethernet	
Function	Ethernet configuration allows to change the speed of each LAN and WAN port of the router. Furthermore, one is able to change between full duplex and half duplex mode for every single port. Changing this configuration disables auto crossover (Auto-MDIX) and uses MDI instead.	
	automatic	Selects best option automatically and uses auto crossover feature.
	100 MBit/s full/half duplex	Allows the port to use speeds up to either only 10 Mbit/s or the full 100 MBit/s. Full duplex allows two-way traffic between sender and receiver, whilst half duplex only allows communication one way at a time.
	disabled	Disables the port completely. Can be used as security measure to disable unused ports.

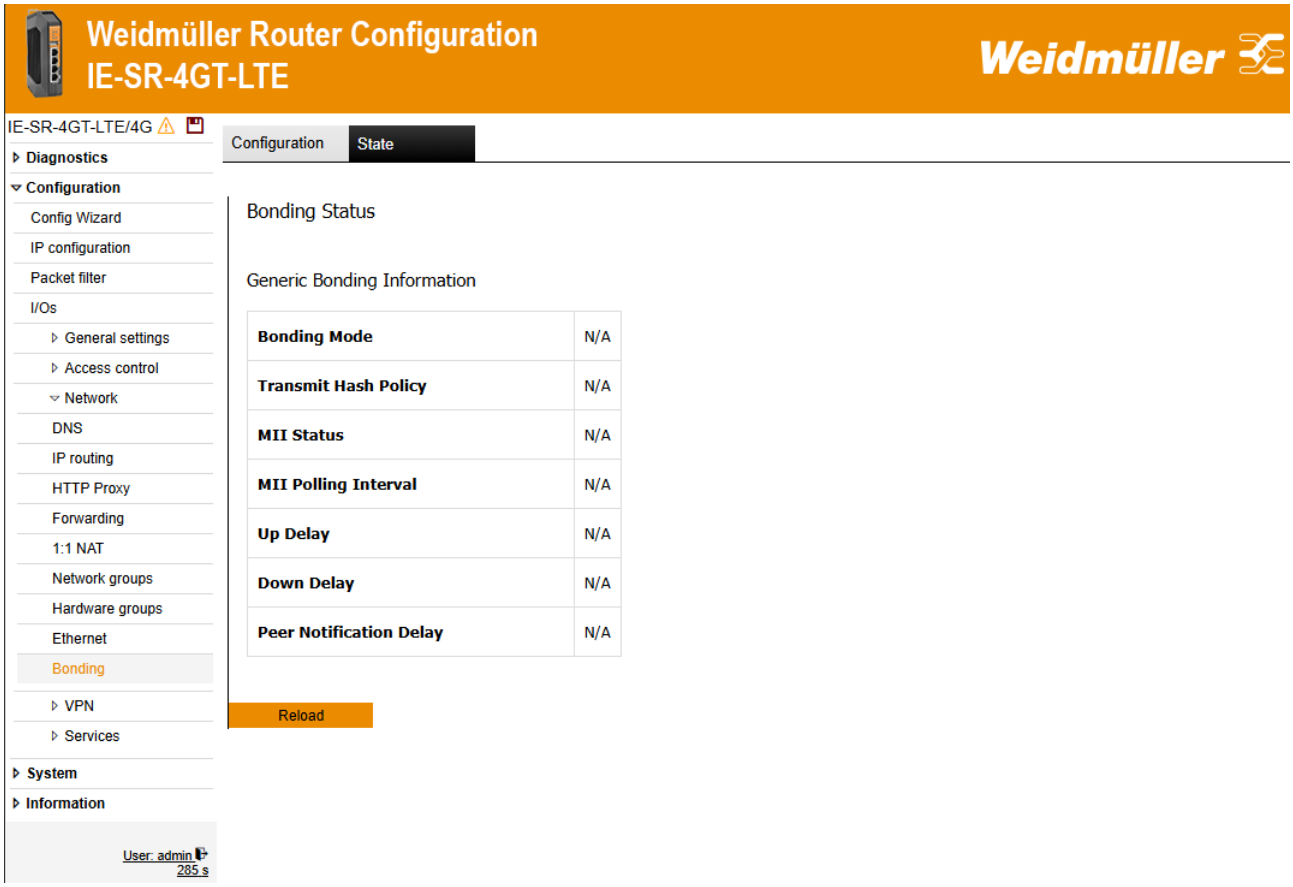
Network → Bonding (Tab Configuration)



Menu	Configuration → Network → Bonding (Tab Configuration)	
Function	This feature allows the WAN switch to operate in bonded Ethernet mode instead of the default bridged mode. In bridged mode, all Ethernet ports function as a Layer 2 switch, forwarding traffic transparently between them. In bonded mode, the Ethernet ports are grouped and used as a single logical WAN interface at Layer 3, enabling load balancing or redundancy depending on the bonding configuration. This feature is only available when the device is set to operation mode IP-router extended.	
	Enable Bonding mode for WAN Switch	Enable this feature to use the WAN switch as bonded Ethernet ports instead of bridged Ethernet ports. The feature can only be enabled in operation mode IP-router extended
	Bonding Mode	• Active Backup: Ensures continuous network availability by keeping one interface active and switching to a backup if the primary fails. Ideal for network redundancy. • 802.3ad / LCAP: An IEEE standard for link aggregation, combining multiple interfaces for increased bandwidth and redundancy. Requires a Switch with 802.3ad support on the other side of the Ethernet link and matching settings.

	MII Monitoring Interval	The MII Monitoring Interval determines how often the link status is checked. Shorter intervals provide faster failure detection but may create false positives. Choose a balance suitable for your needs.
	Up Delay	The Up Delay sets the time the system waits after a link becomes available before it is considered operational. This helps to prevent brief disruptions from causing unnecessary changes.
	Down Delay	The Down Delay determines the time to wait after a link is detected as unavailable before marking it as down. This can help reduce unnecessary failover actions due to temporary issues.
	Minimum Number of Links	The Minimum Number of Links specifies the number of active links required for the bonding group to be considered operational. This ensures a defined level of link redundancy is maintained. Range is: 1-8.
	Primary Interface for Active Backup	Select the primary interface for the Active Backup mode. This interface will be the main link used when available. If set to '(auto)', the system will automatically select the primary interface based on the bonding configuration and link status.
	Primary Reselect Interface	Choose the primary interface for reselection in the Active Backup configuration. This allows a specific interface to take precedence when switching back from a failover. If set to '(auto)', the system will handle reselection automatically based on the bonding configuration and link status.
	LACP Rate	The 802.3ad / LACP (Link Aggregation Control Protocol) Rate determines how frequently LACP packets are sent. 'Fast' sends packets every second for quicker link status detection, while 'Slow' sends packets every 30 seconds.
	Transmit Hash Policy	The Transmit Hash Policy determines how traffic is distributed across the bonded links. 'Layer 2' uses the MAC addresses, 'Layer 2 + 3' includes both MAC and IP addresses, and 'Layer 3 + 4' adds IP and TCP/UDP ports for higher distribution granularity.

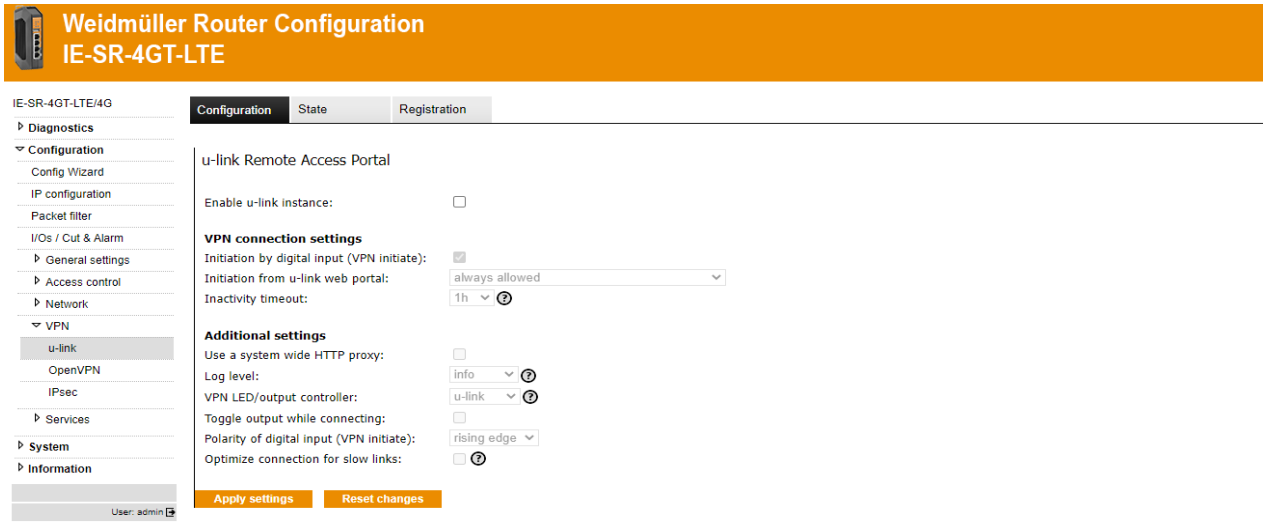
Network → Bonding (Tab State)



Menu	Configuration → Network → Bonding (Tab Configuration)
Function	This feature allows the WAN switch to operate in bonded Ethernet mode instead of the default bridged mode. In bridged mode, all Ethernet ports function as a Layer 2 switch, forwarding traffic transparently between them. In bonded mode, the Ethernet ports are grouped and used as a single logical WAN interface at Layer 3, enabling load balancing or redundancy depending on the bonding configuration. This feature is only available when the device is set to operation mode IP-router extended.

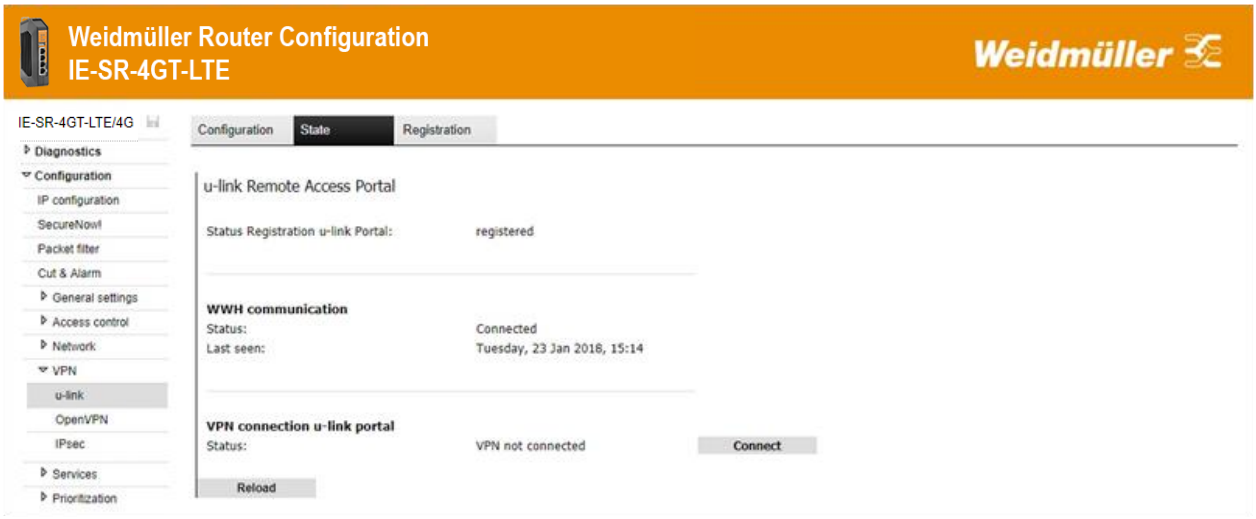
4.2.8 Configuration → VPN

VPN → u-link (Tab Configuration)



Menu	Configuration → VPN → u-link → Tab "Configuration"	
Function	Enable u-link instance	Enables the routers connectivity service to be used for the Weidmüller u-link Remote Access Service.
	Initiation by digital input (VPN initiate):	Allows/Denies to establish a VPN connection to the u-link platform by setting 24 VDC on digital input "VPN initiate".
	Initiation from u-link web portal	Never allowed: u-link cannot be initiated remotely from the u-link portal Always allowed: u-link can be initiated remotely from the u-link portal Allowed if digital input (VPN-Initiate) is active: u-link can be initiated remotely from the u-link portal **only** if the external digital input ('VPN initiate' set to 24 VDC) is active.
	Use a system-wide HTTP proxy	Enable this checkbox if the HTTP/HTTPS based Internet access of the Router (for establishing an u-link VPN tunnel) is controlled by a proxy server which requires an authentication for passing. The system wide HTTP proxy must be configured under Configuration → Network → HTTP proxy.
	Log level	None: Will log no messages through the Event Log Info: Log only some information and critical errors Debug: Log state information too Verbose: Log all possible messages
	VPN LED/output controller	Disabled: The LED and digital output are not used by u-link. u-link: LED is blinking during connecting and on during connection, digital output "VPN active" is set to ON as long as the VPN tunnel is established.
	Toggle output while connecting	Copies the behavior of the VPN LED to the digital output "VPN active"
	Polarity of digital input (VPN initiate)	Rising edge: VPN is triggered by rising edge of input voltage (from 0 V to 24 V) Falling edge VPN is triggered by falling edge of input voltage (from 24 V to 0 V)
	Optimize connection for slow links	Enable this feature if you have links with round trip times above 1000 ms, i.e. satellite connections.

VPN→ u-link (Tab State)



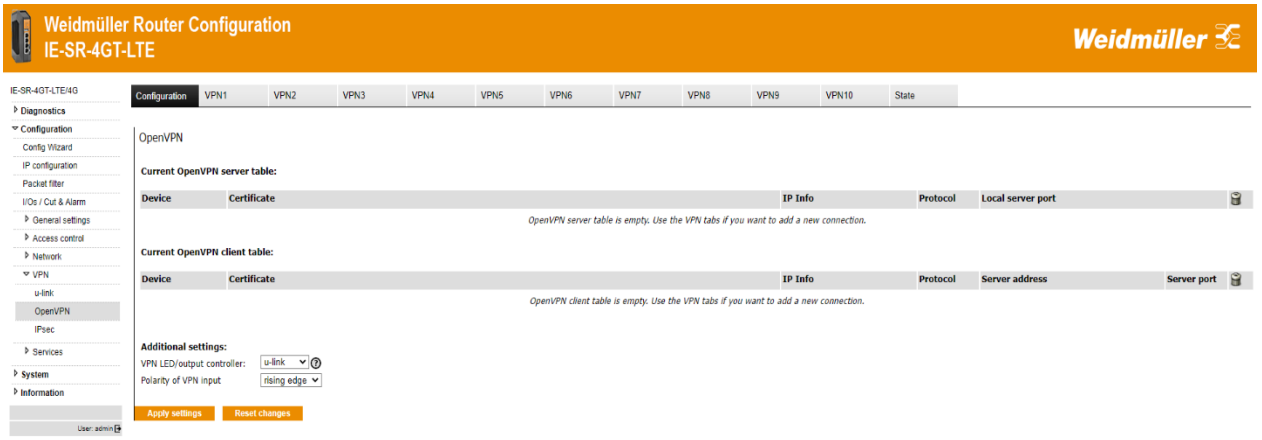
Menu	Configuration → VPN → u-link → Tab “State”	
Function	Displays u-link Remote Access Service status.	
	Status Registration u-link portal	“registered” or “not registered”
	WWH communication	The World-Wide Heartbeat (WWH) is a https connection to the u-link platform which submits status information. The WWH normally refreshes every 170 seconds. If WWH communication is not possible the router may not have an internet connection.
	Status	“Connected” or “Not connected”
	Last seen	Last time the WWH connection was successful
	VPN connection u-link portal	u-link is using OpenVPN to establish an outgoing secure connection from the device to the u-link server. With an u-link account (free trial version) you will then be able to remote access the private networks remotely.
	Status	“VPN connected” or “VPN not connected”, shows whether there is an outgoing safe VPN connection to the u-link server or not. With “Connect” you can manually initiate a connection.
	Button “Connect” (Disconnect)	Can be used to establish (cancel) the VPN tunnel to the u-link VPN server.

VPN→ u-link (Tab Registration)

Menu	Configuration → VPN → u-link → Tab “Registration”
Function	Register or unregister the device at the u-link platform. For this an internet connection of the device is necessary. To register, type in the unique Router Activation code generated in the u-link portal (https://u-link.weidmueller.com) by adding a new router-item or the code of a previously used router-item in section Administration → Device management. The registration process may take several seconds; you can Reload the page to check the process. If there is no progressing screen or the router cannot be registered even if you have internet connection (can be tested via Ping) please contact support (u-link-support@weidmueller.com).

	Note If a Router activation code was already in use before, you must release it for additional activation in the u-link Portal Administration → Device Management → select the specific device → edit Activation code of the device → use “release for additional activation” and close the window.

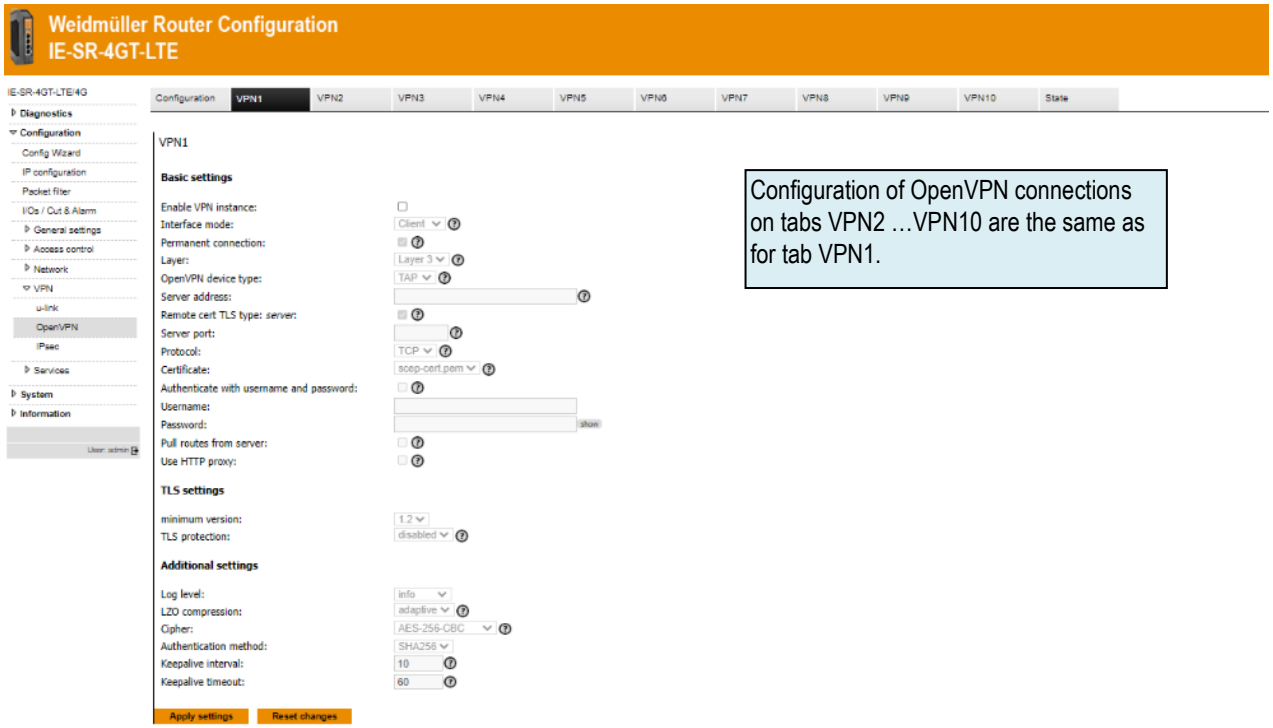
VPN→ OpenVPN (Tab Configuration)



Menu	Configuration → VPN → OpenVPN → Tab „Configuration“

Function	The OpenVPN menu allows to create and establish virtual private network connections based on the Open-VPN implementation. The Router can be configured both as OpenVPN client and OpenVPN server either based on Layer 2 (Bridging) or on Layer 3 (Routing). A maximum of 10 OpenVPN connections (either as client or as server) can be configured and started at the same time. Each VPN connection can be configured individually at Tab's VPN1…VPN10. Note: OpenVPN connections can only be used with encryption based on certificates. On each configured OpenVPN server connection theoretically any number of remote Open-VPN clients can be connected (only limited by the hardware performance of the Router). After configuration of OpenVPN sessions the configured connected will be displayed at a glance in this menu.	
	VPN LED/output controller	Disabled: The LED and digital output are not used by u-link u-link: LED is blinking during connecting and on during connection, digital output is triggered by u-link
	Polarity of digital input (VPN initiate)	rising edge: VPN is triggered by rising edge of input voltage (from 0 V to 24 V) falling edge VPN is triggered by falling edge of input voltage (from 24 V to 0 V)

VPN→ OpenVPN (Tab VPN1)

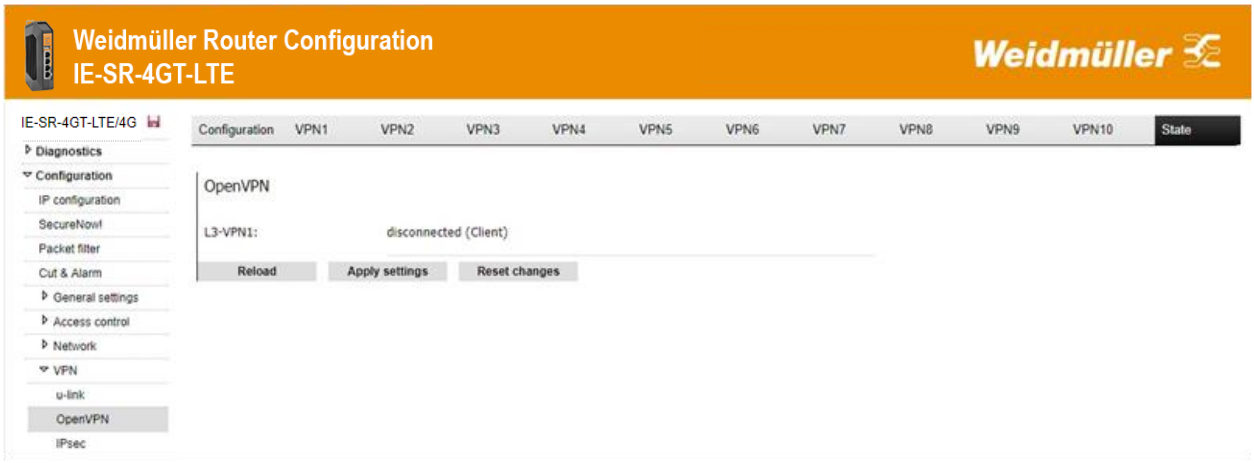


Menu	Configuration → VPN → OpenVPN → Tab „VPN1“	
Function	Screenshot of a configured OpenVPN-Client at tab VPN1	
	Enable VPN instance	Activates this OpenVPN connection
	Interface Mode	Select the connection mode which is either Server or Client Server: The device will run a TCP/UDP server which numerous clients can connect to Client: The device will establish a connection to an OpenVPN server

	Permanent connection	If enabled on a server instance the server will always be up. In enabled on a client instance, the client will try to connect if the connection gets lost. If not enabled the connection can be switched on using the VPN key, CUT or ALARM triggers, Modbus TCP or API.
	Layer	The OpenVPN interface may operate on two different layers: Ethernet Layer (Layer 2), i.e. will be bridged with >LAN (interface)< IP Layer (Layer 3) with its own IP address which must be configured on the IP configuration page.
	OpenVPN device type	L3 interfaces can either be run as TUN or TAP devices. The letter is default on the device type. TUN connections will always use the OpenVPN topology subnet. If subnets behind clients shall be reachable in TUN mode, there are route entries required in the OpenVPN server configuration. These entries will be available only if the routes to the subnets are configured in the client configuration table on the server. Note: Each VPN endpoint must use the same setting on this option.
	Server address	The remote server address can either be a DNS name or an IP address
	Remote cert TLS type: server:	Ensures that the certificate of the server possesses the TLS properties of a server certificate. This option helps preventing Man-in-the-Middle attacks.
	Server Port	TCP/UDP port number e.g. 1194. If a server instance is enabled on TCP Port 443 the HTTPS web server must be disabled manually at the page Configuration → Services → Web server. A potentially configured access restriction for the web server will limit access to the OpenVPN server in this case! Each OpenVPN server instance must use a unique TCP/UDP port!
	Protocol	Transport protocol of this VPN connection. UDP has a slightly better performance and stability but cannot be handled by HTTP proxies and some 4G provides block UDP tunnels. TCP is the default on this device type.
	Certificate	Select certificate for authentication at remote peer. Note: New certificates can be uploaded in Configuration → General settings → Certificates. Please note that certificates which have extended key usage (EKU) fields can only be used as server certificate (EKU TLS Web Server Authentication) or as client certificate (EKU Web Client Authentication). Each client connected to one server and the server itself must use a certificate from the same Certification Authority (CA).
	Client configuration and authentication	Select possible configuration and authentication methods. **IP Address Pool:** Authenticates clients based on their certificates and assigns IP addresses from a defined local pool. The IP Range for an IP address assignment mut be within the IP subnet of the VPN interface and must not be used already by any other interface. **RADIUS Server:** The router sends OpenVPN client credentials to the RADIUS server for authentication, which returns approval, user-specific settings (e.g., IP addresses, policies), or denial. **Configuration table:** In this mode, the router references a local table to match each client's certificate and applies the defined IP, routes, and access settings for authenticated connections.

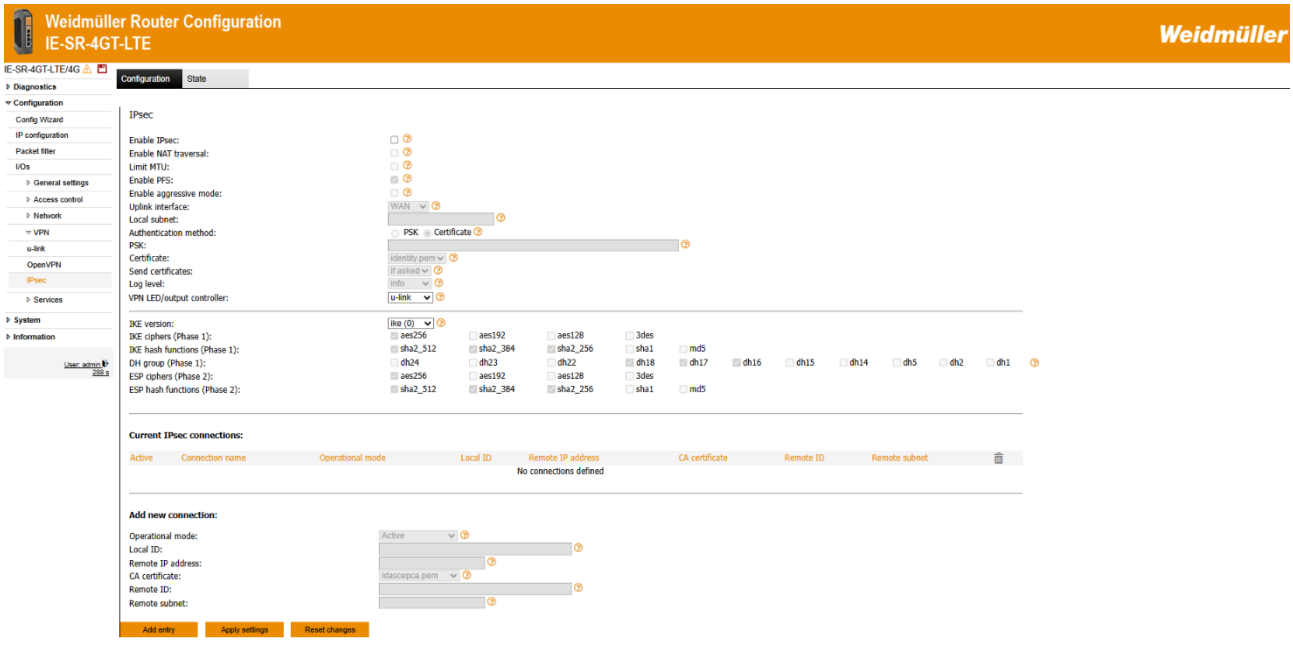
	Allow client-to-client communication	OpenVPN client-to-client blocks or allows all traffic between clients connected to one server.
	Authentication with username and password	Enable additional authentication with username and password
	Pull routes from server	The OpenVPN option “pull” will pull the routes from the server if it pushes them.
	Use HTTP proxy	OpenVPN TCP clients can use a HTTP proxy for tunneling the VPN connection. To the proxy the traffic will look like HTTPS web traffic. The system wide HTTP proxy must be configured under Configuration → Network → HTTP proxy
	TLS minimum version	Minimum TLS version needed for certificate check.
	TLS protection	Add an additional layer of HMAC authentication on top of the TLS control. Available options are tls-auth, tls-crypt or disabled. Regarding tls-auth the OpenVPN direction parameter with the value 0 is used when a server is configured or the value 1 is used when configuring a client.
	Log level	None: Will log no messages through the Event Log Info: Log only some information and critical errors Debug: Log state information too Verbose: Log all possible messages
	LZO compression	Sets the OpenVPN LZO option for all connections. No: Is the default on this device type. Do not use compression. Yes: Always enable LZO compression Adaptive: Use an adaptive algorithm to dynamically detect if compression is useful or not Note: Each OpenVPN endpoint must use the same setting on this option.
	Cipher	Select the OpenVPN cipher to use. BF-CBC is the default cipher. Each OpenVPN endpoint must use the same cipher! You can use none for performance critical layer 2 tunnels or intranets.
	Authentication method	Set an authentication method for this VPN using different algorithms like SHA256, SH512 or MD5.
	Keep alive interval	Ping messages will be sent in a set time interval to avoid a timeout of the connection.
	Keep alive timeout	Checks if there is traffic in a set time interval. Restarts VPN when there is no traffic.

VPN→ OpenVPN (Tab State)



Menu	Configuration → VPN → OpenVPN → Tab „State“
Function	Displays the status of configured and activated OpenVPN instances (1…10) and whether they are connected or disconnected

VPN→ IPsec (Tab Configuration)



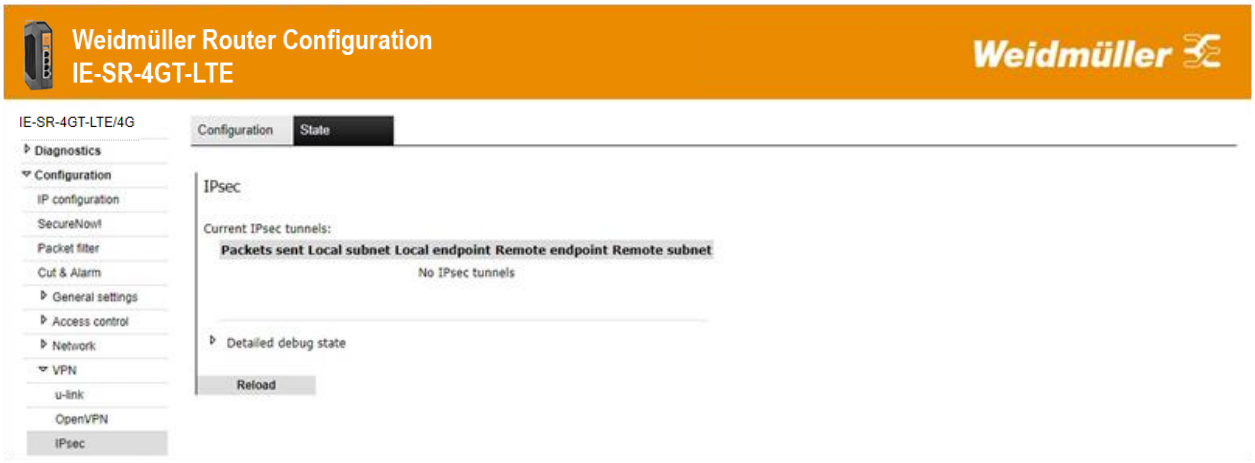
Menu	Configuration → VPN → IPsec → Tab „Configuration“
Func-tion	The IPsec menu allows to create and establish virtual private network connections based on the standard IPsec implementation. The Router can be configured both as IPsec client and IPsec server. IPsec allows the encryption of the complete communication flow between the Router and a remote site on IP level. IPsec provides encryption of subnets, which are located behind the respective VPN peers. IPsec connections can be used with both PSK encryption (pre-shared key using user name and password) as well as certificate based encryption.

	Enable NAT traversal	NAT traversal is required when a router between the local and remote side does Network Address Translation (NAT) Note: IPsec pass through will break NAT traversal! If your router supports it, you must disable IPsec pass through!
	Limit MTU	NAT traversal requires encapsulation of IP packets which possibly increases fragmentation leading to less network performance. If this happens it may help to slightly reduce the size of outgoing packets (MTU).
	Enable PFS	With Perfect Forward Security (PFS) a session key (signed by the private key) is used to encrypt the data instead of the private key itself. This session key will be renewed after relatively short time. Thus, even if the private key (certificate) gets compromised previous communication cannot be decrypted by someone else since the temporary session keys cannot be restored. Therefore, PFS further increased security.
	Enable aggressive mode	Enables IPsec aggressive mode
	Uplink interface	The uplink interface on which the IPsec tunnel is supposed to be established.
	Local next hop	To reach the remote site, it may be possible that IPsec needs to explicitly know the IP address or hostname of the next router. For example, this can be the router that connects you LAN with the internet.
	Use default route	Use the default gateway (either set manually or by a DSL connection) as next hop.
	Local Subnet	This is the local subnet which its traffic to the remote subnet is supposed to be encrypted when going out via the given interface. The subnet must be defined as IP/Network mask, e.g. 192.168.0.0/24. If no subnet is given, the IP address of the interface itself is used. Note: The local and remote subnet must not be equal! Note: Routed traffic is not generally encrypted! Only traffic between exactly the local and the remote network gets encrypted! For instance, if you use two Weidmüller Security Routers and leave both subnets empty the IPsec tunnel will be stablished between two routers. Then only traffic originated from one router destined to the other router is encrypted. The traffic that is routed via both devices from networks behind them is not encrypted at all.
	Authentication method	Either use a pre-shared key (PSK) or a certificate for authentication. Using certificates is recommended since it is much more secure than using PSKs.
	PSK	This is the pre-shared key (must be equal on both sides) Note: Do not use simple words or phrases! A PSK should be a random sequence of 48 characters in base64 format.
	Certificate	This certificate is sent to the remote peer to authenticate on site. New certificates can be uploaded in Configuration → General setting → Certificates
	Send certificates	For security reasons certificates are usually only send on demand. However, this breaks compatibility with some vendors, such as Cisco and Safenet. Set this option to always in this case.

	Log level	None: Will log no messages through the Event Log Info: Log only some information and critical errors Debug: Log state information too Verbose: Log all possible messages
	VPN LED/output controller	The selected device controls the state of the VPN LED and of the digital VPN output.
	IKE version	IKE major version to use for connection (ikev1 (1) uses IKEv1 known as ISAKMP, ikev2 (2) uses IKEv2. A connection using ike (0) accepts both IKEv1 and IKEv2 as responder, and initiates the connection actively with IKEv2.)
	IKE ciphers (Phase 1)	Select the cipher suites for Internet Key Exchange (IKE) this connection will support
	IKE hash functions (Phase 1)	Select the hash functions for Internet Key Exchange (IKE) this connection will support
	DH group (Phase 1)	Select the Diffie-Hellmann Groups for Internet Key Exchange (IKE) this connection will support
	ESP ciphers (Phase 2)	Select the cipher suites for Encapsulating Security Payload (ESP), this connection will support
	ESP hash functions (Phase 2)	Select the hash functions for Encapsulating Security Payload (ESP), this connection will support
	Operational mode	Operational mode of the local side: Active: Try to establish the connection immediately and periodically retry. This is the normal mode. Active (switched): Connection setup is triggered by VPN initiate. Passive: Do not try to establish a connection but wait until a peer attempts to do so. This mode is required to allow connections with an unknown remote IP address (road warrior setup).
	Local ID	This is the name the device will use to identify (not authenticate) itself for a PSK connection. If a certificate is used the ID is always the certificate info. If no ID is given the IP address will be used. Entering the IP address is not the same as leaving the field empty! Blanks are not allowed.
	Remote IP address	This is the IP address or the hostname of the remote IPsec peer. Use “*” to indicate that the remote IP is dynamic and not known in advance. This does only make sense for the operational mode Passive (to wait for the peer to connect). If the subnet is also set to “*” this defines a so-called road warrior setup where e.g. a travelling may connect. While affixed subnet only allows one remote IPsec peer, any number of road warriors may connect (e.g. several laptops at different locations can connect to the companies’ network).
	CA certificate	The remote peer its certificate must have been signed by this CA to be accepted

	Remote ID	The peer will identify (not authenticate) itself with this ID depending on the chose authentication method. PSK: If no remote id is given the IP address of the remote site is checked. Entering the IP address is not the same as leaving the field empty! The remote ID must not contain blanks. Certificate: The complete certificate info of the peer must be specified. In case of another Weidmüller Security Router you can copy and paste the certificate info (C=… ST=…) from its certificates page. The order of info elements C, ST, L, O, OU, CN, E must be kept and all elements separated by a comma followed by a blank. Note: The remote ID must match exactly except when you are waiting for road warriors using certificates. Then also all fields must be present but "*" may be used as wild card (e.g. CN=*). For a road warrior setup with PSK no ids should be used. Note: The remote ID should be unique. If several connections share the same ID their tunnels will get periodically build up and torn down (traffic with interruptions is possible though).
	Remote subnet	This is the remote subnet to which the traffic coming from the local subnet is encrypted when going out via the given interface. The subnet must be defined as IP/Network mask, e.g. 192.168.0.0/24. If no subnet is given, the IP address of the interface itself is used. Note: The local and remote subnet must not be equal! Note: Routed traffic is not generally encrypted! Only traffic between exactly the local and the remote network gets encrypted! For instance, if you use two Weidmüller Security Routers and leave both subnets empty the IPsec tunnel will be established between two routers. Then only traffic originated from one router destined to the other router is encrypted. The traffic that is routed via both devices from networks behind them is not encrypted at all.

VPN→ IPsec (Tab State)



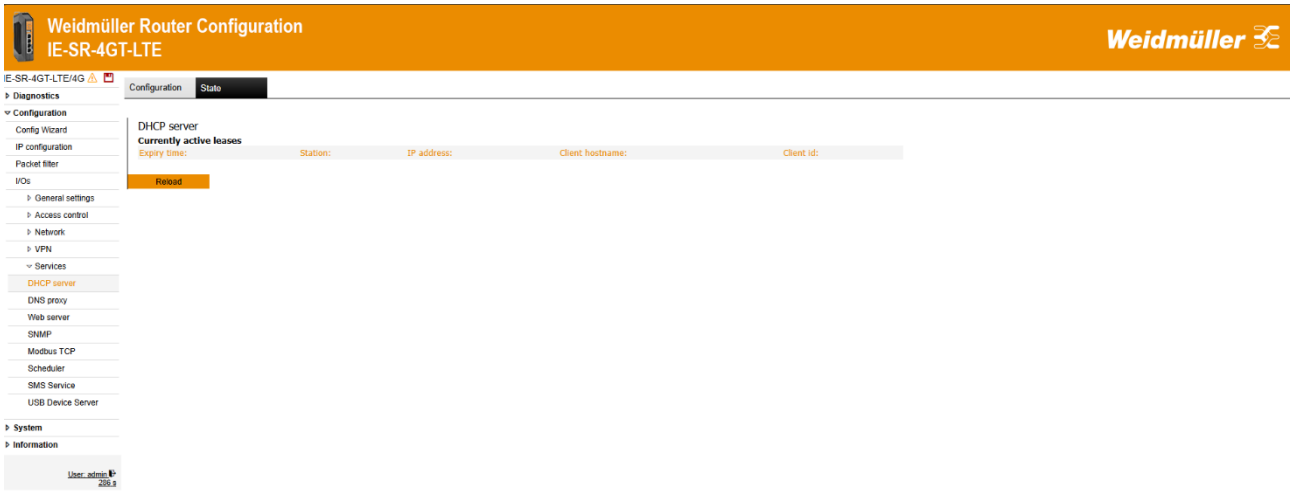
Menu	Configuration → VPN → IPsec → Tab „State“
Function	Displays all IPsec tunnels and their state

4.2.9 Configuration → Services

Services → DHCP Server (Tab Configuration)

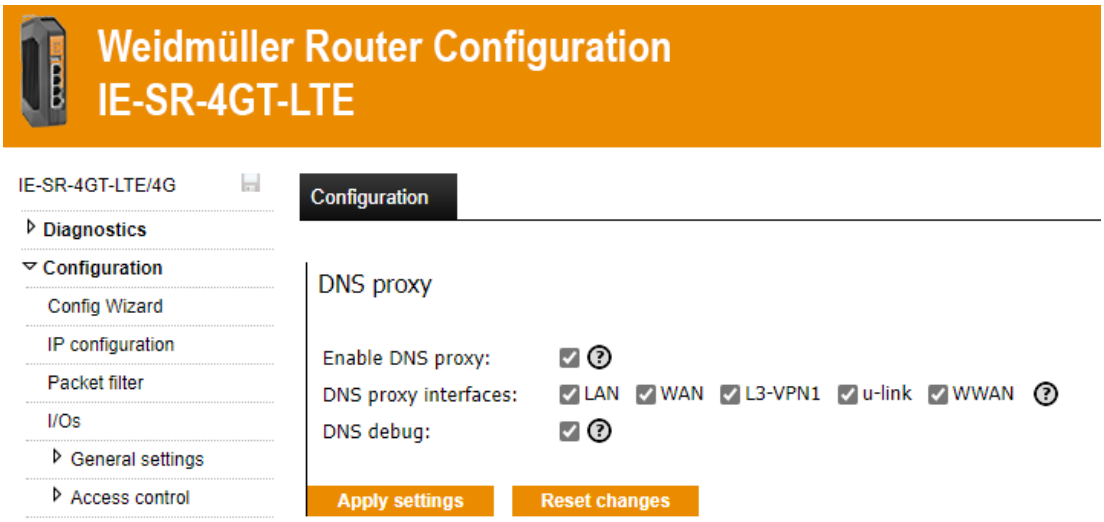
Menu	Configuration → Services → DHCP Server → Tab “Configuration”	
Function	In operating mode "IP Router", the built-in DHCP server can be used for allocating IP addresses on both LAN-side and WAN side. By default, the DHCP server is switched off.	
	Enable DHCP server	Enables the DHCP service. The device will answer to DHCP requests on the selected interfaces with the supplied IP address range and name server configuration. **Note:** The IP address range must be in the same IP subnet as the IP of the selected interface itself.
	DHCP Debugging	Enables the detailed logs for all DHCP requests and responses in the eventlog.
	On following interfaces	Select the Interfaces that should use DHCP server or relay. Displayed interfaces depending on routing mode, integrated modem and virtual interfaces.
	Starting IP address	First IP address that can be assigned via DHCP
	Ending IP address	Last IP address that can be assigned via DHCP Note: Must be in the same IP subnet as Starting IP address.
	DHCP lease time	Value between 3.000 s and 700.000 s

Services → DHCP Server (Tab State)



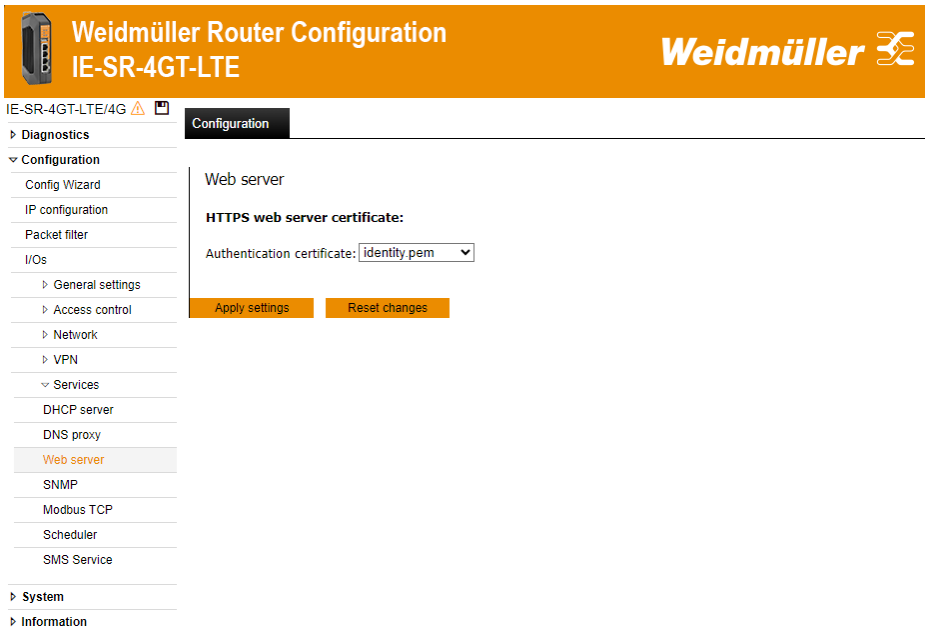
Menu	Configuration → Services → DHCP Server → Tab “State”
Function	Displays all DHCP clients of the device

Services → DNS Proxy



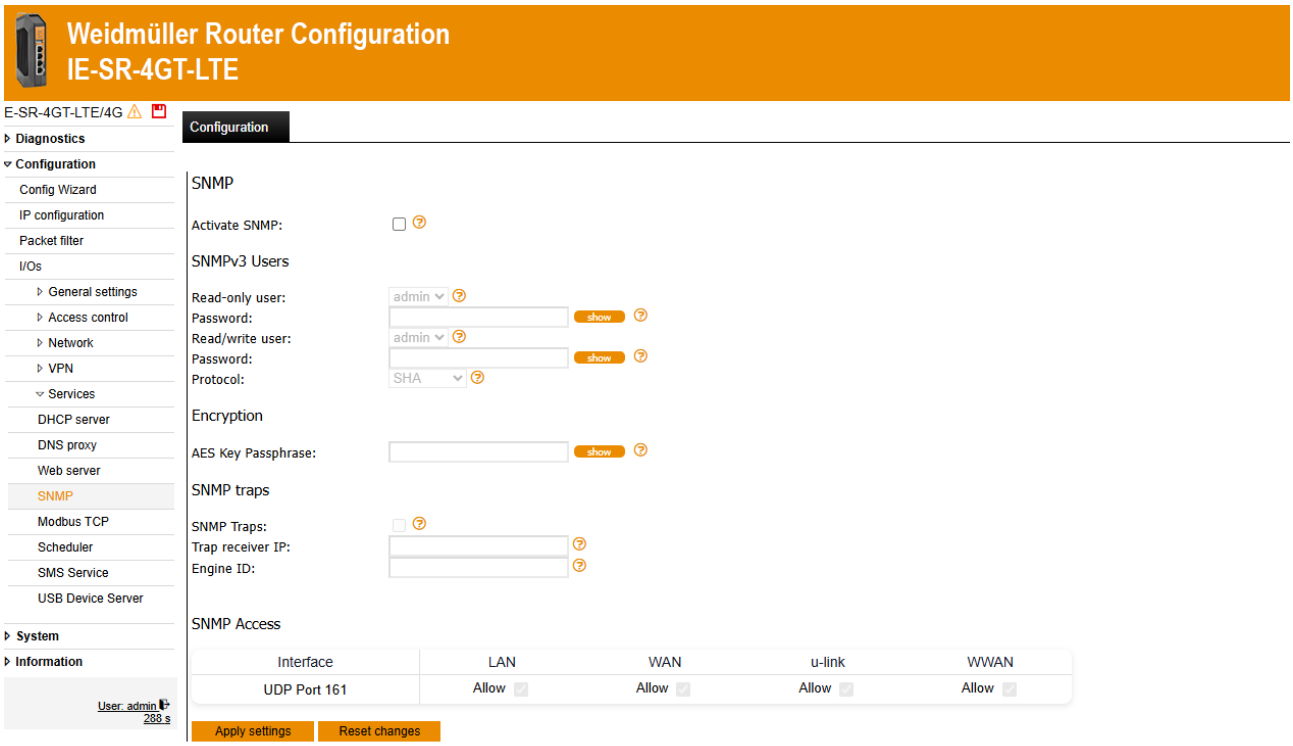
Menu	Configuration → Services → DNS proxy
Function	The router acts as a DNS server on the chosen interfaces and will forward DNS requests to the configured DNS servers. This feature is required if you want to use host or domain names in the packet filter (firewall).

Services → Web server



Menu	Configuration → Services → Web server
Function	Via this menu item the access protocol to the Web interface (http or https) can be configured.

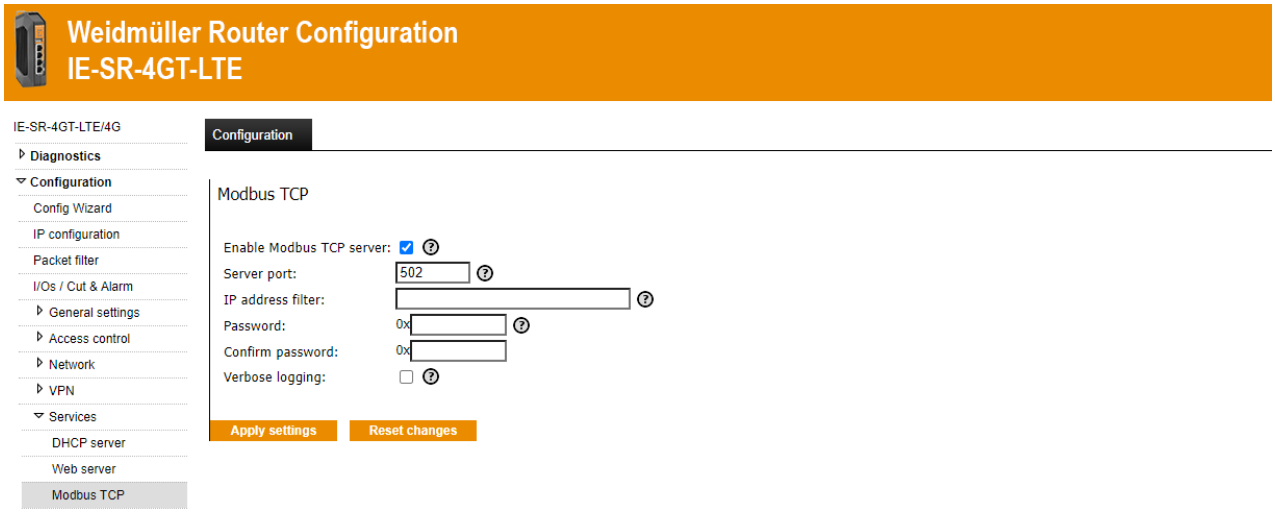
Services → SNMP



Menu	Configuration → Services → SNMP	
Function	Activation / deactivation of the SNMP protocol (Simple Network Management Protocol). Only Version v3 is supported due to security reasons. Router data can be requested using Standard MIB-II.	
	Activate SNMP	Enable the SNMPv3 interface
	Read-only user	Select a user account from the available users which shall be used for the SNMP read service.
	Password	Password for SNMPv3 read only access. More than 8 alphanumerical characters required. Please note that this password is a service password for the SNMP service and not the password for the management interface. The management interface password policy will not be applied. Please use a secure password according to your threat model and risk.
	Read/write user	Select a user account from the available users which shall be used for the SNMP read/write service.
	Password	Password for SNMPv3 read/write access. More than 8 alphanumerical characters required. Please note that this password is a service password for the SNMP service and not the password for the management interface. The management interface password policy will not be applied. Please use a secure password according to your threat model and risk.
	Protocol	Authentication protocol for SNMPv3. It is recommended to use the newer SHA variants (SHA-224, SHA-256, SHA-384, SHA-512) instead of MD5 or SHA, which should only be used if legacy clients do not support the newer algorithms.
	AES Key Passphrase	SNMPv3 Pre-shared key for encryption. Privacy protocol: AES.

	SNMP Traps	Activate the SNMP trap generation subsystem. The read-only user is used for SNMP traps. Traps are sent as SNMPv3 traps with the configured encryption, engine ID and authentication settings.
	Trap receiver IP	Hostname or IP address of the server where the SNMP trap will be send to.
	Engine ID	If left empty the system will generate a unique ID by itself. User specified values must start with 0x and contain 5-64 hex digits.

Services → Modbus TCP



Menu	Configuration → Services → Modbus TCP	
Function	Activation/deactivation of the integrated Modbus TCP-Server. Allows external Ethernet controllers that understand the Modbus TCP protocol to query Router states and control information. Using the Modbus TCP protocol e.g. VPN connections (u-link, IPsec and OpenVPN) can be activated and deactivated. Additionally events like „Cut“ or „Alarm“ can be monitored and reset (acknowledged).	
	Server port:	You can specify the port used by the server to listen for incoming requests. If no port is given the default Modbus port 502 is used.
	IP address filter	Only one connection at a time is allowed. You can specify an IP address or host name to restrict access to one client. If no address is given any client may connect.
	Password	You can specify an eight digit long hexadecimal password (e.g. 0x1a2b3c4d). If not empty and not zero a newly connected client must set the high (first four digits) and low (last four digits) password register correctly before it is allowed to access any other register.
	Verbose logging	By default, only access violations are logged (if client IP address is restricted or a password is required). With this option information about connections, requests and processing time is also logged.

General information about implemented ModbusTCP functionality:

1. ModbusTCP server is running as a ModbusTCP slave.
2. Via the ModbusTCP protocol only following settings and status requests can be done:
   - Monitor, start and stop pre-defined VPN connections (IPsec, OpenVPN, u-link)
   - Acknowledge/Reset of CUT& ALARM
3. The server port can be selected freely. If no port is specified, the default port for ModbusTCP (502) waits for incoming requests.
4. The access can be restricted to a specific ModbusTCP Master by specifying either an IP address or as a host name that is resolved when the server is started. If nothing is specified, the connection can be established from any device (ModbusTCP Master).
5. To increase security, a 32-bit password can be specified. Before a Master can access status and control registers, it must write the password into the password registers. The higher-value 16 bits in

register 0x01 and the lower-value 16 bits in register 0x02. If no password is specified, all registers can be accessed directly.

6. To keep the event log from overfilling, only access violations (if the IP address is restricted or if a password is requested) are normally reported. If checkbox “Verbose logging” is activated, additional information on connection establishment, requests and access times is also logged.

Important information:

a. The password is checked when the lower-value part is written in register 0x02. For example, if the password is 0xaa11bb22, 0xaa11 must first be written in register 0x01 and then 0xbb22 written in register 0x02. The password is valid for the duration of the TCP connection. If a new connection is established, the password registers are reset to 0x0000.
b. If a host name is used for restricting the Modbus Master address, this name is resolved into an IP address when the server is started, i.e., not when the actual connection is established. Thus, if the meaning of a host name changes, ModbusTCP must be restarted.

Modbus/TCP implementation

The slave ID / device ID can be set between 1 and 254.
The following function codes can be processed by the Router:

- 0x03 (Read Holding Registers – read status/control registers)
- 0x10 (Write Multiple Registers – write one or more control registers)

F.or a register that has been read, bit 0 stands for the least significant bit and bit 15 stands for the most significant bit of the register.

If an error occurs while processing a request, the following exception codes will be returned:

Exception code	Meaning	Description
0x01	Invalid function code	Neither 0x03, nor 0x04, nor 0x10 was used as function code.
0x02	Invalid register	Either the register does not exist or the desired operation cannot be performed.
0x03	Invalid register value	The value to be written is invalid for the register.
0x04	Internal server error	An internal error occurred during the processing of the request

Note: The implementation is not time-optimized. For example, it can take approximately 10 seconds to establish an OpenVPN connection. It can take approximately 5 seconds to read out all status registers in one request. A ModbusTCP response from the router takes a corresponding length of time. For performance reasons, the requests must not take place too quickly (in particular, the status should not be queried more than once per minute and should be limited to the necessary registers) and the time-outs of the requester must be long enough. Furthermore, only one ModbusTCP master can be connected to the Router at a time.

Overview Modbus Register

Registers	**Hex code**	**Data**
General registers:	0x00	Version
	0x01	PASSWORD - higher-value 16 bits
	0x02	PASSWORD - lower-value 16 bits
Status registers:	0x10	CUT&ALARM
	0x11	Not used
	0x12	reserved
	0x13	IPsec
	0x14	OpenVPN1
	0x15	OpenVPN2
	….	…
	0x1D	OpenVPN10
	0x1E	u-link VPN
Status registers:	0x20	CUT&ALARM
	0x21	Not used

	0x22	reserved
	0x23	IPsec
	0x24	OpenVPN1
	0x25	OpenVPN2
	….	…
	0x2D	OpenVPN10
	0x2E	u-link VPN

Status registers:	Read-only and cannot be written. The content is similar for all connection-specific status registers
Bit 0	contains information indicating whether the connection is defined at all, i.e., whether the entry exists or the service is activated.
Bit 1	contains information indicating whether the connection has been activated.
Bit 2	contains information indicating whether the connection exists.
Other Bits	The other bits indicate type-specific information.

Control registers:	Can be read and written
	If the corresponding service of a connection-specific register is not active or cannot be configured, each write attempt is invalid and exception code 0x02 (invalid register) is returned. Independent of the success of an action triggered by writing a control register, the value is written in the control register and can be read out. The actual status of the corresponding service must be queried from its status register.

General registers (Version and Password)

0x0100	Version	Read-only	The higher-value byte is the major version number and the lower value byte is the minor version number.
0x01 and 0x02	Password	Read / Write	Register 0x01 contains the higher-value 16 bits, register 0x02 the lower-value 16 bits of the 32-bit password. If a password is requested, it must be entered correctly before status and control registers can be accessed. Password verification is performed as soon as register 0x02 is written (thus, register 0x01 must be set first). The password is valid for the entire duration of the TCP connection. The next time a connection is established, the contents of both registers are reset to zero.

Registers CUT&ALARM

0x10 (Status)	Read-Only	Bits	Meaning	Explanation
		0	Alarm	0=Alarm off, 1=Alarm on
		1	Internal CUT	0=Cut off, 1=Cut on
		2	External CUT	0=Cut off, 1=Cut on (24VDC)
		3-15	Not used	
0x20 (Set)	Read / Write	The register can be written with value 0x0000 to acknowledge/ reset ALARM and internal CUT. 0x0000 is the only allowed value. The external CUT cannot be reset in this way because it is an external digital input and depends on input settings (0 or 24 VDC).		

Registers IPsec

0x13 (Status)	Read-Only	Bits	Meaning	Explanation
		0	IPSec defined	At least one connection is defined
		1	Activated	IPsec generally is activated (Enabled)
		2	Connected	At least one tunnel is established
		3-15	Not used	
0x23 (Set)	Read/Write	This register can be written either with values:		
		0x0000		Deactivate all defined IPsec connections
		0x0001		Activate all defined IPsec connections

Registers OpenVPN

OpenVPN-1

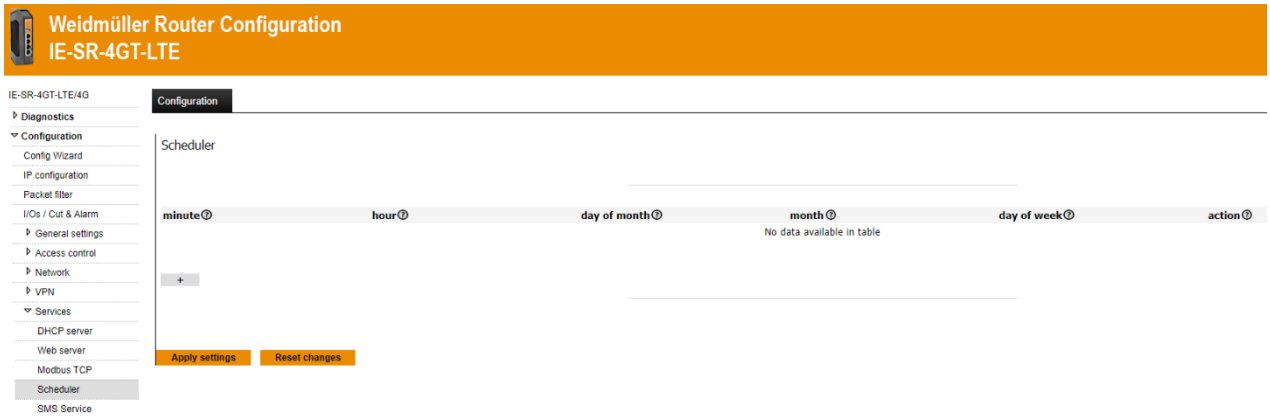
0x14 (Status)	Read-Only	Bits	Meaning	Explanation
		0	Instance defined	0=not defined; 1=defined
		1	Activated	**OpenVPN-1** is activated (Enabled)
		2	Connected	**OpenVPN-1** tunnel is established
		3	Server/Client	0=configured as OpenVPN-Client 1=configured as OpenVPN-Server
		4-7	Not used	
		8-15	Active tunnel	Number of currently OpenVPN clients (if configured as OpenVPN server)
0x24 (Set)	Read/Write	This register can be written either with values:		
		0x0000		Deactivate defined **OpenVPN-1** connection
		0x0001		Activate defined **OpenVPN-1** connection

OpenVPN-2:	0x15 (Status)	Read-Only	→ see OpenVPN-1
	0x25 (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-3	0x16 (Status)	Read-Only	→ see OpenVPN-1
	0x26 (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-4	0x17 (Status)	Read-Only	→ see OpenVPN-1
	0x27 (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-5	0x18 (Status)	Read-Only	→ see OpenVPN-1
	0x28 (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-6	0x19 (Status)	Read-Only	→ see OpenVPN-1
	0x29 (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-7	0x1A (Status)	Read-Only	→ see OpenVPN-1
	0x2A (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-8	0x1B (Status)	Read-Only	→ see OpenVPN-1
	0x2B (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-9	0x1C (Status)	Read-Only	→ see OpenVPN-1
	0x2C (Set)	Read / Write	→ see OpenVPN-1
OpenVPN-10	0x1D (Status)	Read-Only	→ see OpenVPN-1
	0x2D (Set)	Read / Write	→ see OpenVPN-1

Register u-link

0x1E (Status)	Read-Only	Bits	Meaning	Explanation
		0	WWH-Status	0=WWH offline 1=WWH online
		1	Activated	**u-link instance** is activated (Enabled)
		2	Connected	**u-link VPN** tunnel is established
		4	Not used	
		5	Connection activated	The connection is established/ being established
		6-16	Not used	
0x2E (Set)	Read/Write	This register can be written either with values:		
		0x0000		Deactivate **u-link VPN** tunnel
		0x0001		Establish **u-link VPN** tunnel

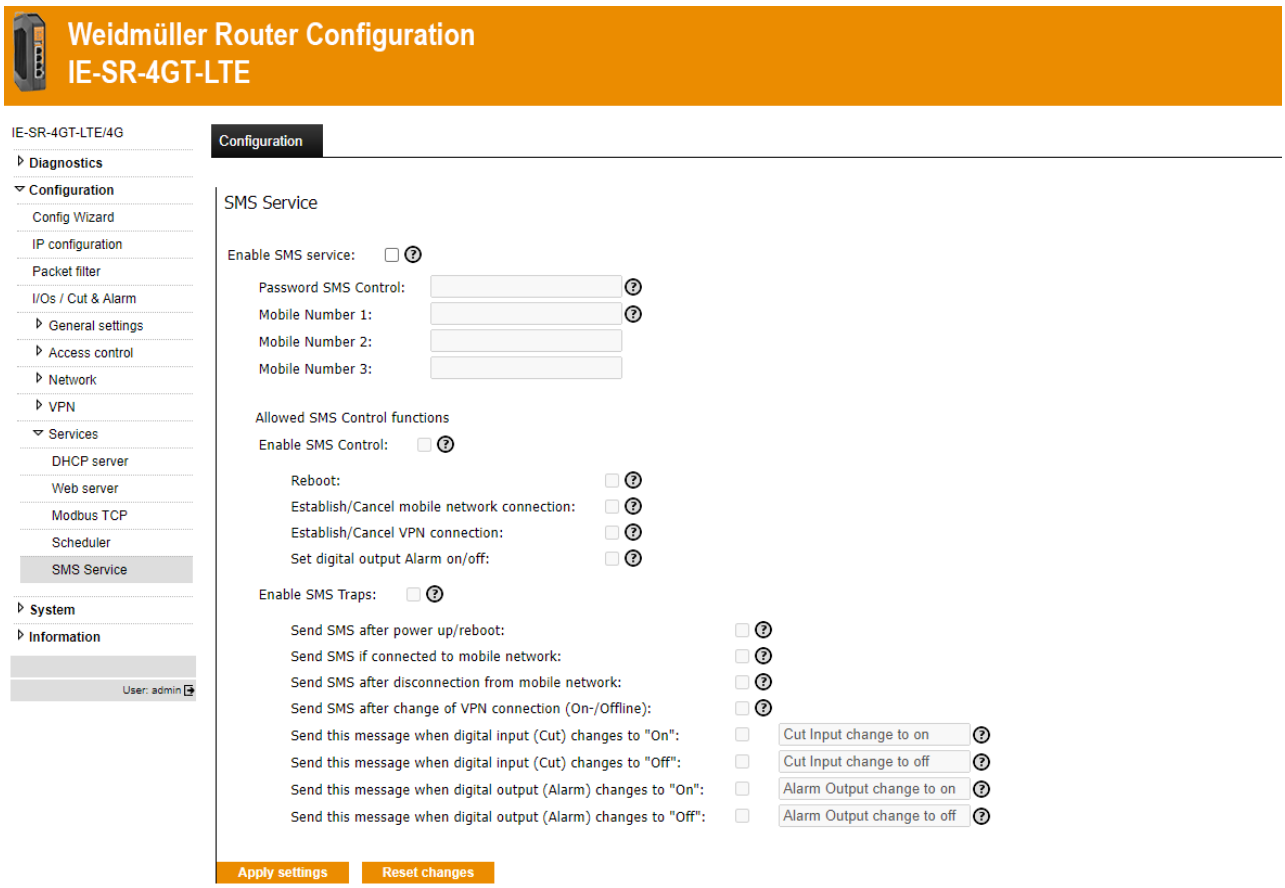
Services → Scheduler



Menu	Configuration → Services → Scheduler
Function	A time can be selected at which the router is rebooting regularly and automatically.

Services → SMS Service

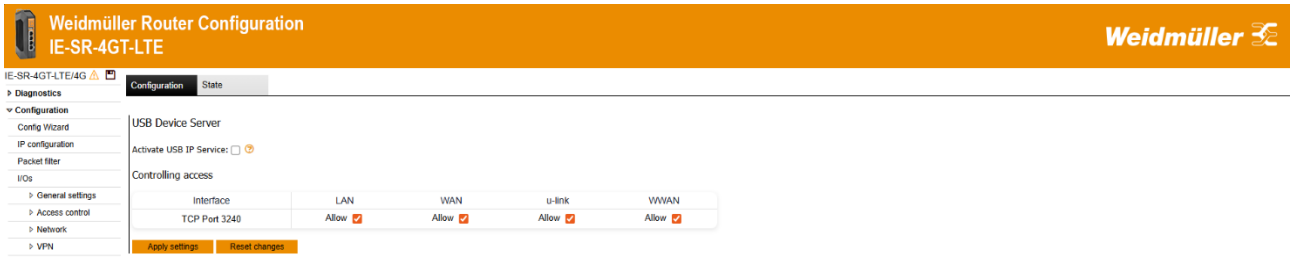
<u>Important note</u>: The SMS Service function is only available for the "IE-SR-4TX-LTE/4G-USEMEA" router (2873930000) or with firmware version 1.3.7 and newer for the "IE-SR-4GT-LTE/4G-EU" router (2873920000).



Menu	Configuration → Services → SMS Service	
Functions	Router sends information via SMS messages (output). Router can be controlled via SMS messages (input). Menu available for LTE/4G-version only.	
	Enable SMS service	Enables or disables generally the use of text messages for control functions (SMS input) and sending information (SMS output).
	Password SMS Control	If a password is entered then each incoming SMS control message must be secured by this password. Otherwise received text message will be dropped. Format of a password-secured SMS control message: #<password>?<command> Examples: #Detmold?reboot or #Detmold?OutputAlarm=on Note: The password is case sensitive, the command is NOT case sensitive.
	Mobile number 1 - 3	Only defined mobile numbers may send SMS control messages to the router and can receive information messages (SMS traps) from the router. For using SMS services at least one mobile number has to be configured. (Use international format +xxxyyyyyyyyyyy).
	Enable SMS Control	Allows or denies generally the use of text messages for control functions (SMS input).
	Reboot	Allows/denies a device reboot via SMS command. Commands: *#password?reboot* or *?reboot* if no password is set. Note: For feedback about a successful reboot please activate SMS trap “Send SMS after power up / reboot”.
	Establish/Cancel mobile network connection	Allows/denies establishing or cancel the Internet connection of the mobile interface via SMS command. Commands: *#password?MobileConnection=on/off* or *?MobileConnection=on/off* if no password is set. Note: For feedback about the required action please activate the related SMS traps (mobile network connection/disconnection).
	Establish/Cancel VPN connection	Allows/denies establishing or cancel a predefined VPN connection (OpenVPN1 - 10, IPsecVPN or u-linkVPN) via SMS command. Commands: *#password?OpenVPN1=on/off* or *?OpenVPN1=on/off* or *#password?u-linkVPN=on/off* or *?IPsecVPN=on/off* if no password is set). Note: For feedback about the required action please activate the related SMS trap “Send SMS after change of VPN connection (On-/Offline)”.
	Set digital output ‘Alarm# on/off	Allows/denies setting the digital output (Alarm) on or off via SMS command Command: *#password?OutputAlarm=on/off* or *?OutputAlarm=on/off* if no password is set. Note: For feedback about the required action please activate the SMS traps related to the digital output (Alarm).

	Enable SMS Traps	Enables/disables the sending of SMS traps. Note: SMS traps only will be sent to the defined mobile numbers 1 - 3.
	Trap: Send SMS after power up/reboot.	If enabled the message *<system name>: Reboot/Power Up at <system time>* will be sent to the defined mobile numbers 1-3 after reboot or power-up.
	Trap: Send SMS if connected to mobile network.	If enabled the message <System-Name>: Connected to <provider>; <network mode>; <signal strength>; <IP> will be sent to the defined mobile numbers 1-3 after connection to the mobile internet.
	Trap: Send SMS after disconnection from mobile network.	If enabled the message *<system name>: Disconnected from mobile network at <system time>* will be sent to the defined mobile numbers 1-3 after disconnection from the mobile internet.
	Trap: Send SMS after change of VPN connection (On-/Offline).	If enabled the message *<system name>: OpenVPN1…10 / Ipsec-VPN / u-linkVPN established/disconnected* will be sent to the defined mobile numbers 1-3 after change of one of the defined VPN connections.
	Trap: Send this message when digital input (Cut) changes to "On".	If enabled the message *<system name>: <Entered text>* will be sent to the defined mobile numbers 1-3 after changing of digital input (Cut) to ON.
	Trap: Send this message when digital input (Cut) changes to "Off".	If enabled the message <system name>: <Entered text> will be sent to the defined mobile numbers 1-3 after changing of digital input (Cut) to OFF.
	Trap: Send this message when digital output (Alarm) changes to "On".	If enabled the message <system name>: <Entered text> will be sent to the defined mobile numbers 1-3 after changing of digital output (Alarm) to ON.
	Trap: Send this message when digital output (Alarm) changes to "OFF".	If enabled the message <system name>: <Entered text> will be sent to the fined mobile numbers 1-3 after changing of digital output (Alarm) to OFF.

Service → USB Device Server (Tab Configuration)



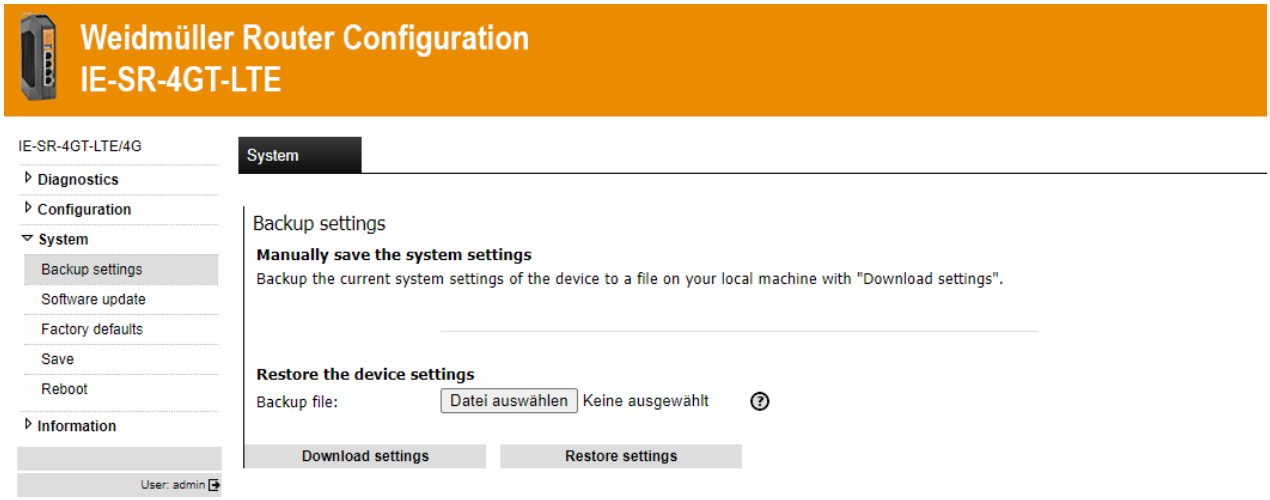
Menu	Configuration → Services → USB Device Server
Functions	This option activates the USB IP service. This enables remote access to USB devices over the network. The other available USB functions, such as firmware and configuration updates and storing logs via USB, are no longer available when the USB IP service is running.

Service → USB Device Server (Tab State)

Menu	Configuration → Services → USB Device Server
Function	Displays current state of the USB Device Server.

4.3 Section System

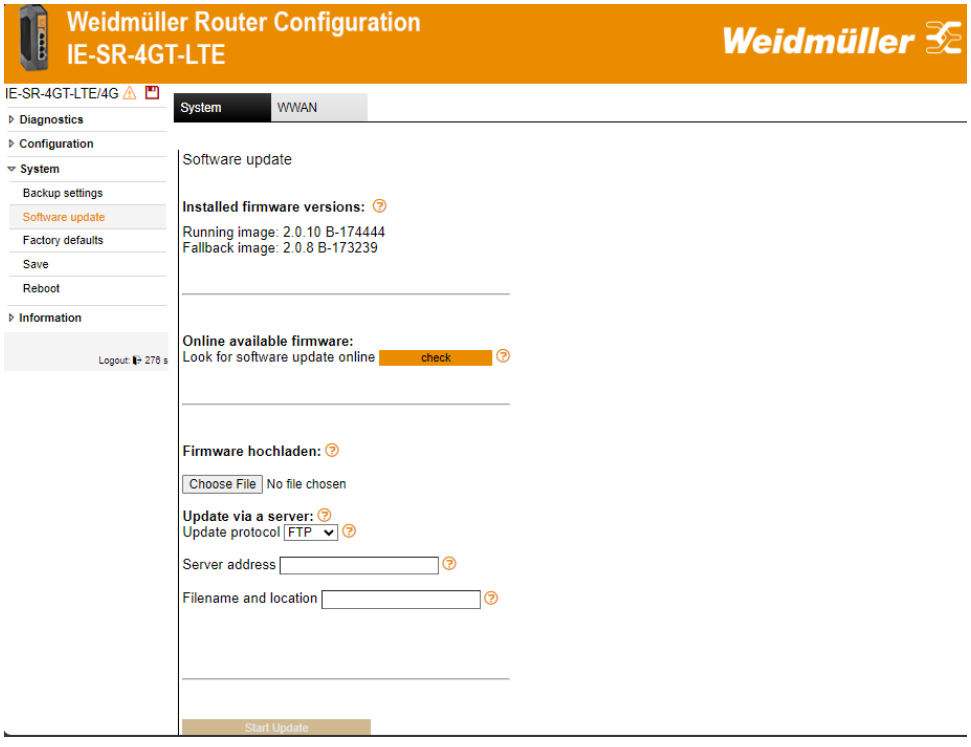
4.3.1 System → Backup settings



Menu	System → Backup settings
Function	With this menu item, the Router configuration can be stored or restored to/from the file system of the connected computer. The exported configuration file is of extension type <name>.cf2 and encrypted.

	Note
	For creating a configuration backup file (.cf2) always the configuration currently stored in the Flash memory will be used. Please save the configuration to Flash memory before creating a backup file.

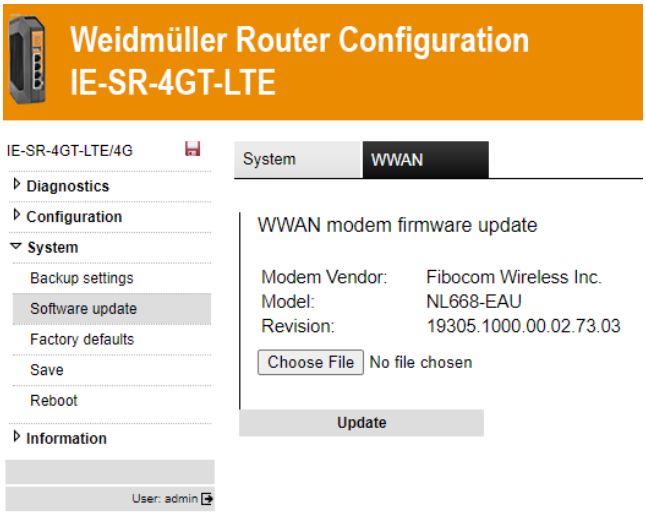
4.3.2 System → Software update



Menu	System → Software update	
Function	With this menu item a firmware update can be carried out. The Weidmüller Firmware for Security Routers can be used for all router models. It can be downloaded e.g. from the Weidmüller online catalog in section “Downloads” of the relevant product. With this action the Running image will become the Fallback image and the Fallback image will be deleted. **The easiest way to update the Router with a new firmware is to use the function „Update by browser upload“.**	
	Online available firmware	Connects to Weidmueller.de via HTTP or by using the u-link VPN to search for the latest firmware. The device must have a working Internet link for this feature to work.

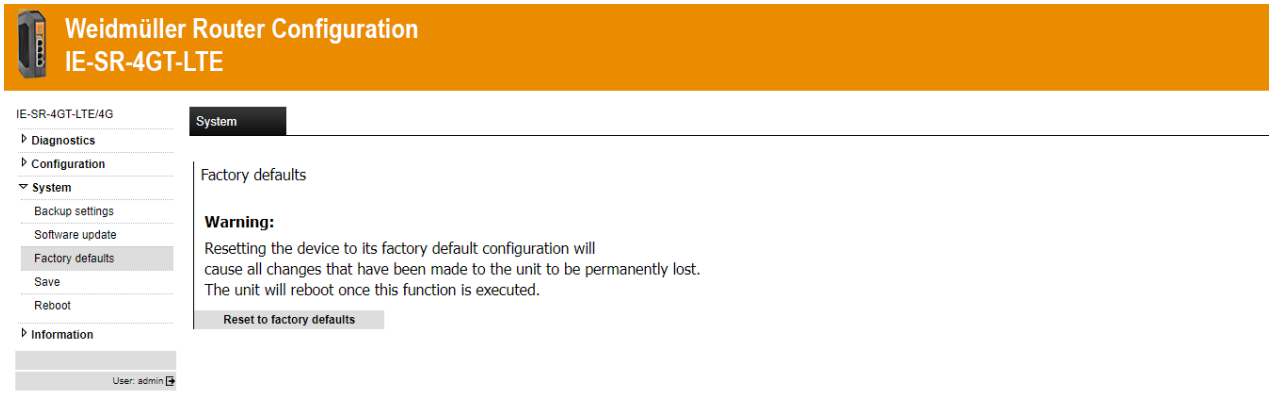
Note: A firmware downgrade from 2.2.2 will not be possible for IE-SR-4GT-LTE/4G-EU, IE-SR-4GT-LTE/4G-USEMEA, IE-SR-4GT-LTE/4G-USEMEA-M models.

Software update → Tab WWAN



Menu	System → WWAN
Function	Allows to update the modem firmware of the router only. ***Note: Only update in coordination with Weidmüller support!***

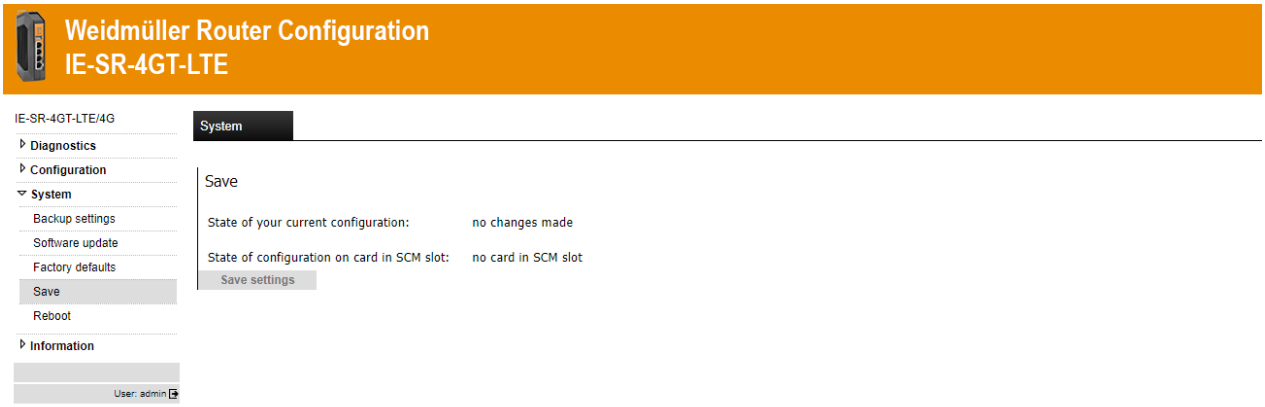
4.3.3 System → Factory defaults



Menu	System → Factory default

Function	With this menu item the Router can be set to factory default settings. Please note that doing a reset to factory values the IP addresses will be changed and the connection between the Router and the configuration PC can be lost. Basic factory settings: IP address ETH1 port: DHCP IP address ETH2…4 ports 192.168.1.110 User name: admin Password: Detmold

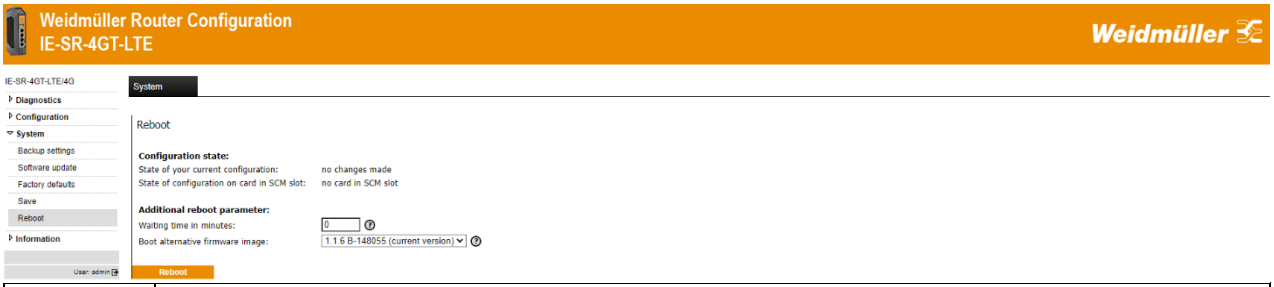
4.3.4 System → Save



Menu	System → Save
Function	Save the configuration into flash memory of the device. If a SIM memory card is inserted in the memory card slot (SCM) at the rear side of the router, then additionally the device configuration will be stored on the SIM memory card.

	Note
	This icon (disk symbol) starts flashing if the configuration has been changed and activated but not saved. Clicking on the icon the web interface jumps into this menu item (regardless the window which currently is displayed)

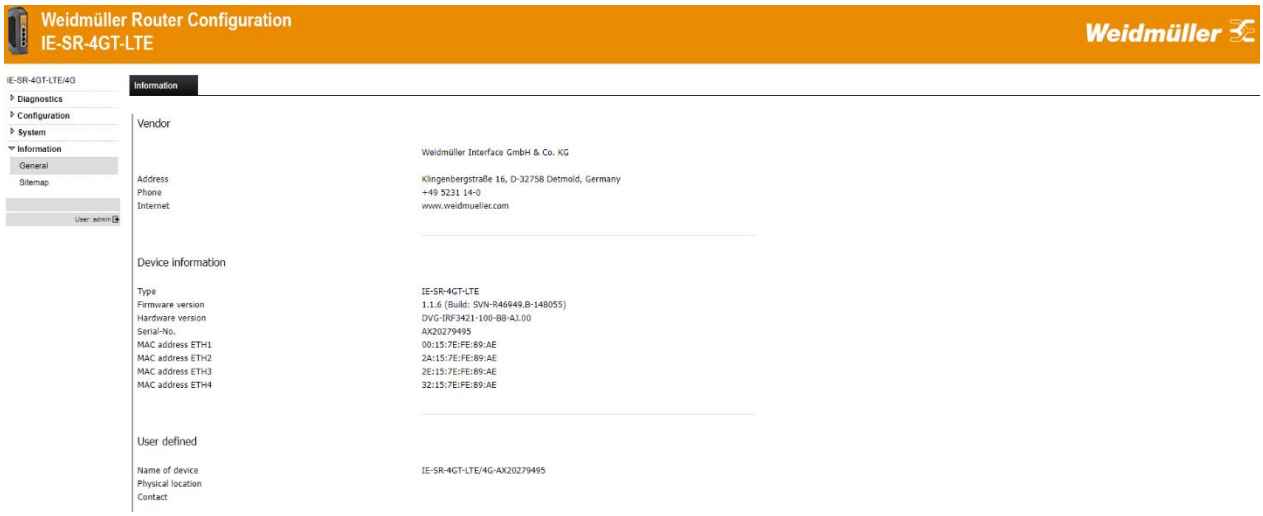
4.3.5 System → Reboot



Menu	System → Reboot	
Function	Forcing a reboot of the Router. The status message indicates whether the current configuration is saved or not.	
	Waiting time in minutes	Start a reboot timer with the given number of minutes to wait. The timer can be aborted on this page. You can use this feature to test new configurations on a remote device if you are unsure whether you will get locked out. The reboot will discard all changes and the remote device should go back online
	Boot alternative firmware image	The router can save up to two different firmware versions. Before the reboot you can choose which firmware the router shall use further on.

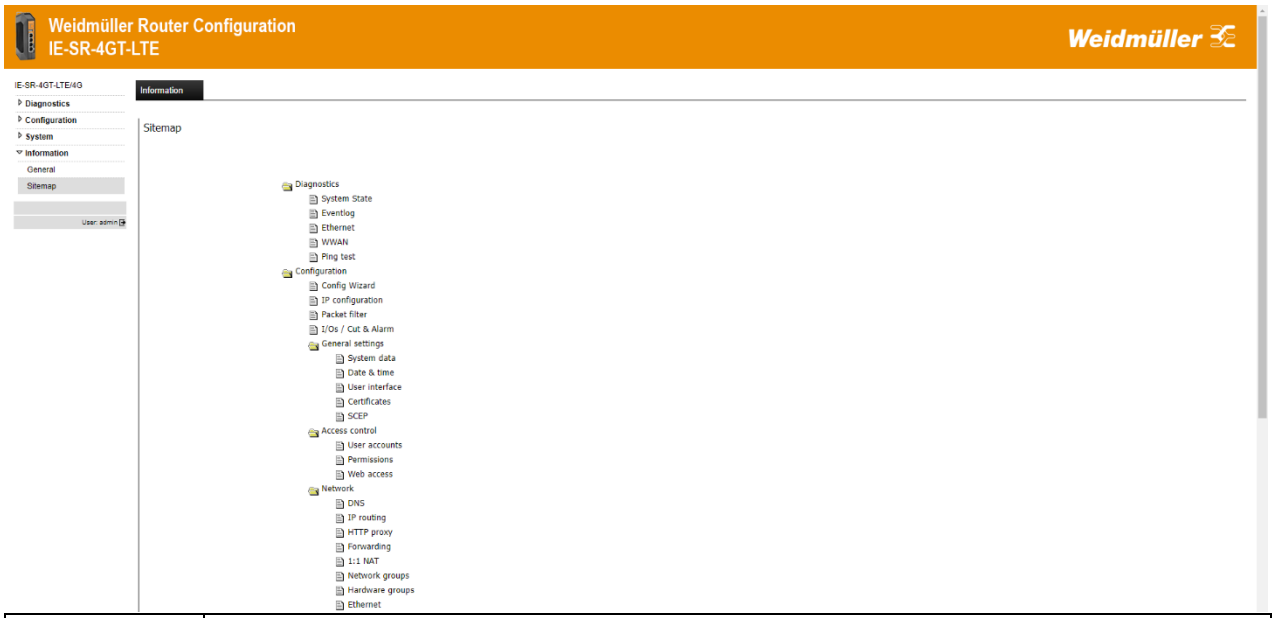
4.4 Section Information

4.4.1 Information → General



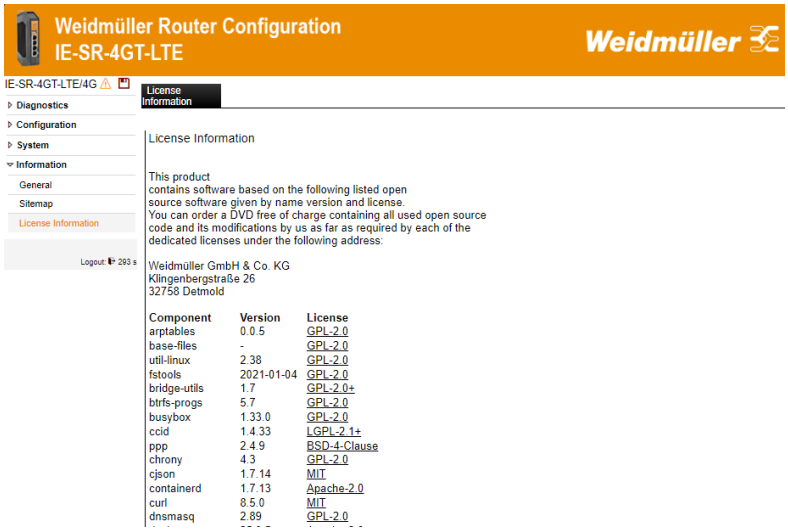
Menu	Information → General
Function	Displays information about Weidmüller and the device.

4.4.2 Information → Sitemap



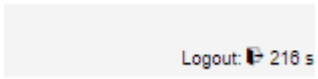
Menu	Information → Sitemap
Function	Displays the sitemap of the user interface and includes links to the menus

4.4.2 Information → License Information



Menu	Information → License Information
Function	Displays the used open source software given by name, version and license.

Additional information: Due to security reasons, you will be logged out of the web interface after 5 minutes of inactivity. A timer can be found at the bottom of the menu tree next to the log out button.



5. Appendix A (Configuration examples)

A1 – Restore configuration from USB stick

This chapter describes how to restore a configuration from a backup file (*.cf2) via the USB port.

How to do:

1. Copy the cf2-backup file to an USB stick (FAT,FAT32 or EXT4) into directory named **settings**.
2. Plug USB stick into the Router and power-up / reboot the device (Router automatically will load the cf2-file).
3. Wait around 1 minute until the Router is ready again (PWR LED is lit constantly), having loaded the parameters of the configuration file.
4. Un-plug USB stick from Router.

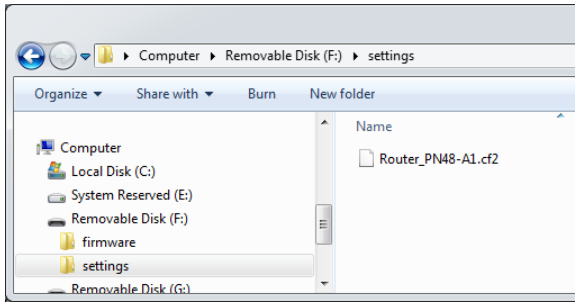
How to check the result of the import procedure via USB stick:

Method 1: Open Web interface and check the configuration.

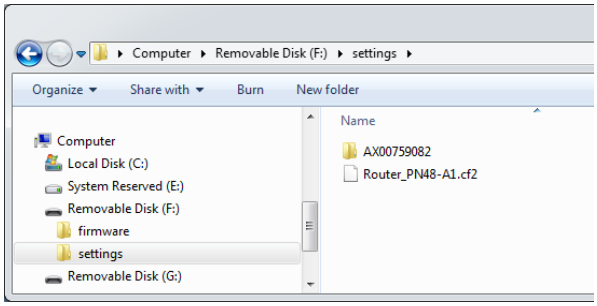
Method 2: Plug the USB stick into a PC and check directory **settings** which now should have a new sub directory with a name same as the device serial number (e.g. **AX1367406**). This directory contains a log file named **settings.log** created by the Router at configuration upload.

Open text file **settings.log** and check the status of the restoring process (e.g. containing message "Device configuration successfully updated").

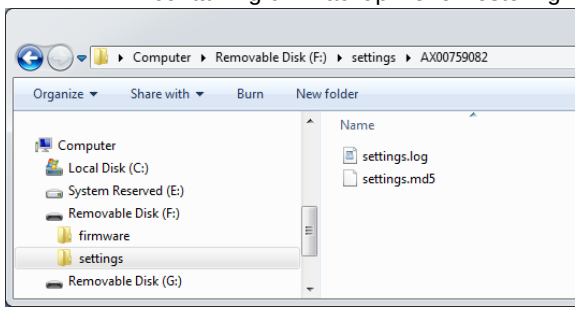
Note: If you will use the same USB stick - containing a general template configuration file - for an initial setup of several Routers, then each Router will create during the restoring process its own sub directory **AX....** (based on the unique serial number) below directory **settings** containing in the **AX...** sub directory the Router specific text file **settings.log**.



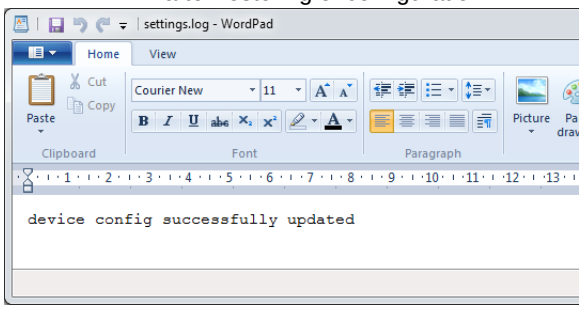
Screenshot 1: Directory "settings" of USB stick containing cf2-Backup file for restoring



Screenshot 2: Directory "settings" of USB stick after restoring of configuration



Screenshot 3: Sub directory below "settings" of USB stick containing status file "settings.log"

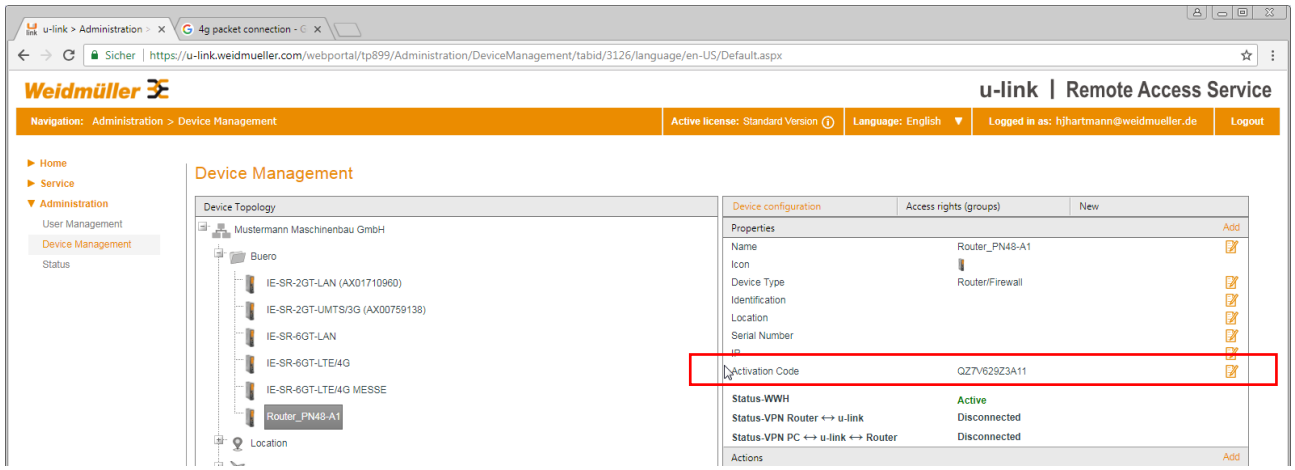


Screenshot 4: Content of status file "settings.log"

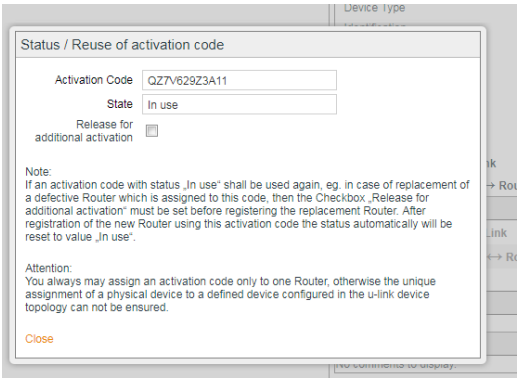
Important note if you will use this method for replacement of an already registered u-link Router!

Before replacing a registered **u-link** Router by another Router (e.g. in case of a defective device) you need to release the assigned activation code for additional activation. Do following steps before restoring the new Router with a backup file via USB stick.

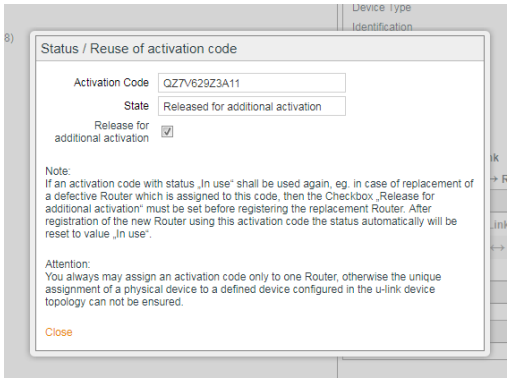
Step 1: Login (as administrator or user) into the u-link web portal.
Step 2: Open menu Administration → Device Management.
Step 3: Expand container “Device Topology” and select the Router object representing the physical Router which shall be replaced.
Step 4: Click “Edit” icon in the row of parameter “Activation code”. A window with name “Status /Reuse of activation code” appears.
Step 5: Activate checkbox “Release for additional activation”.
Step 6: Click button “Close”.
Step 7: Logout from the u-link web portal and start the restoring process on the replacement device.



Device Management of u-link Web portal



Current status of activation code (In use)



New status “Released for additional activation”

A1.1 Updating firmware with USB stick

This chapter describes how to update the firmware (*.bin) using a USB stick

How to do:

1. Download the current firmware from the Weidmüller Onlineshop & Product Catalogue | Home
2. Unpack the firmware zip file.
3. Create a folder named “firmware” on the USB stick.
4. Copy the firmware file (*.bin) into the USB stick “firmware” folder.
5. Plug USB stick into the Router and power-up / reboot the device (Router detects firmware file after 10-20 seconds and will start flashing the firmware).
6. Wait around 1 minute until the Router is ready again (PWR LED is lit constantly), having flashed the new firmware onto the device.
7. Unplug USB stick from Router.

How to check the result of the import procedure via USB stick:

➔ Open Web interface and check the current firmware on the System State tab.

A2 – Basic Router configuration to connect 2 networks with different IP address ranges

Application requirements:

There are 2 industrial Ethernet networks which shall be connected by the Router. Each network has its own IP address range. Each Ethernet node of both networks shall have the possibility to communicate with each other.

This application can be done with all router models. No special firewall filter rules shall be configured.

In this example the IP address ranges are set to

192.168.**10**.0 / 255.255.255.0 for Network 1 and

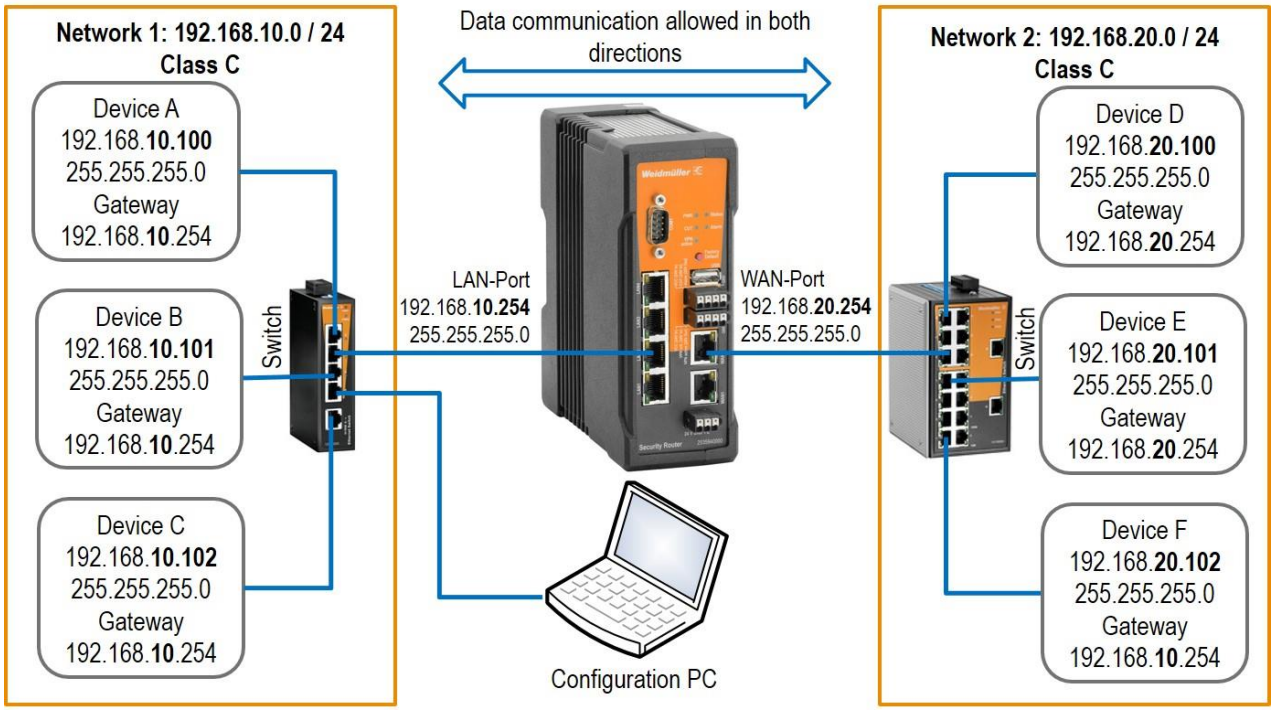
192.168.**20**.0 / 255.255.255.0 for Network 2

The Router interfaces will be set to

192.168.**10**.254 / 255.255.255.0 for LAN interface and

192.168.**20**.254 / 255.255.255.0 for WAN interface

Network diagram of below described application scenario



How to configure the Router

The Router is set to factory default values and can be accessed using the LAN port by IP address 192.168.1.110.

1. Connect the configuration PC to Router LAN Port.

Note: Use auto-negotiation on the Ethernet Interface of the PC

2. Change the IP address of the PC to one of the range 192.168.1.0 / 24

e.g. IP address 192.168.1.99

Subnet mask 255.255.255.0

Standard gateway can be left blank due to direct cable connection

3. Start a web browser and login into the web Interface of Router (http://192.168.1.110)

User: admin

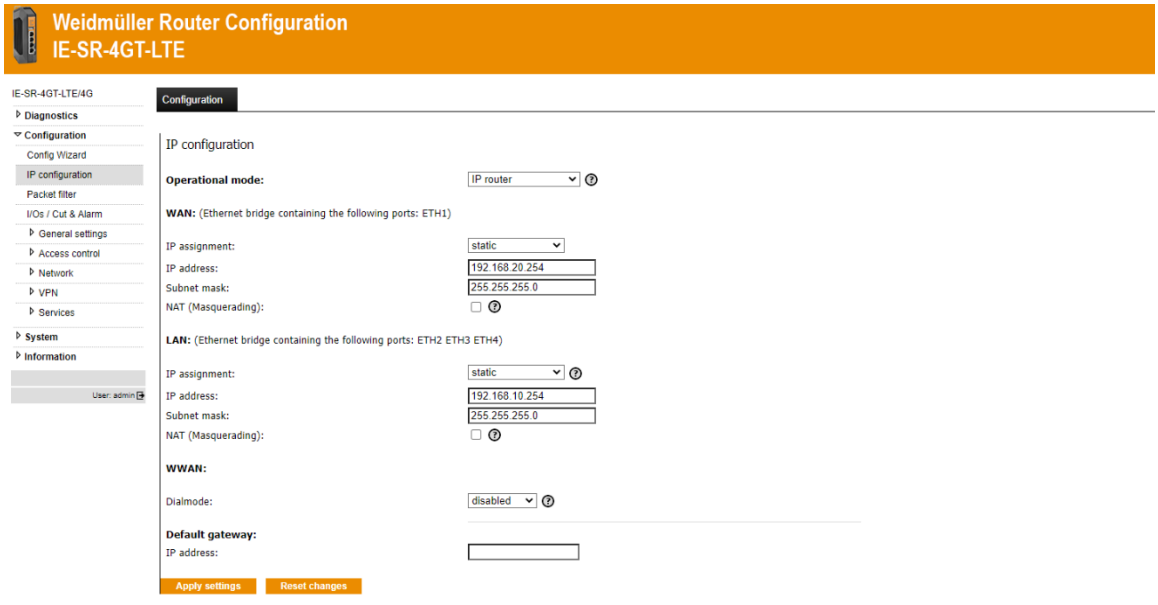
Password: Detmold

4. Set the basic IP configuration

► Select menu **Configuration → IP configuration**

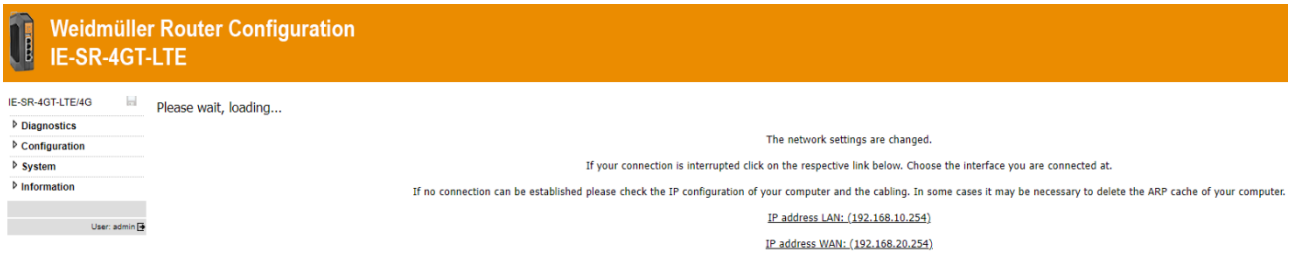
► Configure the menu entries as following shown

Operational mode:	IP Router
IP address parameters **WAN** Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
IP address parameters **LAN** Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
Dialmode	Disabled
Default gateway	Can be left blank because there exists no further target network



► Click button “Apply settings” to activate the new settings.

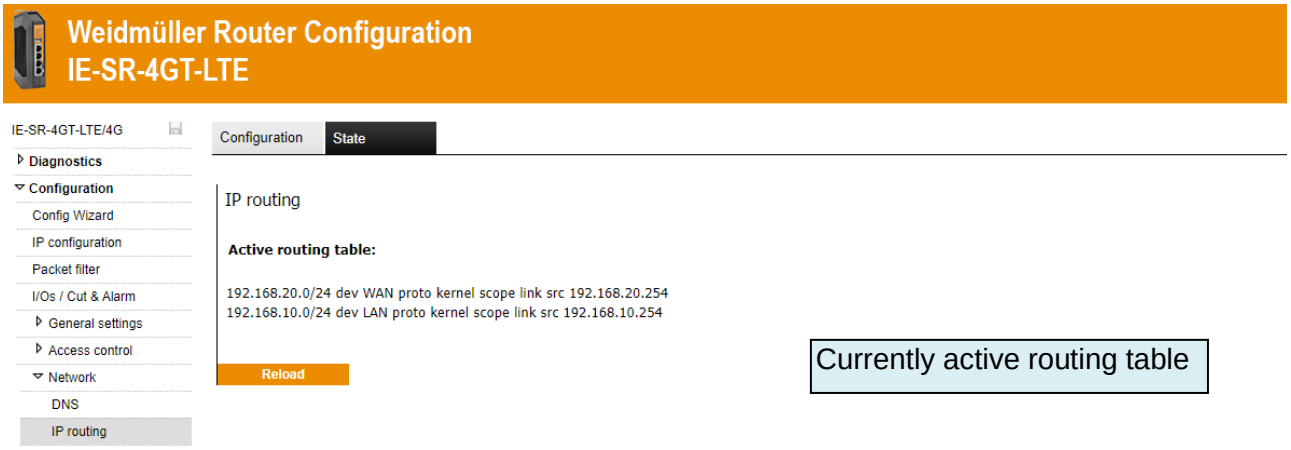
Now the configured parameters will be **activated (but not saved)**. After a few seconds the web interface displays the new IP addresses as shown below. Please keep in mind that you now have lost the Router connection due to changing the IP address range of your connected LAN port.



5. Change the IP address of the configuration PC according to the connected network 192.168.10.0 / 24
   ► To reconnect to the Router now set the IP address of the PC to the new values
   IP address: 192.168.10.99
   Subnet mask: 255.255.255.0
   Standard-Gateway: 192.168.10.254

   ► Again login into the Web interface of the Router using a Web browser
   Use IP address 192.168.10.254 (http://192.10.1.254) on LAN port
   User: admin
   Password: Detmold

6. Check the currently active "routes"
   ► Select menu Configuration → Network → IP routing → Tab "State"



7. Saving the new configuration
   ► Select menu System → Save or Click on the Disk icon in the upper left corner of the web interface

   ► Click on button "Save settings" to save the current configuration to the non-volatile flash memory of the Router. If a SIM memory card is installed the configuration automatically will be stored on the SIM memory card. Additionally, the configuration can be stored on the file system of the PC.

   ► Select menu **System → Backup settings**

   ► Click on button "Download settings" to write the configuration file to the PC hard disk (Backup file has the default extension *.cf2")

Now the configuration of the Router is finished!

Testing the accessibility between Ethernet Devices of both networks

1. Run 3 Ping commands from a device of Ethernet network **1** (192.168.10.0/24) using below described addresses (members of network 2)
   → ping 192.168.20.100
   → ping 192.168.20.101
   → ping 192.168.20.102

   Result: All sent "pings" should be answered by the requested IP addresses correctly.

2. Run 3 Ping commands from a device of Ethernet network **2** (192.168.20.0/24) using below described addresses (members of network 1)
   → ping 192.168.10.100
   → ping 192.168.10.101
   → ping 192.168.10.102

   Result: All sent "pings" should be answered by the requested IP addresses correctly.

	Note
	1. If you perform the ping test using PC's please check your firewall configuration to ensure that ping re-quests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gate-way (IP address is pointing to the Router of the PC's network)

A3 - Connecting 2 Ethernet networks with activated NAT masquerading and using IP address forwarding

Application requirements:

There are 2 industrial Ethernet networks which are connected by the Router. Each network has its own IP address range. For security reasons the IP addresses of network 1 shall be hidden against devices of network 2. As an exception 2 devices (C and D) of network 1 should be accessible directly from devices of network 2.

This application can be done with all router models. No special firewall filter rules shall be configured.

Solution:

1. Activating “NAT masquerading” at **WAN** port of the Router which is connected to network 2. As result the sender IP addresses of any outgoing traffic at WAN port – initiated by devices of network 1 connect to LAN port – will be translated to the IP address of the Router’s WAN port. From the perspective of the receivers the sender is always the Router WAN port. The IP addresses of devices connected to the LAN port will be hidden and are not visible.

2. To get access to the devices C and D of the hidden network 1 the Router’s “IP address forwarding” feature can be used, which assigns devices C and D an additional and unused IP address from the range of network 2. Effectively the Router will have 3 IP addresses at WAN port (Physical WAN IP address and 2 virtual IP addresses). This feature acts as a special kind of “port forwarding” using only IP addresses and omitting the ports.

	Note
	Generally, “masquerading” only hides a sender IP address (e.g. outgoing from LAN to WAN) but does NOT block the access to this LAN IP address from WAN network. This explicitly must be done by a firewall rule.

In this example the IP address ranges are set to

192.168.**10**.0 / 255.255.255.0 for network 1 and

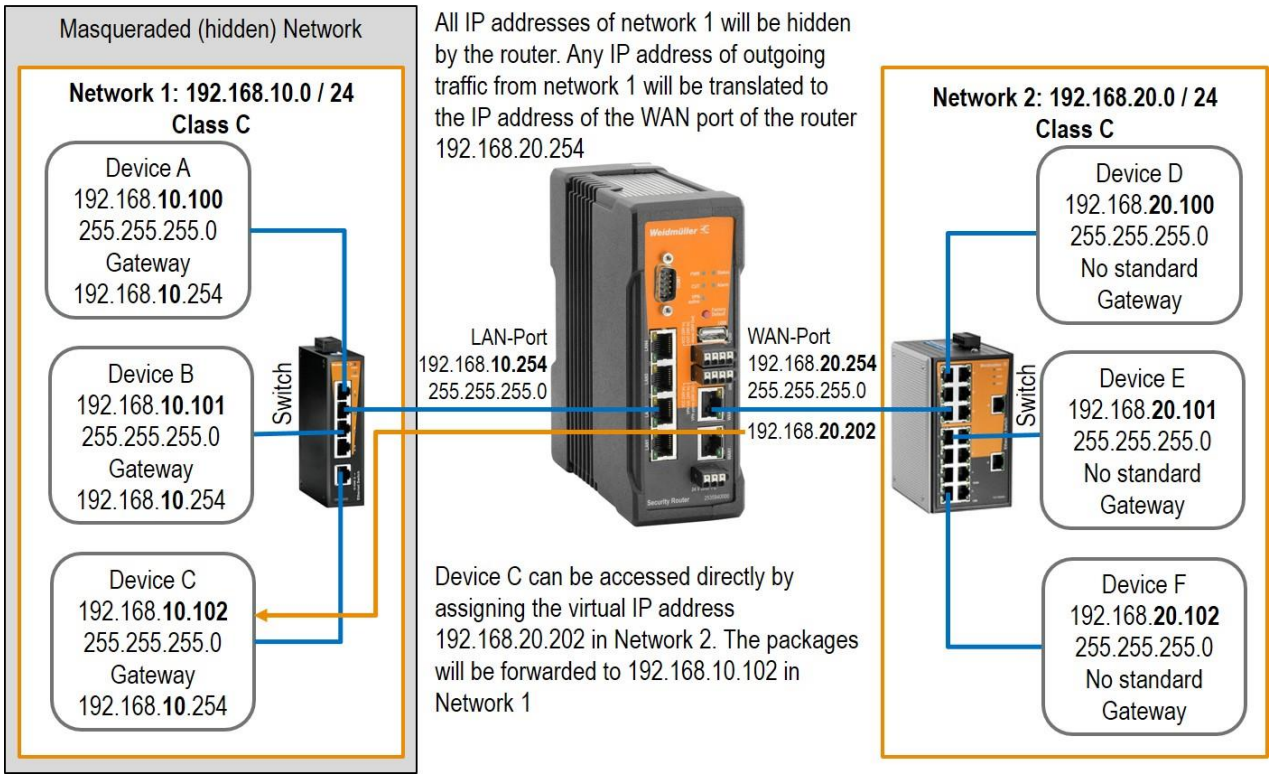
192.168.**20**.0 / 255.255.255.0 for network 2

The Router interfaces will be set to

192.168.**10**.254 / 255.255.255.0 for LAN interface and

192.168.**20**.254 / 255.255.255.0 for WAN interface

Network diagram of below described application scenario



How to configure the Router

Starting situation

The Router is set with factory default values and can be accessed either using the LAN port by IP address 192.168.1.110 or using the WAN port by IP address 192.168.2.110.

1. Connect the configuration PC to the Router using the LAN Port (this port will be used in the example).

Note: Use autonegotiation on the Ethernet Interface of the PC

2. Change the IP address of the PC to one of the range 192.168.1.0 / 24

→ e.g. IP address 192.168.1.99
Subnet mask 255.255.255.0
Standard gateway can be left blank due to direct cable connection

3. Start a Web browser and login into the Web Interface of Router (http://192.168.1.110)

User: admin
Password: Detmold

4. Set the basic IP configuration and activate NAT masquerading

► Select menu **Configuration → IP configuration**

► Configure the menu entries as below described

Operational mode:	IP Router
IP address parameters **WAN** Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) **SET**
IP address parameters **LAN** Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
Dialmode	Disabled
Default gateway	Can be left blank because there exists no further target network

► Click button “Apply settings” to activate the new settings.

Now the configured parameters will be **activated (but not saved)**. After a few seconds the web interface displays the new IP addresses. Please keep in mind that you have lost the Router connection due to changing the IP address range of your connected LAN port.

5. Change the IP address of the configuration PC according to connected network 192.168.10.0 / 24

► To reconnect to the Router now set the IP address of the PC to the new values

IP address: 192.168.10.99
Subnet mask: 255.255.255.0
Standard-Gateway: 192.168.10.254

6. Again login into the Web interface of the Router using a Web browser

Use IP address 192.168.10.254 (http://192.168.10.254) on LAN port
User: admin
Password: Detmold

7. Verify that configured parameters are valid

► Select menu **Configuration → IP configuration**

8. Configuring the accessibility of devices C and D of hidden network 1

► Select menu **Configuration → Forwarding**

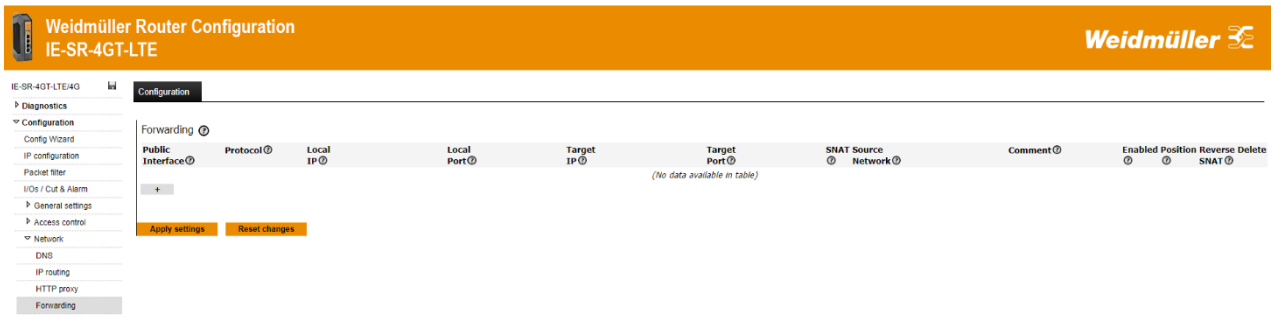


Figure 1: Empty IP forwarding table

► Click icon **+** to add a new line to enter IP forwarding values

► Select or fill the values as shown in the upper entry of Figure 2

→ Ensure that each input will be completed by clicking the icon ☑.

► Now click button “Apply settings” to activate the “IP address forwarding table”

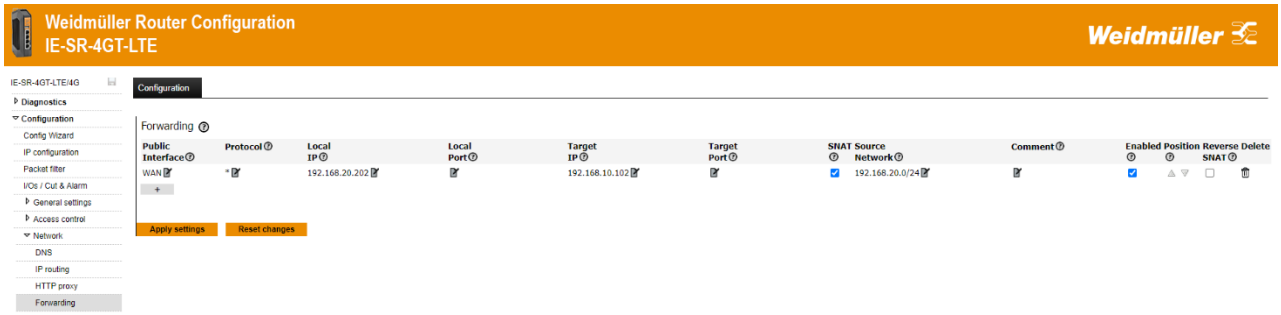


Figure 2: IP forwarding

Now the configuration of the Router is finished!

Testing the NAT masquerading feature

To test the NAT masquerading function, you must use the tool Wireshark on the PC which receives the ping request.

1. Run Wireshark on PC (connected to WAN port) with e.g. IP address 192.168.20.100
2. Start a new live capture session to display sent and received Ethernet packets
3. Run a “ping” request from a device of Ethernet network 1 (e.g. 192.168.10.100) with destination address 192.168.20.100
4. Stop the Wireshark live capture session when the packets have been received and displayed.

Results showing in the Wireshark window:

The original sender of the ping request with IP address 192.168.10.100 is displayed as IP address 192.168.20.254 which is translated (masqueraded) by the Router.

If you disable NAT masquerading at WAN port and repeat the test, then the original sender address 192.168.10.100 will be shown.

Testing the configured IP address forwarding

1. Run a “ping” request from a device of Ethernet network 2 (e.g. 192.168.20.100) with destination address 192.168.20.202 (Note: Real IP address is 192.168.10.102)

Result: The sent “ping” request should be answered correctly (displayed return address: 192.168.20.202)

2. Run a “ping” request from a device of Ethernet network 2 (e.g. 192.168.20.100) with destination address 192.168.20.203 (Note: Real IP address is 192.168.10.103)

Result: The sent “ping” request should be answered correctly (displayed return address: 192.168.20.203)

	Note
	1. If you perform the ping test using PC’s please check your firewall configuration to ensure that ping requests and echoes are allowed. 2. Don’t forget to save the configuration after testing

A4 - Configuring the Router to connect 2 networks with different IP address ranges and additional firewall rules

Application requirements:

There are 2 industrial Ethernet networks which are connected by a Router. Each network has its own IP address range. All Ethernet nodes in both networks shall have the possibility to communicate with each other except that devices B and C of network 1 cannot be accessed by a ping request (ICMP protocol).

This application can be done with all router models.

Solution:

Configure firewall rules to prohibit ping requests from devices of network 2 to devices B and C of network 1.

In this example the IP address ranges are set to

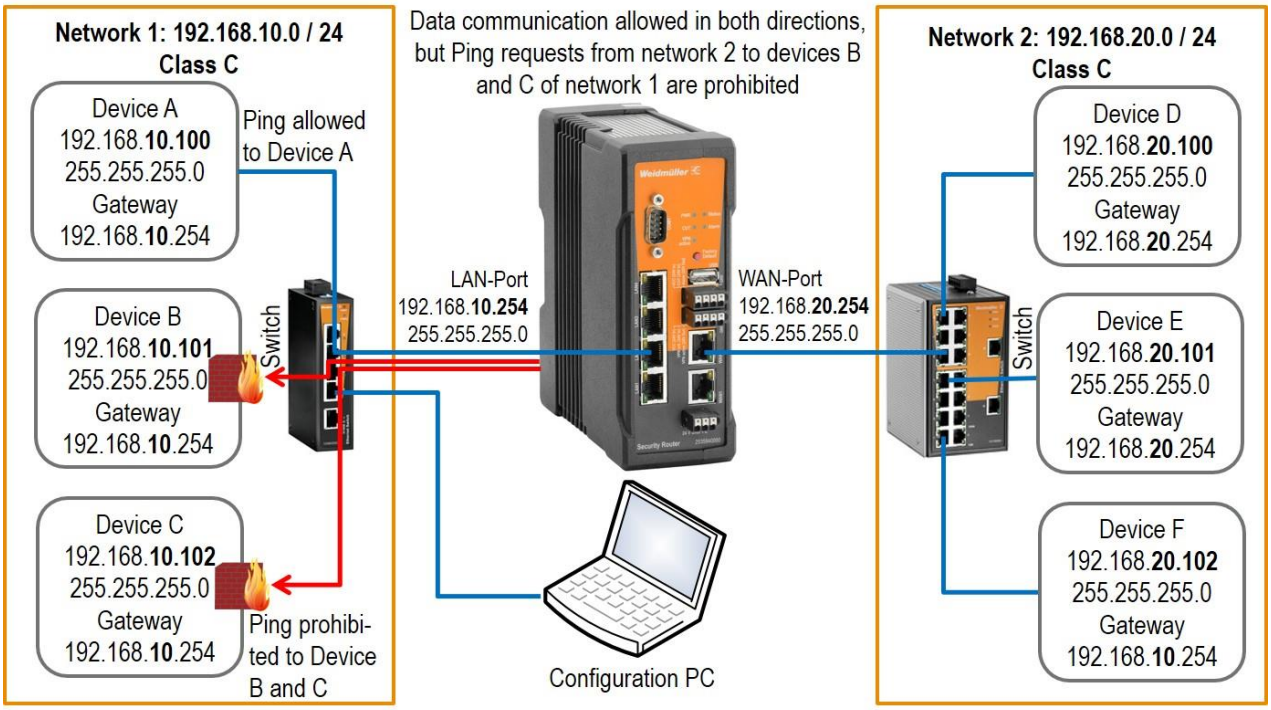
192.168.10.0 / 255.255.255.0 for Network 1 and

192.168.20.0 / 255.255.255.0 for Network 2

The Router interfaces will be set to

192.168.10.254 / 255.255.255.0 for LAN interface and

192.168.20.254 / 255.255.255.0 for WAN interface



Network diagram of below described application scenario

How to configure the Router

Starting situation

The Router is set to factory default values and can be accessed either using the LAN port by IP address 192.168.1.110 or using the WAN port by using the Router Search Utility.

1. Connect the configuration PC to the Router using the LAN Port (this port will be used in the example).

Note: Use autonegotiation on the Ethernet Interface of the PC

2. Change the IP address of the PC to one of the range 192.168.1.0 / 24

→ e.g. IP address 192.168.1.99
Subnet mask 255.255.255.0
Standardgateway can be left blank due to direct cable connection

3. Start a Web browser and login into the Web interface of Router (http://192.168.1.110)

User: admin
Password: Detmold

4. Set the basic IP configuration (Preparing the Router)

► Select menu Configuration → IP configuration

► Configure the menu entries as following shown

Operational mode:	IP Router
IP address parameters **WAN** Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
IP address parameters **LAN** Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
Dialmode	Disabled
Default gateway	Can be left blank because there exists no further target network

► Click button “Apply settings” to activate the new settings.

Now the configured parameters will be **activated (but not saved)**. After a few seconds the web interface displays the new IP addresses as shown in Figure 3. Please keep in mind that you have lost the Router connection due to changing the IP address range of your connected LAN port.

5. Change IP address of configuration PC according to the connected network 192.168.10.0 / 24

► To reconnect to the Router now set the IP address of the PC to the new values

IP address: 192.168.10.99
Subnet mask: 255.255.255.0
Standard-Gateway: 192.168.10.254

► Again login into the Web interface of the Router using a Web browser

Use IP address 192.168.10.254 (http://192.10.1.254) on LAN port

User: admin

Password: Detmold

6. Step-by-step description of creating a new packet filter (firewall rules) to prohibit ping requests from devices of network 2 to devices B and C of network 1

General description of the Packet filter

The feature „Packet filter“ can be used to create firewall rules for IP address (Layer 3) and MAC address level (Layer 2). The packet filter is organized hierarchical by using **rule-sets** which contains several single **rules**.

To define new firewall rules, you first have to create a rule-set or you have to add the rule to an existing rule-set. A rule-set can contain up to 10 firewall rules.

The manner how to configure rule-sets or rules is the same for Layer 2 and Layer 3 packet filters. All created rule-sets are displayed in menu windows „Packet filter“. By clicking on the triangle icon (►) on the left side of a displayed rule-set the belonging rules additionally will be displayed.

By default the Router contains 1 **rule-set** called **Allow_L3*** which is acting as a general permission to allow inbound and outbound traffic without any limitation.

Application method of defined rule-sets

Several configured rule-sets will be applicated top-down. That means every data traffic will first be checked by the top-most displayed rule-set with its containing rules.

If a defined rule match the inspected data, the filter rule will be applied. After that the packet filter function immediately will be left and no further defined rules and rule-sets will be applied.

If a defined rule does **not** match the inspected data, the current filter rule will be skipped and the data will be checked by the next filter rule (from top to down). This method will be conducted step-by-step with each defined rule-set (and belonging rules) until a valid rule will be found and applied or no further rule exists.

7. Setup the firewall rules

► Select menu Configuration → Packet filter →Tab “Layer 3”

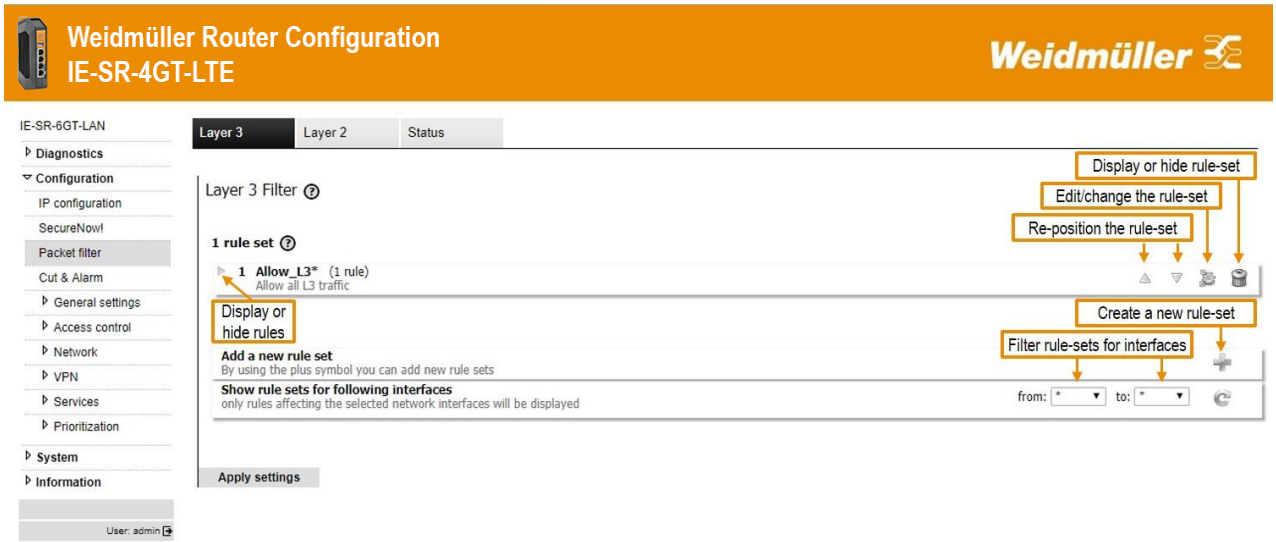


Figure 3: Packet filter

► Click on the icon **+** (right side of line “Add a new rule set”) to create a new rule-set and follow the below described steps (Figure 4)

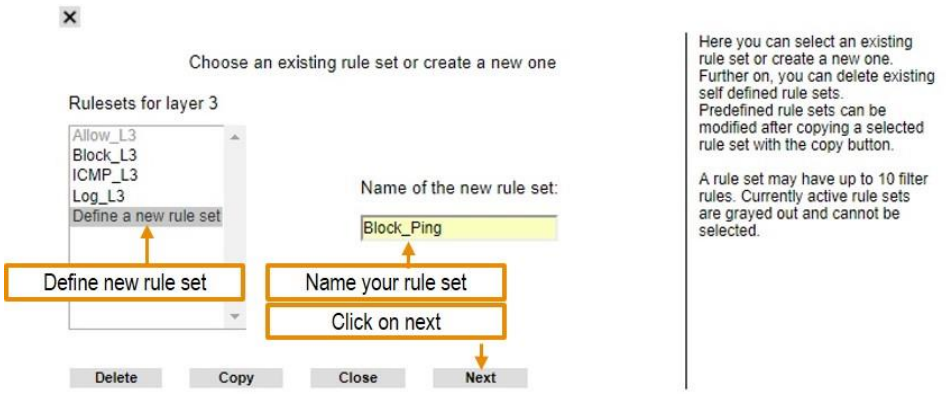


Figure 4: Create a new rule-set

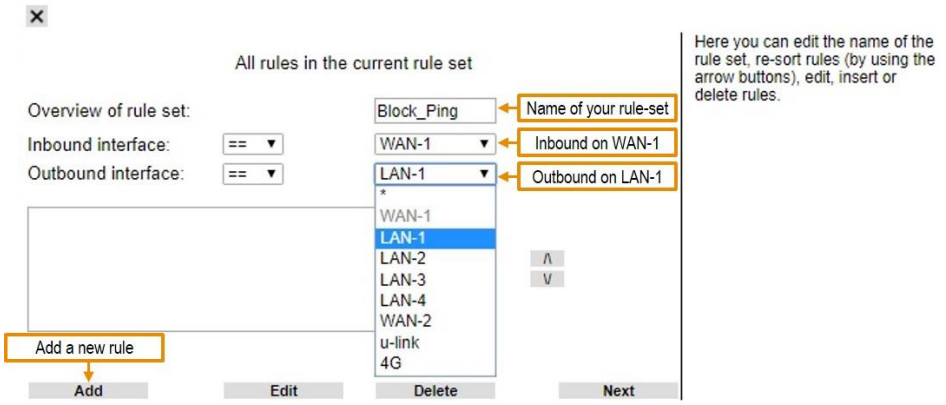


Figure 5: Define additional parameters of the new rule-set

Completing the rule-set which will be used as container for a maximum of 10 rules. The inbound and Outbound interface-rules will be applied before all other rules of this rule-set. The available in- and outbound interfaces are depending on router model, operation mode and active virtual interfaces.

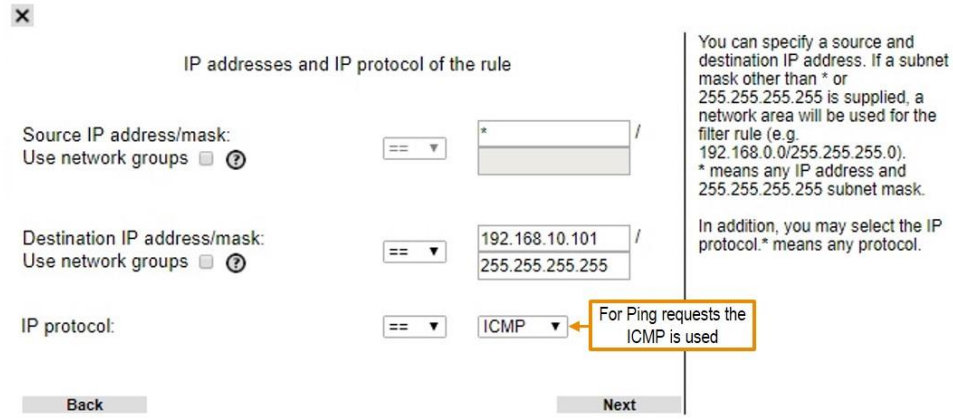


Figure 6: Define the first rule

The rule is valid for communication **from** source addresses that are == *, which means all IP adresses, **to** == 192.168.10.101 with Subnet 255.255.255.255, which means this specific IP. You can also choose to set a rule for all IP adresses EXCEPT (!=) the given one.

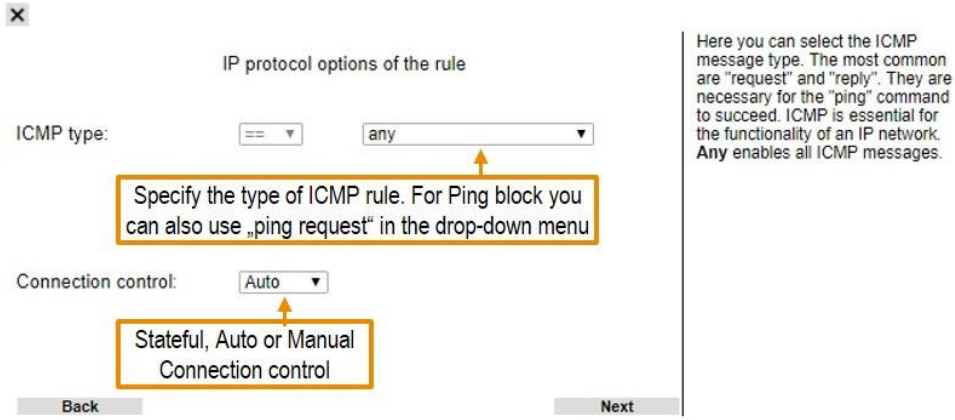


Figure 7: Define additional parameters of the first rule

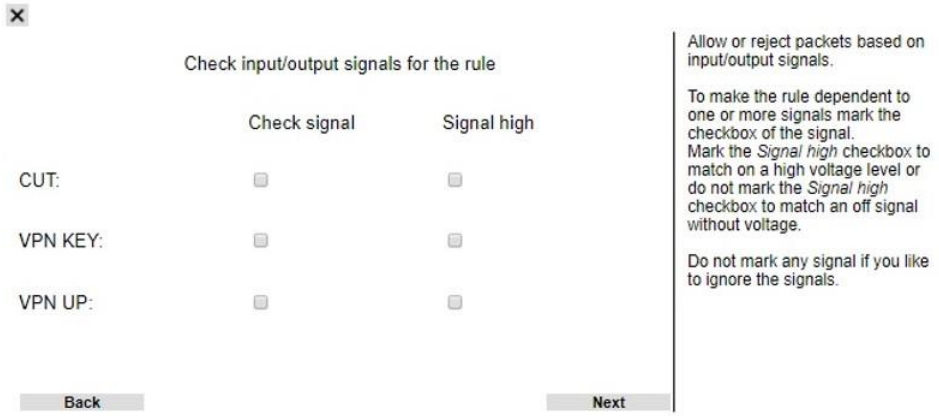


Figure 8: Define influence of other signals on the packet filter

To allow ping messages via VPN there could be a rule which allows ICMP packages if VPN Key is turned and/or VPN tunnel is up.

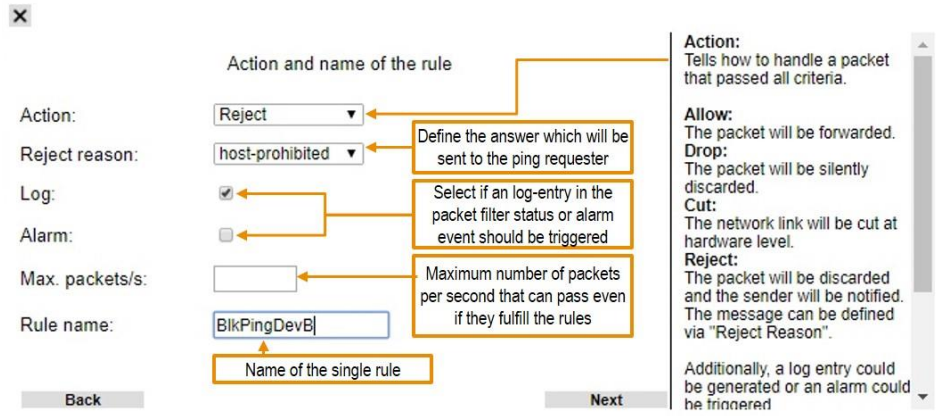


Figure 9: Action and name of the rule

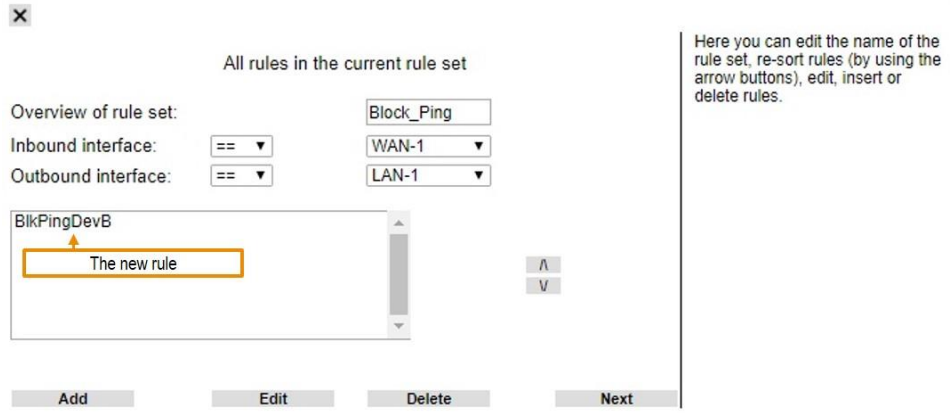


Figure 10: Creation of first rule completed

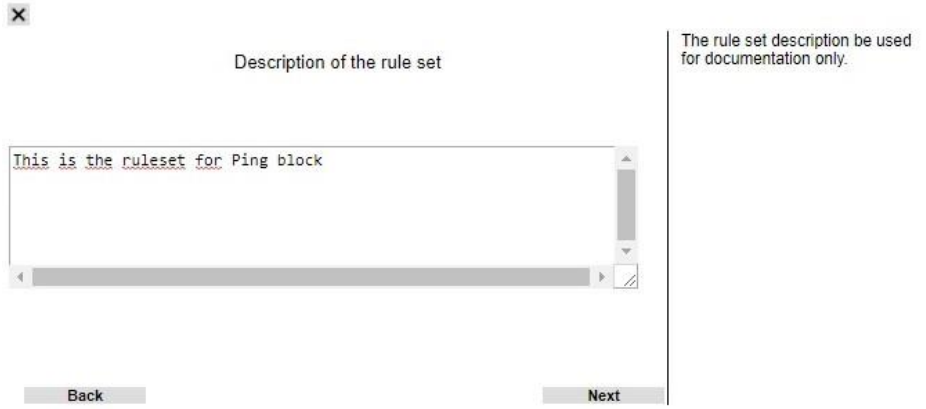


Figure 11: Description of the rule-set

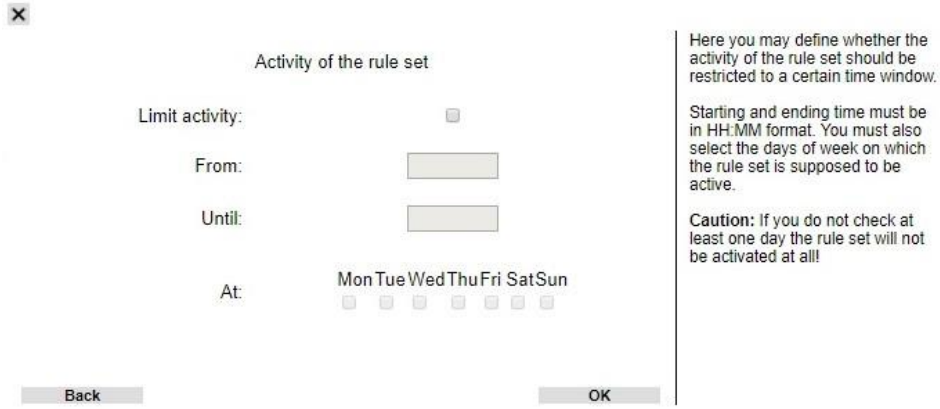


Figure 12: Time limitations on filter rule-sets

Set time and date limitations for the rule-set.

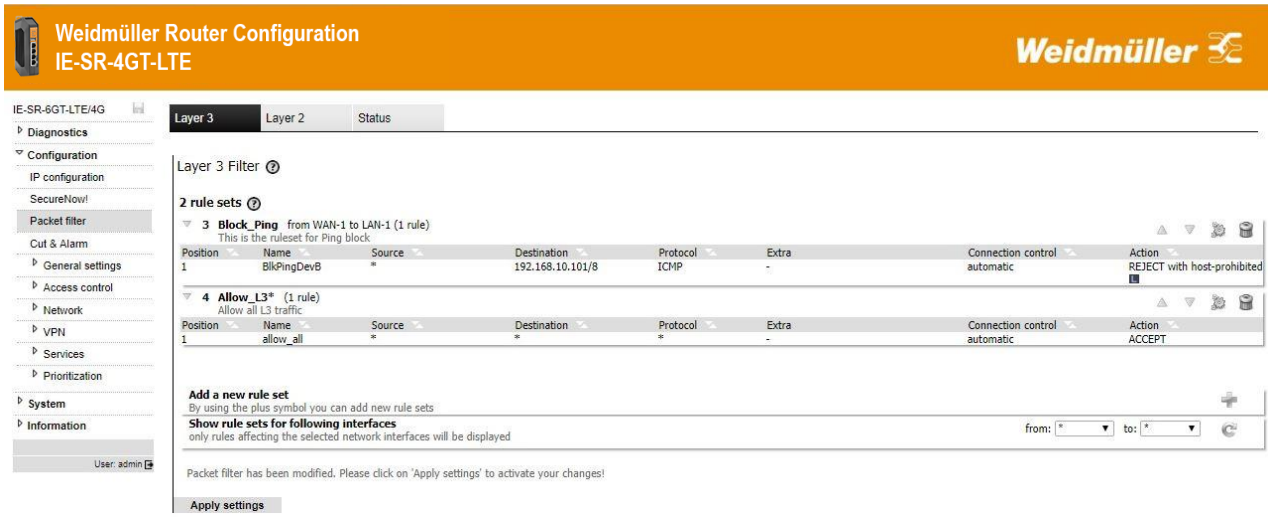


Figure 13: Overview of Packet filter rules

New rule-sets will be generated at the bottom of the list by default. The rule-sets are displayed in hierarchical order. To get the new rule effective, it must be at the top of the list. In default mode, the “Allow_L3” would overrule the “Block_Ping”.

Now the firewall configuration (packet filter) is finished!

Testing the result that Ethernet Devices B (192.168.10.101) and C (192.168.10.102) of network 1 cannot be “pinged” by devices of network 2

Run 3 Ping commands from a device of Ethernet network 2 (192.168.20.0/24) using below described addresses (members of network 1)

→ ping 192.168.10.100 (Device A)
→ ping 192.168.10.101 (Device B)
→ ping 192.168.10.102 (Device C)

Results:

1. **Sent “Ping” to IP address 192.168.10.100 should be answered by the requested IP addresses correctly.**
2. **Sent “Ping” to IP addresses 192.168.10.101 and 192.168.10.102 should be answered by the requested IP addresses as “Destination host unreachable”.**

	Note
	1. If you perform the ping test using a PC please check the PC’s firewall configuration to ensure that ping requests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gateway (IP address is pointing to the Router of the PC’s network)

A5 – Firewall application example: Securing the access to Modbus TCP devices by Layer-2 firewall rules

Task: The communication between Modbus Master devices and Modbus slave devices inside of the same switched network shall be controlled and secured by Firewall rules.
The Router shall act as a Layer-2 firewall (controlling MAC-based Ethernet frames) and being transparent for the devices inside of the switched network.

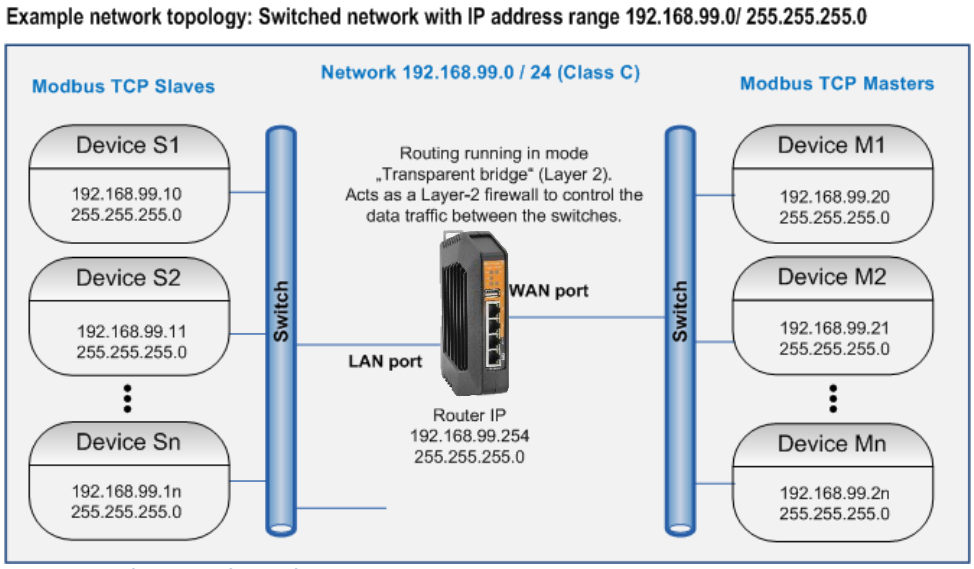


Figure 14: Example network topology

Communication requirements / restrictions:

1. Access from each Modbus Master to any Modbus Slave is allowed (based on Protocol TCP / Port 502, independent of used IP addresses).
2. The PTP communication (precision time protocol) - initiated from devices at LAN port side – shall be allowed (Protocol UDP / Ports 319 and 320).
3. Any NTP communication (network time protocol) – initiated from devices connected at LAN or WAN port– shall be allowed (Protocol UDP / Port 123).
4. Any other communication shall be blocked.

Starting situation:

- The router is set to factory default values.
- The configuration PC is connected to Router's LAN port.
- Router is accessible via IP address 192.168.1.110 (User: admin, PW: Detmold).

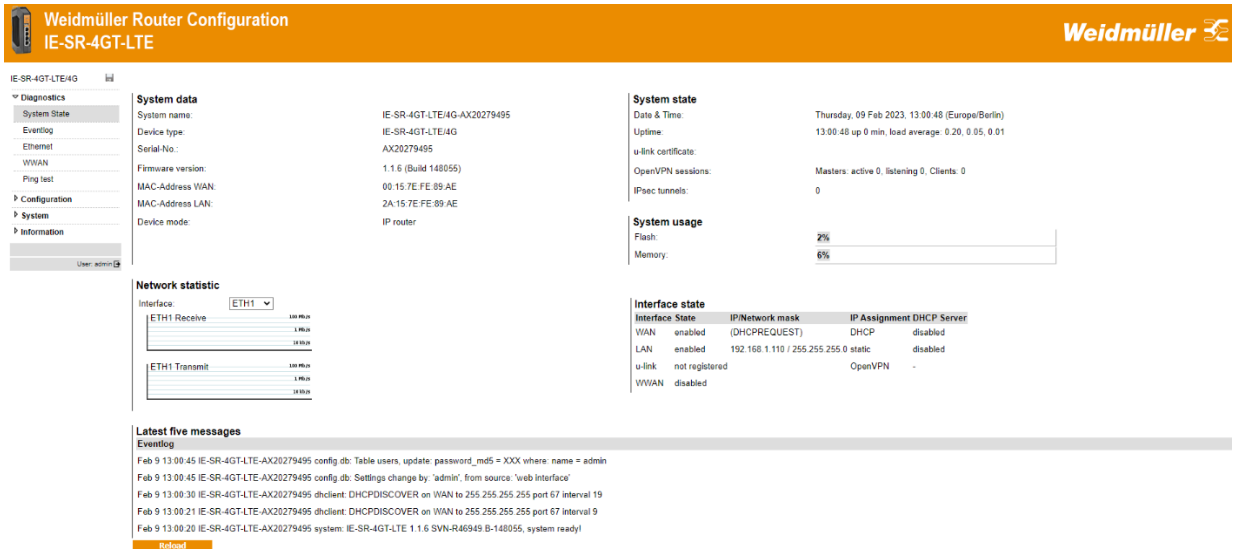


Figure 15: Display of initial web page after login (Menu System state)

A5-1 Configuration of initial parameters

►Go to menu Configuration → IP configuration

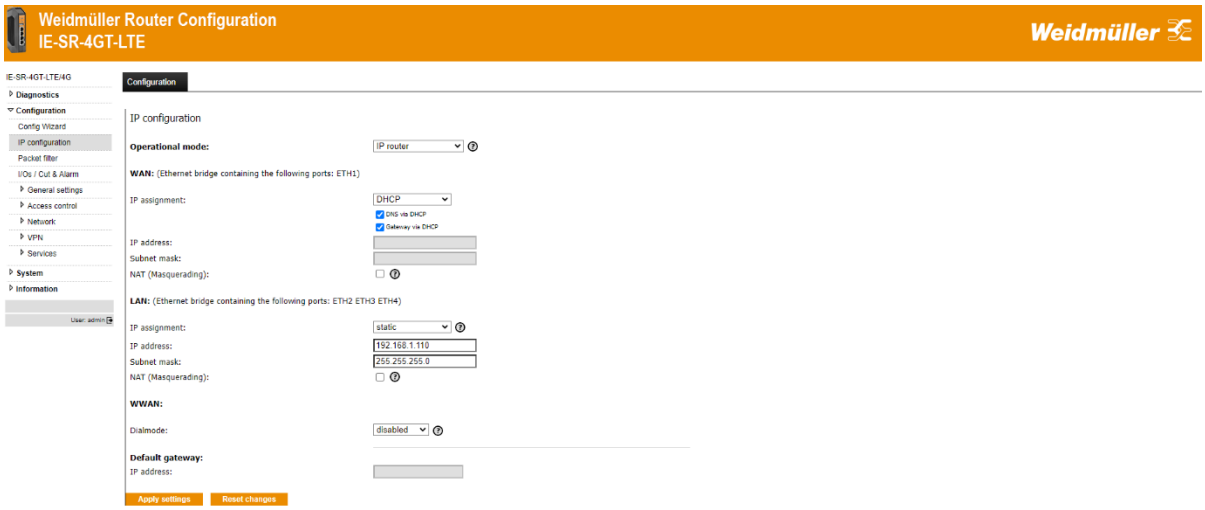


Figure 16: IP configuration factory defaults

►Change operational mode to “Transparent bridge”.

- Router is now working in bridging mode on Layer 2 (Ethernet frames / MAC address based).

►Change LAN IP address as desired (in bridging mode only needed for Web access).

- In this example we use 192.168.99.178.
- If the Router shall be accessed also from another IP network please configure the default gateway. In this example we use gateway address 192.168.99.1.

►Click “Apply Settings”

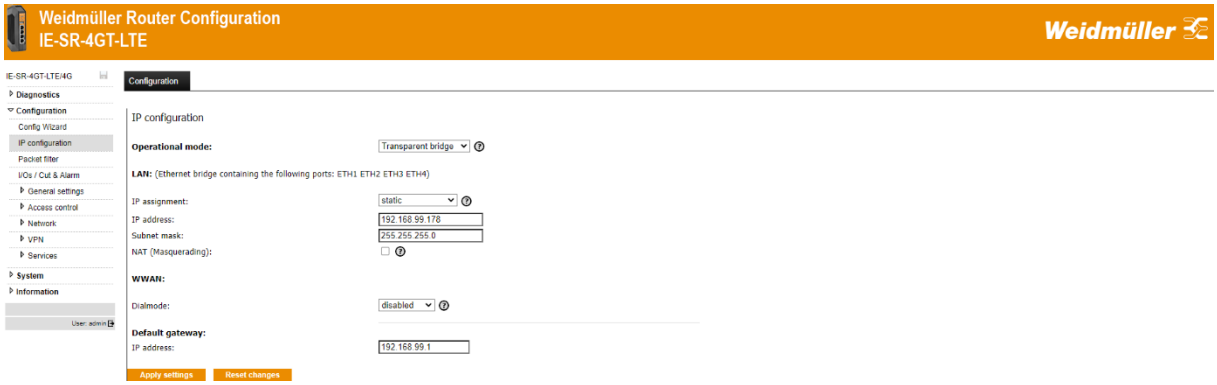


Figure 17: New IP configuration running as "Transparent bridge" (Layer 2)

Configuration of an individual system/device name (Optional step)

►Goto menu Configuration → General settings → System Data.
►Change "System name" according to your needs (e.g. related to your application / machine).
►Click "Apply Settings".

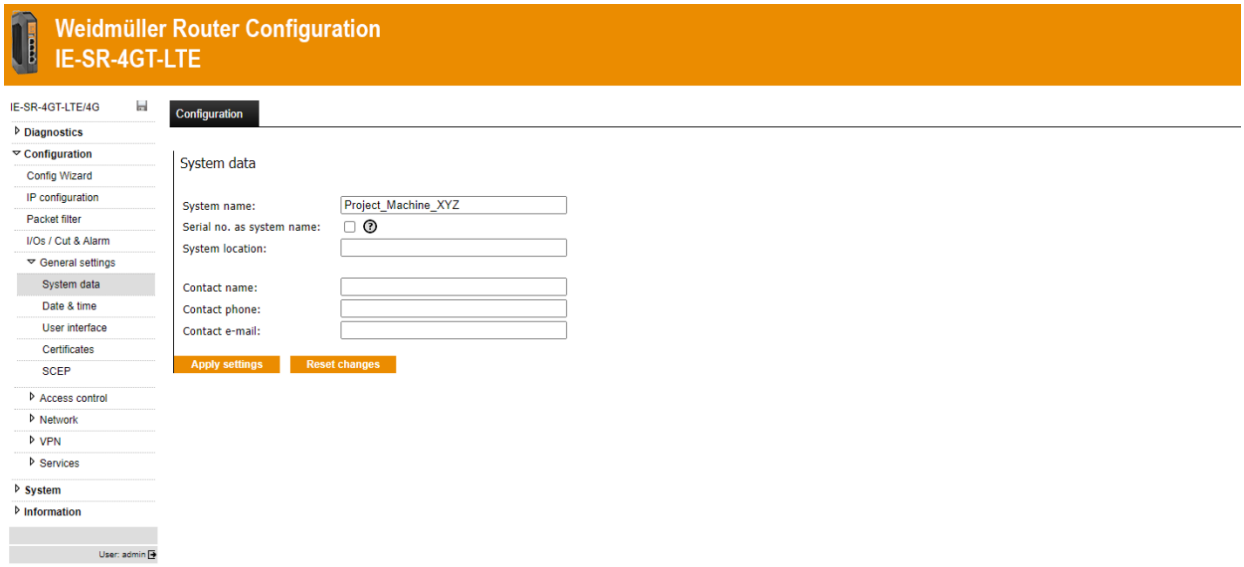


Figure 18: New System name

Configuration of an access to a DNS server (Optional step)

►Goto menu Configuration → Network → DNS.
►Enter at least one DNS server if you want to get/update the Router's time via a NTP request (e.g. typically gateway IP or Google's DNS server 8.8.8.8).
►Click "Apply Settings".

Figure 19: First DNS server (or DNS server relay) is 192.168.99.1

Configuration of date / time settings (Optional step)

►Goto menu Configuration → General Settings → Date & Time.
►Select your time zone.
►Enable checkbox “Enable time server synch...” for getting date and time via NTP server.
A DNS server must be configured and the Router must have access to the internet if you use the default configured DNS names of the NTP server.
►Click “Apply Settings”.

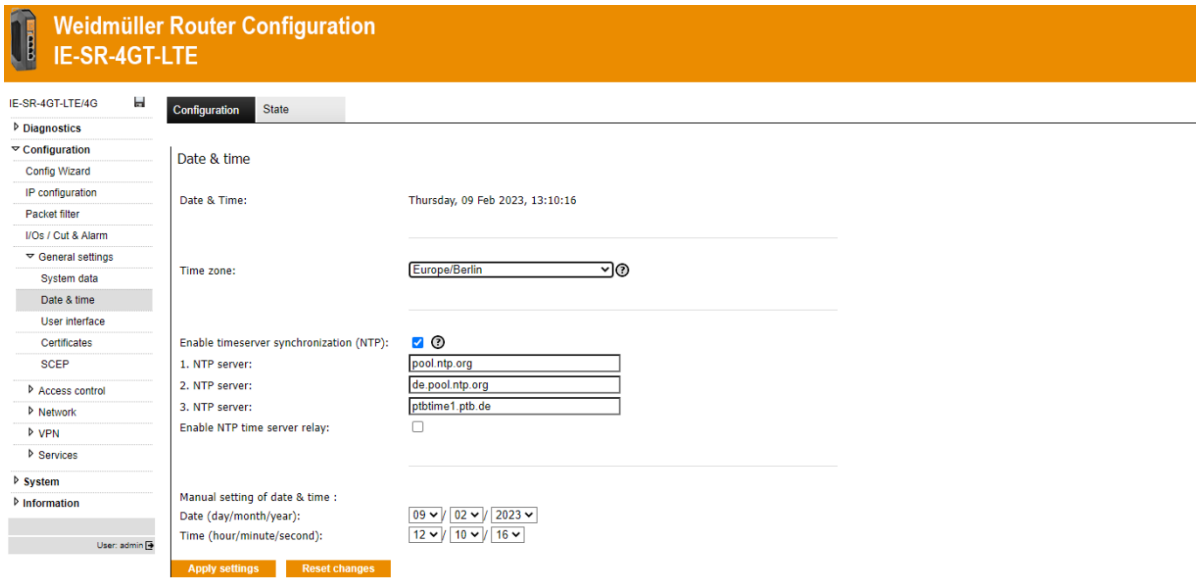


Figure 20: Date & Time settings

►Change to tab “State” to check if an NTP server could be accessed.

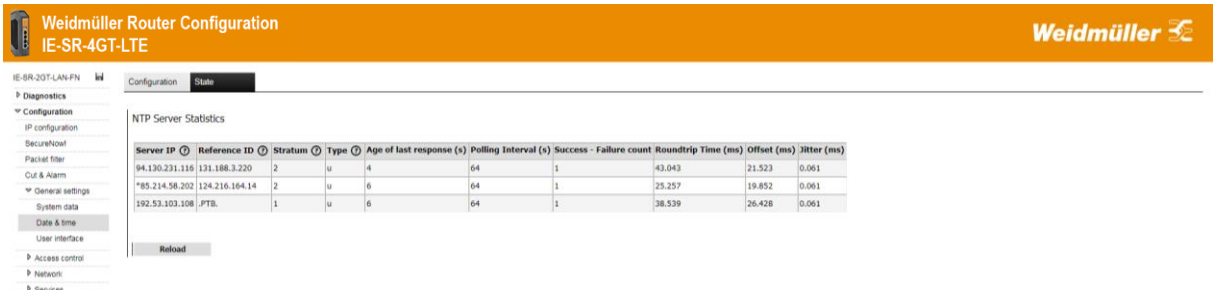


Figure 21: Tab “State” – showing NTP server statistics

A5-2 Configuration of the packet filter (Firewall)

1. General information about behavior and settings of the packet filter settings

If the traffic (Layer 2: Ethernet frames, Layer 3: IP packets) is passing the Router from one interface (e.g. LAN, WAN, 4G) to any other then the firewall checks the data packets according to the defined rules / rule-sets in the order from top to down. If a rule-set condition or a rule (inside of a rule-set) is matching the defined criteria then the action (allow/drop/reject) will be done. After that no further defined rule-set/rule will be applied. If a data packet does not match any of the defined rules then it will be silently dropped (because of the “white list” behavior).

Factory default firewall settings valid for operation mode **“IP Router” (Layer 3)**:

- At operation mode “IP Router” only rules defined on tab “Layer 3” will be applied. Rules defined on tab “Layer 2” are not applied.
- The L3-packet-filter (firewall) behaves according to a “White list”. Only traffic between the interfaces which explicitly is allowed may pass. If the default rule “Allow_L3” (allow each IP based traffic) is deleted then each traffic is blocked. Then the Router’s Web interface only is accessible via the connected interface (from LAN via LAN-IP, from WAN via WAN-IP).

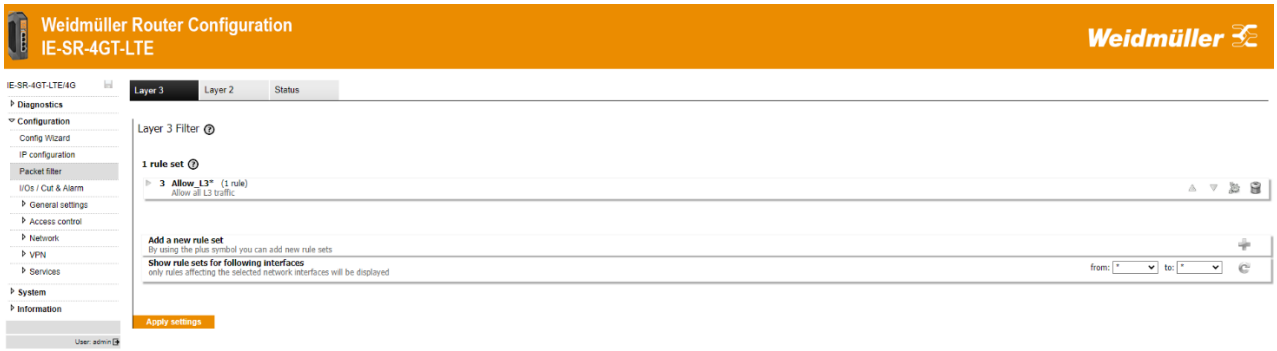


Figure 22: Factory default settings of Layer-3 Packet filter (firewall), valid for operation mode “IP Router”

Factory default firewall settings valid for operation mode **“Transparent bridge” (Layer 2)**:

- At operation mode “Transparent bridge” only rules defined on tab “Layer 2” will be applied. Rules defined on tab “Layer 3” are not applied.
- The L2-packet-filter (firewall) behaves according to a “White list”. Only traffic between the interfaces which explicitly is allowed may pass. If the default rules “ARP*” (ARP protocol) and “Allow_L2*” (allow any Layer 2 traffic including Layer-3 IP packets) are deleted then each traffic is blocked. Then the Router’s Web interface only is accessible via the connected interface (from LAN via LAN-IP, from WAN via WAN-IP).

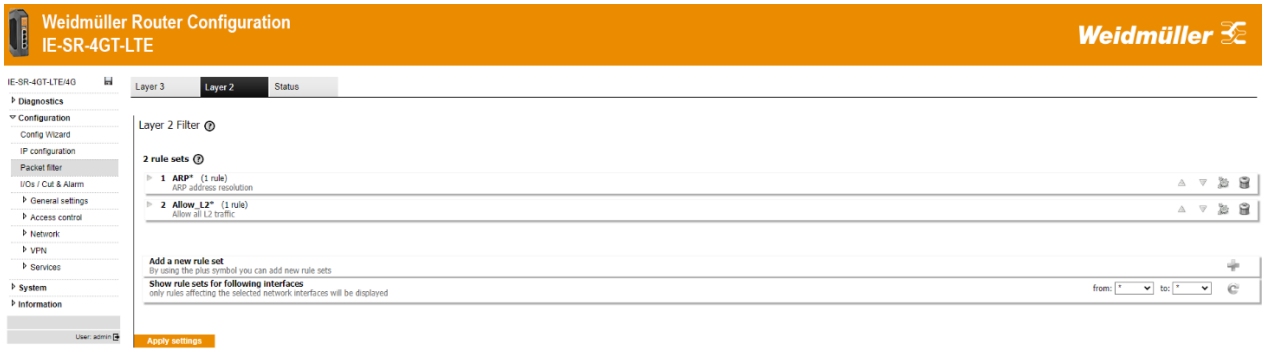


Figure 23: Factory default settings of Layer-2 Packet filter (firewall), valid for operation mode “Transparent bridge”

2. Configuring the packet filter (firewall) according to the above mentioned “Communication requirements”

Note: Since the Router is running in mode “Transparent bridge” we only need to configure new rules on tab “**Layer 2**”.

2. 1 Configuration of a rule-set containing one rule to allow Modbus TCP (protocol TCP and port 502) traffic initiated from WAN port to LAN port.

►Go to menu Configuration → Packet filter.
►Select Tab “Layer 2”.
►Click ‘+’ icon to add a new rule set.

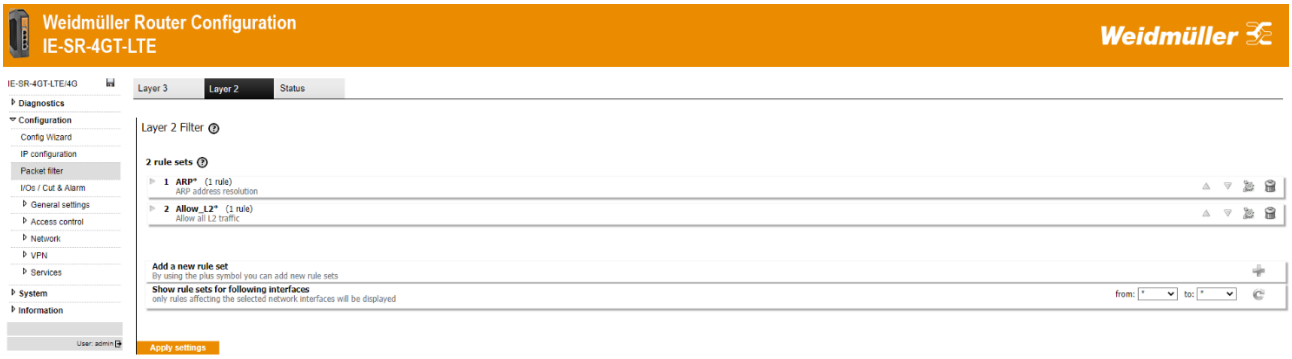


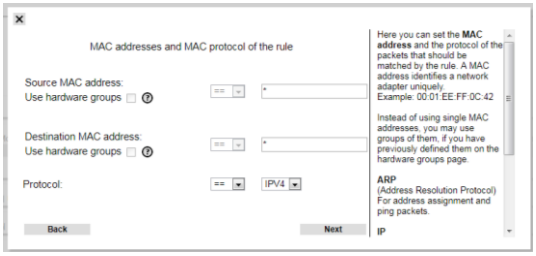
Figure 24: Factory default settings of Layer-2 Packet filter (firewall)

►Add a name for new rule-set (here Modbus_L2).

►Click ‘Next’.

►Select Inbound interface (here WAN) and outbound interface (here LAN).

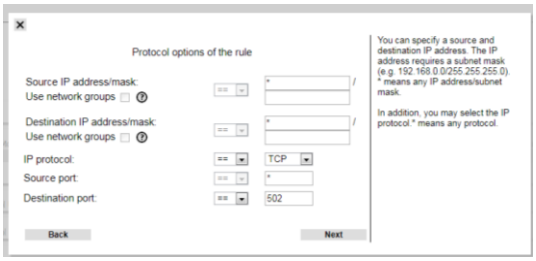
►Click Add to add a new rule inside of this rule-set named Modbus_L2.



►Enter wild character * for source and destination MAC addresses

►Select protocol IPv4 to be checked inside of the Ethernet frame.

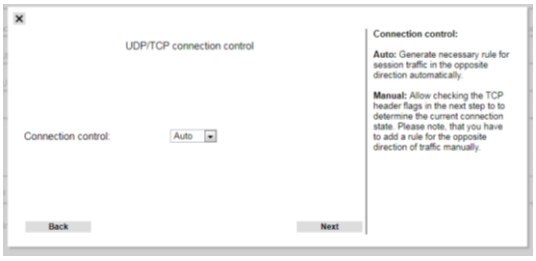
►Click ‘Next’.



►Now define the criteria for investigating an IPv4 packet (check for Modbus communication = TCP/502) .

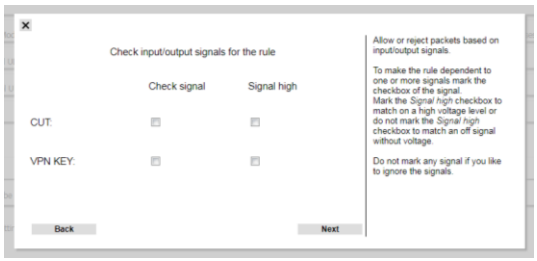
Note: Use always wild character * for source port because it will be created dynamically by the sender (to be used for unique re-addressing of an answer packet by a recipient).

►Click ‘Next’.



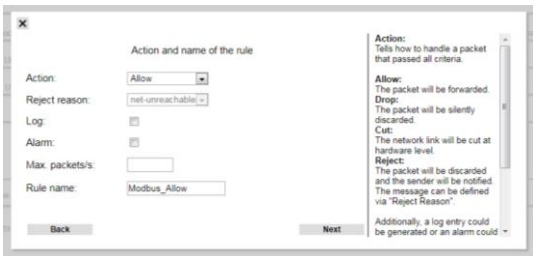
►Select ‘Auto’ for Connection control (Packet filter acts as a stateful inspection firewall and recognizes/allows automatically an answer based on an initiated request).

►Click ‘Next’.



►No signal check and setting.

►Click ‘Next’.



►Now select action (allow) related to the previous defined rules.

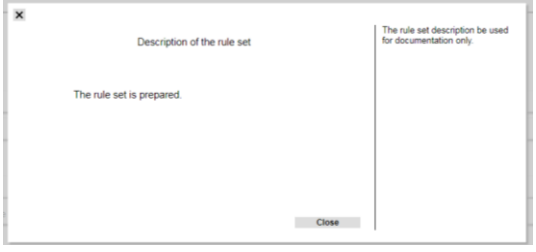
►Add a name for this rule (here Modbus_Allow).

►Click ‘Next’.

Now the new rule “Modbus_Allow” is defined inside of the rule-set container. We do not need to add another rule.

►Add a description text for this rule-set.

►Click ‘Next’.



►Click Close

►Click Next to finish this rule-set (containing 1 rule).

Now the new rule-set Modbus_L2 is displayed in the Layer-2 filter list.

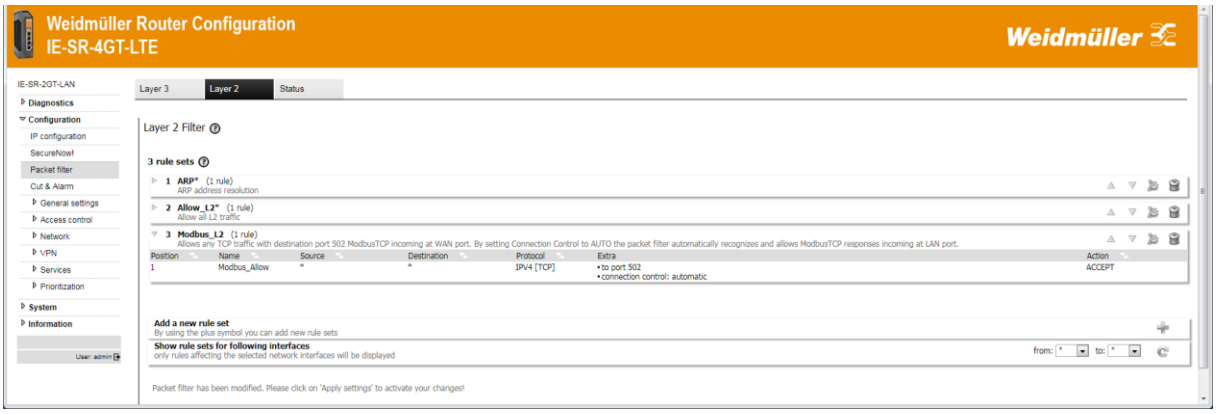
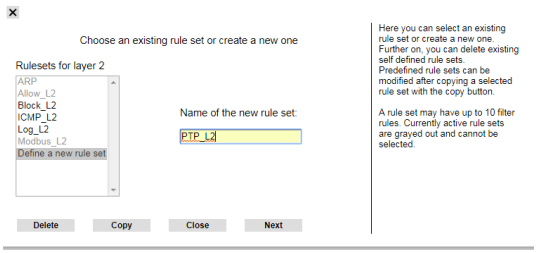


Figure 11: Layer-2 filter list containing new rule-set “Modbus_L2”

As next steps we configure all other necessary firewall settings. After that we will organize all rule-sets in the order (from top to down) and will apply the settings.

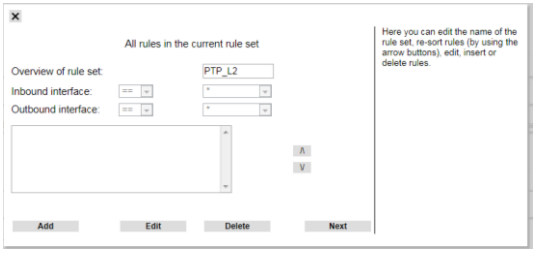
2.2 Configuration of a rule-set containing 2 rules which allow any PTP communication based on protocol UDP, ports 319 and 320, either initially incoming at WAN port or LAN port.

►Click ‘+’ icon to add a new rule-set.

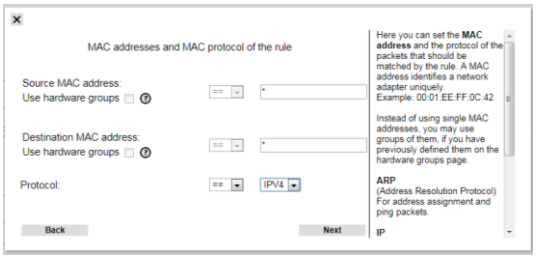


►Add a name for the new rule-set (here PTP_L2).

►Click Next.



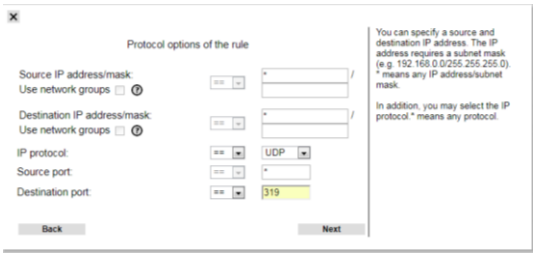
►Click Add to add a new rule to this rule-set (container).



►Enter wild character * for source and destination MAC addresses.

►Select protocol IPv4 to be checked inside of the passing Ethernet frames.

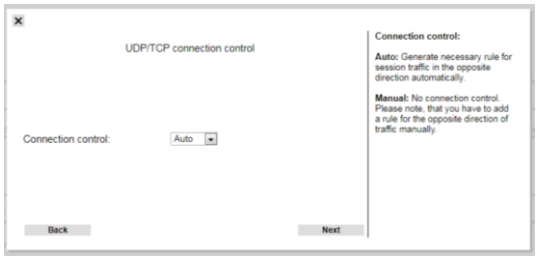
►Click Next.



►Now define the criteria for investigating an IPv4 packet (check for PTP communication UDP/319).

Note: Use always wild character * for source port because it will be created dynamically by the sender (to be used for unique re-addressing of an answer packet by a recipient).

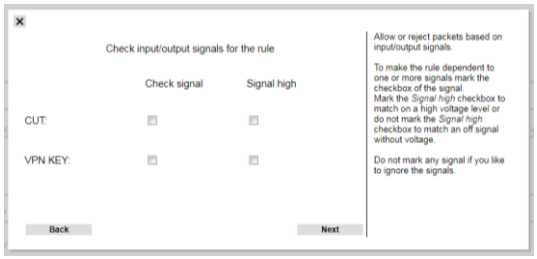
►Click ‘Next’.



►Select auto for Connection control.

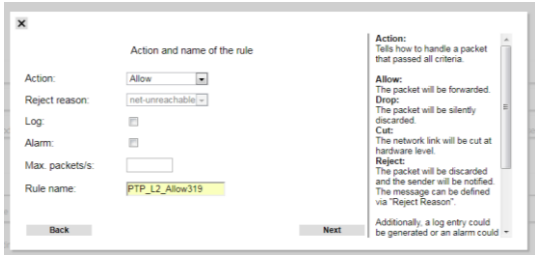
(Packet filter acts as a stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

►Click ‘Next’.



►No signal check and setting.

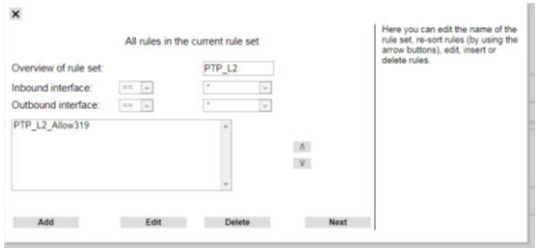
►Click ‘Next’.



►Now select action (allow) related to the previous defined rules.

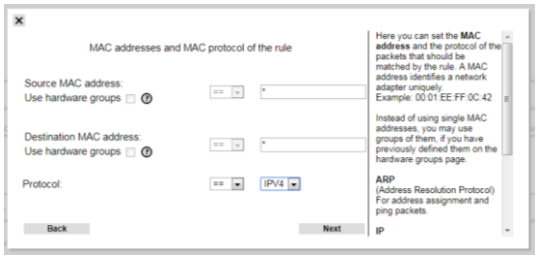
►Add a name for this rule (here PTP_L2_Allow319).

►Click ‘Next’.



Now the new rule PTP_L2_Allow319 is defined inside of the rule-set container. We need to add another rule to allow UDP and port 320 for PTP.

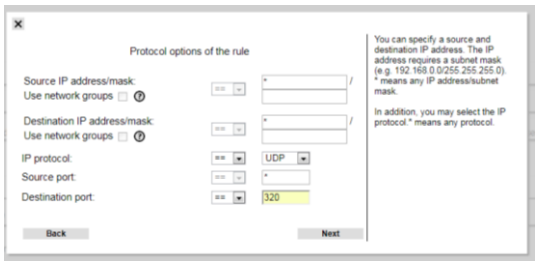
►Click ‘Add’ to add a new rule.



►Enter wild character * for source and destination MAC addresses

►Select protocol IPv4 to be checked inside of the passing Ethernet frames.

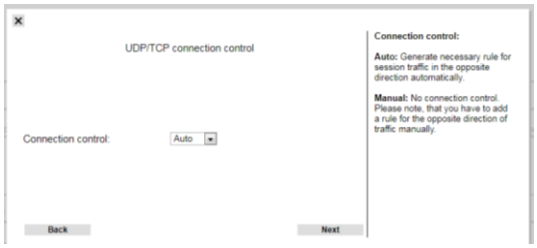
►Click ‘Next’.



►Now define the criteria for investigating an IPv4 packet (check for PTP communication UDP/320).

Note: Use always wild character * for source port because it will be created dynamically by the sender (to be used for unique re-addressing of an answer packet by a recipient).

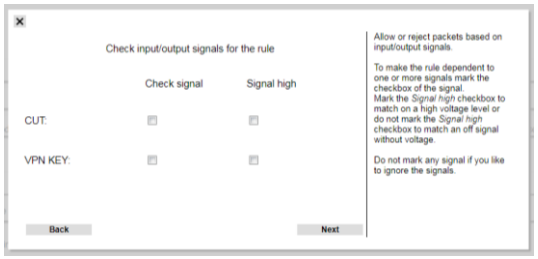
►Click ‘Next’.



►Select auto for Connection control.

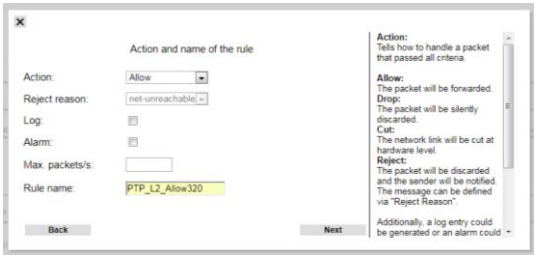
(Packet filter acts as a stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

►Click ‘Next’.



No signal check and setting.

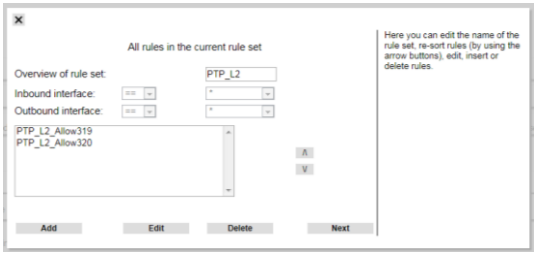
►Click ‘Next’.



►Now select action (allow) related to the previous defined rules.

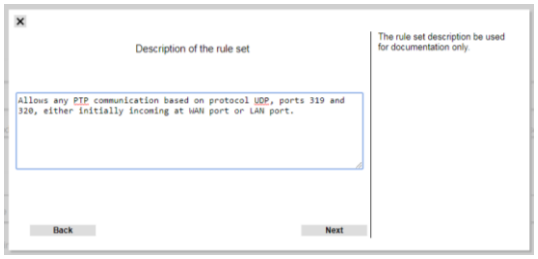
►Add a name for this rule (here PTP_L2_Allow320).

►Click ‘Next’.



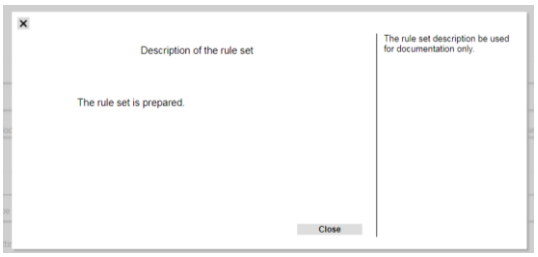
Now both necessary rules are configured.

►Click ‘Next’ to finish the configuration of this rule-set.



►Enter the description text.

►Click ‘Next’.



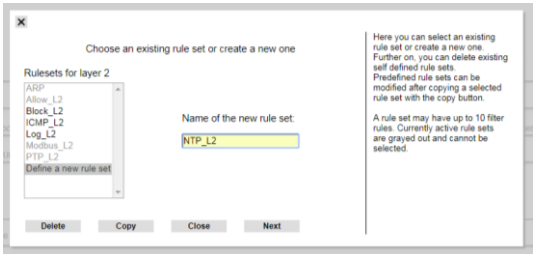
The rule-set is prepared.

►Click ‘Close’.

Figure 12: Layer-2 filter list containing new rule-set “PTP_L2”

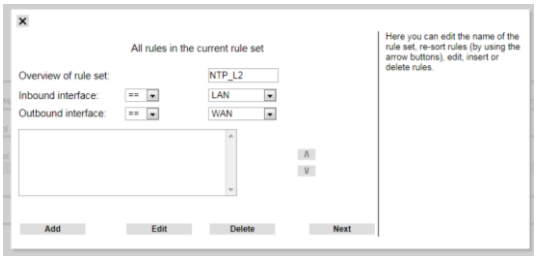
2.3 Configuration of a rule-set containing 1 rule which allows any NTP communication (network time protocol) initiated from devices connected at LAN port (Protocol UDP / Port 123).

►Click ‘+’ icon to add a new rule-set.



►Add a name for the new rule-set (here NTP_L2).

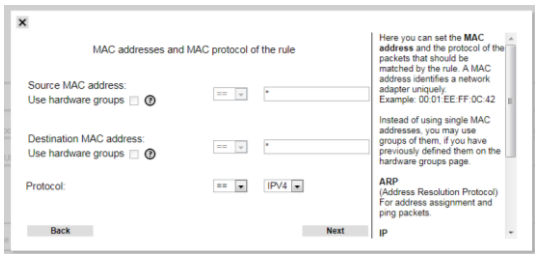
►Click ‘Next’.



►Select inbound and outbound interface.

►Click ‘Add’ to add a new rule.

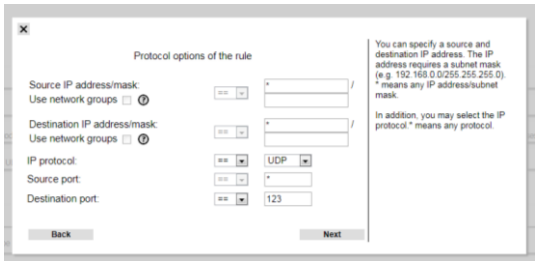
►Click ‘Next’.



►Enter wild character * for source and destination MAC addresses

►Select protocol IPv4 to be checked inside of the passing Ethernet frames.

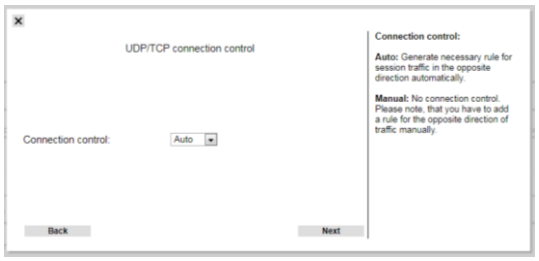
►Click ‘Next’.



►Define the criteria for investigating an IPv4 packet (check for NTP communication UDP/123)

Note: Use always wild character * for source port because it will be created dynamically by the sender (to be used for unique re-addressing of an answer packet by a recipient).

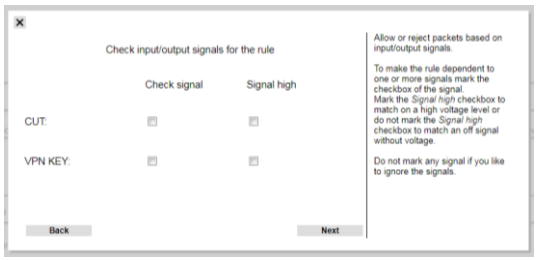
►Click ‘Next’.



►Select auto for Connection control.

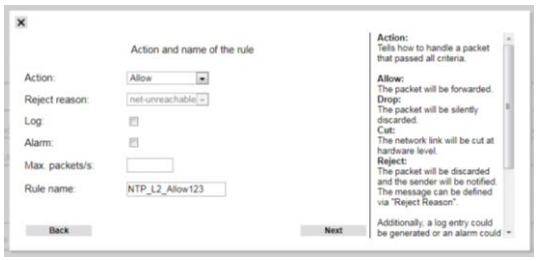
(Packet filter acts as an stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

►Click ‘Next’.



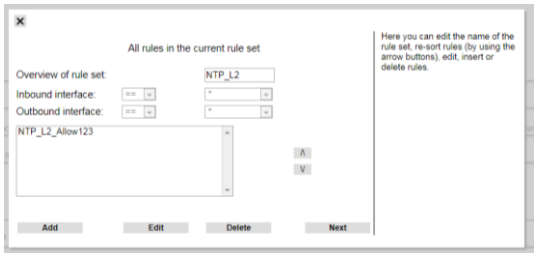
No signal check and setting.

►Click ‘Next’.



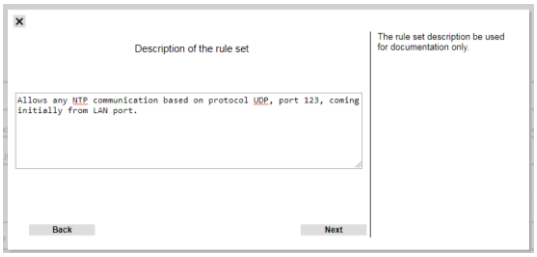
►Select action (allow) related to the previous defined rules. ►Add a name for this rule (here NTP_L2_Allow123).

►Click ‘Next’.



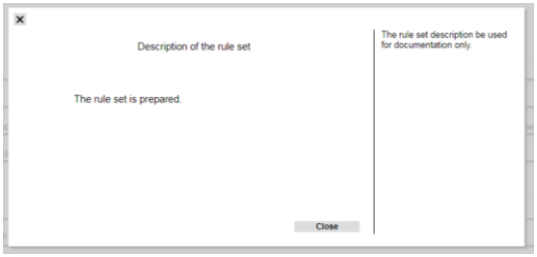
Now the necessary rule is configured.

►Click ‘Next’ to finish the configuration of this rule-set.



►Enter the description text.

►Click ‘Next’.



►Click ‘Close’.

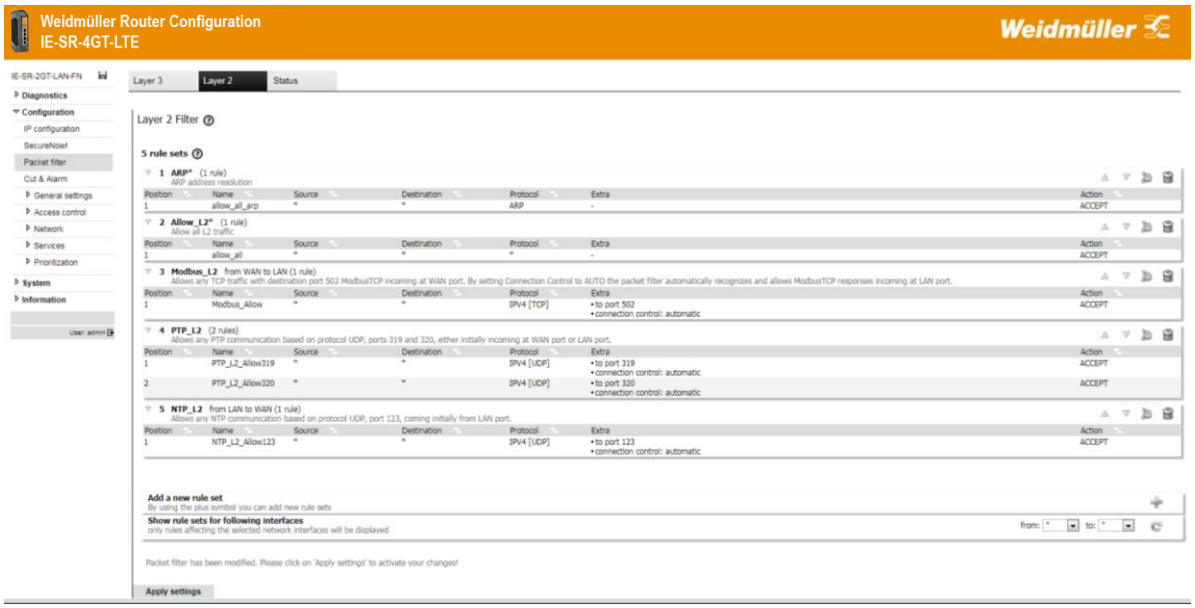


Figure 25: Layer-2 filter list containing new rule-set “NTP_L2”

Finally we have to remove the factory default rule-set “Allow_L2*” which allows each traffic to pass.

►Click the ‘trashcan’ button of row “Allow_L2*” to remove this rule-set. Now all necessary rules are defined.
►Click button “Apply settings” to activate the configured settings.

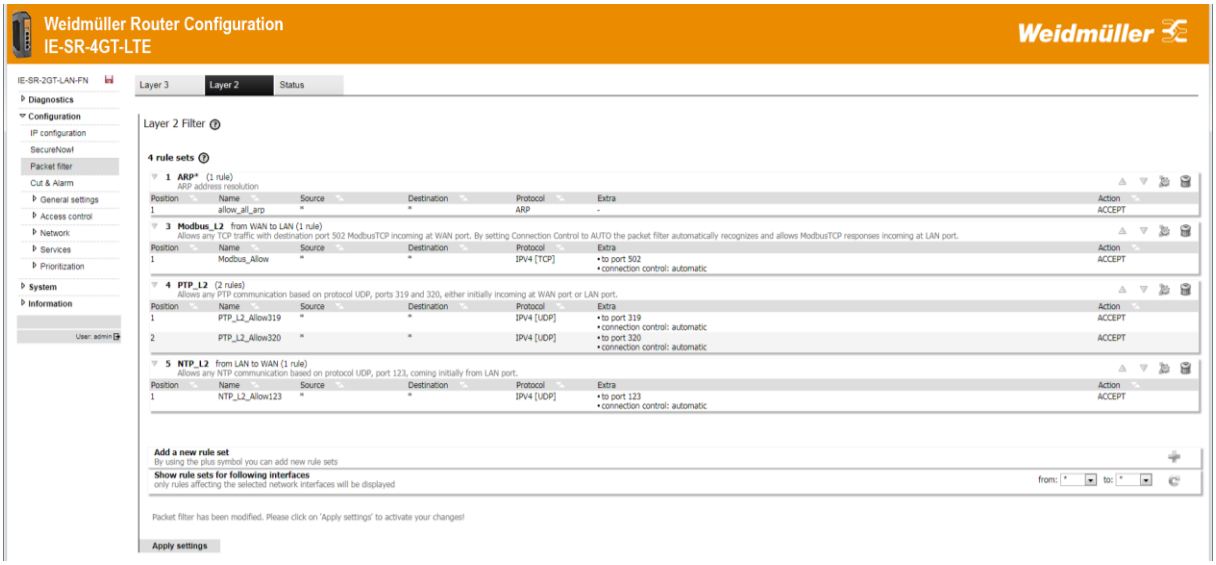
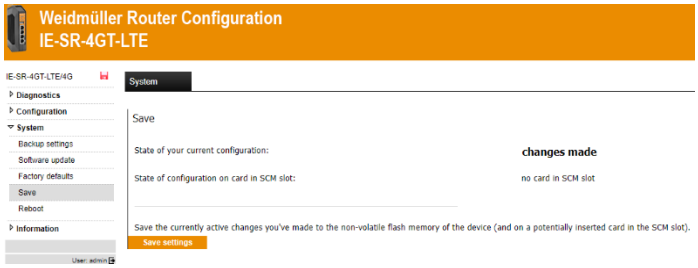


Figure 26: Final list of Layer-2 filter

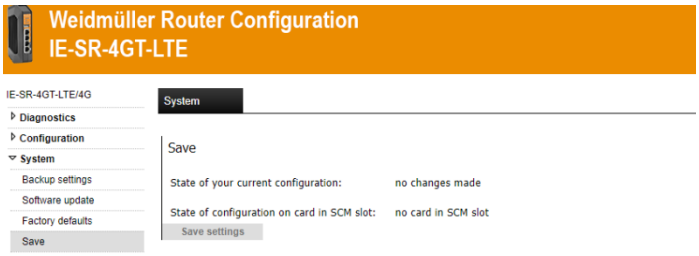
Note: You do not need to configure a special “Block all” rule at the end of the filter list. If a data packet does not match any of these defined rules then it will be silently dropped (because of the “white list” behavior).

A5-3 Save the configuration



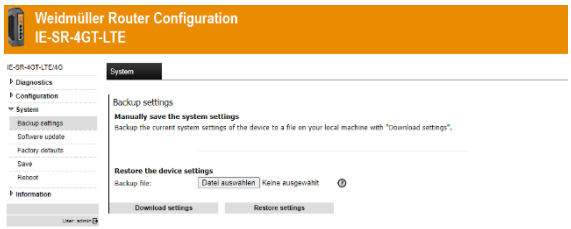
►Goto menu System → Save.

►Click ‘Save settings’.



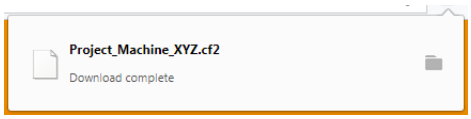
Now the settings are saved in the flush memory.

A5-4 Create a backup file of the configuration



►Goto menu System → Backup Settings.

►Click button ‘Download Settings’.



As result the configuration file (with extension .cf2) will be stored on the PC’s download directory. For re-storing select this file via button ‘Choose file’ and click button ‘Restore settings’.

A6 - Connecting 2 networks with same IP ranges to another network using 1:1 NAT and IP routing (extended)

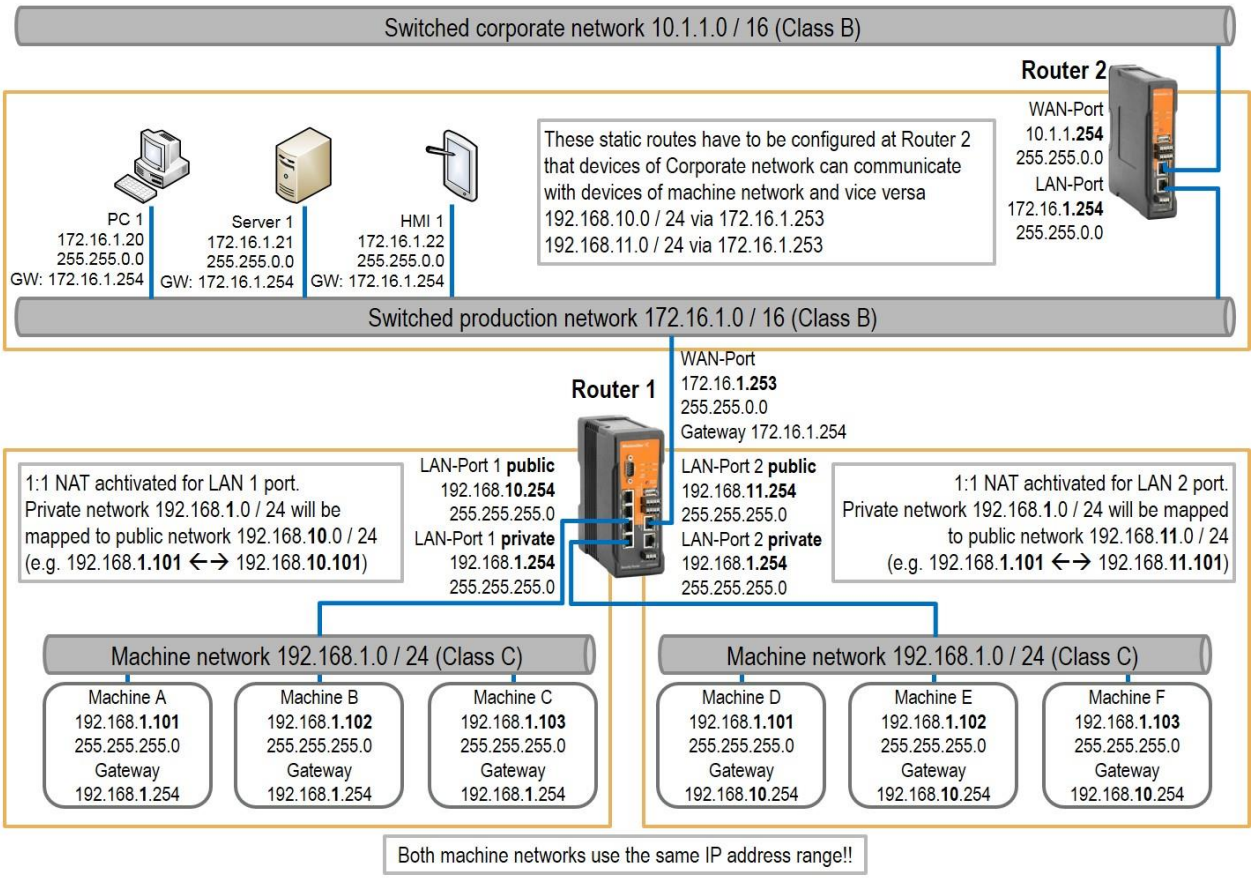
Application scenario:

There are 2 machine networks and one upper-level production network. Both machine networks are connected to the production network by a 4-port Security Router in extended routing mode. The production network itself is connected to the corporate network via its own Router. Both machine networks have the same IP address range 192.168.1.0 of type class C: The production network uses the IP address range 172.16.1.0 of type class B.

Task and solution:

Each Ethernet device of all 3 networks shall have the possibility to communicate with each other. For this reason, it is necessary that each of the machine networks – both configured with the same IP address range - must be translated to unique IP addresses. This can be done by using the network IP address translation feature “1:1 NAT” of the Router.

1:1 NAT means that IP addresses (**private**) of devices connected to the LAN port, internally will be translated to a new IP address (**public**) if they communicate with IP addresses on other interfaces. From the perspective of the WAN network each device of the LAN network is only known and addressable by its **public** IP address. In the case of incoming data from WAN network (outgoing to LAN) the destination IP addresses (public) of LAN network automatically will be translated from their **public** into their **private** IP address.



This document describes an application scenario using 2 Routers. But for a simple test of the feature “1:1 NAT” you only need 1 Router (configured as Router 1). In this case use 2 devices (PC’s or whatever) to simulate one member of “machine network” and one member of the “production network”.

Short description how to solve the task by using 1:1 NAT:

Router 1 must be connected by WAN port to the production network 172.16.1.0. The IP addresses of the WAN ports will be set to 172.16.1.253 / 255.255.0.0

The LAN ports of the Router is to be connected to their corresponding machine network. Due to the fact that each machine network uses the same IP address range each LAN port of the Routers is to be configured with 2 IP addresses, one as a **public** and one as **private** address.

In this example – using the feature 1:1 NAT at **LAN port**s of Router 1 the **public** IP addresses will be set to

LAN 1: 192.168.**10**.254 / 255.255.255.0

LAN 2: 192.168.**11**.254 / 255.255.255.0

and the **private** IP addresses (both the same) will be set to

LAN 1: 192.168.**1**.254 / 255.255.255.0

LAN 2: 192.168.**1**.254 / 255.255.255.0

By assigning the **private** IP address (192.168.1.254) at the Router's LAN port automatically the complete IP address range 192.168.1.0 / 255.255.255.0 is defined as local network IP range for devices connected to the LAN port.

"1:1 NAT" means that for each communication of devices of LAN network to another network the **public** IP addresses of LAN devices will be used. For communication in the LAN network the private IP is used.

<table>
<tr><th colspan="4">Examples of IP address mapping (private/public) using 1:1 NAT at LAN port</th></tr>
<tr><td>IP address and subnet of a device connected to LAN port (used as private IP address)</td><td>Configured private IP address and subnet on Router's LAN port</td><td>Configured public IP address and subnet on Router's LAN port</td><td>Resulting public IP address and subnet of a device connected to LAN port (1:1 NAT)</td></tr>
<tr><td></td><td colspan="2">Subnets of private and public network must be the same</td><td>This IP address is known by devices of other subnets</td></tr>
<tr><td>192.168.1.101 / 255.255.255.0</td><td rowspan="3">192.168.1.254 / 255.255.255.0</td><td rowspan="3">192.168.10.254 / 255.255.255.0</td><td>192.168.10.101 / 255.255.255.0</td></tr>
<tr><td>192.168.1.102 / 255.255.255.0</td><td>192.168.10.102 / 255.255.255.0</td></tr>
<tr><td>192.168.1.103 / 255.255.255.0</td><td>192.168.10.103 / 255.255.255.0</td></tr>
<tr><td>10.8.1.10 / 255.255.0.0</td><td rowspan="2">10.8.1.254 / 255.255.0.0</td><td rowspan="2">172.16.1.254 / 255.255.0.0</td><td>172.16.1.10 / 255.255.0.0</td></tr>
<tr><td>10.8.2.10 / 255.255.0.0</td><td>172.16.2.10 / 255.255.0.0</td></tr>
<tr><td colspan="4">In a class C network with subnet mask 255.255.255.0 only the last segment of an IP address is translated</td></tr>
<tr><td colspan="4">In a class B network with subnet mask 255.255.0.0 the last two segments of an IP address are translated</td></tr>
</table>

How to configure Router 1 (Machine networks) and Router 2 (Production network)

General note:

The configuration of all Routers is very similar and will be described below together for the Routers of both machine networks and the production network. Different configuration parameters between the Routers are marked individually.

In this example Router 2 of the production network is to be configured with 2 static IP routes pointing to networks 1 and 2 that Ethernet devices behind Router 1 (connected at LAN port 1 and 2) can find each other. As an alternative all Routers can be configured to use dynamic IP routing (either RIP or OSPF or both) to announce their connected networks to the other Routers automatically without configuring static routes at Router 3 manually. Using dynamic routing is more convenient if it is planned to extend the Ethernet network with additional machine networks. Then you don't have to add a new static route to Router 2 in the case of

connecting a further machine network to the production network. This would be automatically done by RIP- or OSPF-based dynamic IP routing.

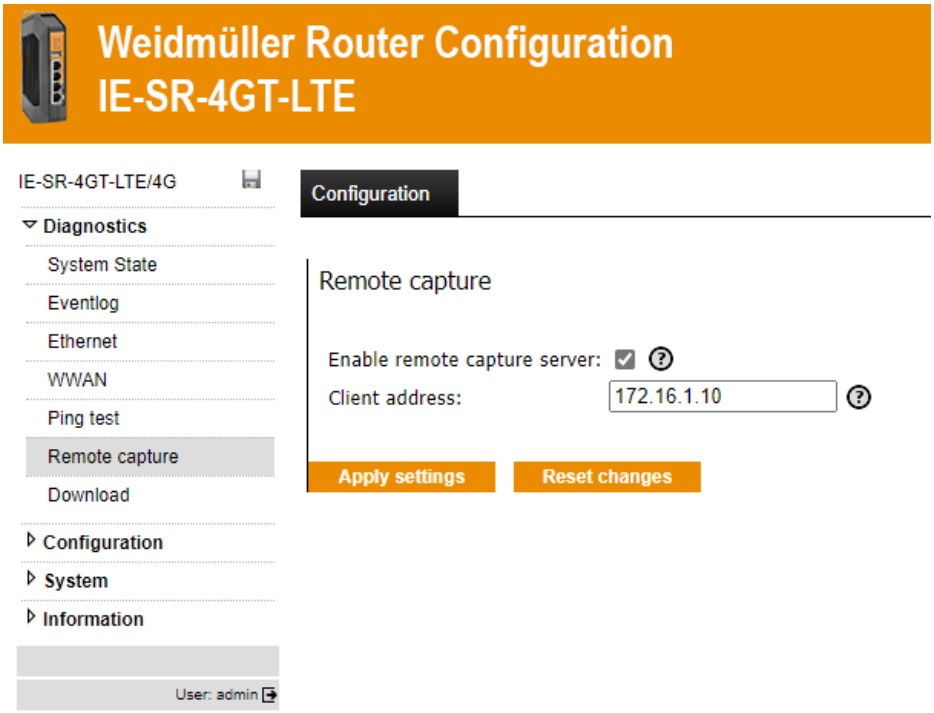
→ The alternative method using dynamic routing is described in chapter A6 - How to use feature “Remote Capture” with Wireshark to analyse Router’s LAN/WAN traffic

The function “Remote Capture” can be used to record the traffic at Router’s LAN- or WAN port using a remote connected PC running Wireshark. The PC is located somewhere in the network and must be able to access one of the IP addresses of the Router.

Step-by-step guidance

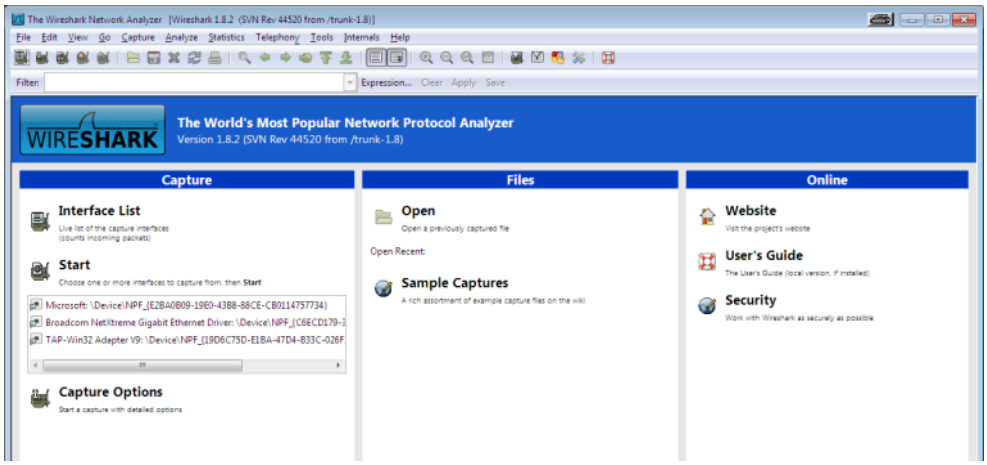
1. Activate the “Remote capture” feature of the Router as shown below (Menu Diagnostics → Remote Capture)

Note: Only one Wireshark-Client-PC (here 172.16.1.10) can be used at the same time record the traffic by Wireshark. Please deactivate this feature if you no longer need to analyse the traffic because it has an impact on the performance of the Router.

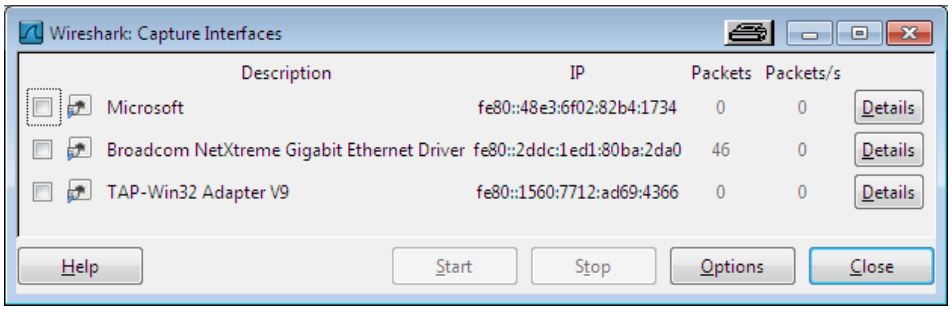


2. Start Wireshark at your PC

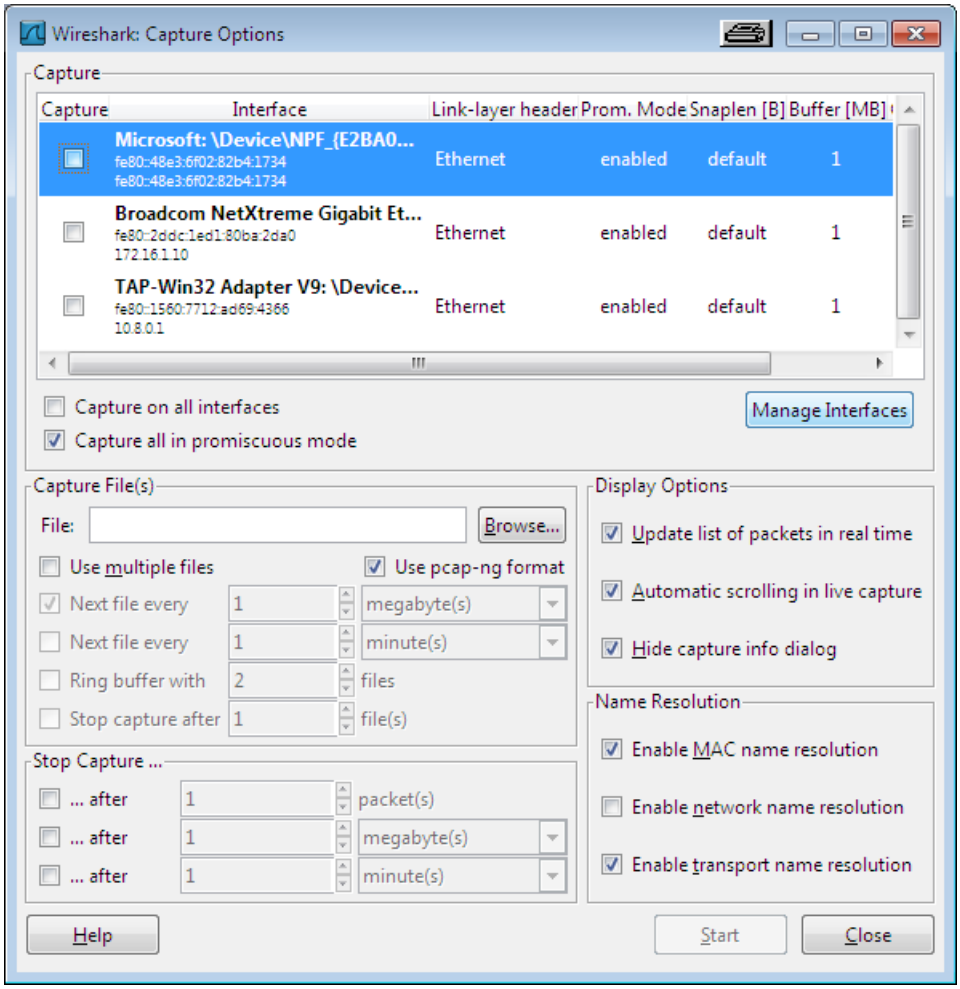
3. Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”



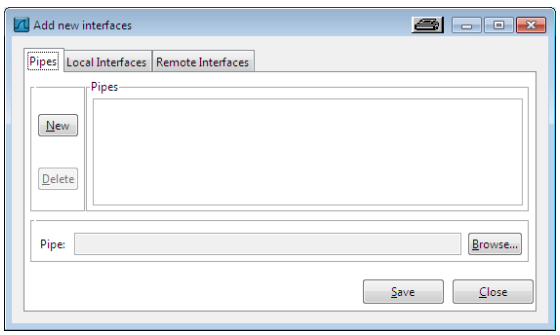
The local Ethernet Interfaces of the computer will be displayed.

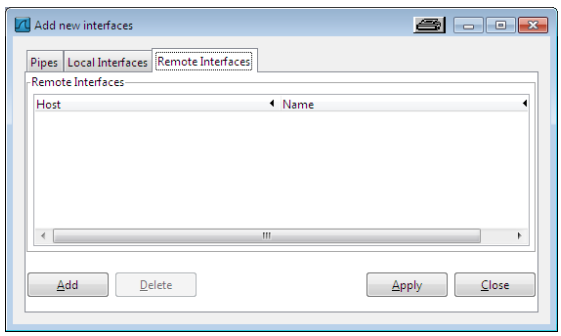


4. Click button “Options”

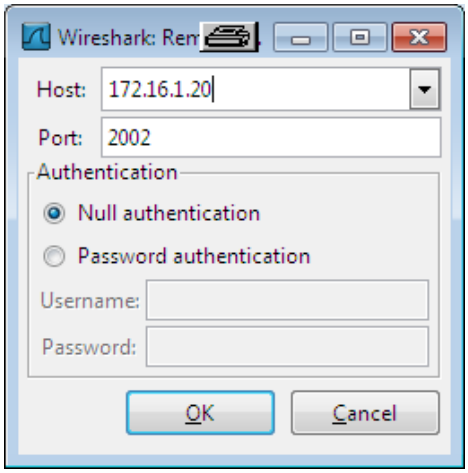


5. Click button “Manage Interfaces” and change to tab “Remote Interfaces”





6. Click button “Add”



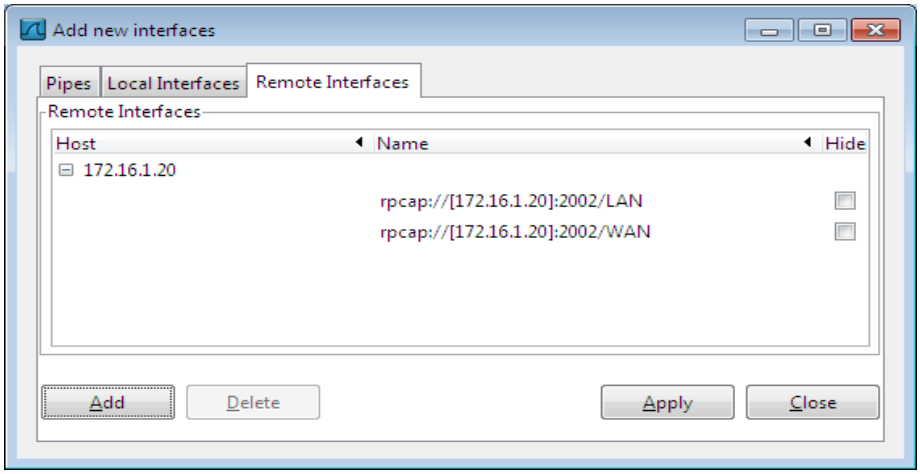
7. Enter the IP address of the Router to field “Host”

Note: You can enter either the IP address of LAN or WAN port. The import fact is that the Routers IP address is accessible by the Wireshark-PC.

8. Enter into field “Port” the value 2002 (will be filled automatically if you enter an IP address)

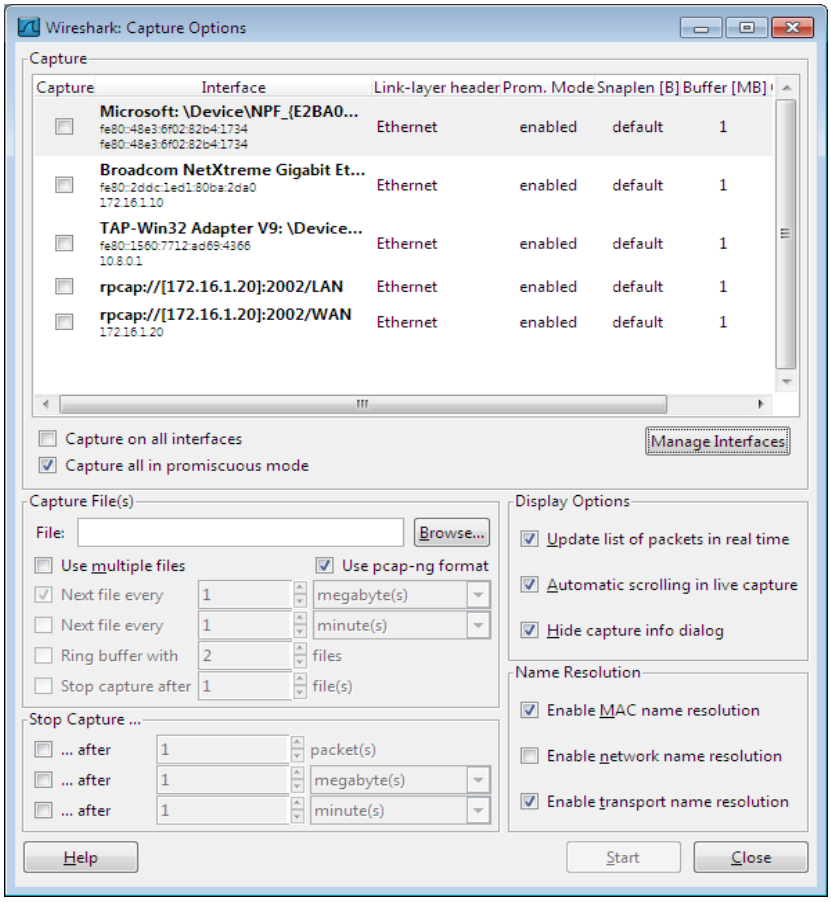
9. Click button OK

Now both Interfaces of the Router (= Host 172.16.1.20) should be displayed.



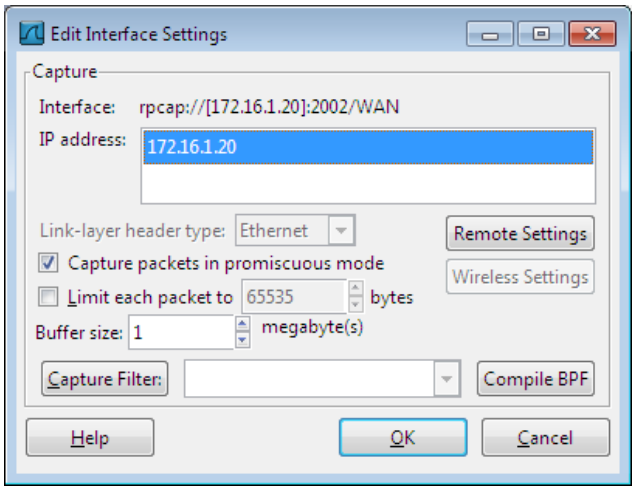
10. Click button Close

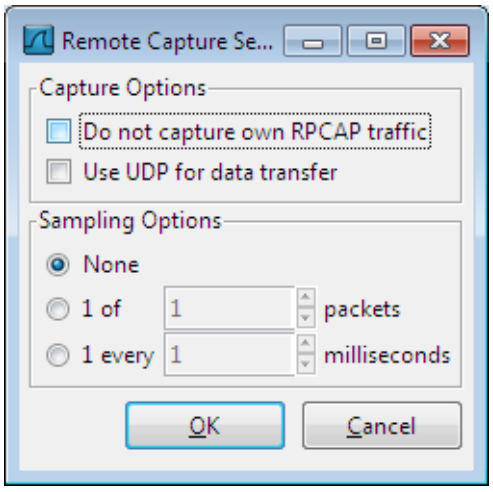
The “remote capture interfaces” will be displayed in the list of selectable interfaces.



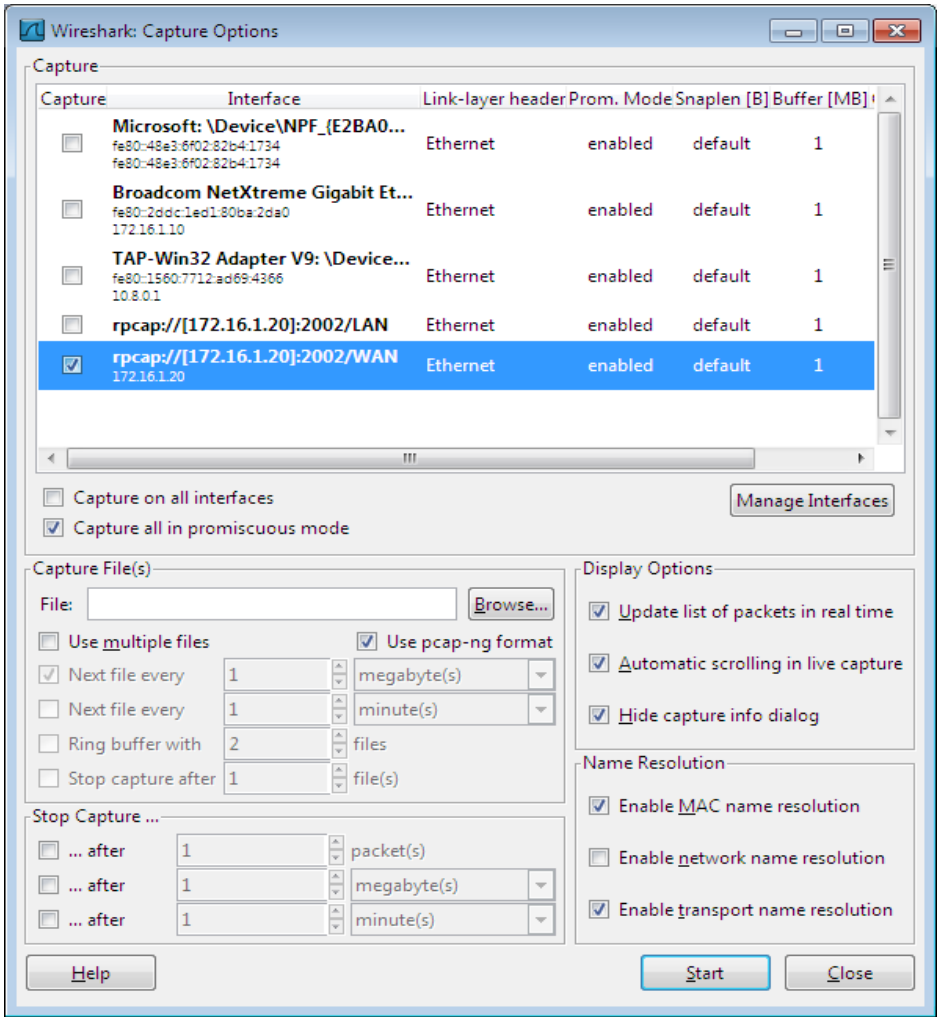
In this example we want to capture the traffic at WAN port.

11. Double-Click the line **rpcap//[172.16.1.20]:2002/WAN**



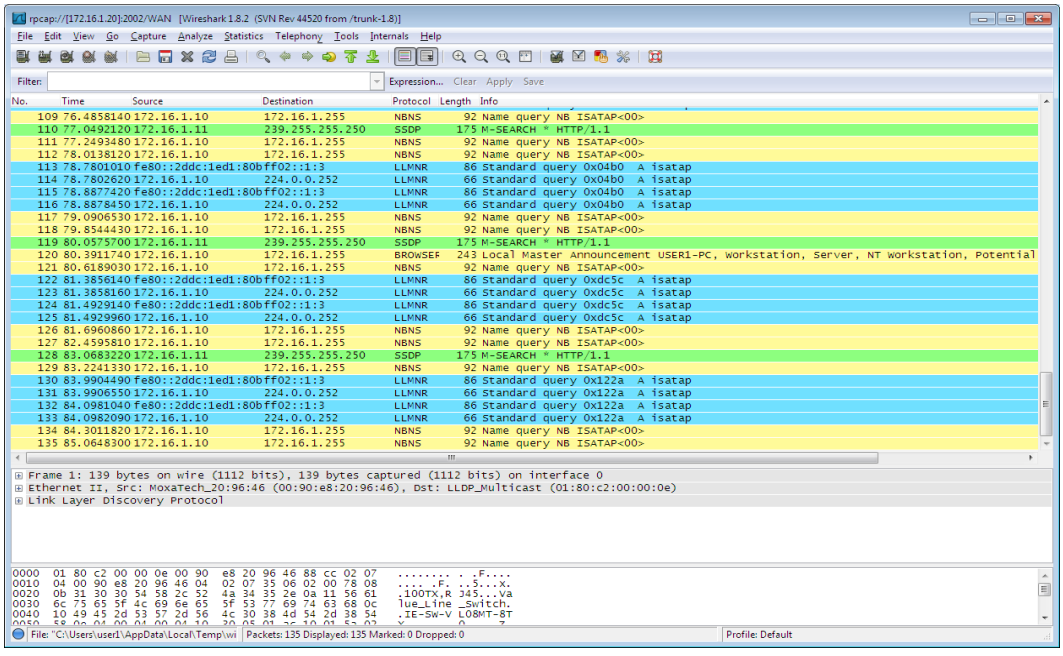


12. Click button “Remote Settings”
13. **Clear** the checkbox “Do not capture own RPCAP traffic”
14. Click button “OK”
15. Again click button “OK” to close the window “Edit Interface Settings”



16. Activate the checkbox in line **rpcap//[172.16.1.20]:2002/WAN**

17. Click button “Start” to record the traffic at Routers WAN port



A7 - Using dynamic IP routing alternatively to manually configured static routes.

Starting situation
All Routers have the factory default configuration and can be accessed either using the LAN port by IP address 192.168.1.110 or using the WAN port and find the IP address with the Router Search Utility. Since the machine network Router 1 must be configured on the LAN port with 1:1 NAT (with a private and a public IP address), which means setting two times new IP addresses (private and a public) on this port during the configuration process, it is more comfortable to connect the Configuration PC to the WAN port of the Routers. Then the IP address of the PC has only one time to be changed after setting the new WAN port IP address.

1. Connect the configuration PC to the Router using the WAN Port

→ Use auto-negotiation on the Ethernet Interface of the PC

2. Change the IP address of the PC to one of the range of WAN IP

→ e.g. IP address 192.168.xxx.xxx
Subnet mask 255.255.255.0
Standard gateway can be left blank due to direct cable connection

3. Start a Web browser and login into the Web server of Router (http://192.168.2.110)

User: admin
Password: Detmold

4. Set the basic IP configuration

► Select menu Configuration → IP configuration

► Configure the menu entries as following shown

Configuration Router 1:

Operational mode:	**IP Router (extended)**
IP address parameters **WAN** Port:	Static
	172.16.1.253
	255.255.0.0 (Class B)
	NAT (masquerading) **NOT SET**
IP address parameters **ETH 2** Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
IP address parameters **ETH 3** Port:	Static
	192.168.11.254
	255.255.255.0 (Class C)
	NAT (masquerading) **NOT SET**
ETH 4 Port	Leave it as it is, we do not need the port in this application
WWAN	Leave it in the status “disabled”.
Default gateway	172.16.1.254

Configuration Router 2:

Operational mode:	IP Router

IP address parameters **WAN** Port:	Static
	10.1.1.254
	255.255.0.0 (Class B)
	NAT (masquerading) **NOT SET**
IP address parameters **LAN** Port:	Static
	172.16.1.254
	255.255.0.0 (Class C)
	NAT (masquerading) **NOT SET**
WWAN	Disabled
Default gateway	leave field empty (not necessary in this example)

► Click button “Apply settings” to activate the new settings.

Now the configured parameters will be **activated (but not saved)**. After a few seconds the web interface displays the new IP addresses as shown in Figure 3. Please keep in mind that now the Router connection is lost due to changing the IP address range of your connected WAN port.

5. Change the IP address of configuration PC

► To reconnect to the Router now change the IP address of the PC to an IP address of the new IP address range

- Router 1: 172.16.1.0/16 WAN side
- Router 2: 172.16.1.0/16 LAN side

For re-connecting to Routers 1 and 2 chose e.g. IP address 172.16.1.100 and subnet mask 255.255.0.0. The input field “Standard-Gateway” can be left empty. For reconnecting Router 2 you also can chose e.g. IP address 172.16.1.100 (subnet mask 255.255.0.0) but you must change the cable connection from WAN to LAN port due to the fact that Router 2 is connected to the production network by LAN port (see network diagram). Otherwise you must use an IP address of the WAN port range 10.1.0.0.

► Again login into the web interface of the Router using a web browser

Only for Router 1: Use IP address 172.16.1.253 (http://172.16.1.252) on WAN port
Only for Router 2: Use IP address 172.16.1.254 (http://172.16.1.254) on LAN port

User: admin
Password: Detmold

► Select menu **Configuration → IP configuration** to verify that IP parameters are configured correctly

6. Configuring 1:1 NAT address translation for Router 1

► Select menu Configuration → Network → 1:1 NAT

Configure below described entries on **Router 1** in the section **ETH 2..3:** of the “1:1 NAT configuration menu”.

► Activate parameter “Enable 1:1 NAT” → Click on checkbox

► Private IP address/subnet mask: 192.168.1.254/24

Note: No further settings have to be done (Do not activate checkbox “Advanced settings”)

► Click button “Apply settings” to activate the new settings.

Note:
The **private** IP address 192.168.1.254 now is the new IP address of the Router from the perspective of connected devices at the LAN port. All devices connected to the LAN port must be configured in the private IP range 192.168.1.0 with subnet mask 255.255.255.0.

The 1:1 NAT (address translation) is working in that way that every address of the private Class C network will be changed to the corresponding public address.
Exemplary result of IP address mapping of configured 1:1 NAT of **Router 1**:

- Machine A of network 1 (**192.168.1.101**) can be accessed by **public IP 192.168.10.101**
- Machine B of network 1 (**192.168.1.102**) can be accessed by **public IP 192.168.10.102**
- Machine C of network 1 (**192.168.1.103**) can be accessed by **public IP 192.168.10.103**

Exemplary result IP address mapping of configured 1:1 NAT of **Router 2**:

- Machine D of network 1 (**192.168.1.101**) can be accessed by **public IP 192.168.11.101**
- Machine E of network 1 (**192.168.1.102**) can be accessed by **public IP 192.168.11.102**
- Machine F of network 1 (**192.168.1.103)** can be accessed by **public IP 192.168.11.103**

From the perspective of an addressed receiver in the production network the sender has always the **public** IP address.

7. Configuring static routes for Router 2

Next 2 static routes must be configured on Router 2 that all Ethernet devices of machine networks (behind LAN ports of Routers 1) can get access to each other.

► Select menu **Configuration → Network → IP routing→ Tab "Configuration"**
Configure below described entries in the area **Add new static route** of the menu:

Static routes for Router 2 (This Router has 2 static routes)

Values for the first route:	
Destination network	192.168.10.0 (Public address range of machine network 1 at LAN port of Router 1)
Subnet mask	24 (Class C)
Gateway	172.16.1.253 (Public address of WAN port of Router 1)
Metric	Can be left blank (only one route, therefore no need for prioritization)
Interface	**LAN** (Router 1 can be reached by LAN port)
Values for the second route:	
Destination network	192.168.11.0 (Public address range of machine network 1 at LAN port of Router 1)
Subnet mask	24 (Class C)
Gateway	172.16.1.253 (Public address of WAN port of Router 1)
Metric	Can be left blank (only one route, therefore no need for prioritization)
Interface	**LAN** (Router 1 can be reached by LAN port)

►Click button "Add entry" to add the new static route to the routing table.
►Click button "Add entry" to add the new static route to the routing table.
►Then click button "Apply settings" to activate the new settings.

8. Monitoring the new activated "routes" at Router 3

► Select menu Configuration → Network → IP routing → Tab "State"

9. Saving the new configuration

► Select menu System → Save

► Click on button “Save settings” to save the current configuration to the non-volatile flash memory of the Router. If a SIM memory card is installed the configuration additionally will be stored on the SIM memory card. Additionally, the configuration can be stored on the file system of the PC.

► Select menu **System → Backup settings**

► Click on button “Download settings” to write the configuration file to the PC hard disk (Backup file has the default extension *.cf2”)

Now Router configuration is finished!

1. Testing the accessibility between an Ethernet device of machine network 1 and an Ethernet device of production network (“Simple scenario” if you have only 1 Router for testing)

Note: You can use a PC for simulating an Ethernet device (machine) of networks 1. Use a second PC to be a member of the production network.
Ensure that the PC simulating machine A of network 1 is configured using following parameters:
→ IP: 192.168.1.101, net mask: 255.255.255.0, Standard Gateway: 192.168.1.254
Ensure that the PC of production network is configured using following parameters:
→ IP: 172.16.1.20, net mask: 255.255.255.0, Standard Gateway: 172.16.1.252 (pointing to WAN port of your Router)

1.1 Try to to send a ping request from machine **A** (192.168.1.101) to PC of production network (172.16.1.20).

Result: PC of production network should reply the “ping request” with original reply IP address 172.16.1.20.

1.2 Try to to send a ping request from PC of production network (172.16.1.20) to machine **A** (192.168.1.101) by using the public IP address 192.168.**10**.101.

Result: Machine A should reply the “ping request” with reply IP address 192.168.**10**.101 (due to configured 1:1 NAT).

2. Testing the accessibility between Ethernet devices of machine networks 1 and 2 according to the described application scenario (using 3 Routers)

Note: You can use PC’s for simulating the Ethernet devices (machines) of networks 1 and 2.
Ensure that the Ethernet devices of both machine networks are configured using following parameters:
IP: 192.168.1.100, net mask: 255.255.255.0, Standard Gateway: 192.168.1.254

2.1 Try to send a ping request from machine **A** (192.168.1.101) to machine **D** (same IP 192.168.1.101) by using the public IP address 192.168.**11**.101.

Result: Machine **D** should reply the “ping request” with reply IP address 192.168.**11**.101 (due to configured 1:1 NAT).

2.2 Try to send a ping request from machine **D** (192.168.1.101) to machine **A** (same IP 192.168.1.101) by using the public IP address 192.168.**10**.100.

Result: Machine A should reply the “ping request” with reply IP address 192.168.**20**.100 (due to configured 1:1 NAT).

	Note
	1. If you perform the ping test using a PC please check the PC’s firewall configuration to ensure that ping requests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gateway (IP address is pointing to the Router of the PC’s network)

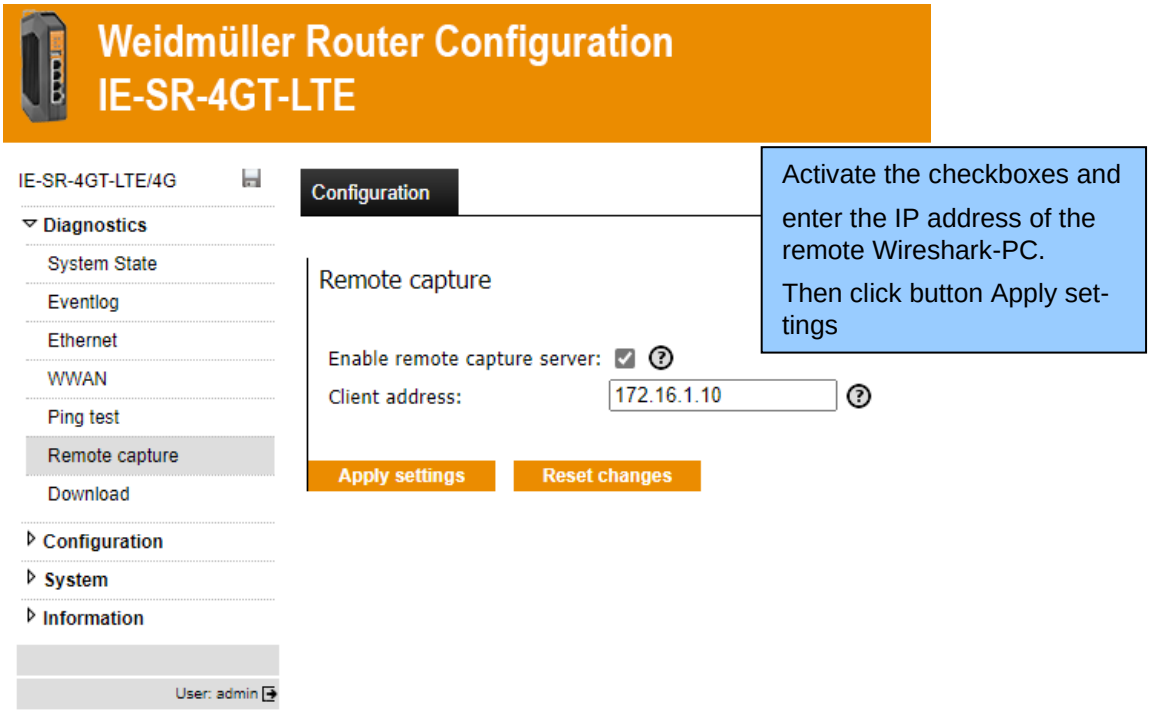
A6 - How to use feature “Remote Capture” with Wireshark to analyse Router’s LAN/WAN traffic

The function “Remote Capture” can be used to record the traffic at Router’s LAN- or WAN port using a remote connected PC running Wireshark. The PC is located somewhere in the network and must be able to access one of the IP addresses of the Router.

Step-by-step guidance

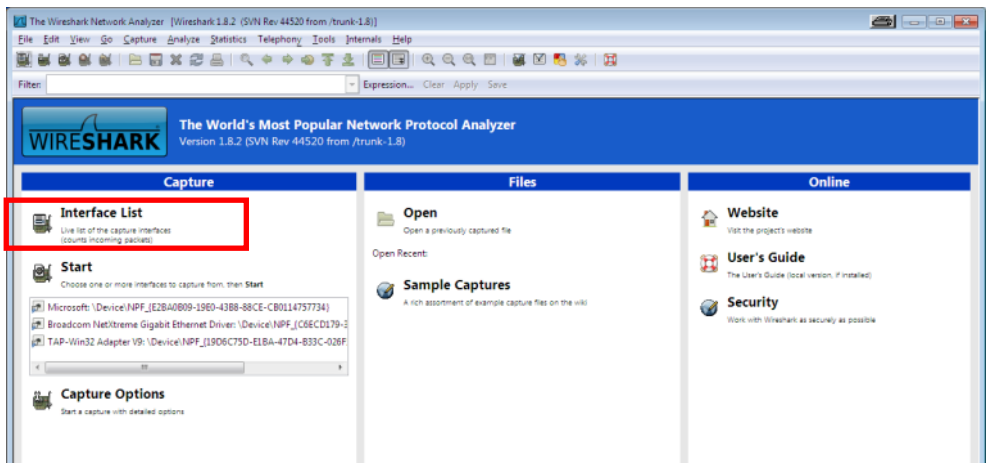
1. Activate the “Remote capture” feature of the Router as shown below (Menu Diagnostics → Remote Capture)

Note: Only one Wireshark-Client-PC (here 172.16.1.10) can be used at the same time record the traffic by Wireshark. Please deactivate this feature if you no longer need to analyse the traffic because it has an impact on the performance of the Router.

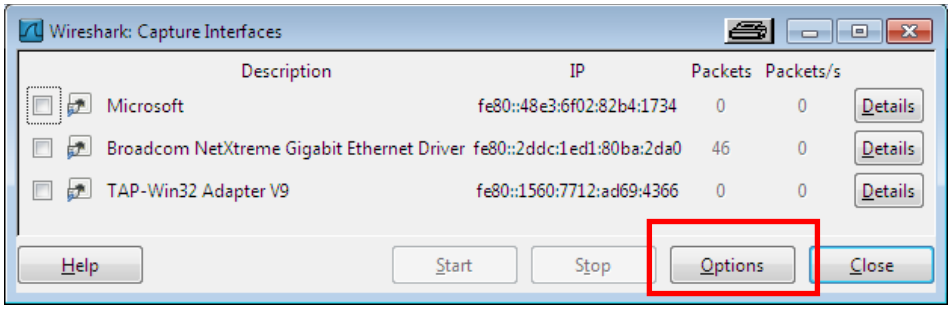


2. Start Wireshark at your PC

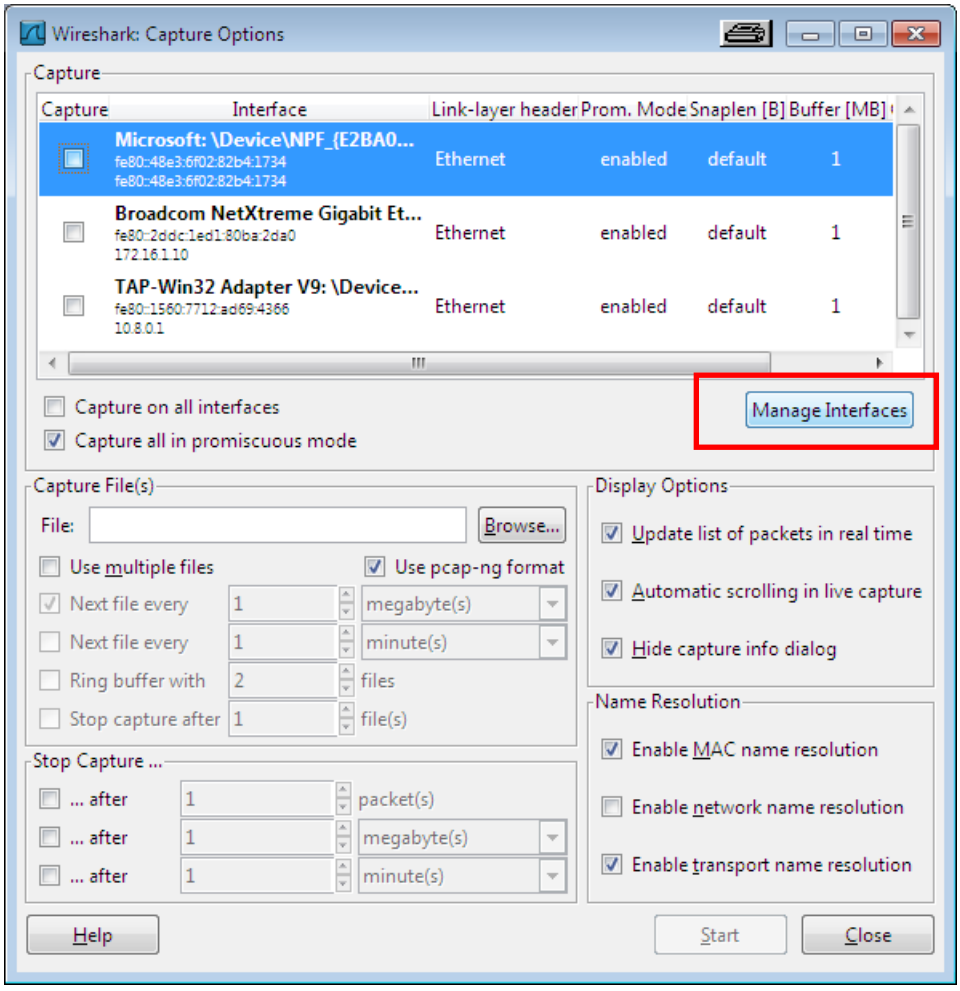
3. Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”



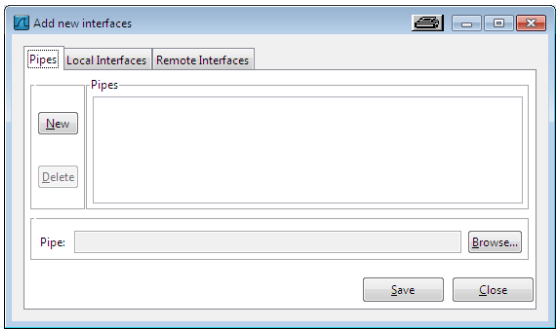
The local Ethernet Interfaces of the computer will be displayed.

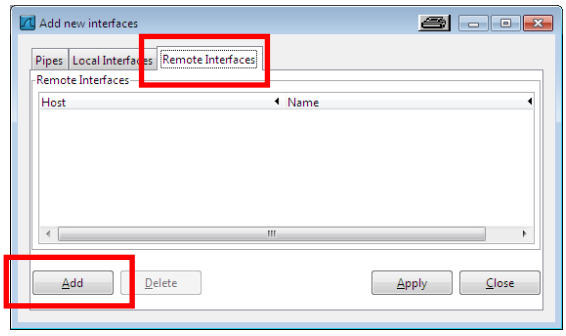


4. Click button “Options”

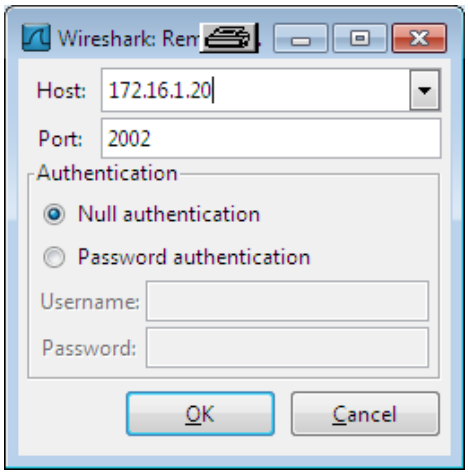


5. Click button “Manage Interfaces” and change to tab “Remote Interfaces”





6. Click button “Add”



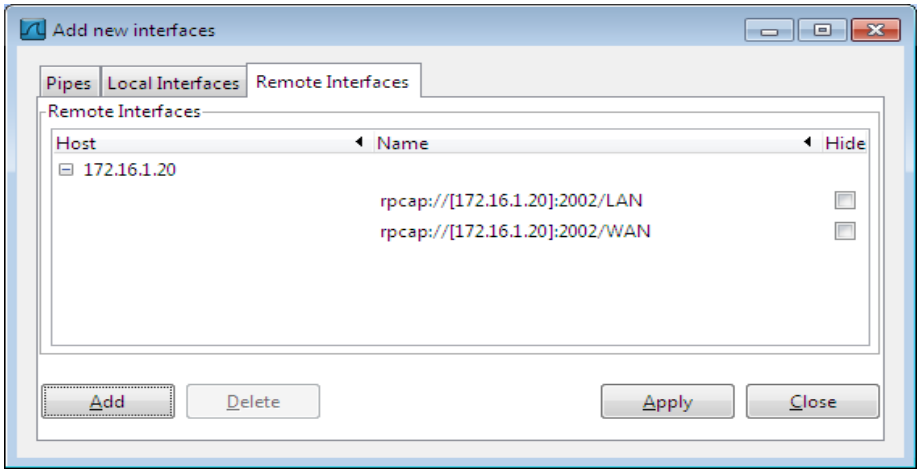
7. Enter the IP address of the Router to field “Host”

Note: You can enter either the IP address of LAN or WAN port. The import fact is that the Routers IP address is accessible by the Wireshark-PC.

8. Enter into field “Port” the value 2002 (will be filled automatically if you enter an IP address)

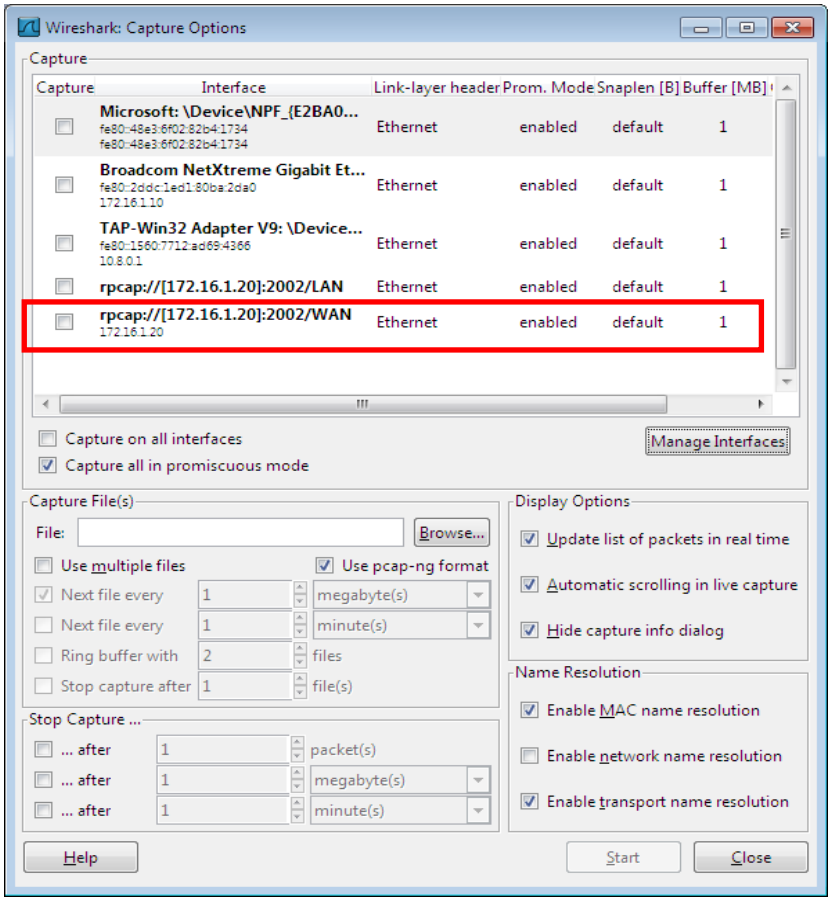
9. Click button OK

Now both Interfaces of the Router (= Host 172.16.1.20) should be displayed.



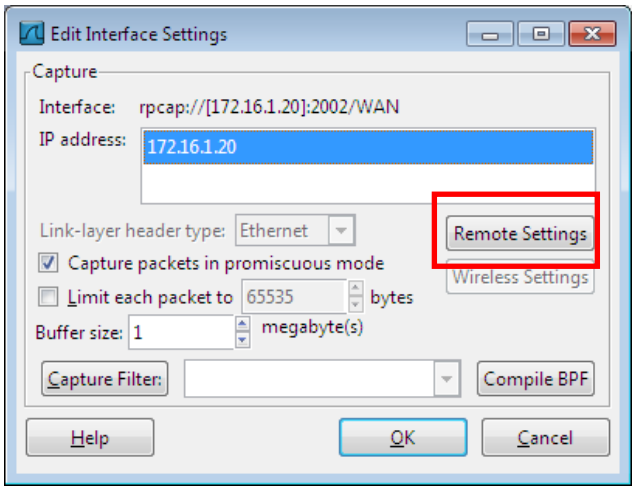
10. Click button Close

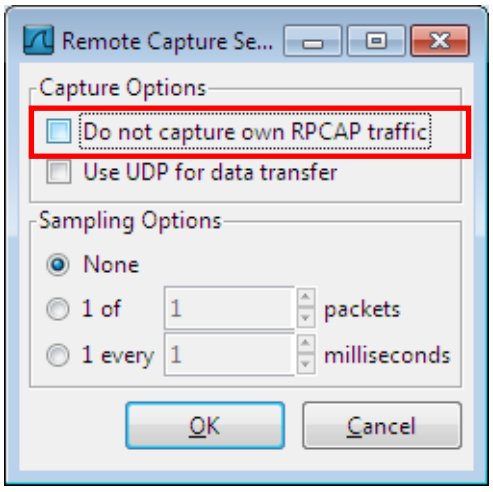
The “remote capture interfaces” will be displayed in the list of selectable interfaces.



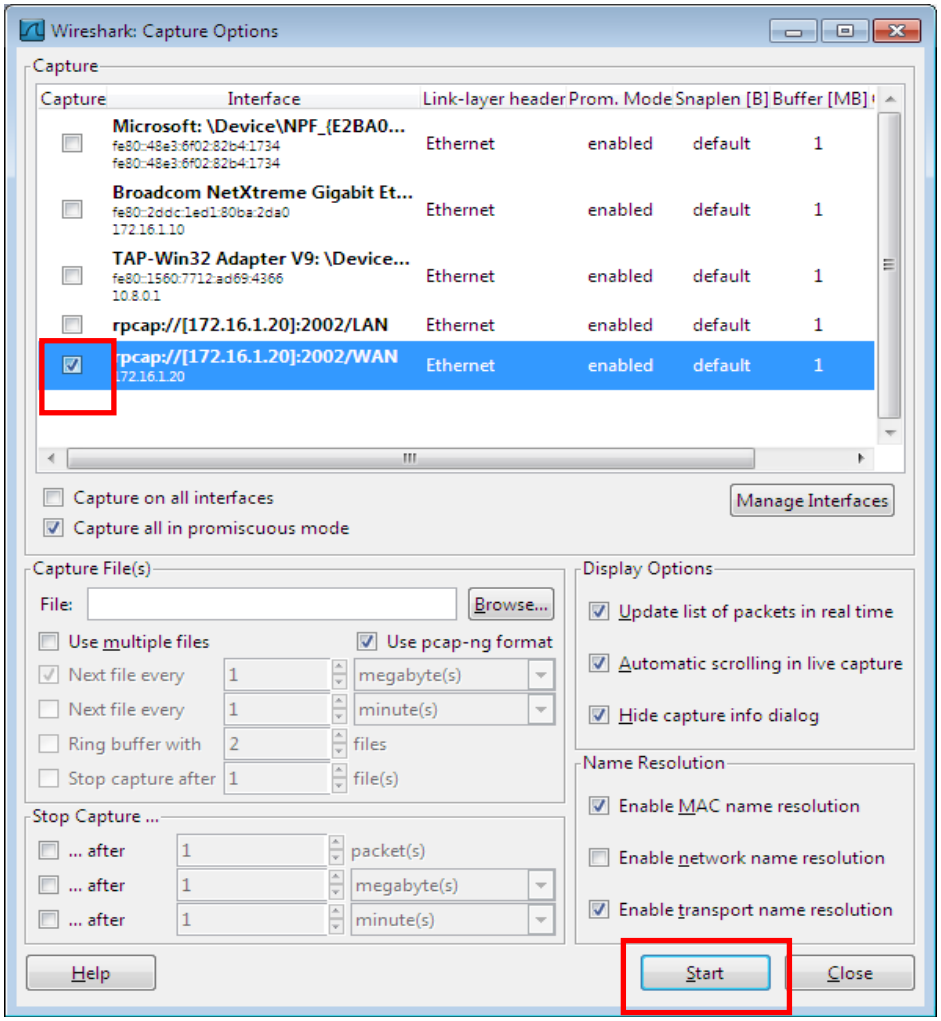
In this example we want to capture the traffic at WAN port.

11. Double-Click the line **rpcap//[172.16.1.20]:2002/WAN**



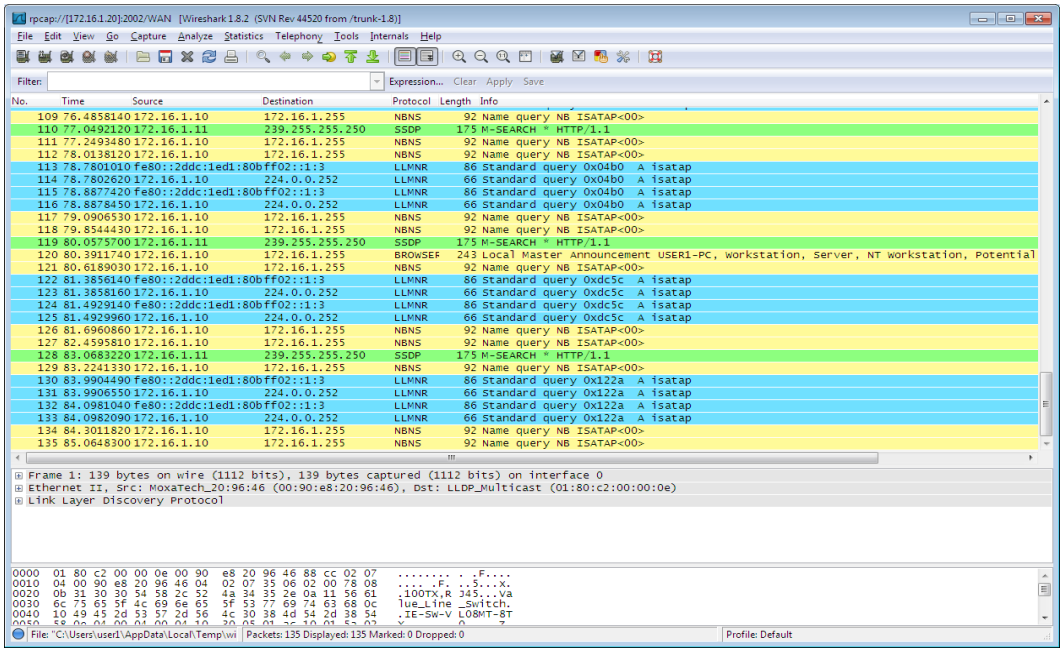


12. Click button “Remote Settings”
13. **Clear** the checkbox “Do not capture own RPCAP traffic”
14. Click button “OK”
15. Again click button “OK” to close the window “Edit Interface Settings”



16. Activate the checkbox in line **rpcap//[172.16.1.20]:2002/WAN**

17. Click button “Start” to record the traffic at Routers WAN port



A7 - Using dynamic IP routing alternatively to manually configured static routes (refers to example A6)

Instead of configuring static routes on Router 2 it is more comfortable to use the “dynamic IP routing” feature to announce the routes of all Router network interfaces to each Router. For announcing the routing information the protocols RIP or OSPF can be used.

	Note
	If dynamic routing is activated but e.g. only the industrial Routers of the machine networks and the production network should participate, this can be done by assigning additionally a password to the used Router information protocol (RIP or OSPF). The result is that only the Routers with the same password exchange their routing tables. With this method you can avoid that routing tables of the industrial networks will be announced also in an upper-level corporate network.

Configuring dynamic IP routing

In this example the protocol RIP (Router information protocol) is set for dynamic IP routing. You can choose alternatively the “newer” protocol OSPF (Open shortest path first). Both are working properly.

► Select menu **Configuration → Network → IP routing→ Tab “Configuration”**

Configure below described entries in the section <u>Dynamic routing</u> of the menu:
→ Configure the below described parameters for all Routers 1 and 2 and all used interfaces

Interfaces Router 1: ETH 1, ETH 2, ETH 3, Router 2: LAN, WAN	
Type	RIP
Simple password	Free text
Active Interface	Activate the checkbox if the Router shall send the routing table to the **LAN/WAN** port (other Routers)

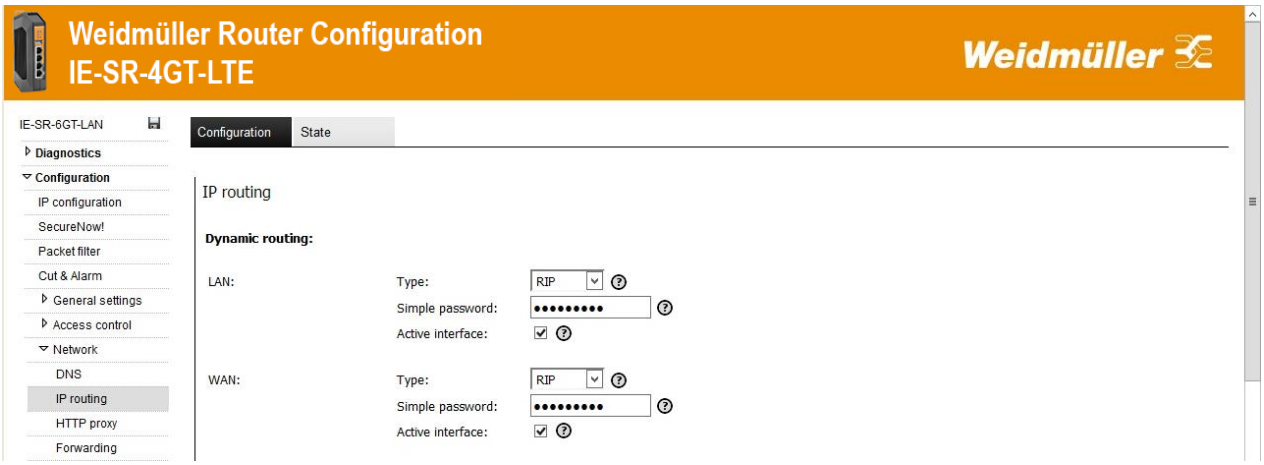


Figure 27: Configuration of dynamic routing using RIP

	Note
	1. If there are several Routers with activated RIP but only the Routers 1 and 2 should exchange their routing tables, then you must use the same password for each Router. 2. You should always use the same value for “Type” on both ports (LAN and WAN). For example, if you leave Type=disabled on LAN port and you activate only the parameters Type=RIP and Active interface=set on WAN port, then the Router will **not** announce (outgoing WAN port) the configured network connected to its LAN port.

The checkbox “Redistribute static routes” can be left blank because we don’t use static routes. As log level, you can choose how detailed information about RIP will be shown in the menu Event Log.

►Click button “Apply settings” to activate the new settings.

Now Router configuration is finished!

Testing the accessibility between Ethernet Devices of network 1 and 2

1. Send a ping request from Machine A to Machine D
Send “ping 192.168.11.101”
Note: This is the public IP address of Machine 1 of Network 2, translated 1:1 NAT from 192.168.1.101 to from 192.168.11.101

2. Send a ping request from Machine D to Machine A
Send “ping 192.168.10.101”
Note: This is the public IP address of Machine 1 of Network 1, translated by 1:1 NAT from 192.168.1.101 to from 192.168.10.101

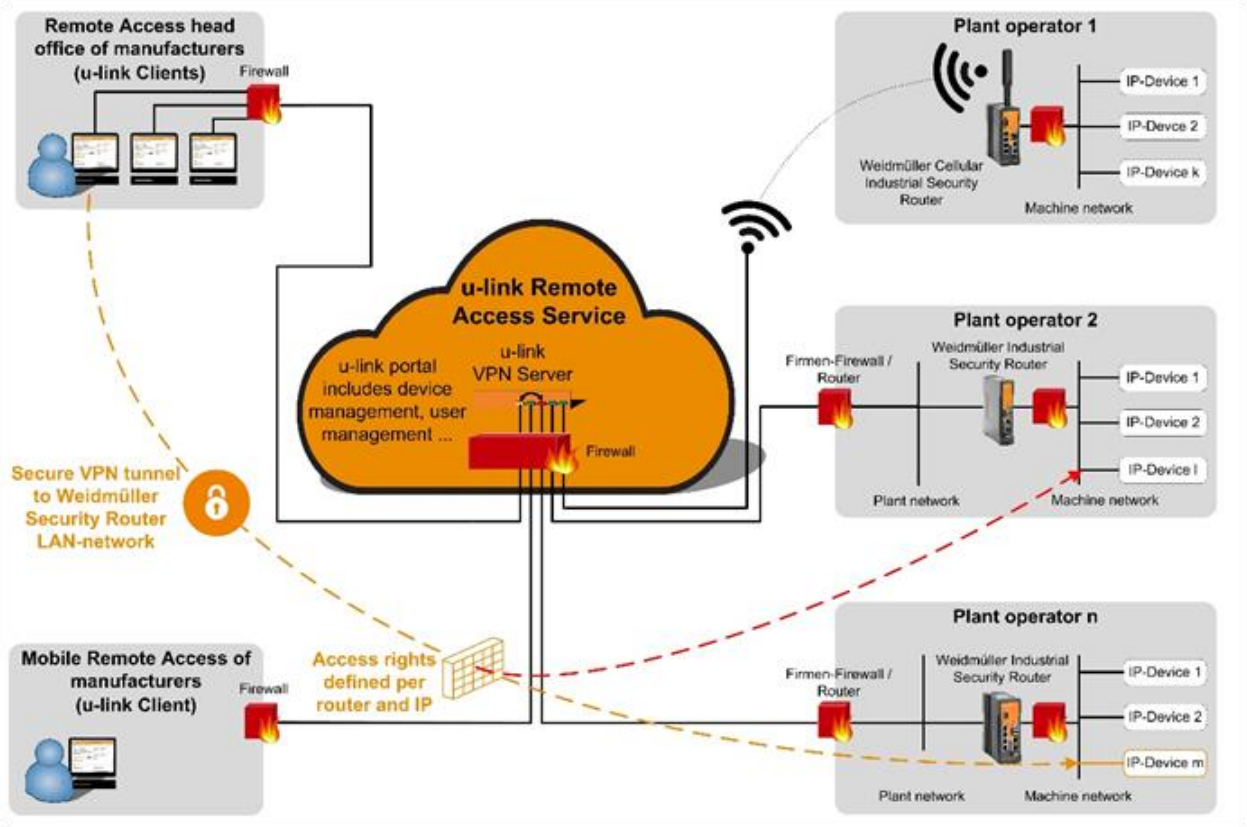
Result: All sent “pings” should be answered by the requested IP addresses correctly.

	Note
	1. If you perform the ping test using PC’s please check your firewall configuration to ensure that ping requests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gateway (IP address is pointing to the Router of the PC’s network).

A8 - u-link Remote Access Service → VPN based connection to remote locations

General:

Weidmüller is providing the cloud-based ‘u-link Remote Access Service’ which can be used with all Weidmüller Router models having implemented VPN functionality.



What is u-link?

Web based Portal application for an easy and secure remote access.

- Provides a central switching agency (VPN-Server / Meeting-Point) for the VPN client communication (Service PC ←→ Router/Remote network).
- Secures data integrity by providing for each u-link system account its own server and database instances (secure separation of u-link accounts).
- Provides secure communication via certificate-based OpenVPN connections (RSA 2048 data encryption, x509-based certificates).
- High availability portal application.

What is necessary to use u-link? (Components of the u-link application)

u-link system account

- Has to be created via registration on web page ‘u-link.weidmueller.com’.

Windows PC

- Having any Internet access and installed software “u-link VPN-Client”.
- Downloadable after registration from u-link web portal.

Weidmüller Router (VPN capable)

- Having any Internet access.
- Target remote network devices connected at Router’s LAN port.

6. Further Application Notes

In our Weidmüller - Support Center, you will find a range of Application Notes and videos that provide additional configuration examples and explain advanced router features, including topics such as:

Configuration of network groups for security routers

This application note explains how to configure network groups in the firewall of Weidmüller security routers, enabling domain-based filtering instead of only IP addresses. This allows secure access to selected domains (e.g. NTP servers, HMIs, or e-mail alerts) while blocking all unauthorized traffic.

Configuration of network groups for security routers

Configuring static routes with a Weidmueller router

This application note explains how to configure static routes with Weidmüller routers, using WAN connections and NAT to connect separate networks. It shows how to enable communication between, for example, office and production networks by directing traffic through defined routes.

Configuring static routes with a Weidmueller router

Configuring the DHCP Server of a Weidmueller router

This application note describes how to configure the DHCP server on Weidmüller routers to automatically assign IP addresses and network parameters. It shows how to simplify network setup, avoid conflicts, and reduce manual configuration effort for connected devices.

Configuring the DHCP Server of a Weidmueller router

Router as DHCP (Video)

Configuring the firewall on a Weidmueller security router

This application note explains how to configure the packet filtering firewall on Weidmüller security routers. It demonstrates how to allow only trusted devices and block all unknown traffic, ensuring maximum security of industrial networks against potential threats.

Configuring the firewall on a Weidmueller security router

Layer 3 Network Security on the Security Router (Video)

IP Forwarding with Weidmueller security routers

This application note explains how to configure IP forwarding on Weidmüller security routers using IP aliases. It enables secure external access to devices inside the LAN (e.g. switches or machines) via the WAN port, supporting remote maintenance and flexible network integration.

IP Forwarding with Weidmueller security routers

IP Forwarding with Router (Video)

Masquerading on the Router

This video demonstrates how to configure NAT masquerading on a Weidmüller security router. It explains how outgoing traffic from the LAN is translated to the router's IP, enabling communication with external networks while keeping internal device addresses hidden.

Masquerading on the Router (Video)

NAT: Network Address Translation with Router

This video explains how to configure Network Address Translation (NAT) on a Weidmüller security router. It shows how NAT enables devices in the LAN to communicate with external networks by mapping private IPs to the router's public IP.

NAT: Network Address Translation with Router (Video)

Port Forwarding with Weidmueller security routers

This application note shows how to configure port forwarding on Weidmüller security routers. It enables external access to specific services or devices inside the LAN by forwarding defined ports, allowing secure remote connectivity without exposing the entire network.

Port Forwarding with Weidmueller security routers

Port Forwarding with Router (Video)

Remote Capture with Router

This video demonstrates how to use the Remote Capture feature on a Weidmüller security router. It shows how to record and analyze network traffic directly from the router for troubleshooting and diagnostics.

Remote Capture with Router (Video)

Router configuration

This video demonstrates how to configure a Weidmüller security router step by step, showing the essential settings for secure and reliable operation in industrial networks.

Router configuration (Video)

Static and Dynamic Routing with Router

This video explains how to configure routing on a Weidmüller security router. It demonstrates how to set up static and dynamic routes to enable communication between separate networks such as office and production environments.

Static and Dynamic Routing with Router (Video)

Using the Router between 2 Networks

This video shows how to configure LAN and WAN interfaces on a Weidmüller security router. It explains how to separate internal and external networks to enable secure communication and proper routing.

Using the Router between 2 Networks (Video)

Using u-link Easy Access feature via web

This application note explains how to configure the u-link Easy Access feature to reach local device web interfaces remotely. It shows how to securely connect to PLCs, HMIs, or IPCs via VPN, enabling simple and encrypted remote visualization from smartphones, tablets, or PCs.

Using u-link Easy Access feature via web

Using u-link remote access service

This application note describes how to set up and use Weidmüller's u-link remote access service. It explains how to create an account, install the VPN client, and configure routers for secure VPN connections, enabling encrypted remote access to devices and networks outside the local site.

Using u-link remote access service