

# Industrial Security Router / Firewall

IE-SR-4TX  
IE-SR-4TX-4G-EU  
IE-SR-4TX-4G-USEMEA



## Manual

Version 1.8

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-4TX” 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](mailto:info@weidmueller.com)  
Internet [www.weidmueller.com](http://www.weidmueller.com)



# Table of Contents

<b>INDUSTRIAL SECURITY ROUTER / FIREWALL .....</b>	<b>1</b>
<b>1. INTRODUCTION.....</b>	<b>5</b>
1.1 Proper and intended usage.....	5
1.2 Package Checklist.....	5
1.3 Safety instructions .....	5
1.4 Mounting the device .....	7
1.5 Technical data.....	8
<b>2. HARDWARE RELATED FUNCTIONAL DESCRIPTIONS.....</b>	<b>13</b>
2.1 DESCRIPTION OF LED STATUS INDICATORS .....	13
2.2 INTERFACES .....	14
2.3 PIN ASSIGNMENTS.....	15
Pin assignment of 4-pin connector for „24 V DC power supply and digital input “.....	15
Pin assignment of RJ45 Ethernet ports (LAN and WAN) .....	15
Pin assignment of Smartcard Reader (ISO 7816 Standard) .....	15
<b>3. INITIAL START-UP / GETTING STARTED .....</b>	<b>16</b>
3.1 Configuration of the Router by using an Internet browser .....	16
3.2 Starting the Web interface.....	17
3.3 Default factory settings of the Router: .....	19
3.4 Reset to factory default settings by external push button.....	19
3.5 Using the Weidmüller Router-Search-Utility.....	20
3.6 Basic description of Router's configuration interface (menu items) .....	21
<b>4. WEB CONFIGURATION .....</b>	<b>22</b>
4.1 SECTION DIAGNOSTICS.....	22
4.1.1 Diagnostics → System State .....	22
4.1.2 Diagnostics → Event Log (Tab State).....	23
4.1.3 Diagnostics → Event Log (Tab Configuration) .....	23
4.1.4 Diagnostics → WAN.....	24
4.1.5 Diagnostics → LAN .....	27
4.1.6 Diagnostics → WWAN .....	28
4.1.7 Diagnostics → Ping test .....	28
4.1.8 Diagnostics → Remote capture .....	29
4.1.9 Diagnostics → Download.....	30
4.2 SECTION CONFIGURATION .....	30
4.2.1 Configuration → Config Wizard.....	30
4.2.1 Configuration → IP Configuration .....	34
IP Configuration → Operational mode “IP Router” .....	34
IP Configuration → Operational mode “Transparent bridge” .....	36
4.2.3 Configuration → Packet filter (Firewall) .....	36
Packet filter → Tab Layer 3 .....	36
Packet filter → Tab Layer 2 .....	37
Packet filter → Tab Status.....	38
4.2.4 Configuration → General settings .....	38
General settings → System data .....	38
General settings → Date & Time.....	39
General settings → Date & Time Tab State.....	40
General settings → User Interface .....	41
General settings → Certificates.....	41
General settings → SCEP (Tab Configuration) .....	42
General settings → SCEP (Tab State).....	42
4.2.6 Configuration → Access Control .....	43
Access Control → User accounts.....	43



Access Control → Permissions .....	46
Access Control → Web access.....	49
<b>4.2.7 Configuration → Network.....</b>	<b>51</b>
Network → DNS (Tab Configuration) .....	51
Network → IP Routing (Tab Static).....	53
Network → IP Routing (Tab Dynamic).....	55
Network → IP Routing (Tab State) .....	56
Network → HTTP proxy.....	57
Network → Forwarding.....	57
Network → 1:1 NAT .....	60
Network → Network Groups.....	61
Network → Hardware Groups.....	62
Network → Ethernet.....	63
<b>4.2.8 Configuration → VPN.....</b>	<b>64</b>
VPN → u-link (Tab Configuration) .....	64
VPN → u-link (Tab State).....	66
VPN → u-link (Tab Registration).....	67
VPN → OpenVPN (Tab Configuration) .....	68
VPN → OpenVPN (Tab VPN1) .....	69
VPN → OpenVPN (Tab State) .....	71
VPN → IPsec (Tab Configuration).....	73
VPN → IPsec (Tab State) .....	76
<b>4.2.9 Configuration → Services.....</b>	<b>76</b>
Services → DHCP Server (Tab Configuration).....	76
Services → DHCP Server (Tab State) .....	77
Services → DNS proxy .....	77
Services → Web server .....	78
Services → SNMP .....	78
Services → Modbus TCP.....	79
Services → Scheduler .....	84
Services → SMS Service .....	84
<b>4.3 SECTION SYSTEM .....</b>	<b>86</b>
<b>4.3.1 System → Backup settings.....</b>	<b>86</b>
<b>4.3.2 System → Software update .....</b>	<b>87</b>
System → Software Update (Tab WWAN) .....	88
<b>4.3.3 System → Factory defaults .....</b>	<b>89</b>
<b>4.3.4 System → Save.....</b>	<b>90</b>
<b>4.3.5 System → Reboot.....</b>	<b>91</b>
<b>4.4 SECTION INFORMATION.....</b>	<b>92</b>
<b>4.4.1 Information → General.....</b>	<b>92</b>
<b>4.4.2 Information → Sitemap .....</b>	<b>93</b>
<b>4.4.2 Information → License Information.....</b>	<b>94</b>
<b>5. APPENDIX A (CONFIGURATION EXAMPLES) .....</b>	<b>95</b>
A1 – BASIC ROUTER CONFIGURATION TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES .....	95
A2 - CONNECTING 2 ETHERNET NETWORKS WITH ACTIVATED NAT MASQUERADING AND USING IP ADDRESS FORWARDING.....	99
A3 - CONFIGURING THE ROUTER TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES AND ADDITIONAL FIREWALL RULES ....	104
A4 – FIREWALL APPLICATION EXAMPLE: SECURING THE ACCESS TO MODBUS TCP DEVICES BY LAYER-2 FIREWALL RULES.....	111
A5 - USING DYNAMIC IP ROUTING ALTERNATIVELY TO MANUALLY CONFIGURED STATIC ROUTES (REFERS TO EXAMPLE A6) .....	125
A6 - HOW TO USE FEATURE “REMOTE CAPTURE” WITH WIRESHARK TO ANALYSE ROUTER’S LAN/WAN TRAFFIC .....	127
A7 - U-LINK REMOTE ACCESS SERVICE → VPN BASED CONNECTION TO REMOTE LOCATIONS.....	132



# 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. By connecting an external DSL modem (via PPPoE) at WAN the Router can provide a direct connection to the Internet. 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

### All models


- 1 x Industrial Security Router (IE-SR-4TX or IE-SR-4TX-4G-\*)
- 1 x 3-pin connector
- 1 x 4-pin connector
- 1 x Antenna for mobile connection (only models with integrated 4G modem)
- 1 x Hardware Installation Guide


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


## 1.3 Safety instructions


	<b>Warning</b>
	<ul style="list-style-type: none"><li>- 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.</li><li>- 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.</li><li>- 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.</li></ul>



	Caution
	<ul style="list-style-type: none"> <li>- This device is designed only for an operating voltage range from 19,2 to 28,8 V DC. Do not use a higher voltage; this could destroy the Router and other devices.</li> <li>- 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.</li> </ul>


	Caution
	<p>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.</p> <p>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.</p>


	Caution
	<ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- 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.</li> </ul>


	Note
	<ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> </ul>



## 1.4 Mounting the device

	<b>Caution</b>
	<ul style="list-style-type: none"> <li>- This device is designed only for an operating voltage range from 19,2 to 28,8 V DC. Do not use a higher voltage; this could destroy the Router and other devices.</li> <li>- 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.</li> <li>- Electrical devices should not be installed or removed during operations. Never install or remove the Router while it is running.</li> </ul>

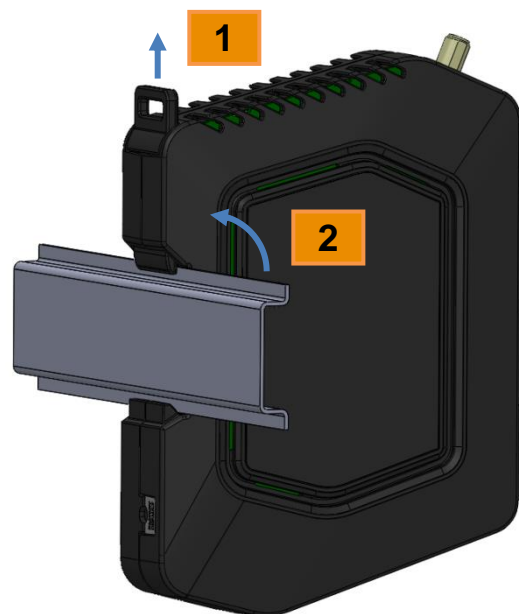
	<b>Caution</b>
	<ul style="list-style-type: none"> <li>- It is important to provide sufficient clearance between devices which cause strong electromagnetic interference (such as frequency converters, transformers or motor regulators). The clearance gap between such devices and the Router should be as wide as possible. The Router can be further shielded by using a mu-metal partition.</li> <li>- 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.</li> </ul>

	<b>Note</b>
	<ul style="list-style-type: none"> <li>- A minimum of 2-inch (5 cm) gap should be kept between the Router and neighboring devices <u>from the top and bottom</u>. This will ensure that the Router is sufficiently ventilated.</li> <li>- 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.</li> </ul>

### 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 the DIN-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	<ul style="list-style-type: none"> <li>• IPv4-Routing between the interfaces (LAN ports / WAN port / optional 4G modem). LAN-Ports behave as unmanaged switch.</li> <li>• Static or dynamic routing according to RIPv2 or OSPF protocol.</li> </ul>
Network Services	<ul style="list-style-type: none"> <li>• DHCP Server</li> <li>• DNS-Relay</li> <li>• NTP-Server/Client</li> </ul>
Firewall	<ul style="list-style-type: none"> <li>• IPv4 Stateful inspection Firewall</li> <li>• NAT-Masquerading, 1:1 NAT, Port forwarding</li> <li>• Layer-2/3-Filter (VLAN ID, VLAN QoS Tag, MAC address based, Ethertype Frame)</li> </ul>

OpenVPN	<ul style="list-style-type: none"> <li>• Configurable as OpenVPN server or client (Layer 2 and Layer 3)</li> <li>• Authentication with X.509 Certificates</li> <li>• Tunnel support via HTTP-Proxy</li> <li>• A maximum of 10 different server configurations</li> <li>• Unlimited number of client connections in server mode</li> </ul>
IPsec	<ul style="list-style-type: none"> <li>• Can be configured as an IPsec server or client.</li> <li>• Authentication with PSK (user ID, password) or X.509 certificates.</li> <li>• Hardware encryption for faster data flow rate.</li> <li>• A maximum of 64 simultaneous connections (subnet with subnet or as IPsec server)</li> <li>• Encryption algorithms such as SHA512, AES256, DH24, 3DES</li> </ul>
u-link	<ul style="list-style-type: none"> <li>• Based on certificate-secured OpenVPN technology</li> <li>• To be used with the Weidmüller Remote Access Service</li> <li>• Simplifies VPN connections and management</li> <li>• Fast and easy connections</li> <li>• Free of charge</li> <li>• Visit <a href="https://u-link.weidmueller.com">https://u-link.weidmueller.com</a> for further information.</li> </ul>



## Configuration

Management	<ul style="list-style-type: none"> <li>• Configuration with web interface (HTTP/HTTPS)</li> <li>• Web interface selectable in English or German language</li> <li>• Configuration support through wizard</li> <li>• Configuration support through detailed help information (tooltip)</li> <li>• Configurable Multi-user access with definable rights</li> <li>• Support for SNMP v3</li> <li>• Event log / audit log / syslog</li> </ul>
------------	---

## Other features

Modbus/TCP (Slave mode)	<p>The integrated Modbus/TCP Slave provides control functions sent by a Modbus/TCP master. Following functions are imaged in the registers:</p> <ul style="list-style-type: none"> <li>• Cut &amp; Alarm: Get status / Set acknowledgment</li> <li>• IPsec /OpenVPN/u-link: Switch configured VPN connections on or off *</li> </ul>
Diagnosis	<ul style="list-style-type: none"> <li>• „Remote Capture“ - feature for network diagnostics via a connected PC (Wireshark)</li> </ul>

## Interfaces

RJ45-Ports	<ul style="list-style-type: none"> <li>• 4 x 10/100 BaseT(X)</li> </ul>
SCM card reader	<ul style="list-style-type: none"> <li>• Save and restore the configuration using a smart card (SIM card without mobile provider data, only the storage capacity of the chip will be used)</li> </ul>
SIM card slot* <sup>1</sup>	<ul style="list-style-type: none"> <li>• Insert SIM card for mobile communication</li> </ul>
LED displays	<ul style="list-style-type: none"> <li>• Signaling the status for power, device status, active VPN connection and an active cellular connection*<sup>1</sup></li> </ul>
Digital Inputs	<ul style="list-style-type: none"> <li>• 1 DI to trigger different functions as VPN, Firewall or CUT</li> </ul>
Reset-Button	<ul style="list-style-type: none"> <li>• Restore to the factory settings</li> </ul>

\*<sup>1</sup> for LTE/4G models only

## Power

Input Voltage	<ul style="list-style-type: none"> <li>• 1* 24 VDC (19,2 to 28,8 V DC) Use a power supply according to NEC Class 2 for use according to UL certification</li> </ul>
Current consumption	<ul style="list-style-type: none"> <li>• Max. 500 mA @ 24 VDC for IE-SR-4TX</li> <li>• Max. 800 mA @ 24 VDC for IE-SR-4TX-4G*</li> </ul>

## Technical data (housing)

Housing	<ul style="list-style-type: none"> <li>• Plastic, protection IP30</li> </ul>
Mounting	<ul style="list-style-type: none"> <li>• TS35 (DIN rail)</li> </ul>



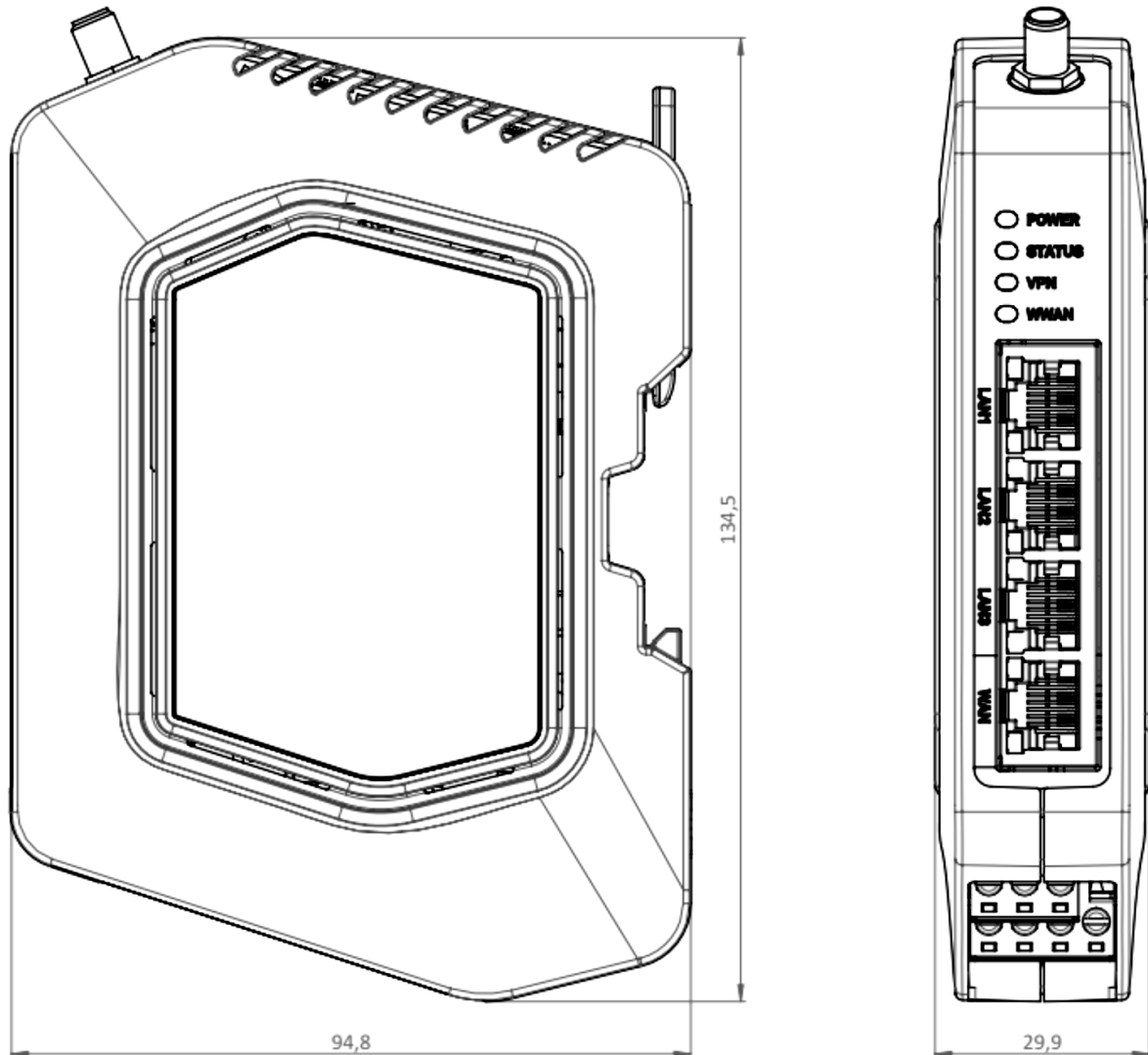


Figure 1: Dimensional drawings



### Environmental conditions

Operating Temperature	<ul style="list-style-type: none"> <li>-30°C to +70°C</li> </ul>
Storage Temperature	<ul style="list-style-type: none"> <li>-40°C to + 85°C</li> </ul>
Ambient Humidity	<ul style="list-style-type: none"> <li>5 to 90% non-condensing</li> </ul>

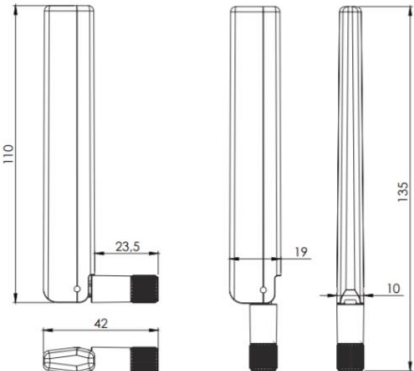
### DSL and 4G/LTE

DSL	<ul style="list-style-type: none"> <li>DSL Internet access by connecting to an external DSL modem via LAN or WAN port</li> <li>Free configuration of the PPPoE login</li> </ul>
LTE/4G*	<ul style="list-style-type: none"> <li>Built-in 4G/LTE modem with 150 Mbps peak downlink and 50 Mbps peak uplink</li> <li>FCC, CE</li> </ul>
Standards*	<ul style="list-style-type: none"> <li>LTE: 3GPP Release 9</li> <li>UMTS: 3GPP Releases 5, 6, 7, 8</li> <li>GSM/GPRS/EDGE: 3GPP Release 99, GERAN Feature Package #1**</li> <li>CDMA (Americas): <ul style="list-style-type: none"> <li>TIA/EIA/IS-2000.1 through .6. cdma2000® Standards for Spread Spectrum Systems. Release 0. April 2000</li> <li>TIA/EIA/IS-2000.1-1 through .6-1. cdma2000® Addendum 1. April 2000</li> <li>TIA/EIA/IS-2000.1-2 through .6-2. cdma2000® Addendum 2. June 2001</li> <li>TIA/EIA/IS-95-B. Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Systems. December 4, 1998</li> <li>TIA/EIA/IS-. cdma2000® High Rate Packet Data Air Interface Specification. November 2000</li> </ul> </li> </ul>
Frequency bands IE-SR-4TX-LTE/4G-EU	<ul style="list-style-type: none"> <li><b>LTE:</b> B1 (2100), B2 (1900), B3 (1800), B4 (AWS), B5 (850), B7 (2600), B12 (700ac), B13 (700c), B20 (800DD), B25 (1900), B26 (US 850 Ext), B29 (US 700de Lower), B30 (2300 WCS), B41 (TDD 2500)</li> <li><b>UMTS:</b> B1 (2100), B2 (1900), B3 (1800), B4 (AWS), B5 (850), B8 (900)</li> </ul>
Frequency bands IE-SR-4TX-LTE/4G-USEMEA	<ul style="list-style-type: none"> <li><b>LTE:</b> 2100(B1), 1900(B2), 1800(B3), 1700(B4), 850(B5), 2600(B7), 700L(B12), 800(B20), 1900(B25), 850(B26), 700SDL(B29), 2300(B30), 2500TDD(B41)</li> <li><b>UMTS:</b> 2100(B1), 1900(B2), 1800(B3), 1700(B4), 850(B5), 900(B8)</li> </ul>

\*Only IE-SR-4TX-4G\* Models

\*\* Only IE-SR-4TX-4G-EU Model



Antennas*	<p>Antenna gain and frequencies:</p> <ul style="list-style-type: none"> <li>• -1,1 dBi @ 617-960 MHz</li> <li>• 0,5 dBi @ 1427-2690 MHz</li> <li>• 0,3 dBi @ 3300-5000 MHz</li> <li>• 1,6 dBi @ 5150-5925 MHz</li> </ul> 
-----------	---

\* Only 4G models

### Approvals

Safety	<ul style="list-style-type: none"> <li>• cULus (UL 61010)</li> </ul>
EMC	<ul style="list-style-type: none"> <li>• FCC Part 15 Class A,</li> <li>• EN61000-6-2 Immunity for industrial environments</li> <li>• EN61000-6-4 Emission Standard for industrial environments</li> </ul>
Shock	<ul style="list-style-type: none"> <li>• DIN EN 60068-2-27</li> </ul>
Vibration	<ul style="list-style-type: none"> <li>• DIN EN 60068-2-6</li> </ul>

### Warranty

Period	3 years
--------	---------

### Order Information

	Model name	Order number
4-Port LAN/WAN Router <b>with</b> VPN features	IE-SR-4TX	2751270000
4-Port LAN / WAN Router <b>with</b> VPN features and additional integrated LTE/4G modem	EU: IE-SR-4TX-4G-EU Global: IE-SR-4TX-4G-USEMEA	2751280000 2739630000



## 2. Hardware related functional descriptions

### 2.1 Description of LED status indicators








Description of LED status indicators

LED	Signal	Meaning
<b>Power</b>	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
<b>Status</b>	Off	The device is not powered or has no error
	Red	Error during boot process or recovering an image
<b>VPN</b>	Off	No VPN tunnel active
	Red	A VPN tunnel is established
<b>Only LTE/4G models</b>		
<b>4G (LTE)</b>	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




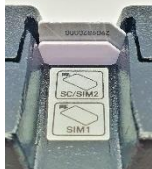


2.2 Interfaces



<b>Description of device interfaces at top and front side</b>	
	Connectors for LTE/4G antennas at top side; Connector type: <b>SMA female</b> ( only 4G/LTE models )
	3 x RJ45-Connector LAN (10/100BaseTX)
	1 x RJ45-Connector WAN (10/100BaseTX)
	4-pin connector for 24 V DC power supply and digital input

Description of device interfaces at rear side

	<b>SIM1 slot / socket</b> Slot for mobile SIM card (only 4G/LTE models)	 	Connectors for LTE/4G antenna of type <b>SMA female</b> (only 4G/LTE models).  2 x SMA connectors, MAIN and AUX (AUX = Diversity / MIMO)  <b>External antennas:</b>  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.
	<b>SCM/SIM2 slot / socket</b> SIM memory card reader for external backup and restore of the Router configuration. A second SIM-card currently is not supported. <b>Only SCM cards</b> are supported!   See picture above for correct insertion of the cards		
	<b>Factory Default Button</b> Resetting the router		

**Note: Only SCM Cards with Hardware revision AI (for non 4G router) or AJ (4G Router) and newer are supported.**



## 2.3 Pin assignments

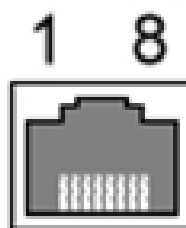
### Pin assignment of 4-pin connector for „24 V DC power supply and digital input “

Pin number	Description
DI	Digital Input
FE	Functional Earth
0V	GND
V+	24 V DC $\pm$ 20 %



### Pin assignment of RJ45 Ethernet ports (LAN and WAN)

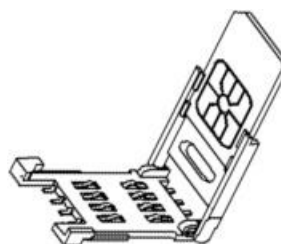
Pin number	SIGNAL NAME (MDI)	
	10/100Base T(x)	1000Base T
1	TX +	BI_DA+
2	TX -	BI_DA-
3	RX +	BI_DB+
4	NC	BI_DC+
5	NC	BI_DC-
6	RX -	BI_DB-
7	NC	BI_DD+-
8	NC	BI_DD-



### Pin assignment of 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, both Ethernet ports are configured with auto negotiation.

The configuration and control of the Router is 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:**

**LAN ports:** 192.168.1.110 / 255.255.255.0

**WAN port** : DHCP client



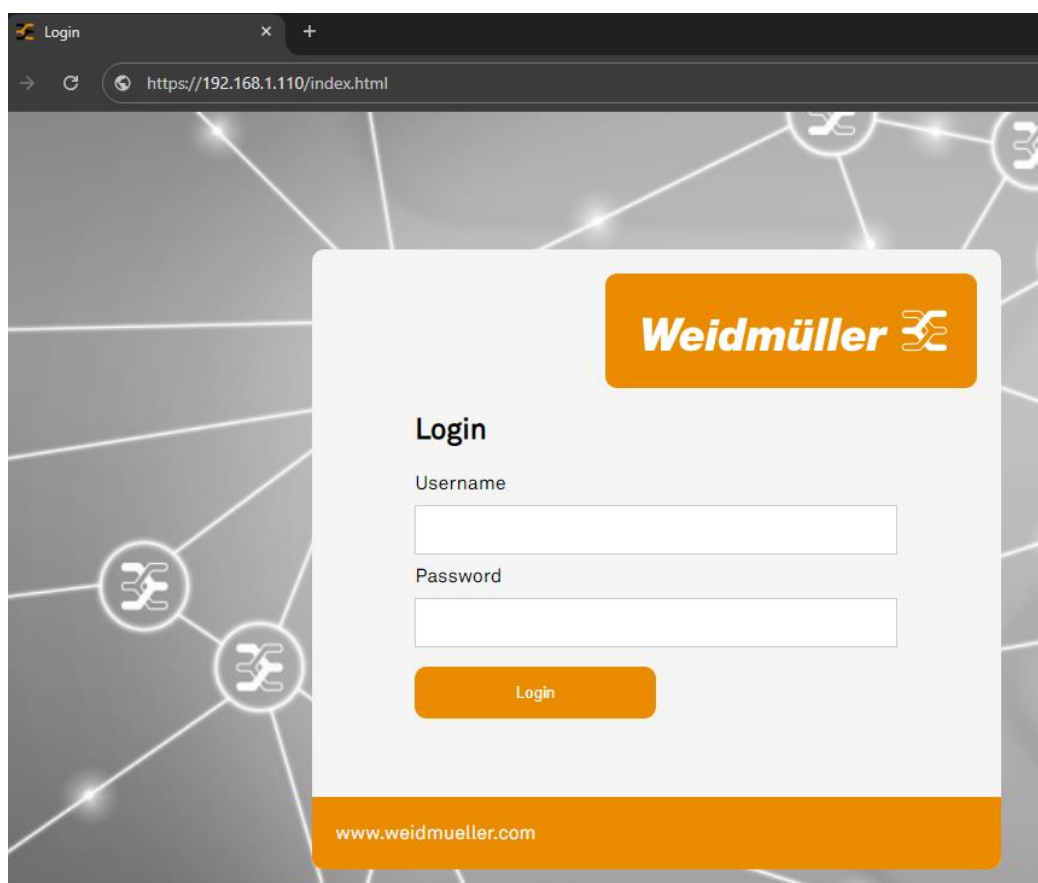
### 3.2 Starting the Web interface

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

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:

	<b>Note</b>
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 client
Subnet Mask	255.255.255.0
NAT (Masquerading) on WAN Port	Not activated
Default gateway	No entry
DNS	Not 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
Data prioritization	Disabled
4G Modem (for 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

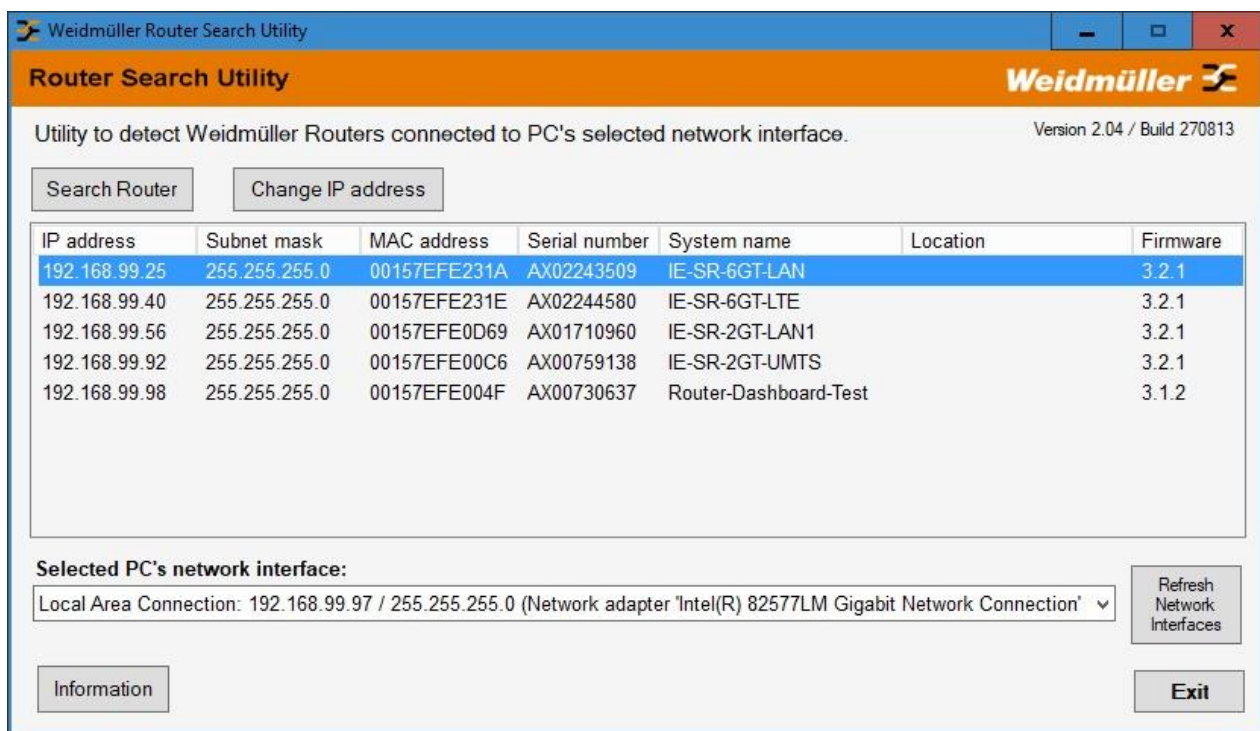
The software tool Weidmüller Router-Search-Utility can be used to find Weidmüller Routers and detect their IP addresses within a switched network. This software is very helpful if you don't know the current IP address of a Router. This can e.g. happen in cases that you have forgotten the current IP configuration 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 [www.catalog.weidmueller.com](http://www.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 (LAN/WAN/4G)
- 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 of basic network parameters (IP addresses, Default gateway)
- Setting of firewall rules (Packet filter)
- 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, 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**

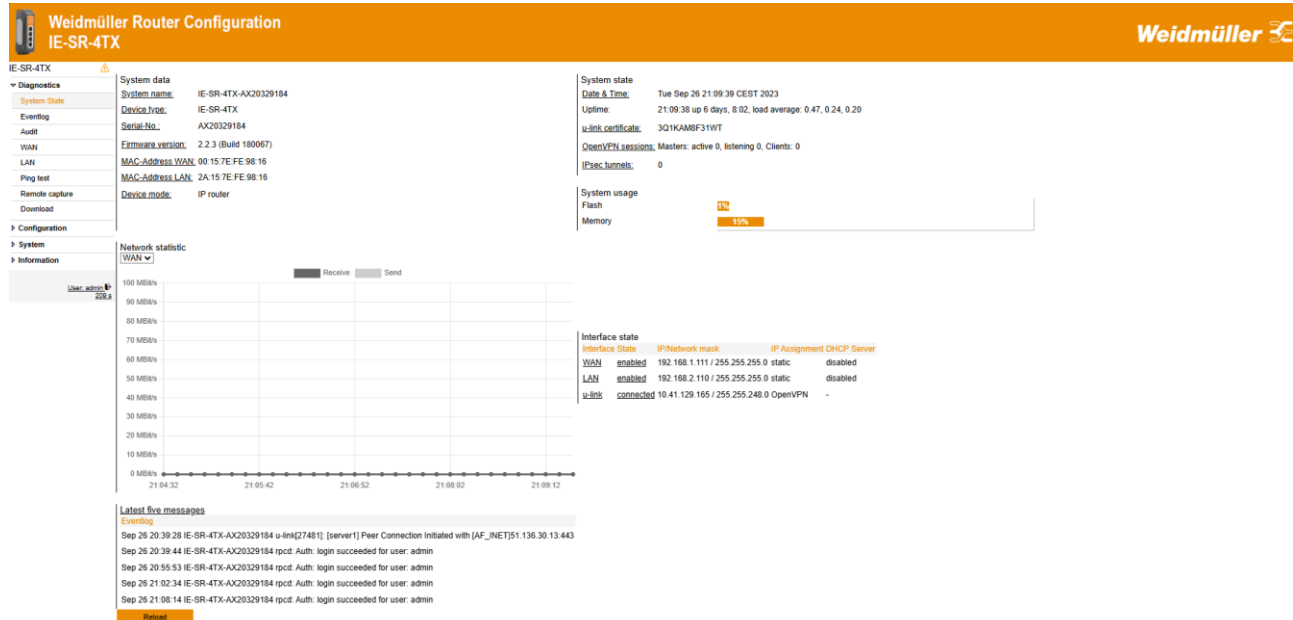
- Display of technical data and hardware information (e.g. serial number and MAC address)
- License information



## 4. Web Configuration

### 4.1 Section Diagnostics


#### 4.1.1 Diagnostics → System State




Menu	Diagnostics → System State	
Function	<b>Startup screen of the web interface after login.</b> 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)


**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-4TX-LTE/4G

Diagnostics
System State
Eventlog
WAN
LAN
WWAN
Ping test
Remote capture
Download
Configuration
System
Information

State
Configuration

Eventlog


```


Oct 17 11:24:28 IE-SR-4TX-LTE-AK2011010 chronyd[14127]: Selected source 192.53.109.108 (ptbtime1.ptb.de)
Oct 17 11:23:43 IE-SR-4TX-LTE-AK2011010 systemd: save_now [save Settings] triggered
Oct 17 11:23:43 IE-SR-4TX-LTE-AK2011010 systemd: Settings change by: 'admin', from source: 'JSON RPC'
Oct 17 11:23:21 IE-SR-4TX-LTE-AK2011010 chronyd[14127]: System clock was stepped by 12090669.226223 seconds
May 30 12:52:12 IE-SR-4TX-LTE-AK2011010 chronyd[14127]: System clock wrong by 12090669.226223 seconds
May 30 12:52:12 IE-SR-4TX-LTE-AK2011010 chronyd[14127]: Selected source 185.41.106.152 (de.pool.ntp.org)
May 30 12:52:07 IE-SR-4TX-LTE-AK2011010 chronyd[14127]: chronyd version 4.3 starting [+CHRON +NTP +REFCLOCK +BTC +PRIVDROP -SCFILTER -SIGMOD +ASYNCDNS -NTS -SECHASH -IPV6 -DEBUG]
May 30 12:51:53 IE-SR-4TX-LTE-AK2011010 systemd: Set system time to Tue May 30 12:51:53 CEST 2023
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'day [day]' = '30'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'month [month]' = '05'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'hour [hour]' = '12'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'minute [minute]' = '51'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'second [seconds]' = '53'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: 'ntp_service [Enable timeserver synchronisation (NTP)]' = 'enabled'
May 30 12:52:06 IE-SR-4TX-LTE-AK2011010 systemd: Settings change by: 'admin', from source: 'JSON RPC'
May 30 12:45:30 IE-SR-4TX-LTE-AK2011010 dhclient: bound to 192.168.9.67 -- renewal in 5930 seconds.
May 30 12:45:29 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: using nameserver 192.168.9.1#53
May 30 12:45:29 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: reading /var/config/resolv.conf
May 30 12:45:29 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: no servers found in /var/config/resolv.conf, will retry
May 30 12:45:28 IE-SR-4TX-LTE-AK2011010 dhclient: Set ip address of wlan to 192.168.9.67/255.255.255.0
May 30 12:45:27 IE-SR-4TX-LTE-AK2011010 dhclient: DHCPACK of 192.168.9.67 from 192.168.9.1
May 30 12:45:27 IE-SR-4TX-LTE-AK2011010 dhclient: DHCPREQUEST for 192.168.9.67 on wlan to 192.168.9.1 port 67
May 30 11:00:56 IE-SR-4TX-LTE-AK2011010 dhclient: bound to 192.168.9.67 -- renewal in 5791 seconds.
May 30 11:00:54 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: using nameserver 192.168.9.1#53
May 30 11:00:54 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: reading /var/config/resolv.conf
May 30 11:00:54 IE-SR-4TX-LTE-AK2011010 dnsmasq[3223]: no servers found in /var/config/resolv.conf, will retry
May 30 11:00:53 IE-SR-4TX-LTE-AK2011010 dhclient: Set ip address of wlan to 192.168.9.67/255.255.255.0
May 30 11:00:52 IE-SR-4TX-LTE-AK2011010 dhclient: DHCPACK of 192.168.9.67 from 192.168.9.1
May 30 11:00:52 IE-SR-4TX-LTE-AK2011010 dhclient: DHCPREQUEST for 192.168.9.67 on wlan to 192.168.9.1 port 67
May 30 09:33:04 IE-SR-4TX-LTE-AK2011010 dhclient: bound to 192.168.9.67 -- renewal in 5747 seconds.

```

<b>Menu</b>	Diagnostics → Event Log → Tab State
<b>Function</b>	<p>Display events and error messages that have occurred in chronological order.</p> <p>Message syntax: &lt;Month&gt; &lt;Day&gt; &lt;hh:mm:ss&gt; &lt;System name&gt; &lt;Service&gt;: Message</p> <p>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.</p>

## 4.1.3 Diagnostics → Event Log (Tab Configuration)


**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-4TX-LTE/4G

Diagnostics
System State
Eventlog
WAN
LAN
WWAN
Ping test
Remote capture
Download
Configuration
System
Information

State
Configuration

Eventlog settings

Enable remote syslog: ☐
Address of syslog server: 
Use TCP instead of UDP: ☐


Apply settings
Reset changes

<b>Menu</b>	Diagnostics → Event Log → Tab Configuration	
<b>Function</b>	Event and error messages can be sent to a syslog server (PC on the network) or sent as emails.	
	Enable remote syslog	Write log messages to a remote machine
	Address of syslog server	Local syslog server address
	UDP port of syslog server	514 standard port





### 4.1.4 Diagnostics → Audit

#### Diagnostics → Audit (Tab Authentication)



Weidmüller Router Configuration  
IE-SR-4GT-LTE



IE-SR-4GT-LTE/4G 

Authentication

Configuration

Packet filter

Anomaly

Download

▼ Diagnostics

System State

Eventlog

Audit

Ethernet

WWAN

Ping test


Remote capture

Download

► Configuration

► System

► Information


Authentication audit 


Date	Time	Username	Action Taken	Session	Method	Source	Result
07/14/25	08:36:49	admin	logged-in	c5cd	web		success
07/14/25	08:41:49	admin	ended-session	c5cd	web		success
07/14/25	10:36:18	admin	logged-in	8dba	web	192.168.1.12	success
07/14/25	10:42:28	admin	logged-in	e65a	web	192.168.1.12	success
07/14/25	10:47:34	admin	ended-session	e65a	web		success
07/14/25	11:12:00	admin	logged-in	5e3a	web	192.168.1.12	success
07/14/25	11:17:06	admin	ended-session	5e3a	web		success
07/14/25	11:34:45	admin	logged-in	cf5a	web	192.168.1.12	success
07/14/25	11:41:02	admin	ended-session	cf5a	web		success
07/14/25	12:56:24	admin	logged-in	2777	web	192.168.1.12	success
07/14/25	13:07:45	admin	ended-session	2777	web		success
07/14/25	13:16:57	admin	logged-in	07f8	web	192.168.1.12	success
07/14/25	13:25:09	admin	ended-session	07f8	web		success
07/14/25	13:33:10	admin	logged-in	0e09	web	192.168.1.12	success

Menu	Diagnostics → Audit → Tab Authentication
Function	<p>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.</p> <p>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</p>



## Diagnostics → Audit (Tab Configuration)


**Weidmüller Router Configuration**  
**IE-SR-4GT-LTE**



IE-SR-4GT-LTE/4G

Diagnostics
System State
Eventlog
**Audit**
Ethernet
WWAN
Ping test
Remote capture
Download
Configuration
System
Information

Authentication
**Configuration**
Packet filter
Anomaly
Download


Configuration audit ⓘ  


Date	Time	Username	Action Taken	Result	Table	Operation	Key	Value	Condition
There are no audits available.									

User: admin 249 s

<b>Menu</b>	Diagnostics → Audit → Tab Configuration
<b>Function</b>	<p>This audit log view shows all configuration changes to the main configuration database. Passwords will be shown as XXX.</p> <p>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.</p>

## Diagnostics → Audit (Tab Packet filter)


**Weidmüller Router Configuration**  
**IE-SR-4GT-LTE**



IE-SR-4GT-LTE/4G

Diagnostics
System State
Eventlog
Audit
Ethernet
WWAN
Ping test
Remote capture
Download
Configuration
System
Information

Authentication
Configuration
**Packet filter**
Anomaly
Download

Packet filter audit ⓘ  


Date	Time	Source address	Destination address	Protocol
There are no audits available.				


User: admin 297 s


<b>Menu</b>	Diagnostics → Audit → Tab Packet filter
<b>Function</b>	<p>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.</p>



Diagnostics → Audit (Tab Anomaly)

Weidmüller Router Configuration  
IE-SR-4GT-LTE

Weidmüller 

IE-SR-4GT-LTE/4G 

▼ Diagnostics

System State

Eventlog

Audit

Ethernet

WWAN

Ping test


Remote capture

Download

► Configuration

► System

► Information

User: admin 

290 s


Authentication

Configuration

Packet filter


Anomaly

Download

Anomaly audit 


DateTimeTitleDescription


There are no audits available.




Menu	Diagnostics → Audit → Tab Anomaly
Function	<p>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.</p> <p>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.</p>

Diagnostics → Audit (Tab Download)

Weidmüller Router Configuration  
IE-SR-4GT-LTE

Weidmüller 

IE-SR-4GT-LTE/4G 

▼ Diagnostics

System State

Eventlog

Audit

Ethernet

WWAN

Ping test


Remote capture

Download

► Configuration

► System

► Information

User: admin 

290 s

Authentication

Configuration

Packet filter

Anomaly

Download

Audit download

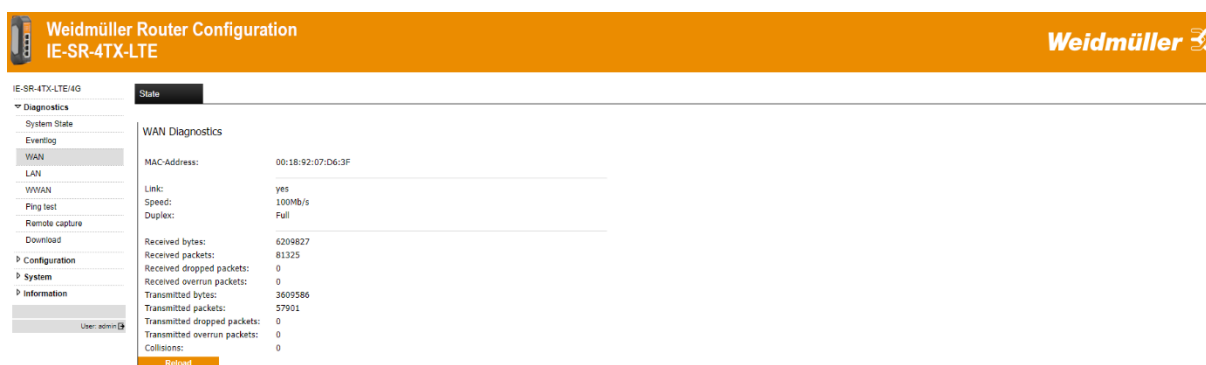
The complete Audit Log can be downloaded here as a tar archive. Please note that the original output of the Linux *auditd* service is preserved. These raw files contain more detailed information than what is displayed in the user interface, which only shows selected important entries. This file is intended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

Download audits

Menu	Diagnostics → Audit → Tab Download
Function	<p>The complete Audit Log can be downloaded here as a tar archive. Please note that the original output of the Linux <i>auditd</i> 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.</p>



## 4.1.5 Diagnostics → WAN



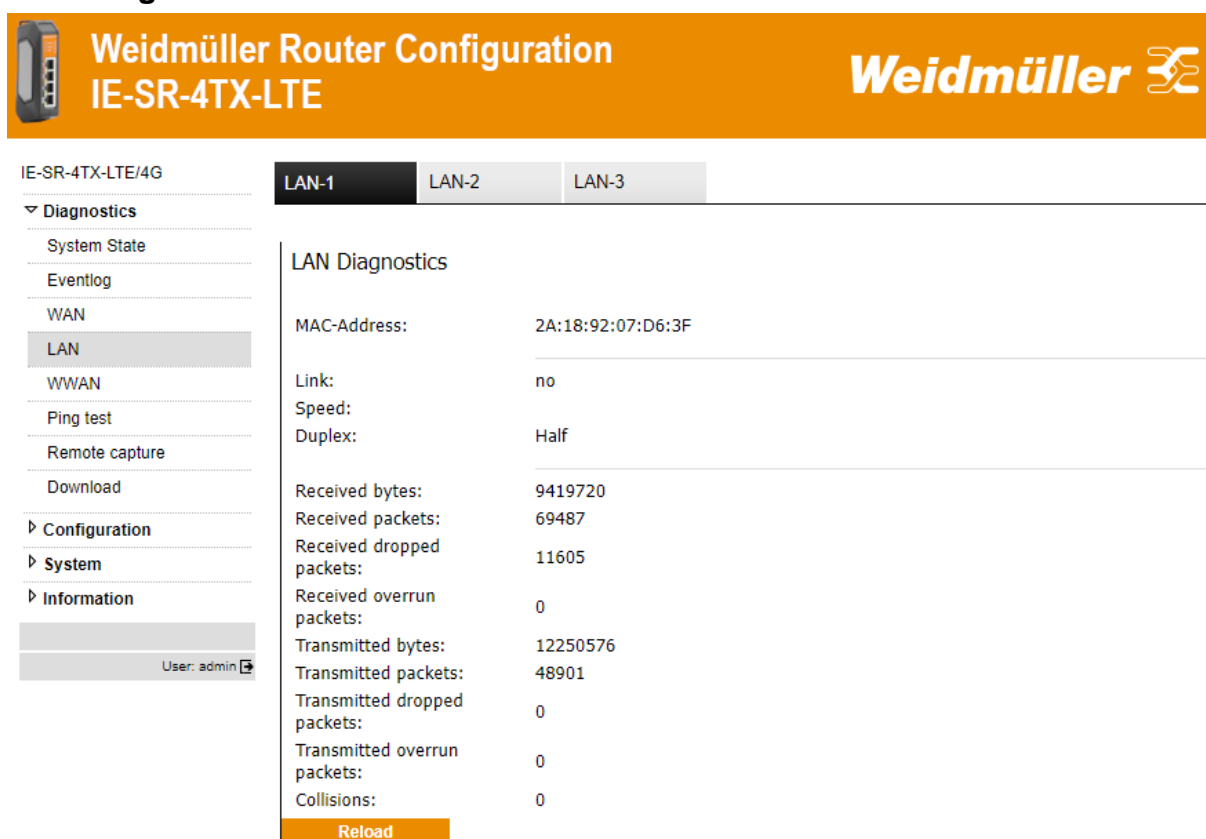
The screenshot shows the 'WAN Diagnostics' page in the Weidmüller Router Configuration interface. The left sidebar contains a menu with options: System State, Eventlog, WAN (selected), LAN, WWAN, Ping test, Remote capture, Download, Configuration, System, and Information. The main content area displays the following data:

MAC-Address:	00:18:92:07:D6:3F
Link:	yes
Speed:	100Mb/s
Duplex:	Full
Received bytes:	6209827
Received packets:	81325
Received dropped packets:	0
Received overrun packets:	0
Transmitted bytes:	3609586
Transmitted packets:	57901
Transmitted dropped packets:	0
Transmitted overrun packets:	0
Collisions:	0

A 'Reload' button is located at the bottom of the data section.

<b>Menu</b>	Diagnostics → WAN
<b>Function</b>	Displays the current status of the WAN ports Diagnose the WAN-port.

## 4.1.6 Diagnostics → LAN



The screenshot shows the 'LAN Diagnostics' page in the Weidmüller Router Configuration interface. The left sidebar contains a menu with options: System State, Eventlog, WAN, LAN (selected), WWAN, Ping test, Remote capture, Download, Configuration, System, and Information. The main content area displays the following data:


MAC-Address:	2A:18:92:07:D6:3F
Link:	no
Speed:	
Duplex:	Half
Received bytes:	9419720
Received packets:	69487
Received dropped packets:	11605
Received overrun packets:	0
Transmitted bytes:	12250576
Transmitted packets:	48901
Transmitted dropped packets:	0
Transmitted overrun packets:	0
Collisions:	0

A 'Reload' button is located at the bottom of the data section.


<b>Menu</b>	Diagnostics → LAN
<b>Function</b>	Displays the current status of the LAN ports. Diagnose the LAN-port.



4.1.7 Diagnostics → WWAN



Weidmüller Router Configuration  
IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

State

▼ Diagnostics

System State

Eventlog

WAN

LAN

WWAN

Ping test

Remote capture

Download

► Configuration

► System

► Information

3G/4G modem state

Modem Vendor: GOSUNCN

Model: ME3630

Revision: ME3630E1CV1.0B12


State: disabled

Reload


User: admin

Menu	Diagnostics → 4G
Function	Displays the current status of the 4G mobile connection. Menu available for cellular models only.

4.1.8 Diagnostics → Ping test



Weidmüller Router Configuration  
IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

State

▼ Diagnostics

System State

Eventlog

WAN

LAN

WWAN

Ping test

Remote capture

Download

► Configuration

► System

► Information

Ping

Destination 8.8.8.8

Packet count 4

Ping once


Start cyclic ping

User: admin


Menu	Diagnostics → Ping test
Function	Allows sending of ICMP packets (ping) to test network connections between the Router and other Ethernet devices. You can either ping once or start a cyclic ping to the destination.  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:



Weidmüller Router Configuration  
IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

▼ Diagnostics

System State

Eventlog

WAN

LAN

WWAN

Ping test

Remote capture

Download

► Configuration

► System

► Information

User: admin

State

Ping

Destination 8.8.8.8


Packet count 4

PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: seq=0 ttl=118 time=27.243 ms  
64 bytes from 8.8.8.8: seq=1 ttl=118 time=27.095 ms  
64 bytes from 8.8.8.8: seq=2 ttl=118 time=26.645 ms  
64 bytes from 8.8.8.8: seq=3 ttl=118 time=32.205 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 packets received, 0% packet loss  
round-trip min/avg/max = 26.645/28.297/32.205 ms


Ping once

Start cyclic ping

4.1.9 Diagnostics → Remote capture



Weidmüller Router Configuration  
IE-SR-4TX



IE-SR-4TX

▼ Diagnostics

System State

Eventlog

Audit

WAN

LAN

Ping test

Remote capture

Download

► Configuration

► System

► Information

User: admin

Configuration

Remote Capture Server

Security Notice

The Remote Capture Server is meant for debugging purposes only. For security reasons it should always be disabled if not needed. Only enable interfaces that are trusted in your environment, like VPN interfaces or internal networks. Please note that traffic is unencrypted by the remote capture protocol of Wireshark and confidential data might leak if used on untrusted networks without an extra VPN channel.

Enable remote capture server: ☐

Client address:


Controlling access

Interface	LAN	WAN	u-link
TCP Port 2002	Allow <input type="checkbox"/>	Allow <input type="checkbox"/>	Allow <input type="checkbox"/>

Apply settings


Reset changes

Menu	Diagnostics → Remote capture	
Function	By using the "remote capture" function data packets on both the LAN and the WAN port of the Router can be recorded for diagnostic purposes. The receiver of the diagnostic data is a PC/Server which must have installed the tool "Wireshark" listening on Port 2002. How to use please refer to application note in <b>Appendix A</b> .	
	Enable remote capture server	Enables the function
	Client address	IP address of permitted remote capture client (e.g. your service pc)


	Note
	No authentication is possible for remote capture. Therefore, this feature should only be activated for a limited time during diagnosis.



4.1.10 Diagnostics → Download



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Weidmüller** 

IE-SR-4TX-LTE/4G

State

▼ Diagnostics

System State

Eventlog

WAN

LAN

WWAN

Ping test

Remote capture

Download

► Configuration

► System

► Information

User: admin

Create and download diagnostic file



The diagnostic file contains all important data for the support. Please download this file and submit it together with your problem description. It contains system internal debugging information and all configuration data except the credentials like passwords or private keys.

Download

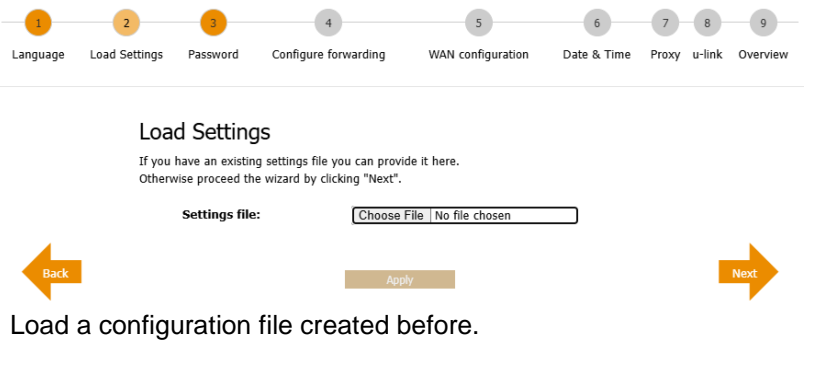
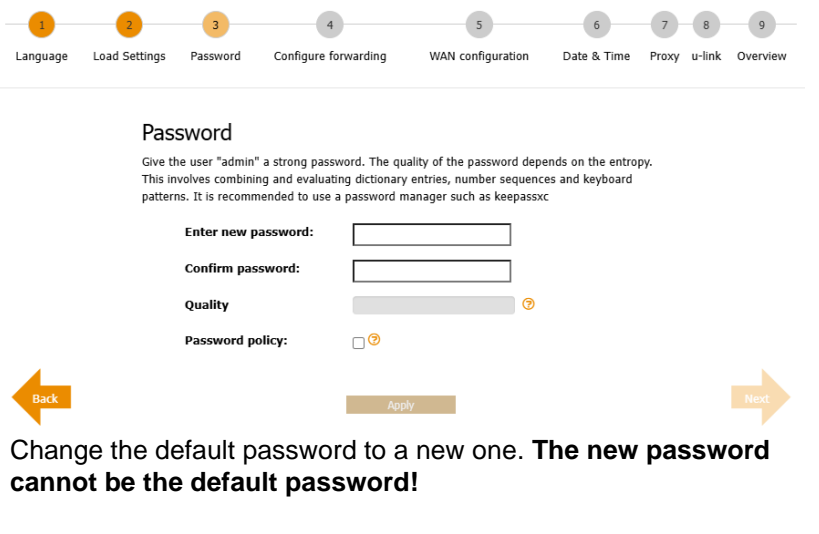
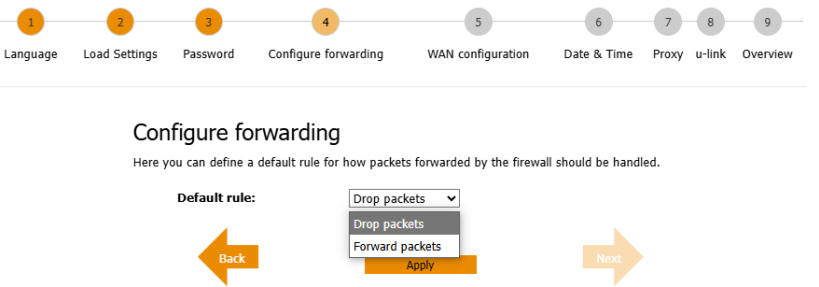
Menu	Diagnostics → Download
Function	Allows to create and download a diagnostic file with internal debugging information for the support. When downloaded, you get a GZ File that can be sent to the support with a problem description

4.2 Section Configuration

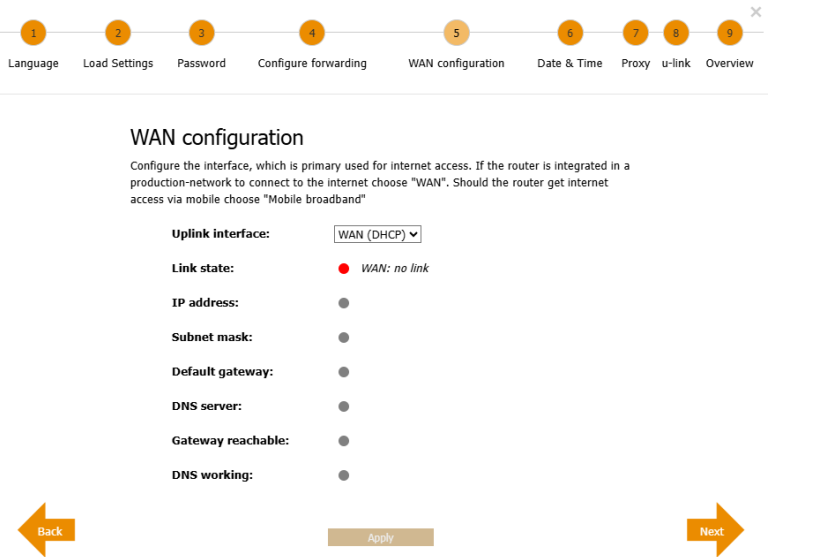
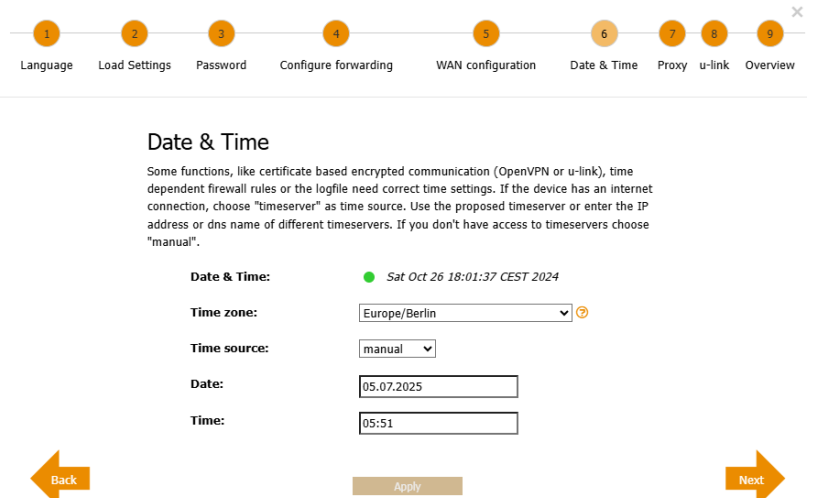
4.2.1 Configuration → Config Wizard

Menu	Configuration → Config Wizard
Function	<div><div>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.</div><div><div>Language</div><div><div><div>1</div>Language</div><div><div>2</div>Load Settings</div><div><div>3</div>Password</div><div><div>4</div>Configure forwarding</div><div><div>5</div>WAN configuration</div><div><div>6</div>Date &amp; Time</div><div><div>7</div>Proxy</div><div><div>8</div>u-link</div><div><div>9</div>Overview</div></div><div><div>Language</div><div>Please choose the language of the user interface</div><div><div></div><div></div></div><div>Setting the language of the Router Web interface</div></div></div></div>



	<h2>Load settings</h2>	 <p>Load a configuration file created before.</p>
	<h2>Password</h2>	 <p>Change the default password to a new one. <b>The new password cannot be the default password!</b></p>
	<h2>Configure Forwarding</h2>	 <p>Here you can define a default rule for how packets forwarded by the firewall should be handled.</p> <ul style="list-style-type: none"> <li>• Drop packets: Network traffic is blocked</li> <li>• Forward packets: Network traffic is allowed</li> </ul>



	<h2>WAN configuration</h2>	 <p>Configure the WAN-Interface of the router. This can be done via DHCP client (factory default), static IP and Mobile Broadband.</p> <p>The status LED's will turn green, if settings work. For more information on the settings please refer to the respective chapter.</p>
	<h2>Date &amp; Time</h2>	 <p>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.</p>




<p>Proxy</p>	<div><div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>8</div><div>9</div></div><div>LanguageLoad SettingsPasswordConfigure forwardingWAN configurationDate &amp; TimeProxyu-linkOverview</div></div> <div><h3>Proxy</h3><p>If you need a proxy-server to get an internet connection you can configure it here.</p><div><div>Use HTTP proxy:</div><div>no</div></div><div><div>Internet connection to u-link server:</div><div><input type="checkbox"/></div></div><div><div>Back</div><div>Apply</div><div>Next</div></div></div> <p>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.</p>
<p>u-link</p>	<div><div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>8</div><div>9</div></div><div>LanguageLoad SettingsPasswordConfigure forwardingWAN configurationDate &amp; TimeProxyu-linkOverview</div></div> <div><h3>u-link</h3><p>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 <a href="http://www.u-link.weidmueller.com">www.u-link.weidmueller.com</a> and create a router-object to get a Registration code.</p><div><div>Registration code:</div><div></div></div><div><div>Internet connection to u-link server:</div><div><input type="checkbox"/></div></div><div><div>Registration state:</div><div><input type="checkbox"/></div></div><div><div>u-link Heartbeat:</div><div><input type="checkbox"/></div></div><div><div>u-link VPN connection state:</div><div><input type="checkbox"/></div></div><div><div>Back</div><div>Apply</div><div>Next</div></div></div> <p>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 <a href="http://www.u-link.weidmueller.com">www.u-link.weidmueller.com</a> and create a router-object to get a registration code. The status LED's will turn green, if settings work.</p>
<p>Overview</p>	<div><div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>8</div><div>9</div></div><div>LanguageLoad SettingsPasswordConfigure forwardingWAN configurationDate &amp; TimeProxyu-linkOverview</div></div> <div><h3>Overview</h3><div><div>Link state:</div><div><input type="checkbox"/></div></div><div><div>IP address:</div><div><input type="checkbox"/></div></div><div><div>World-wide heartbeat connectivity:</div><div><input type="checkbox"/></div></div><div><div>u-link Heartbeat:</div><div><input type="checkbox"/></div></div><div><div>u-link VPN connection state:</div><div><input type="checkbox"/></div></div></div> <div><div>Back</div><div>Download settings</div><div>Save settings</div></div>




## 4.2.1 Configuration → IP Configuration

### IP Configuration → Operational mode “IP Router”



## Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration**
  - Packet filter
  - General settings
  - Access control
  - Network
  - VPN
  - Services
- System
- Information

Configuration

**IP configuration**

**Operational mode:** IP router ?

**WAN:**

IP assignment: DHCP ?

☒ DNS via DHCP

☒ Gateway via DHCP

NAT (Masquerading): ☒ ?

**LAN:**

IP assignment: static ?

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒ ?

**WWAN:**

Dialmode: disabled ?

**Default gateway:**

IP address:

Screenshot shows factory default operation mode 'IP Router'.

At factory default the IP assignment mode is set to DHCP at WAN port.

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

Section 4G 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.

Apply settings
Reset changes

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).	
	<b>Operational mode</b>	<p><u>Transparent bridge:</u> 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).</p> <p><u>IP Router:</u> 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.</p>
	<b>LAN / WAN</b> IP assignment	<p>All interfaces can be configured with static or dynamic (DHCP) IP addresses.</p> <p><u>Static:</u> Assign a static IP address and subnet mask to the interface.</p> <p><u>DHCP:</u> Request an IP address from a DHCP (Dynamic Host Configuration Protocol) server.</p> <p><u>DHCP + fallback:</u> First, try to request an IP address by DHCP and if it fails use the static one.</p> <p><u>PPPoE/DHCP:</u> The IP address will be assigned by the provider.</p>
	<b>4G (optional)</b>	Configuration of 4G network connection



Dialmode	<p>Disabled: Do not use 4G modem.</p> <p>Manual: Dialing can be triggered manually from 4G status page.</p> <p>Permanent: The 4G link will be established automatically on system boot.</p> <p>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.</p>
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) for which the 4G interface shall be used as fallback.
Fallback for IP address	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 4G	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. <b>NAT is always activated for 4G modem.</b>
Gateway via 4G	If activated as soon as mobile connection is active (Online) it will be used as the Router's <b>default</b> gateway.
<b>Default gateway</b>	<p>Assign the IP address of the Routers default gateway.</p> <p>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 4G" is enabled then the default gateway IP address will be set automatically and cannot be edited manually.</p>

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

Manual band selection: ☒

3G ☒ any ☒ B8 ☐ B5 ☒ B4 ☒ B3 ☒ B2 ☐ B1

4G ☒ any ☒ B41 ☒ B30 ☒ B29 ☐ B26 ☒ B25 ☒ B20 ☐ B13 ☒ B12 ☒ B8 ☒ B7 ☐ B5 ☒ B4 ☒ B3 ☒ B2 ☒ B1




## 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).



### Weidmüller Router Configuration

#### IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration**
  - Packet filter
  - General settings
  - Access control
  - Network
  - VPN
  - Services
- System
- Information

User: admin

Configuration

---

**IP configuration**

**Operational mode:** Transparent bridge ⓘ

**LAN:**

IP assignment: static ⓘ

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒ ⓘ

**WWAN:**

Dialmode: disabled ⓘ


**Default gateway:**

IP address:

Apply settings
Reset changes


## 4.2.3 Configuration → Packet filter (Firewall)

### Packet filter → Tab Layer 3



### Weidmüller Router Configuration

#### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter**
  - General settings
  - Access control
  - Network
  - VPN
  - Services
- System
- Information

User: admin

Layer 3

Layer 2

Status

**Packet filter layer 3** ⓘ

**2 rule sets** ⓘ

▸ **1 block\_dns** (1 rule)

block dns

▲ ▼ 🔍 🗑️

▸ **2 Allow\_L3\*** (1 rule)

Allow all L3 traffic

▲ ▼ 🔍 🗑️

**Add a new rule set** +

By using the plus symbol you can add new rule sets

**Show rule sets for following interfaces**

only rules affecting the selected network interfaces will be displayed

from: \*
to: \*


↻

Apply settings




Menu	Configuration → Packet filter → Tab „Layer 3”
Function	<p>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.</p> <p>For more detailed information about using the packet filter please refer to firewall-related application notes in appendix A.</p>

Packet filter → Tab Layer 2



Weidmüller Router Configuration  
IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

Diagnostics

Configuration

Config Wizard

IP configuration

**Packet filter**

General settings

Access control

Network

VPN

Services

System

Information

User: admin

Layer 3

**Layer 2**

Status

Packet filter layer 2 ?

2 rule sets ?

1 ARP\* (1 rule)  
ARP address resolution

2 Allow\_L2\* (1 rule)  
Allow all L2 traffic

Add a new rule set  
By using the plus symbol you can add new rule sets

Show rule sets for following interfaces

only rules affecting the selected network interfaces will be displayed

from: \* to: \*

Apply settings

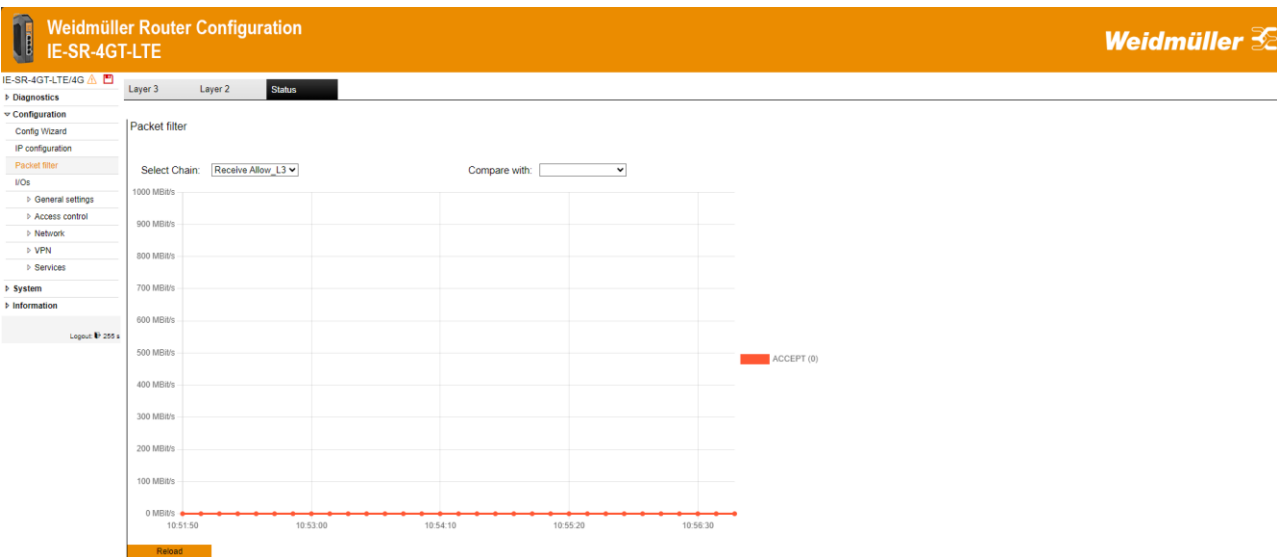
Menu	Configuration → Packet filter → Tab „Layer 2”
Function	<p>This is the window for the manual configuration of firewall filter rules based on Layer 2 (MAC layer). The screenshot shows the firewall settings as delivered with the 2 default rules "Allow_L2*" and „ARP*" (Address resolution protocol). 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.</p>

Version 1.8 /August 2025

Page 37 / 134



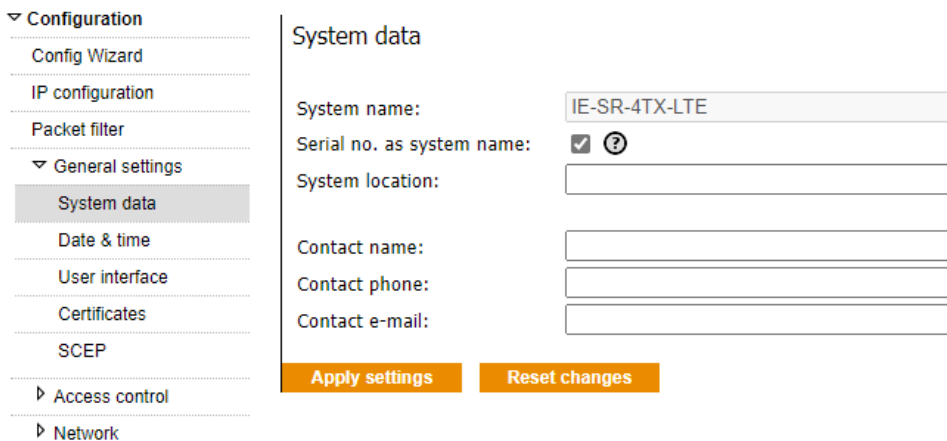
## Packet filter → Tab Status




<b>Menu</b>	Configuration → Packet filter → Tab „Status“
<b>Function</b>	Overview of transmit and receive activities of the physical and virtual interfaces.

## 4.2.4 Configuration → General settings

### General settings → System data



The screenshot shows the 'System data' configuration page. The left sidebar contains navigation options: Configuration (Config Wizard, IP configuration, Packet filter), General settings (System data, Date & time, User interface, Certificates, SCEP), Access control, and Network. The main area contains the following fields:

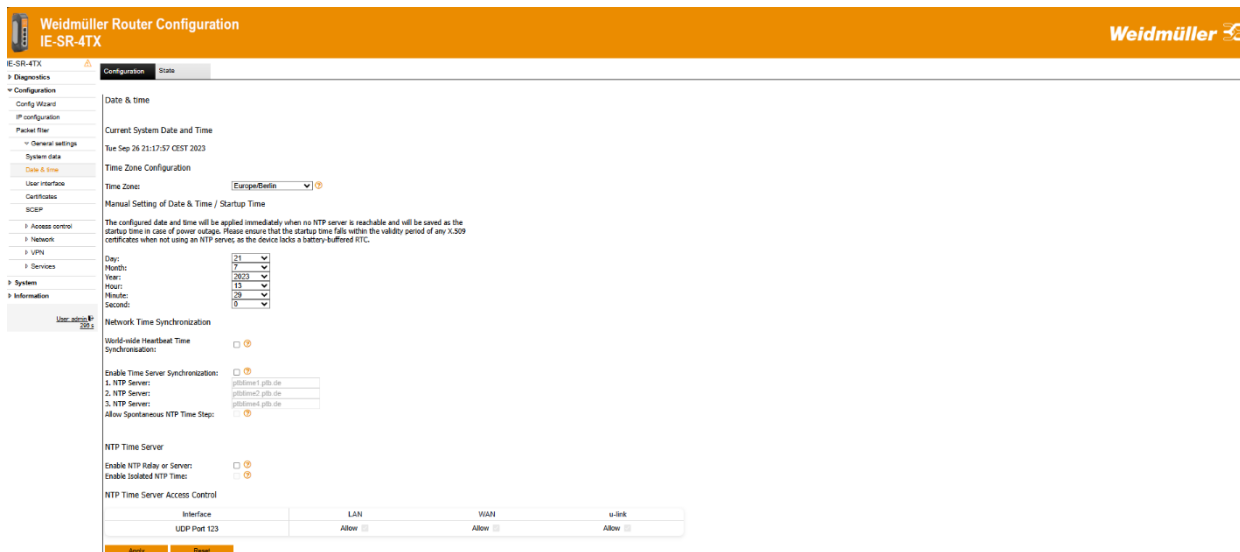
- System name:** IE-SR-4TX-LTE
- Serial no. as system name:** ☒ 
- System location:**
- Contact name:**
- Contact phone:**
- Contact e-mail:**

At the bottom, there are two buttons: 'Apply settings' and 'Reset changes'.

<b>Menu</b>	Configuration → General settings → System data	
<b>Function</b>	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. <b>Note:</b> 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-4TXAX20131010).



## 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

1. **The Router has no battery-buffered, but a capacity-buffered system clock.**
2. General behavior of date/time settings:
3. 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.

## General settings → Date & Time Tab State


**Weidmüller Router Configuration**  
**IE-SR-4TX**



IE-SR-4TX  
Diagnostics  
Configuration  
Config Wizard  
IP configuration  
Packet filter  
General settings  
System data  
**Date & time**  
User interface  
Certificates  
SCEP  
Access control  
Network  
VPN  
Services  
System  
Information

Configuration State  
NTP Source Statistics  

Mode	State	Name/IP	Stratum	Polling rate	NTP reach register	Time since last response (s)	Offset (s)	Measured (s)	Error margin (s)
^	?	192.53.103.108	1	6	3	0	-61585624.000000000	-61585624.000000000	0.019810431
^	?	192.53.103.104	1	6	3	0	-61585624.000000000	-61585624.000000000	0.017454591
^	?	194.94.95.123	1	6	3	0	-61585624.000000000	-61585624.000000000	0.019171223

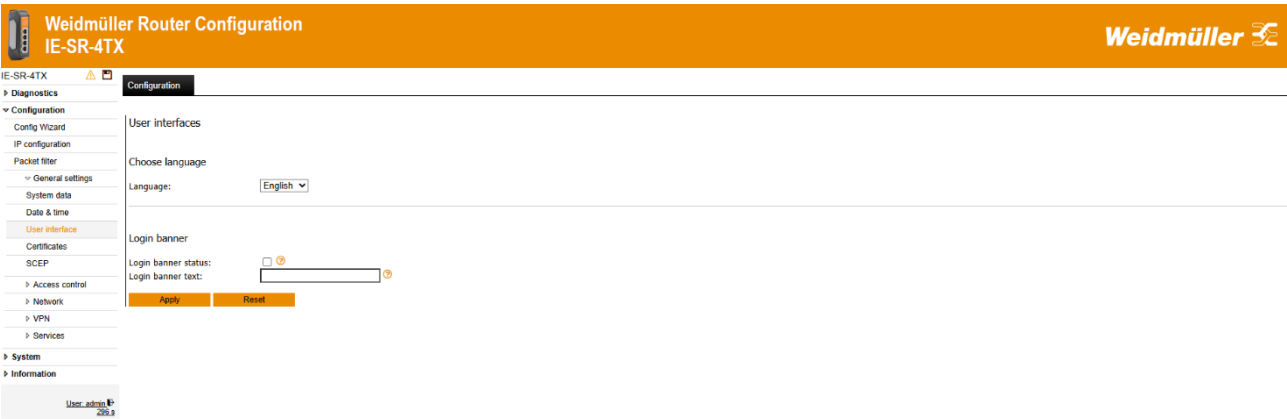
  
Reset

User admin  
202.8

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

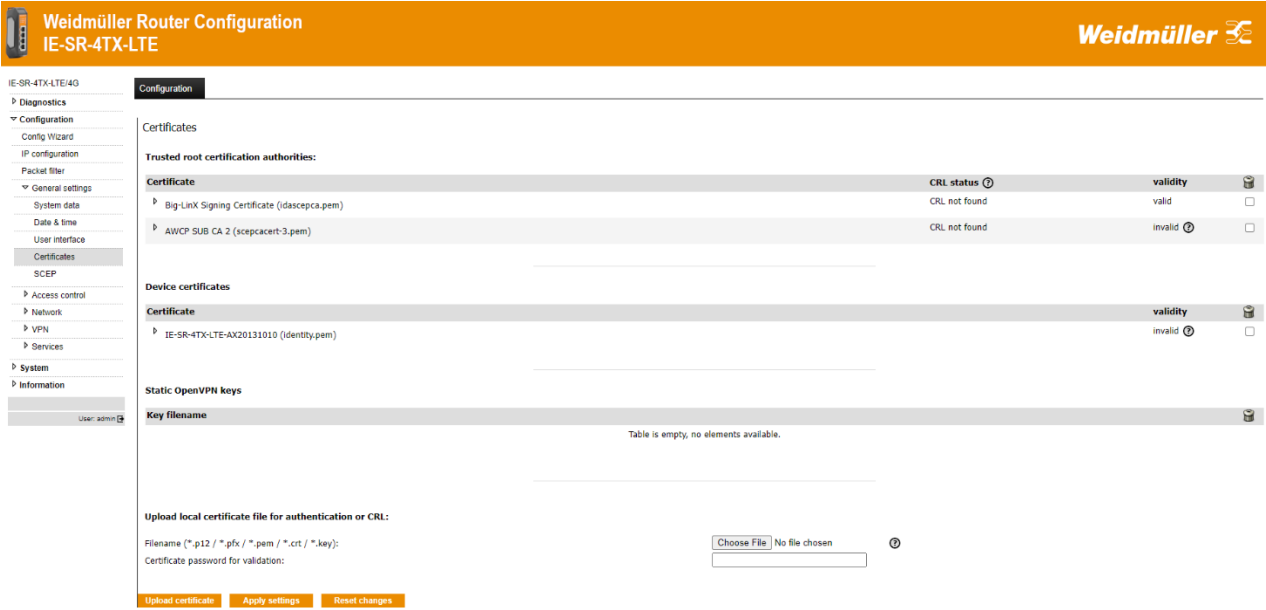


General settings → User Interface



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

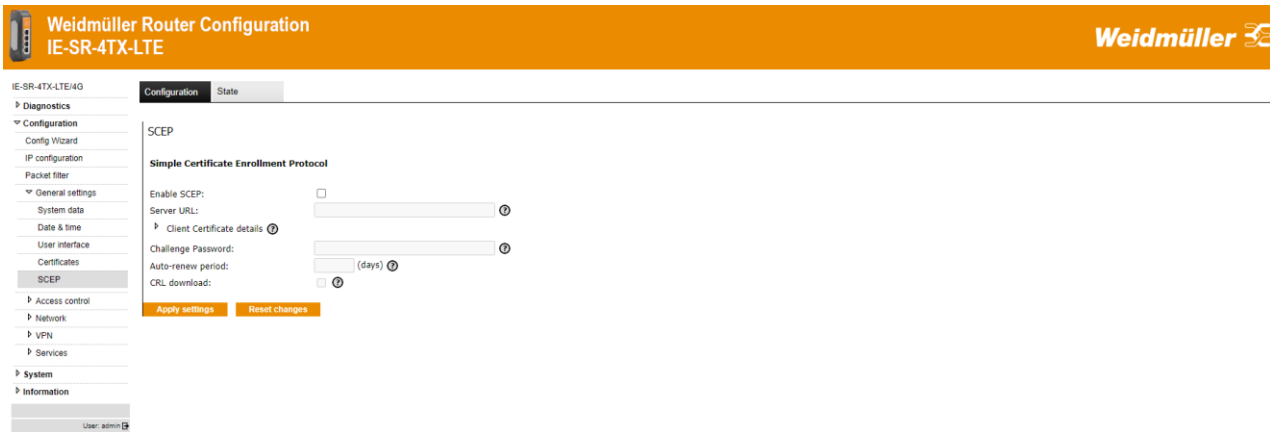
General settings → Certificates



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

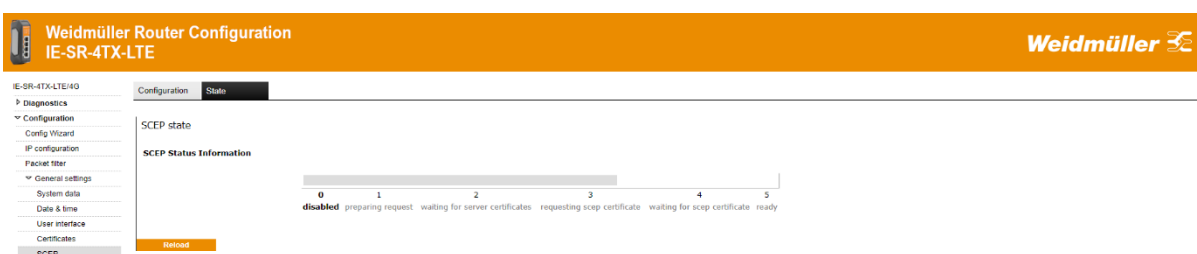


## General settings → SCEP (Tab Configuration)



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

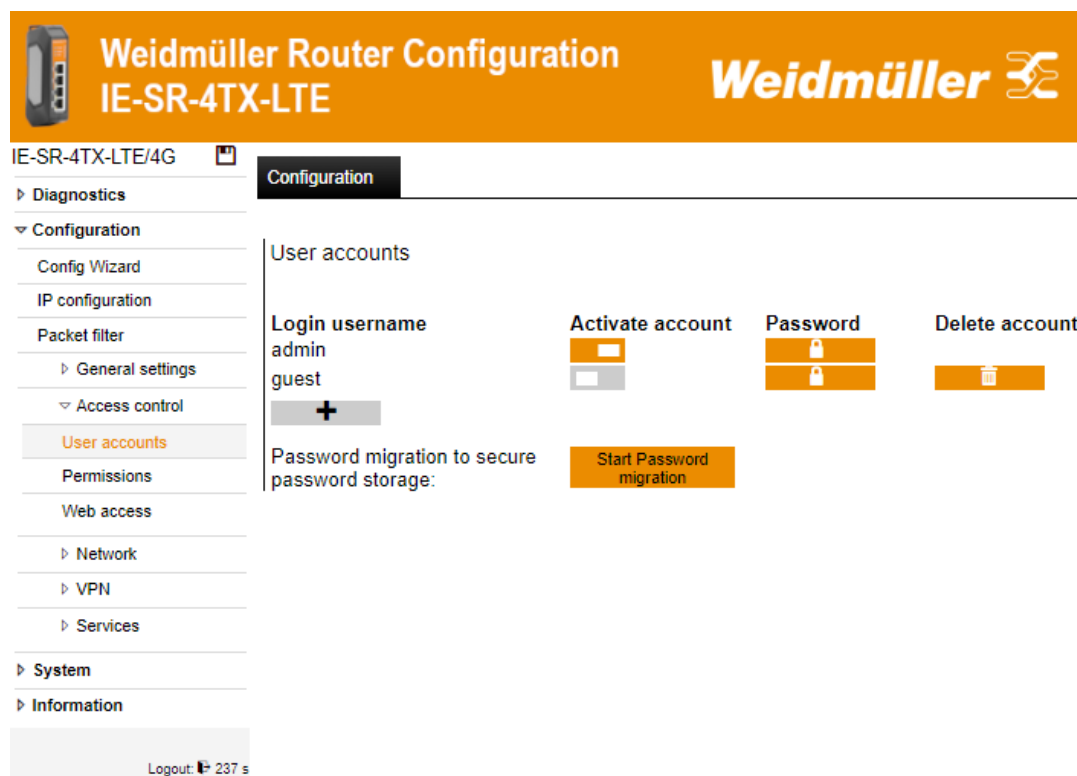
All user passwords must meet the following requirements:

- 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!*

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




<b>Function</b>	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.
--	--------------------------	---





# Weidmüller Router Configuration IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G  

Configuration

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▼ Access control

User accounts

Permissions

Web access

▸ Network






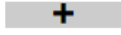
▸ VPN

▸ Services


▸ System


▸ Information


User accounts

Login username	Activate account	Password	Delete account
admin			
guest			
			

Password migration to insecure password storage (compability mode):  
Password migration to secure passwords:

Start Password migration 


Password migration to secure passwords 

Logout:  289 s

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 ( <b>compability mode</b> )	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!**



## Weidmüller Router Configuration IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

Configuration
Security

Diagnostics
Configuration
Config Wizard
IP configuration
Packet filter
General settings
Access control
User accounts
Permissions
Web access
Custom menu
Network
VPN
Services
System
Information

User accounts

Username	Activate account	Set password	Delete account
admin			
guest			

Password migration

Storage

Due to EN18031-1 (RED) requirements the password storage can not be downgraded to old MD5-Hashes

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.

Enforce


User\_admin

180 s


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)




**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**





E-SR-4TX-LTE/4G    
**Configuration** | **Security**  




---





- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
    - General settings
    - ▾ Access control
      - User accounts**
      - Permissions
      - Web access
      - Custom menu
    - Network
    - VPN
    - Services
- System
- Information





User: admin  290 s

### Security-Settings

**Session timeout**  
Session timeout:  300 [ Seconds ] 

**Password history**  
Number of stored Passwords:  0 [ Count ] 

**Password lifetime**  
This lets you configure a security feature ensuring regular password changes for its duration.  
☒ Security feature: password lifetime:  
Maximal password lifetime:  365 [ Days ]   
Minimal password lifetime:  0 [ Days ] 

**Login ban**  
Password tries:  10 [ Count ]   
Login ban timeout:  60 [ Seconds ] 

Apply
Reset


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



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

Configuration

▸ Diagnostics

▾ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▾ Access control

User accounts

Permissions

Web access

▸ Network

▸ VPN

▸ Services

▸ System

▸ Information

User: admin

Permissions

Editing variable permissions for user : 

guest

 Default Write Permission: ☐

Page name

▸ 1:1 NAT

▸ 3G/4G modem state

▸ Backup settings

▸ Certificates

▸ Cut & Alarm state


▸ DHCP server

▸ DNS

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




# Weidmüller Router Configuration

## IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - ▾ Access control
    - User accounts
    - Permissions
    - Web access
  - Network
  - VPN
  - Services
- System
- Information

User: admin 

Configuration

### Web access

Allow protocol access on interface	LAN	WAN	u-link	WWAN
HTTP:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HTTPS:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

---

Report access violations using syslog

☒


Apply settings

Reset changes

<b>Menu</b>	Configuration → Access control → Web access
<b>Function</b>	<p>Select the possible access modes of the web interface (via http and / or https) for the different interfaces.</p> <p>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.</p> <p><i>Note: The web interface on firmware 2.0.0 and above 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.</i></p>



Access Control → Custom menu



Weidmüller Router Configuration  
IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

Information

Configuration

System

Information

User: admin

288 s

Custom menu

Visible menu entries for specific users guest

All

Diagnostics

- u-link
- Eventlog
- Audit
- WAN
- LAN
- WLAN
- WWAN
- Ping test
- Remote capture
- Download

Configuration


- Config Wizard
- IoT Wizard
- IP configuration
- Packet filter
- I/Os

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)



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-4TX-LTE/4G

Configuration State

Diagnosics

Configuration

Config Wizard

IP configuration

Packet filter

General settings

Access control

Network

**DNS**

IP routing

HTTP Proxy

Forwarding

1:1 NAT

Network groups

Hardware groups

Ethernet

### DNS

Hostname:

IE-SR-4TX-LTE ?

Serial no. as hostname:

☒ ?

Domain name (search suffix):

?

1st DNS server:

?

2nd DNS server:

3rd DNS server:

Register hostname at DHCP server:

☒ ?

Use all servers concurrently:

☐ ?


DNS proxy and DNS server services can be configured at Configuration->Services->DNS proxy.

Apply settings
Reset changes


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	
1 <sup>st</sup> , 2 <sup>nd</sup> , 3 <sup>rd</sup> DNS server	<p>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).</p> <p>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.</p> <p>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.</p> <p>Note: See Tab „State“ to check the currently configured name server(s).</p>	
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)



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Weidmüller** 

IE-SR-4TX-LTE/4G

Configuration

State

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▸ Access control

▼ Network

DNS

IP routing

HTTP Proxy

DNS state

**Current DNS configuration**

Domain suffix:   lan

Domain suffix:   lan


Nameserver:     192.168.9.1

Reload

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




## Network → IP Routing (Tab Static)



### Weidmüller Router Configuration

#### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - ▾ Network
    - DNS
    - IP routing
    - HTTP Proxy
    - Forwarding
    - 1:1 NAT
  - Network groups

Static

Dynamic

State

#### Static

Active Destination ? ?	Prefix ?	Gateway ?	Interface ?	Metric ?	Push to u-link ?
No data available in table					

+

Apply settings
Reset changes


Menu	Configuration → Network → IP Routing → Tab „Static“	
Function	<p>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.</p> <p>Up to 20 static IP routes can be configured.</p>	
	Static Routing Routing Table	<p>Displays all configured static routes</p> <p>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.</p> <p>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).</p> <p>Another example is 192.168.0.0 and subnet mask 16. Any IP of the format 192.168.xxx.xxx belongs to this network.</p>
	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)



### Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
- General settings
- Access control
- ▼ Network
  - DNS
  - IP routing
  - HTTP Proxy
  - Forwarding
  - 1:1 NAT
  - Network groups
  - Hardware groups
  - Ethernet
- VPN
- Services
- System
- Information

User: admin

Static

Dynamic

State

#### Dynamic

**Dynamic routing:**

LAN:

Type: disabled ▾ ?

Simple password: ?

Active interface: ☒ ?

WAN:

Type: disabled ▾ ?

Simple password: ?

Active interface: ☒ ?

u-link:

Type: disabled ▾ ?

Simple password: ?

Active interface: ☒ ?

Redistribute static routes: ☐ ?

Log level: none ▾ ?

Apply settings


Reset changes

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. <ul style="list-style-type: none"> <li>- RIP the Routing Information Protocol is frequently used and helps routers to dynamically adapt to changes</li> <li>- OSPF Open Shortest Path First is newer and made RIP obsolete</li> <li>- Both Select this if you want to use both protocols at a time</li> </ul>
	Dynamic Routing Simple Password	This field is optional. The OSPF/RIP simple password authentication will protect all packets with this password. <b>Note that this password will be send as clear text!</b> 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 advertisement 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)



# Weidmüller Router Configuration

## IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - ▼ Network
    - DNS
    - IP routing

Static
Dynamic
State

IP routing state

**Active routing table:**

```
192.168.9.0/24 dev WAN proto kernel scope link src 192.168.9.67
192.168.2.10 dev WAN scope link
192.168.1.0/24 dev LAN proto kernel scope link src 192.168.1.10
default via 192.168.9.1 dev WAN
```

Reload

Use this menu for checking the Router's current routing table.

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



## Network → HTTP proxy

### Weidmüller Router Configuration

#### IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - ▼ Network
    - DNS
    - IP routing
    - HTTP Proxy

Configuration

### HTTP Proxy

HTTP proxy IP address or hostname:

HTTP proxy TCP port:

HTTP proxy authentication method: none

HTTP proxy username:

HTTP proxy password:

Apply settings
Reset changes

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

### Weidmüller Router Configuration

#### IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - ▼ Network
    - DNS
    - IP routing
    - HTTP Proxy
    - Forwarding

Configuration

### Forwarding

Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT Source Network	Comment	Enabled	Position	Reverse	Delete
WAN	TCP		502	192.168.1.125	502	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			
WAN	*	192.168.99.223		192.168.1.151		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			

Apply settings
Reset changes

**Screenshot shows 2 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 192.168.99.223 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	
Function	<p>Configuring of forwardings based on IP address, protocol and port number.</p> <p>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.</p> <p>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. <b>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.</b> 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.</p> <p>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”.</p>	
	Public interface	Incoming interface on which the IP packet - which shall be forwarded - will arrive.
	Protocol	<p>Select protocol TCP or UDP if you want to forward a special port.</p> <p>Use “*” if you want to forward all IP packets (ICMP, TCP, UDP) independent from protocol and port.</p>
	Local IP	<p>Enter a free available IP address which will behave as an <b>additional</b> (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.</p> <p>If you leave it empty, the current IP address of the defined (incoming) interface will be used as ‘Local IP’.</p>
	Local port	The addressed port belonging to “Local IP” if protocol TCP or UDP is selected. Leave empty if entry “*” is selected for protocol.
	Target IP	The target IP to which the IP packet – addressed to “Local IP” will be forwarded. This can be any reachable IP address.
	Target Port	The addressed port belonging to “Target IP” if protocol TCP or UDP is selected. Leave empty if entry “*” is selected for protocol.
	SNAT	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.
	Reverse SNAT	On connections being initiated from the Target IP and leaving the Public Interface the sender address will be mapped to the Local IP. This is only valid for Protocol “*”.
	Source Network	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.
	Comment	An optional comment
	Enabled	Enables or disables the entry.



	Position	<p>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.</p> <p><u>Example:</u> 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.</p> <p>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.</p>
	<p>Note after editing a value, press accept ✓ or delete x, otherwise the message "Syntax error applying data" will appear.</p>	






## Network → 1:1 NAT



# Weidmüller Router Configuration

## IE-SR-4TX-LTE




IE-SR-4TX-LTE/4G  


- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
    - General settings
    - Access control
  - ▼ Network
    - DNS
    - IP routing
    - HTTP Proxy
    - Forwarding
    - 1:1 NAT
    - Network groups
    - Hardware groups
    - Ethernet
      - VPN
      - Services
- System
- Information


Configuration

### 1:1 NAT - network mapping

**WAN:**


Enable 1:1 NAT: ☐ 


Public IP address/subnet mask: disabled (DHCP) 


Private IP address/subnet mask:  

▸ Advanced settings

**LAN:**

Enable 1:1 NAT: ☐ 


Public IP address/subnet mask: 192.168.1.10/24 

Private IP address/subnet mask:  

▸ Advanced settings

Apply settings

Reset changes


Logout:  208 s


Menu	Configuration → Network → 1:1 NAT	
Function	<p>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.</p> <p>1:1 NAT can be configured for all active (physical and virtual) interfaces.</p> <p>Note: While the private subnets may be equal they must not conflict with the public IP subnets.</p> <p><b>For more detailed information about using 1:1 NAT please refer to application notes in appendix A.</b></p>	
	Enable 1:1 NAT	<p>Enable 1:1 NAT for this interface.</p> <p>Note: 1:1 NAT only can be activated if NAT (masquerading) is <b>not</b> enabled for this interface</p>
	Public IP address	<p>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.</p>



	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


**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-4TX-LTE4G

Configuration

Diagnosics

Configuration

Config Wizard

IP configuration

Packet filter

General settings

Access control

Network

DNS

IP routing

HTTP Proxy

Forwarding

1:1 NAT

**Network groups**

Hardware groups

Ethernet

VPN

Services

System

Information

User: admin

Network groups

**Machine1**

192.168.2.100/32

192.168.2.102/32

**Domains**

google.com

weidmueller.com

Group name:

Network address:


Apply settings

Reset changes

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	<p>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.</p> <p>Hint: Click on an existing group name will fill the empty text field.</p>
	Network address	<p>Network address using format 'IP/network mask' (CIDR) e.g. 192.168.0.0/24 – to be added to a given group. These groups can be referred to by other services like filter rules e.g.</p> <p>Caution: Filter rules, that use a rule with a recently modified group, will not be updated until &lt;Apply settings&gt; is triggered (or &lt;Save settings&gt; respectively)</p>




Network → Hardware Groups



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

Configuration

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▸ Access control

▼ Network

DNS

IP routing

HTTP Proxy

Forwarding

1:1 NAT

Network groups

Hardware groups

Hardware groups

no groups have been stored yet

add groups by using the form below

Group name:

?

Hardware address:

?


Apply settings

Reset changes

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



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

Configuration

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▸ Access control

▼ Network

DNS

IP routing

HTTP Proxy

Forwarding

1:1 NAT

Network groups

Hardware groups

Ethernet

Ethernet configuration

WAN link mode :  
LAN-1 link mode :  
LAN-2 link mode :  
LAN-3 link mode :

automatic  
automatic  
automatic  
automatic

▼▼▼▼  
②②②②

Apply settings

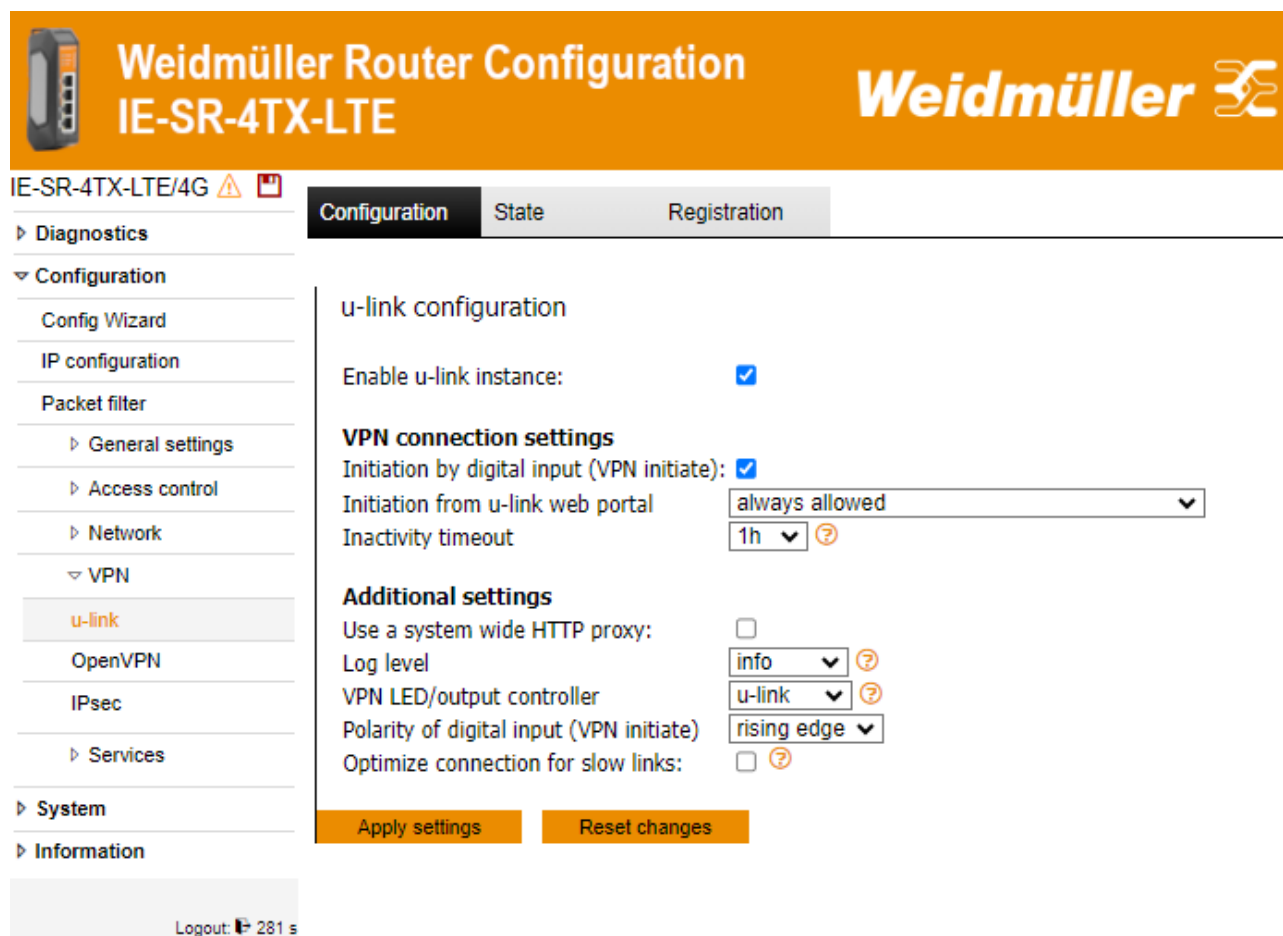
Reset changes

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.	
	auto-matic	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.



## 4.2.8 Configuration → VPN

VPN → u-link (Tab Configuration)



The screenshot shows the Weidmüller Router Configuration web interface for the IE-SR-4TX-LTE model. The left sidebar contains a navigation menu with options like Diagnostics, Configuration, System, and Information. The 'Configuration' tab is active, and the 'u-link' option is selected under the VPN section. The main content area displays the 'u-link configuration' settings, including a checkbox to 'Enable u-link instance', 'VPN connection settings' for initiation and timeout, and 'Additional settings' for HTTP proxy and log level. Buttons for 'Apply settings' and 'Reset changes' are at the bottom.


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	<p><u>Never allowed:</u> u-link cannot be initiated remotely from the u-link portal</p> <p><u>Always allowed:</u> u-link can be initiated remotely from the u-link portal</p> <p><u>Allowed if digital input (VPN-Initiate) is active:</u> u-link can be initiated remotely from the u-link portal <b>only</b> if the external digital input (‘VPN initiate’ set to 24 VDC) is active.</p>
	Inactivity timeout	Close a switched VPN connection if less than 100kB data were sent for the set amount of time.
	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	<u>None:</u> Will log no messages through the Event Log <u>Info:</u> Log only some information and critical errors <u>Debug:</u> Log state information too <u>Verbose:</u> Log all possible messages
	VPN LED	<u>Disabled:</u> The LED is not used by u-link. <u>u-link:</u> The LED is <u>blinking</u> during connecting and is <u>on</u> when connected. <u>IPSec:</u> The LED is <u>blinking</u> during connecting and is <u>on</u> when connected.
	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	Enabling this feature optimizes slow connections with timings above 1000ms, i.e. satellite connections.




## VPN→ u-link (Tab State)



### Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - Network
  - ▾ VPN
    - u-link**
    - OpenVPN
    - IPsec
  - Services
- System
- Information

Configuration

State

Registration

#### u-link status

Status Registration u-link Portal:
registered

---

#### WWH communication

Status:
Connected

Last seen:
Friday, 20 Oct 2023, 13:02

---

#### VPN connection u-link portal


Status:
VPN not connected
Connect

Reload

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)



### Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control

Configuration

State

Registration


#### u-link registration

Status Registration u-link Portal: registered

Registration code


Unregister
Reload

Menu	Configuration → VPN → u-link → Tab “Registration”
Function	<p>Register or unregister the device at the u-link platform. For this an internet connection of the device is necessary.</p> <p>To register, type in the unique Router Activation code generated in the u-link portal (<a href="https://u-link.weidmueller.com">https://u-link.weidmueller.com</a>) by adding a new router-item or the code of a previously used router-item in section Administration → Device management.</p> <p>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 (<a href="mailto:u-link-support@weidmueller.com">u-link-support@weidmueller.com</a>).</p>

Note
 <p>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.</p>




## VPN→ OpenVPN (Tab Configuration)



# Weidmüller Router Configuration

## IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - Network
  - ▼ VPN
    - u-link
    - OpenVPN
    - IPsec
  - Services
- System
- Information

User: admin

Configuration
VPN1
VPN2
VPN3
VPN4
VPN5
VPN6
VPN7
VPN8
VPN9
VPN10
State

### OpenVPN

**Current OpenVPN server table:**

Device	Certificate	IP Info	Protocol	Local server port
OpenVPN server table is empty. Use the VPN tabs if you want to add a new connection.				

**Current OpenVPN client table:**

Device	Certificate	IP Info	Protocol	Server address	Server port
OpenVPN client table is empty. Use the VPN tabs if you want to add a new connection.					

**Additional settings:**

VPN LED/output controller: u-link ?

Polarity of VPN input: rising edge

Apply settings
Reset changes

Menu	Configuration → VPN → OpenVPN → Tab „Configuration“	
Function	<p>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.</p> <p>Note: OpenVPN connections can only be used with encryption based on certificates.</p> <p>On each configured OpenVPN server connection theoretically any number of remote OpenVPN clients can be connected (only limited by the hardware performance of the Router).</p> <p>After configuration of OpenVPN sessions the configured connected will be displayed at a glance in this menu.</p>	
VPN LED	<p><u>Disabled:</u> The LED is not used by u-link.</p> <p><u>u-link:</u> The LED is <u>blinking</u> during connecting and is <u>on</u> when connected.</p> <p><u>IPSec:</u> The LED is <u>blinking</u> during connecting and is <u>on</u> when connected.</p>	
Polarity of digital input (VPN initiate)	<p>rising edge: VPN is triggered by rising edge of input voltage (from 0 V to 24 V)</p> <p>falling edge VPN is triggered by falling edge of input voltage (from 24 V to 0 V)</p>	



VPN→ OpenVPN (Tab VPN1)




## Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▼ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - Network
  - ▼ VPN
    - u-link
    - OpenVPN
    - IPsec
  - Services
- System
- Information


User: admin 


Configuration
VPN1
VPN2
VPN3
VPN4
VPN5
VPN6
VPN7
VPN8
VPN9
VPN10
State


### VPN1


#### Basic settings


Enable VPN instance: ☐


Interface mode: Client 


Permanent connection: ☒ 


Layer: Layer 3 


OpenVPN device type: TAP 


Server address:  

Remote cert TLS type: server: ☒ 

Server port:  


Protocol: TCP 


Certificate: scep-cert.pem 

Authenticate with username and password: ☐ 


Username:


Password:  show

Pull routes from server: ☐ 


Use HTTP proxy: ☐ 


#### TLS settings


minimum version: 1.2 


TLS protection: disabled 


#### Additional settings


Log level: info 

LZO compression: adaptive 

Cipher: AES-256-CBC 

Authentication method: SHA256 

Keepalive interval: 10 

Keepalive timeout: 60 

Apply settings
Reset changes

Configuration of OpenVPN connections on tabs VPN2 ... VPN10 are the same as for 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	<p>Select the connection mode which is either Server or Client</p> <p>Server: The device will run a TCP/UDP server which numerous clients can connect to</p> <p>Client: The device will establish a connection to an OpenVPN server</p>





	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. <b>IP Address Pool:</b> Authenticates clients based on their certificates and assigns IP addresses from a defined local pool. The IP Range for an IP address assignment must be within the IP subnet of the VPN interface and must not be used already by any other interface. <b>RADIUS Server:</b> 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. <b>Configuration table:</b> 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)

IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings

Configuration
VPN1
VPN2
VPN3
VPN4
VPN5
VPN6
VPN7
VPN8
VPN9
VPN10
State

OpenVPN state

OpenVPN table is empty

Reload



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



## VPN → IPsec (Tab Configuration)

The screenshot shows the 'IPsec' configuration tab in the Weidmüller Router Configuration interface. The left sidebar contains a navigation menu with options like 'Diagnostics', 'Configuration', 'Config Wizard', 'IP configuration', 'Packet filter', 'General settings', 'Access control', 'Network', 'VPN', 'Link', 'QoS/PIV', 'IPsec', 'Services', 'System', and 'Information'. The main area is titled 'IPsec' and contains several sections: 'Enable IPsec', 'Enable NAT traversal', 'Limit MTU', 'Enable PFS', 'Enable aggressive mode', 'Uplink interface', 'Local next hop', 'Local subnet', 'Authentication method', 'PSK', 'Certificate', 'Send certificate', 'Log level', 'VPN LED/output controller', 'IKE version', 'IKE ophers (Phase 1)', 'IKE hash functions (Phase 1)', 'DH group (Phase 1)', 'ESP ophers (Phase 2)', and 'ESP hash functions (Phase 2)'. Below these settings is a table titled 'Current IPsec connections' with columns for 'Active', 'Connection name', 'Operational mode', 'Local ID', 'Remote IP address', 'CA certificate', 'Remote ID', and 'Remote subnet'. At the bottom, there is an 'Add new connection' section with fields for 'Operational mode', 'Local ID', 'Remote IP address', 'CA certificate', 'Remote ID', and 'Remote subnet'.

Menu	Configuration → VPN → IPsec → Tab „Configuration“	
Func-tion	<p>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.</p> <p>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.</p> <p>IPsec connections can be used with both PSK encryption (pre-shared key using user name and password) as well as certificate based encryption.</p>	
	Enable NAT traversal	<p>NAT traversal is required when a router between the local and remote side does Network Address Translation (NAT)</p> <p>Note: IPsec pass through will break NAT traversal! If your router supports it, you must disable IPsec pass through!</p>
	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	<p>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.</p> <p>Note: The local and remote subnet must not be equal!</p> <p>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.</p>
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	<p>This is the pre-shared key (must be equal on both sides)</p> <p>Note: Do not use simple words or phrases! A PSK should be a random sequence of 48 characters in base64 format.</p>
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	<p>None: Will log no messages through the Event Log</p> <p>Info: Log only some information and critical errors</p> <p>Debug: Log state information too</p> <p>Verbose: Log all possible messages</p>
VPN LED/output controller	<p><u>Disabled</u>: The LED is not used by u-link.</p> <p><u>u-link</u>: The LED is <u>blinking</u> during connecting and is <u>on</u> when connected.</p> <p><u>IPSec</u>: The LED is <u>blinking</u> during connecting and is <u>on</u> when connected.</p>
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	<p>Operational mode of the local side:</p> <p>Active: Try to establish the connection immediately and periodically retry. This is the normal mode.</p> <p>Active (switched): Connection setup is triggered by VPN initiate.</p> <p>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).</p>
	Local ID	<p>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.</p>
	Remote IP address	<p>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).</p>
	CA certificate	<p>The remote peer its certificate must have been signed by this CA to be accepted</p>
	Remote ID	<p>The peer will identify (not authenticate) itself with this ID depending on the chose authentication method.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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).</p>
	Remote subnet	<p>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.</p> <p>Note: The local and remote subnet must not be equal!</p> <p>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.</p>


#### Note






By default, the Router uses the parameters AES128, MD5, DH group 2 for Main-Mode and AES128, SHA1 for Quick-Mode.  
Authentication by „Aggressive-Mode is due to security reasons not supported!

#### VPN → IPsec (Tab State)



## Weidmüller Router Configuration

### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control

Configuration

State

### IPsec state

Current IPsec tunnels:

Reload

<b>Menu</b>	Configuration → VPN → IPsec → Tab State
<b>Function</b>	Displays all IPsec tunnels and their state.

## 4.2.9 Configuration → Services

### Services → DHCP Server (Tab Configuration)



## Weidmüller Router Configuration

### IE-SR-4TX



IE-SR-4TX

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - Network
  - VPN
  - ▾ Services
    - DHCP server**
    - DNS proxy
    - Web server
    - Modbus TCP
    - Scheduler
- System
- Information

Configuration

State

### DHCP server

☐ Enable DHCP server:
☐ Enable DHCP debugging:

☐ On following interfaces:

☐ LAN
☐ WAN

Interface: LAN

Starting IP address:

Ending IP address:

DHCP lease time:

 (seconds)

Interface: WAN

Starting IP address:

Ending IP address:

DHCP lease time:

 (seconds)

Apply settings

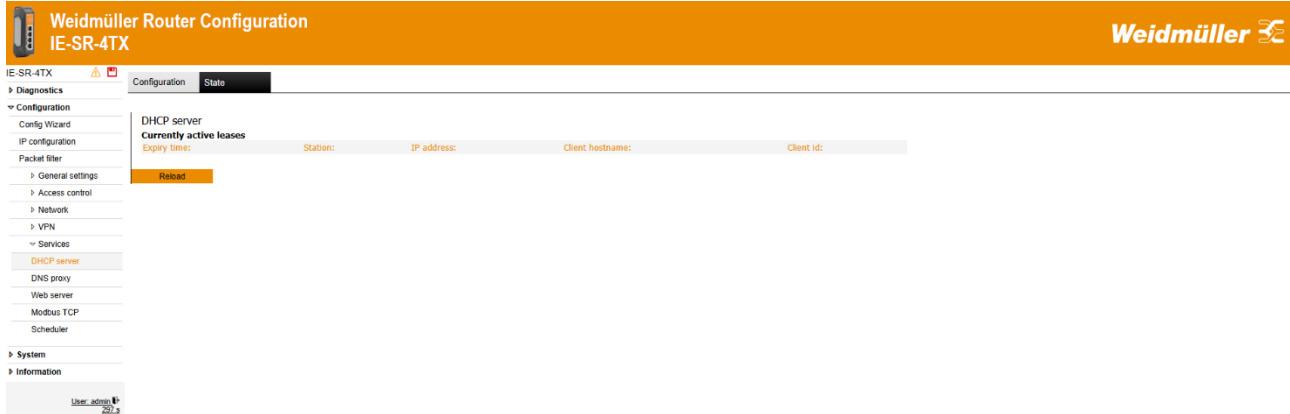
Reset changes

<b>Menu</b>	Configuration → Services → DHCP Server → Tab “Configuration”	
<b>Function</b>	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	<p>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.</p> <p><b>Note:</b> The IP address range must be in the same IP subnet as the IP of the selected interface itself.</p>
	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. 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

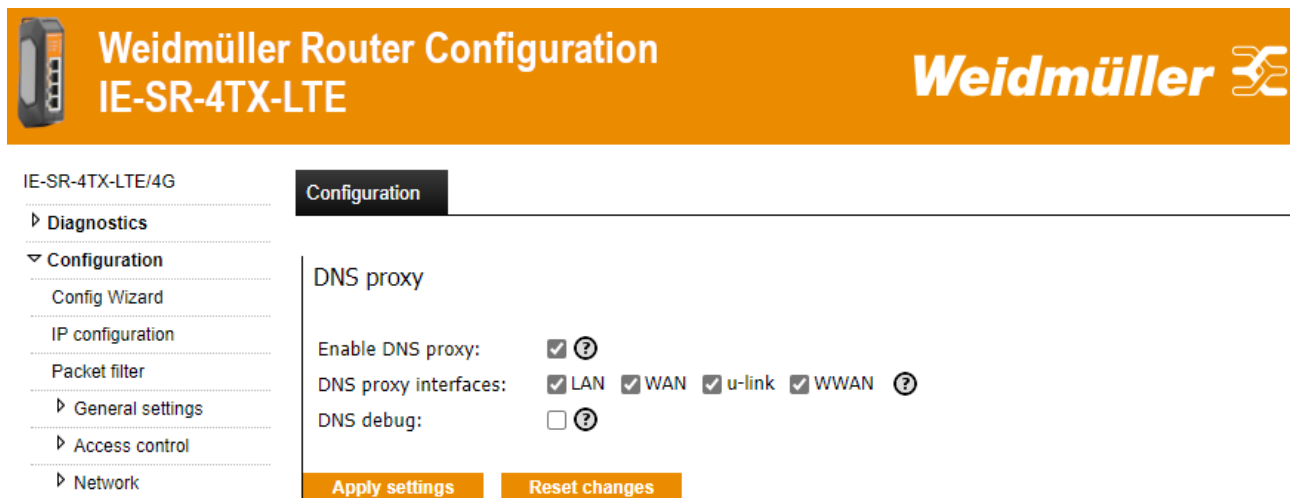
## Services → DHCP Server (Tab State)



The screenshot shows the Weidmüller Router Configuration interface for the IE-SR-4TX model. The 'DHCP server' section is active, and the 'State' tab is selected. It displays 'Currently active leases' with columns for Expiry time, Station, IP address, Client hostname, and Client id. A 'Reload' button is visible. The left sidebar shows the navigation menu with 'DHCP server' highlighted under the 'Services' section.

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

## Services → DNS proxy




The screenshot shows the Weidmüller Router Configuration interface for the IE-SR-4TX-LTE/4G model. The 'DNS proxy' configuration page is displayed under the 'Configuration' tab. It includes options to 'Enable DNS proxy' (checked), 'DNS proxy interfaces' (LAN, WAN, u-link, WWAN all checked), and 'DNS debug' (unchecked). 'Apply settings' and 'Reset changes' buttons are at the bottom. The left sidebar shows the navigation menu with 'DNS proxy' highlighted under the 'Services' section.

<b>Menu</b>	Configuration → Services → DNS proxy
<b>Function</b>	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



Weidmüller Router Configuration  
IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G  

Configuration

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▸ Access control

▸ Network

▸ VPN

▼ Services

DHCP server

DNS proxy

Web server


SNMP

Modbus TCP

Scheduler

▸ System

▸ Information

Logout:  251 s

Web server

HTTPS web server certificate:

Authentication certificate: 

identity.pem ▾

Apply settings


Reset changes

Menu	Configuration → Services → Web server
Function	Via this menu item the authentication certificate for the HTTPS web server can be configured.

Services → SNMP



Weidmüller Router Configuration  
IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

Configuration

▸ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▸ General settings

▸ Access control

▸ Network

▸ VPN

▼ Services

DHCP server

DNS proxy

Web server

SNMP

Modbus TCP

Scheduler

▸ System

▸ Information

User: admin

SNMP

Enable SNMP: ☐ ⓘ

SNMPv1/v2: ☐ ⓘ

SNMPv3: ☐ ⓘ

SNMP read only access:

Community Name:  ⓘ

Community IP:  ⓘ

Community network mask:  ⓘ

SNMP read/write access:

Community Name:  ⓘ

Community IP:  ⓘ

Community network mask:  ⓘ

SNMPv3 username and encryption:

User name read only:  ⓘ

Password:  ⓘ

User name read/write:  ⓘ

Password:  ⓘ

SNMP protocol for authentication: 

SHA ▾

Pre-shared Key for encryption:  ⓘ 

Generate PSK

SNMP traps:

Enable SNMP Trap Generation: ☐ ⓘ

SNMP Trap Community Name:  ⓘ

SNMP Trap Receiver IP:  ⓘ

Apply settings

Reset changes

Menu	Configuration → Services → SNMP
Function	Activation / deactivation of the SNMP protocol (Simple Network Management Protocol). Versions v1/v2/v3 are supported. Router data can be requested using Standard MIB-II.



	SNMPv1/v2	Use SNMPv1 or SNMPv2 protocol specifications. This protocol version is not encrypted and thus regarded as insecure
	SNMPv3	Use the SNMPv3 protocol. You must enter additional usernames and passwords in the fields below. SNMPv3 is regarded as secure.
	SNMP read or read/write access	You can decide whether the access with SNMP protocol should be “read only” or read and write. For pure diagnostics, the read-only option is recommended. You can also create two different accesses.
	Community name	The SNMP community name is used for authentication purposes like a password. Most devices use the strings public (read only) and private (read write) by default.
	Community IP	Restricted access with the given community name to the following IP-Address. Use 0.0.0.0 for any source.
	Community network mask	Network mask for the IP given above. Use 32 for a single host or 24 for a classic class C network.
	User name	SNMPv3 only: Username for SNMPv3. More than 4 alphanumerical characters are required.
	Password	SNMPv3 only: Password for SNMPv3. Authentication Protocol: MD5. More than 8 alphanumerical characters are required.
	SNMP protocol for authentication	Protocols like SHA and MD5 used to authenticate the SNMP connection.
	Pre-shared Key for encryption	SNMPv3 Pre-shared key for encryption. Privacy protocol AES
	Enable SNMP Trap generation	Activate the SNMP trap generation subsystem.
	SNMP Trap Community Name	SNMP trap community name for general trap identification
	SNMP Trap Receiver IP	IP address of the server where the SNMP trap will be send to

## Services → Modbus TCP



# Weidmüller Router Configuration

## IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

▶ Diagnostics

▼ Configuration

Config Wizard

IP configuration

Packet filter

▶ General settings

▶ Access control

▶ Network

▶ VPN

▼ Services

DHCP server

DNS proxy

Configuration

Modbus TCP

Enable Modbus TCP server: ☐ ?

Server port: 502 ?

IP address filter:  ?

Password: 0x  ?

Confirm password: 0x 

Verbose logging: ☐ ?

Apply settings

Reset changes

Menu

Configuration → Services → Modbus TCP



<b>Function</b>	Modbus TCP allows to control various aspects of the device via Modbus TCP, i.e. VPN connections.	
	Server port	Specify the port used by the server to listen for requests. The default Modbus port is 502.
	IP address filter	Restricts the IP addresses that can connect to the Modbus server. No filter means any IP Address can connect to the server.
	Password	An eight digit long hexadecimal password (e.g. 0x1a2b3c4d) can be specified to restrict user access.
	Verbose logging	By default only access violations like wrong password or restricted IP address connections are logged. Enabling this also logs information about connections, requests and processing times.

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 overflowing, 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)

For 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
	<p>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.</p> <p>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.</p> <p>The actual status of the corresponding service must be queried from its status register.</p>

## 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	<b>OpenVPN-1</b> is activated (Enabled)
		2	Connected	<b>OpenVPN-1</b> 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 <b>OpenVPN-1</b> connection
		0x0001		Activate defined <b>OpenVPN-1</b> connection

<b>OpenVPN-2:</b>	0x15 (Status)	Read-Only	→ see OpenVPN-1
	0x25 (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-3</b>	0x16 (Status)	Read-Only	→ see OpenVPN-1
	0x26 (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-4</b>	0x17 (Status)	Read-Only	→ see OpenVPN-1
	0x27 (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-5</b>	0x18 (Status)	Read-Only	→ see OpenVPN-1
	0x28 (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-6</b>	0x19 (Status)	Read-Only	→ see OpenVPN-1
	0x29 (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-7</b>	0x1A (Status)	Read-Only	→ see OpenVPN-1
	0x2A (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-8</b>	0x1B (Status)	Read-Only	→ see OpenVPN-1
	0x2B (Set)	Read / Write	→ see OpenVPN-1
<b>OpenVPN-9</b>	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	<b>u-link instance</b> is activated (Enabled)
		2	Connected	<b>u-link VPN</b> 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 <b>u-link VPN</b> tunnel
		0x0001		Establish <b>u-link VPN</b> tunnel



## Services → Scheduler



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-4TX-LTE/4G  
 ▸ Diagnostics  
 ▾ Configuration  
   Config Wizard  
   IP configuration  
   Packet filter  
   ▸ General settings  
   ▸ Access control  
   ▸ Network  
   ▸ VPN  
   ▾ Services  
     DHCP server  
     DNS proxy  
     Web server  
     SNMP  
     Modbus TCP  
     **Scheduler**

Configuration

Scheduler
No data available in table


minute Ⓢ	hour Ⓢ	day of month Ⓢ	month Ⓢ	day of week Ⓢ	action Ⓢ
+					

Apply settings
Reset changes


<b>Menu</b>	Configuration → Services → Scheduler
<b>Function</b>	Allows to schedule a regular reboot of the device.

## Services → SMS Service

**Important note:** The SMS Service function is only available for the “IE-SR-4TX-LTE/4G-USEMEA” router (2739630000) or with firmware version 1.6.7 or newer and with hardware revision number “AQ” for the “IE-SR-4TX-LTE/4G-EU” router (2751280000).



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE-USEMEA**



IE-SR-4TX-LTE/4G-USEMEA  
 ▸ Diagnostics  
 ▾ Configuration  
   Config Wizard  
   IP configuration  
   Packet filter  
   ▸ General settings  
   ▸ Access control  
   ▸ Network  
   ▸ VPN  
   ▾ Services  
     DHCP server  
     Web server  
     SNMP  
     Modbus TCP  
     Scheduler  
     **SMS Service**

Configuration

SMS Service

Enable SMS service: ☐ Ⓢ

Password SMS Control:  Ⓢ  
 Mobile Number 1:  Ⓢ  
 Mobile Number 2:   
 Mobile Number 3:

Allowed SMS Control functions  
 Enable SMS Control: ☐ Ⓢ

Reboot: ☐ Ⓢ  
 Establish/Cancel mobile network connection: ☐ Ⓢ  
 Establish/Cancel VPN connection: ☐ Ⓢ  
 Set digital output Alarm on/off: ☐ Ⓢ

Enable SMS Traps: ☐ Ⓢ

Send SMS after power up/reboot: ☐ Ⓢ  
 Send SMS if connected to mobile network: ☐ Ⓢ  
 Send SMS after disconnection from mobile network: ☐ Ⓢ  
 Send SMS after change of VPN connection (On-/Offline): ☐ Ⓢ  
 Send this message when digital input (Cut) changes to "On": ☐  Ⓢ  
 Send this message when digital input (Cut) changes to "Off": ☐  Ⓢ  
 Send this message when digital output (Alarm) changes to "On": ☐  Ⓢ  
 Send this message when digital output (Alarm) changes to "Off": ☐  Ⓢ

Apply settings
Reset changes




<b>Menu</b>	Configuration → Services → SMS Service	
<b>Function</b>	Enables or disables generally the use of text messages for control functions (SMS input) and sending information (SMS output). Only available for the US variant!	
	Password SMS Control	<p>If a password is entered, then each incoming SMS must include the password and the command. Otherwise, the message will be dropped. The password always starts with a “#” and ends with a “?”. Example password: #password? Example command: #password? reboot</p>
	Mobile number	<p>Only defined 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 number has to be configured using international format: +xxx yyyyyyyy</p>
	Enable SMS Control	Allows or denies the use of text messages for control functions (SMS input)
	Reboot	<p>Allows or denies a device reboot via SMS command. Command format with password: #password? reboot Command format without password: reboot</p>
	Establish/Cancel mobile network connection	<p>Allows/denies to establish/cancel the Internet connection of the mobile interface via SMS command. Command format with password: #password? MobileConnection=on/off Command format without password: MobileConnection = on/off</p>
	Establish/Cancel VPN connection	<p>Allows/denies to establish/cancel a predefined VPN (OpenVPN, IP-Sec, u-link) connection via SMS command. Command format with password: #password? u-linkVPN = on/off Command format without password: OpenVPN1 = on/off</p>
	Enable SMS traps	Enables/disables the sending of SMS traps to the defined mobile numbers 1-3.
	Send SMS (reboot, mobile network, VPN change)	Sends a predefined text SMS notification to the defined mobile numbers 1-3 if any of the events is triggered.
	Send this message when digital input (Cut) changes to on/off	If enabled a self defined text message will be sent to the mobile numbers 1-3 after the changing of digital input to on/off.




### 4.3 Section System

#### 4.3.1 System → Backup settings



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

System

Diagnostics

Configuration

System

Backup settings

Software update

Factory defaults

Save

Reboot

Information

User: admin

System

Backup settings


Manually save the system settings

Backup the current system settings of the device to a file on your local machine with "Download settings".

Restore the device settings

Backup file: 


Choose File

 No file chosen 

Download settings

Restore 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.


	<div>Note</div> <div>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.</div>
---	---

Version 1.8 /August 2025


Page 86 / 134





#### 4.3.2 System → Software update




## Weidmüller Router Configuration IE-SR-4TX-LTE




IE-SR-4TX-LTE/4G  

System
WWAN

Diagnostics
Configuration
System
Backup settings
Software update
Factory defaults
Save
Reboot
Information


Logout:  220 s

### Software update


**Installed firmware versions:** 

Running image: 2.0.10 B-174437  
Fallback image: 1.6.9 B-163587


---

**Online available firmware:**  
Look for software update online  


---


**Firmware hochladen:** 

No file chosen

**Update via a server:** 

Update protocol  

Server address  

Filename and location  


---

Menu	System → Software update	
Function	<p>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.</p> <p>With this action the Running image will become the Fallback image and the Fallback image will be deleted.</p> <p><b>The easiest way to update the Router with a new firmware is to use the function „Update by browser upload“.</b></p>	
	Online available firm-ware	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.



	Specify update from firmware server	<p>Update the device with a firmware from a remote HTTP/FTP/TFTP server.</p> <p>Update protocol: Protocol of the remote server which will serve the firmware file. FTP is only supported by using anonymous user. You can choose between HTTP, FTP and TFTP.</p> <p>Server address: HTTP/FTP/TFTP server address. Valid values are hostnames and IP addresses optionally combined with a port number i.e. 192.168.0.1:8080 or <a href="http://ftp.fw-server.net">ftp.fw-server.net</a>.</p> <p>Filename and location: Filename of the firmware file including the path on the remote server i.e. updates/firmware-1.0.0.bin</p> <p>Note: There must be no leading / on HTTP</p>
	Select file for browser update	<p>Update the device with a firmware by using a browser file upload. The firmware will be transmitted from the connected service PC to the router by browse accessible folders.</p>
	Set the factory defaults of the new firmware	<p>Additionally, it can be determined whether the router should be reset to factory default settings after the firmware update. If not set, then the Router will use current configuration after firmware update.</p>

## System → Software Update (Tab WWAN)



IE-SR-4TX-LTE/4G

- Diagnostics
- Configuration
- ▼ System
  - Backup settings
  - Software update
  - Factory defaults
  - Save
  - Reboot
- Information

User: admin

System WWAN

WWAN modem firmware update

Modem Vendor: GOSUNCN  
Model: ME3630  
Revision: ME3630E1CV1.0B12


Choose File No file chosen

Update

<b>Menu</b>	System → Software update → WWAN
<b>Function</b>	<p>Allows to update the modem firmware of the router only.</p> <p><b>Note: Only update in coordination with Weidmüller support! Do not attempt to update with non-authorized Weidmüller firmware!</b></p>




4.3.3 System → Factory defaults



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

System

Factory defaults

**Warning:**

Resetting the device to its factory default configuration will cause all changes that have been made to the unit to be permanently lost. The unit will reboot once this function is executed.

Reset to factory defaults

▸ Diagnostics

▸ Configuration

▼ System

Backup settings

Software update

Factory defaults

Save

Reboot

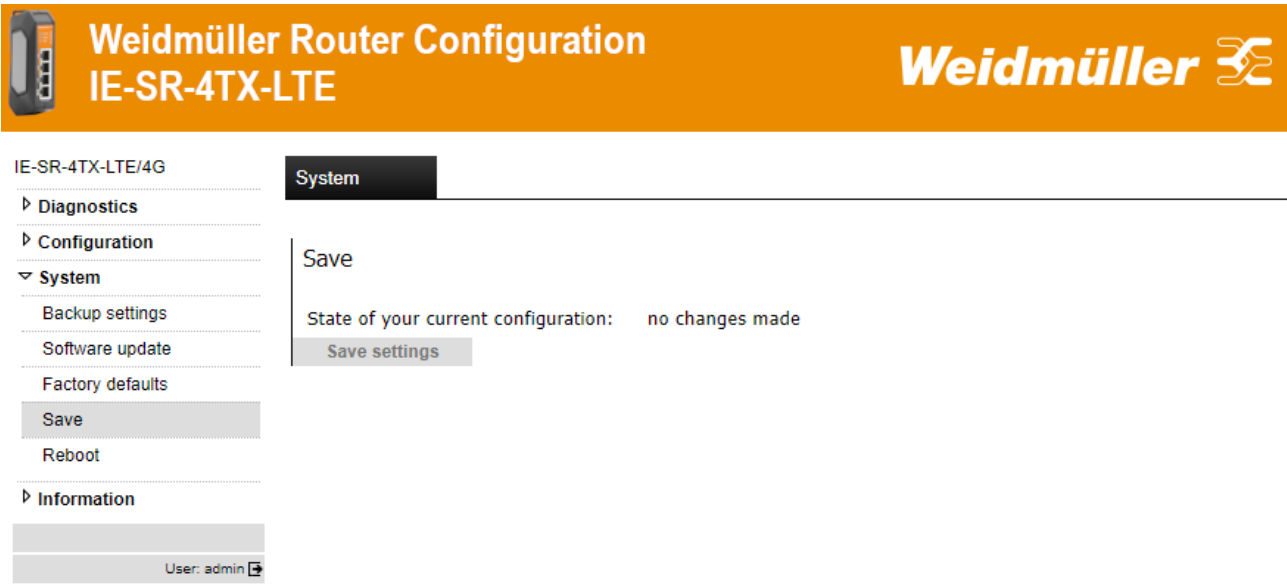
▸ Information

User: admin

Menu	System → Factory default
Function	<div>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.</div> <div><u>Basic factory settings:</u></div> <div><div>IP address LAN port(s):192.168.1.110</div><div>IP address WAN port (2-Port models):192.168.2.110</div><div>IP address WAN ports (6-Port models):DHCP</div><div>User name:admin</div><div>Password:Detmold</div></div>




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**



Weidmüller  
IE-SR-4TX

IE-SR-6GT-LAN

▸ Diagnostics


▾ Configuration

  IP configuration

  SecureNow!

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



IE-SR-4TX-LTE/4G

▸ Diagnostics

▸ Configuration

▾ **System**

  Backup settings

  Software update

  Factory defaults

  Save

**Reboot**

▸ Information

User: admin

**System**

Reboot

**Configuration state:**  
State of your current configuration: no changes made

**Additional reboot parameter:**

Waiting time in minutes:  ?

Boot alternative firmware image:  ?


**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



Weidmüller Router Configuration

IE-SR-4TX-LTE

Weidmüller 

IE-SR-4TX-LTE/4G

▸ Diagnostics


▸ Configuration

▸ System

▼ Information

General

Sitemap

User: admin 

Information

Vendor

Weidmüller Interface GmbH & Co. KG

AddressKlingenbergstraße 26, D-32758 Detmold, Germany

Phone+49 5231 14-0

Internetwww.weidmueller.com

Device information

TypeIE-SR-4TX-LTE

Firmware version1.6.4 (Build: SVN-R52274.B-157902)

Hardware versionDVG-IRF1421-201-AA-AD.00

Serial-No.AX20131010

MAC addressWAN00:18:92:07:D6:3F

MAC addressLAN2A:18:92:07:D6:3F

User defined

Name of deviceIE-SR-4TX-LTE/4G-AX20131010


Physical location

Contact

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




## 4.4.2 Information → Sitemap



### Weidmüller Router Configuration

#### IE-SR-4TX-LTE



IE-SR-4TX-LTE/4G

- Diagnostics
- Configuration
- System
- ▼ Information
  - General
  - Sitemap

User: admin

Information


### Sitemap

- 📁 Diagnostics
  - 📄 System State
  - 📄 Eventlog
  - 📄 WAN
  - 📄 LAN
  - 📄 WWAN
  - 📄 Ping test
  - 📄 Remote capture
  - 📄 Download
- 📁 Configuration
  - 📄 Config Wizard
  - 📄 IP configuration
  - 📄 Packet filter
  - 📁 General settings
    - 📄 System data
    - 📄 Date & time
    - 📄 User interface
    - 📄 Certificates
    - 📄 SCEP
  - 📁 Access control
    - 📄 User accounts
    - 📄 Permissions
    - 📄 Web access
  - 📁 Network
    - 📄 DNS
    - 📄 IP routing
    - 📄 HTTP Proxy
    - 📄 Forwarding
    - 📄 1:1 NAT
    - 📄 Network groups
    - 📄 Hardware groups
    - 📄 Ethernet

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





4.4.2 Information → License Information



Weidmüller Router Configuration

IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G  

▸ Diagnostics

▸ Configuration


▸ System

▼ Information

General

Sitemap

License Information

Logout:  222 s

License Information

License Information


This product contains software based on the following listed open source software given by name version and license. You can order a DVD free of charge containing all used open source code and its modifications by us as far as required by each of the dedicated licenses under the following address:

Weidmüller GmbH & Co. KG  
Klingenbergstraße 26  
32758 Detmold

Component	Version	License
arptables	0.0.5	<a href="#">GPL-2.0</a>
base-files	-	<a href="#">GPL-2.0</a>
util-linux	2.38	<a href="#">GPL-2.0</a>
fstools	2021-01-04	<a href="#">GPL-2.0</a>
bridge-utils	1.7	<a href="#">GPL-2.0+</a>
btrfs-progs	5.7	<a href="#">GPL-2.0</a>
busybox	1.33.0	<a href="#">GPL-2.0</a>
ccid	1.4.33	<a href="#">LGPL-2.1+</a>
ppp	2.4.9	<a href="#">BSD-4-Clause</a>

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.

Logout:  216 s



## 5. Appendix A (Configuration examples)

### A1 – 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

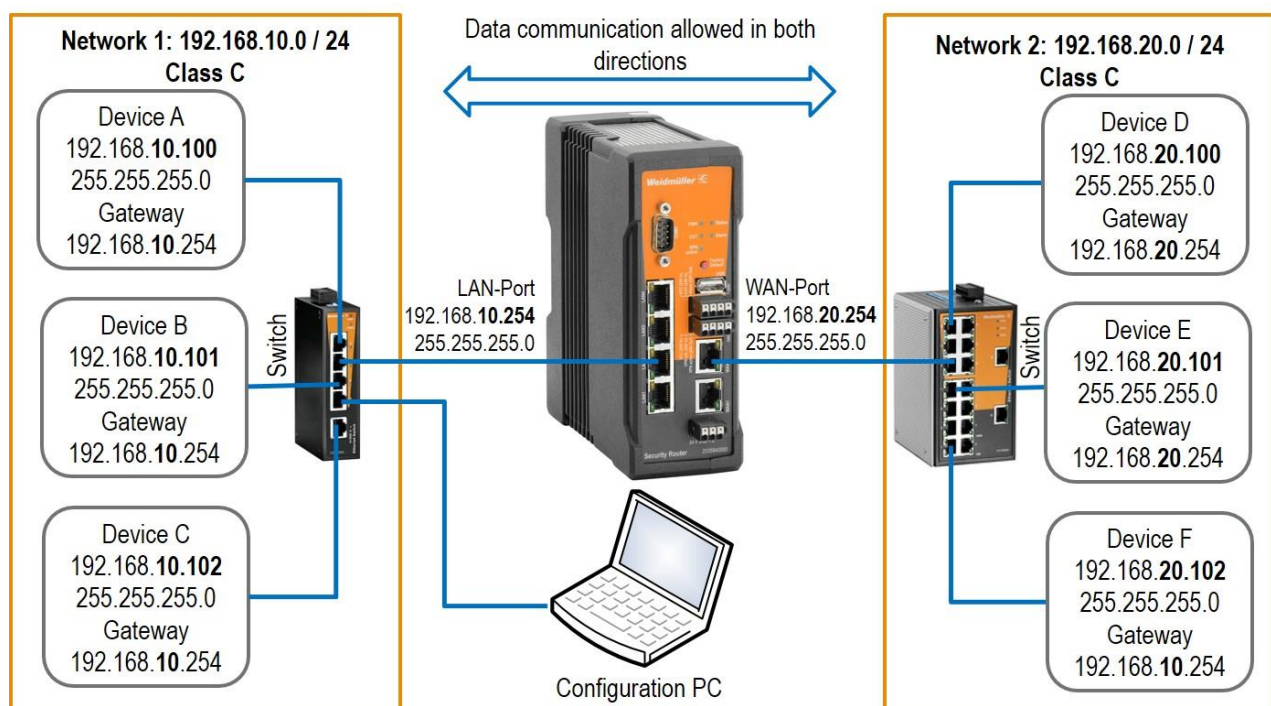
192.168.**20**.0 / 255.255.255.0 for Network 2

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 <b>WAN Port:</b>	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>NOT SET</b>
IP address parameters <b>LAN Port:</b>	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>NOT SET</b>
Default gateway	Can be left blank because there exists no further target network



### Weidmüller Router Configuration

#### IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

- Diagnostics
- ▾ Configuration
  - Config Wizard
  - IP configuration
  - Packet filter
  - General settings
  - Access control
  - Network
  - VPN
  - Services
- System
- Information

User: admin

Configuration

**IP configuration**

**Operational mode:** IP router ⓘ

**WAN:**

IP assignment: static ⓘ

IP address: 192.168.20.254

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒ ⓘ

**LAN:**

IP assignment: static ⓘ

IP address: 192.168.10.254

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒ ⓘ

**WWAN:**

Dialmode: disabled ⓘ

**Default gateway:**

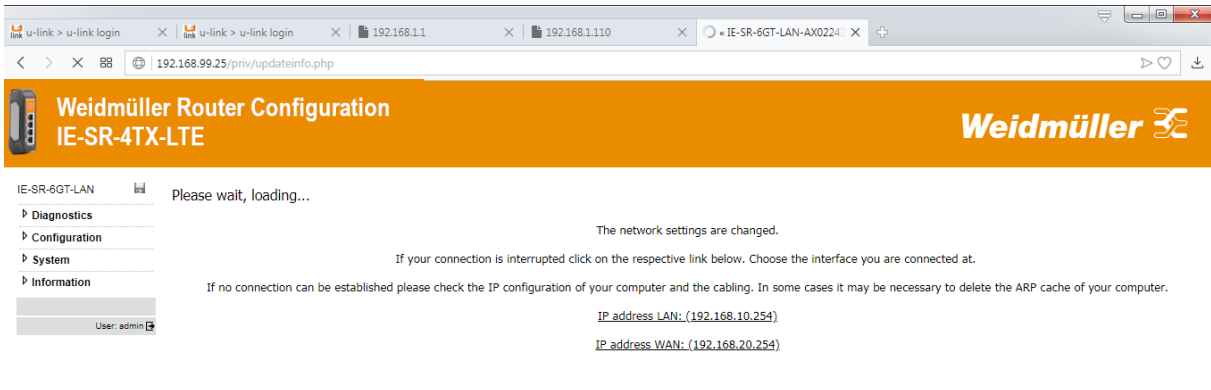
IP address:

Apply settings
Reset changes



- 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.



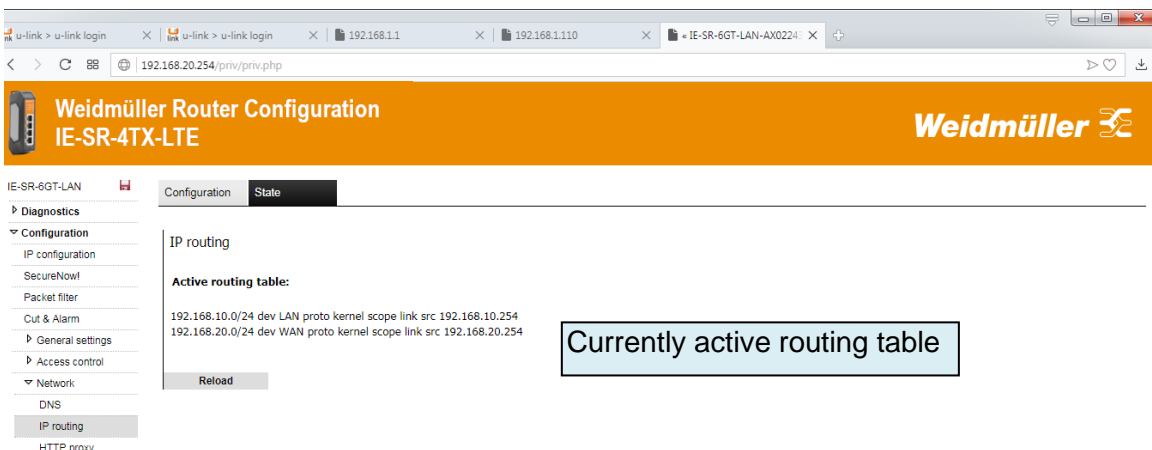
##### 5. Change the IP address of the configuration PC according to the connected network 192.168.10.0 / 24

- 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)



## A2 - 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

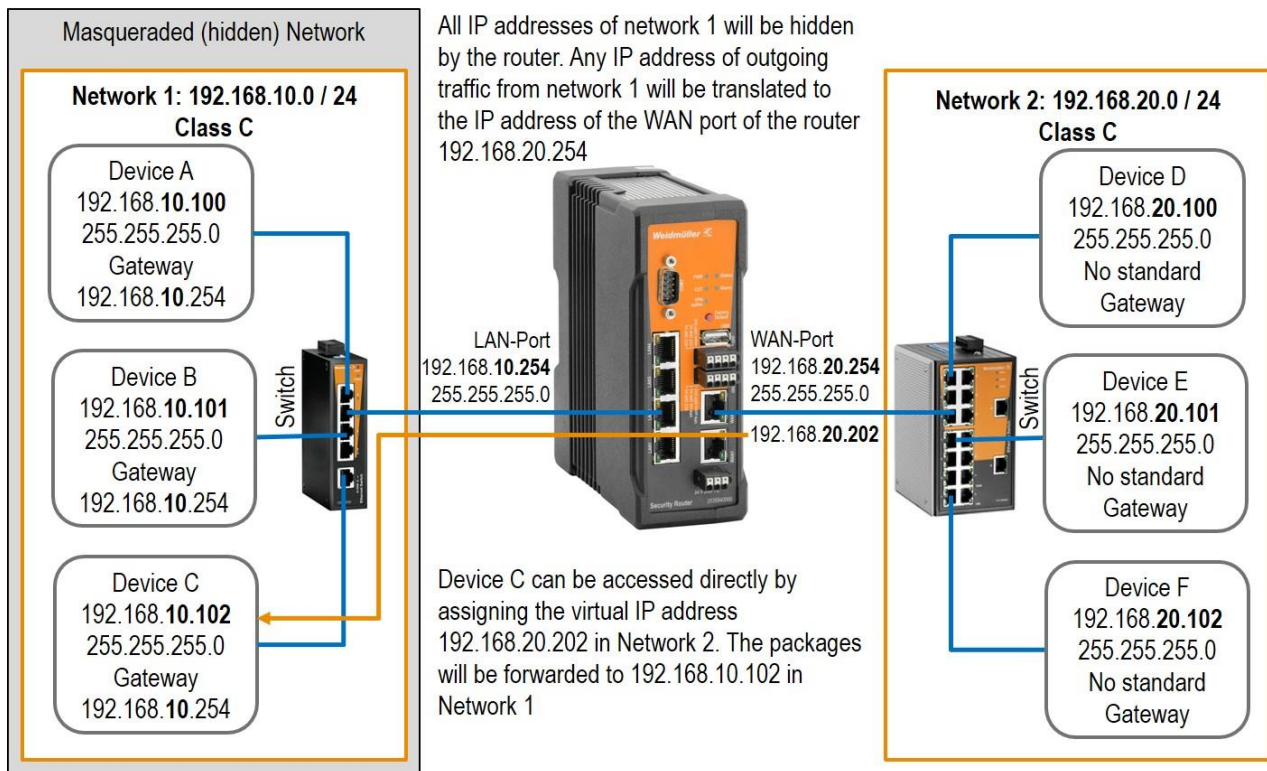
192.168.**10**.0 / 255.255.255.0 for network 1 and  
192.168.**20**.0 / 255.255.255.0 for network 2

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 <b>WAN</b> Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>SET</b>
IP address parameters <b>LAN</b> Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>NOT SET</b>
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**



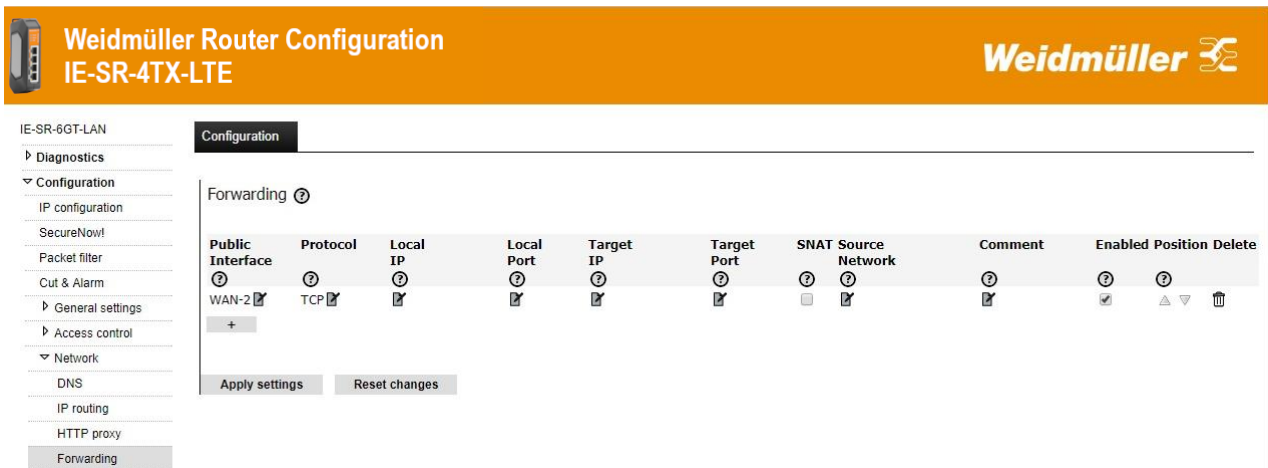



Figure 2: Empty IP forwarding table

- 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 3
  - Ensure that each input will be completed by clicking the icon .
- Now click button “Apply settings” to activate the “IP address forwarding table”

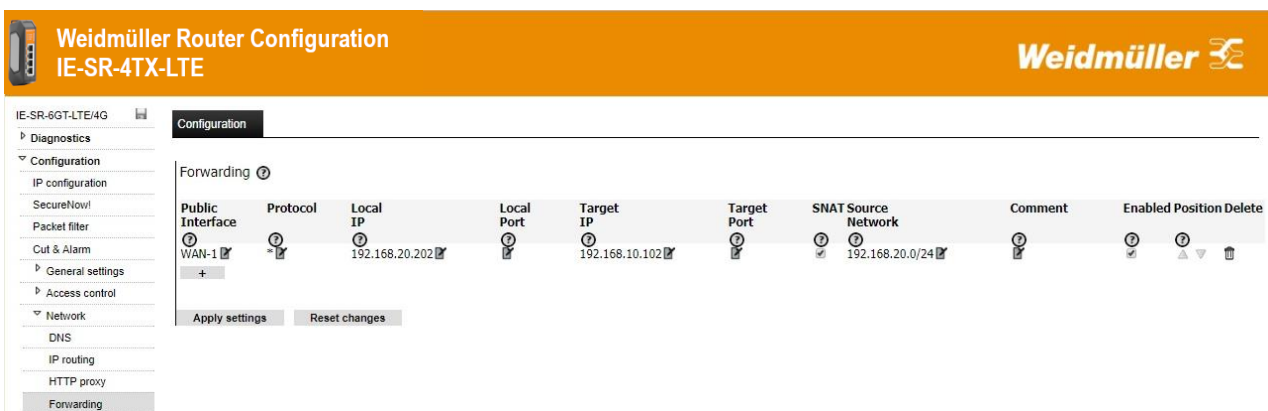


Figure 3: IP forwarding

**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



## A3 - 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

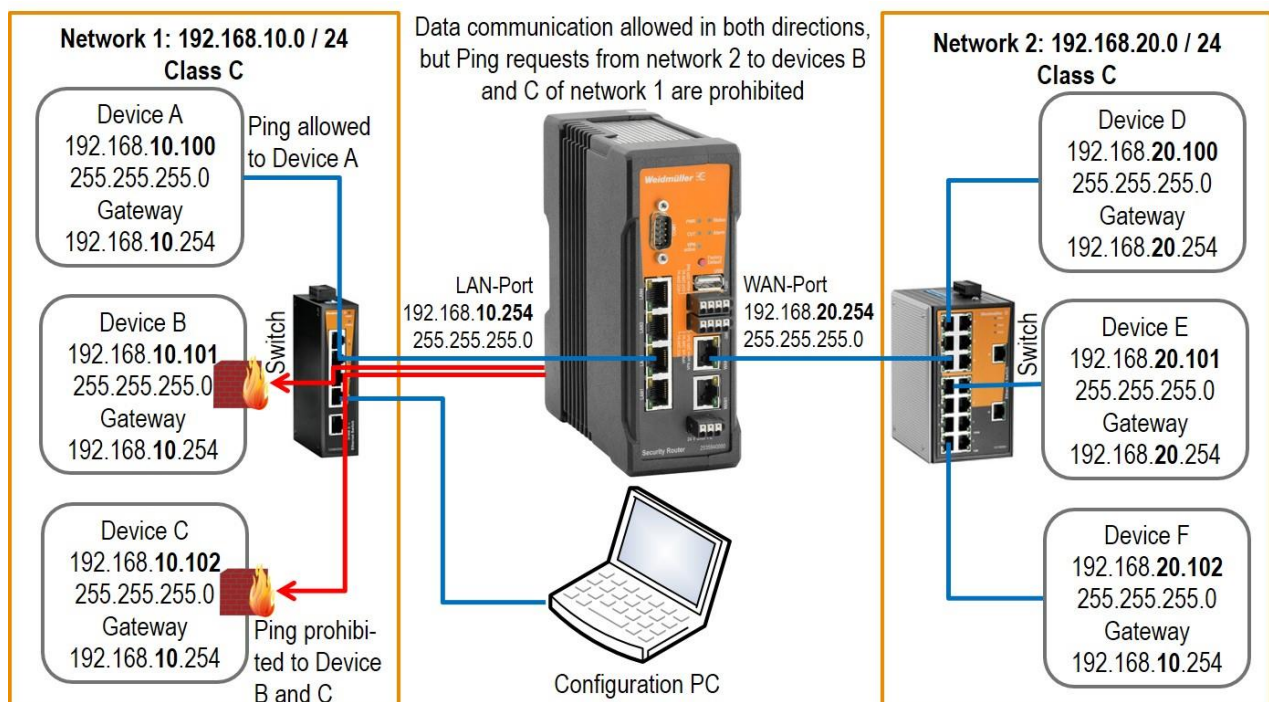
192.168.10.0 / 255.255.255.0 for Network 1 and

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 <b>WAN</b> Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>NOT SET</b>
IP address parameters <b>LAN</b> Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) <b>NOT SET</b>
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 applied 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

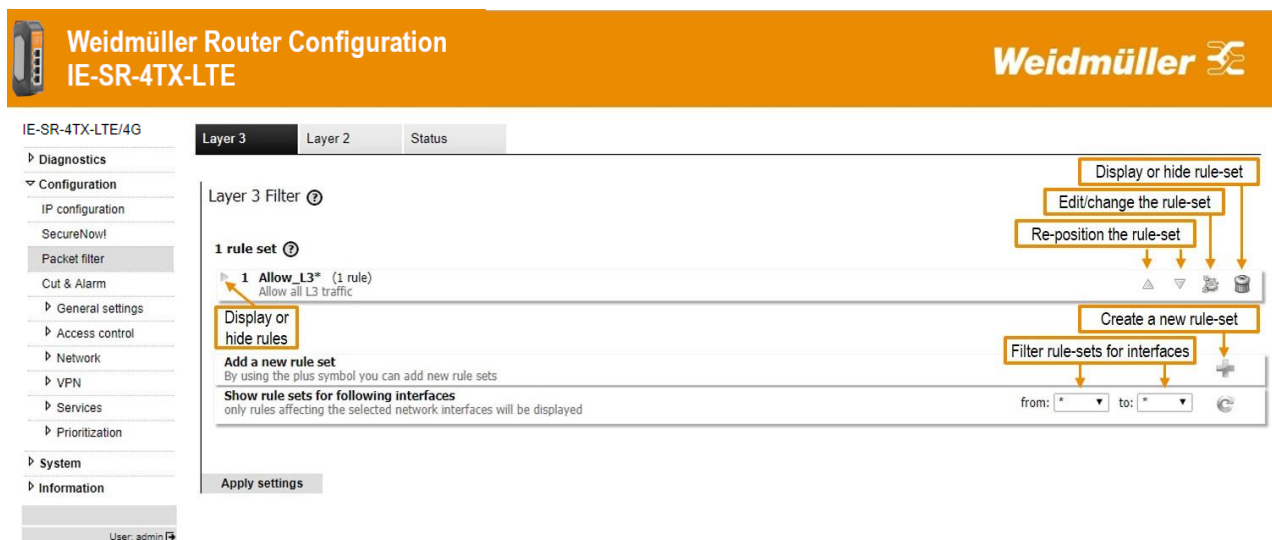


Figure 4: Packet filter

- 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 5)



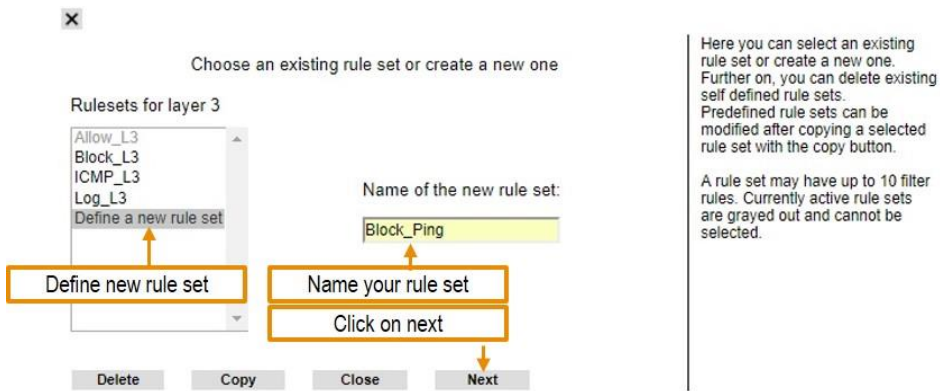


Figure 5: Create a new rule-set

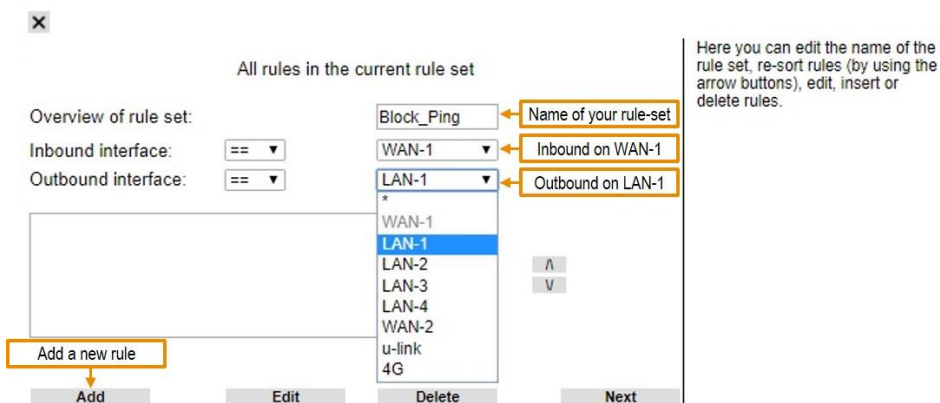


Figure 6: Define additional parameters of the new rule-set

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.

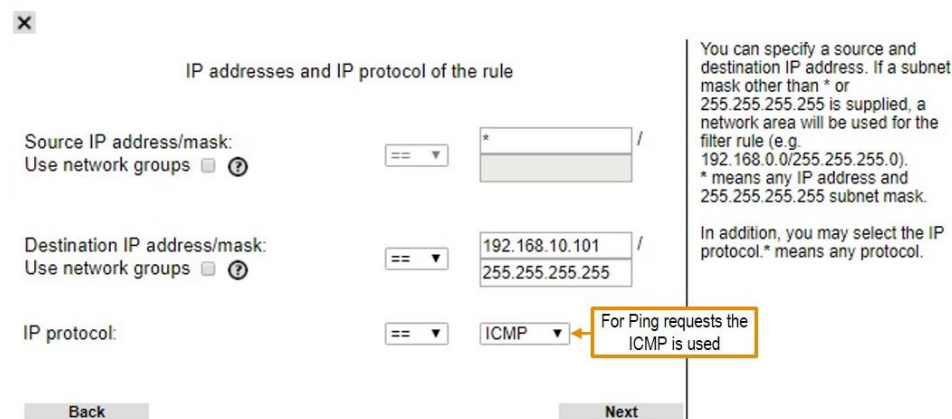


Figure 7: Define the first rule

The rule is valid for communication **from** source addresses that are == \*, which means all IP addresses, **to** == 192.168.10.1 with Subnet 255.255.255.255, which means this specific IP. You can also choose to set a rule for all IP addresses EXCEPT (!=) the given one.



IP protocol options of the rule

ICMP type:

Specify the type of ICMP rule. For Ping block you can also use „ping request“ in the drop-down menu

Connection control:

Stateful, Auto or Manual Connection control

Back Next

Here you can select the ICMP message type. The most common are "request" and "reply". They are necessary for the "ping" command to succeed. ICMP is essential for the functionality of an IP network. Any enables all ICMP messages.

Figure 8: Define additional parameters of the first rule

Check input/output signals for the rule

	Check signal	Signal high
CUT:	<input type="checkbox"/>	<input type="checkbox"/>
VPN KEY:	<input type="checkbox"/>	<input type="checkbox"/>
VPN UP:	<input type="checkbox"/>	<input type="checkbox"/>

Back Next

Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal. Mark the *Signal high* checkbox to match on a high voltage level or do not mark the *Signal high* checkbox to match an off signal without voltage.

Do not mark any signal if you like to ignore the signals.

Figure 9: 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.

Action and name of the rule

Action:

Reject reason:

Log: ☒

Alarm: ☐

Max. packets/s:

Rule name:

Name of the single rule

Back Next

**Action:**  
Tells how to handle a packet that passed all criteria.

**Allow:**  
The packet will be forwarded.

**Drop:**  
The packet will be silently discarded.

**Cut:**  
The network link will be cut at hardware level.

**Reject:**  
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

Additionally, a log entry could be generated or an alarm could be triggered

Define the answer which will be sent to the ping requester

Select if an log-entry in the packet filter status or alarm event should be triggered

Maximum number of packets per second that can pass even if they fulfill the rules

Figure 10: Action and name of the rule



✕

All rules in the current rule set

Overview of rule set:

Block\_Ping

Inbound interface:

== ▾

WAN-1 ▾

Outbound interface:

== ▾

LAN-1 ▾

BlkPingDevB

The new rule

⬆

⬆

⬇

Add

Edit

Delete

Next

Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

Figure 11: Creation of first rule completed

✕

Description of the rule set

This is the ruleset for Ping block

Back

Next

The rule set description be used for documentation only.

Figure 12: Description of the rule-set

✕

Activity of the rule set

Limit activity:

☐

From:

Until:

At:

Mon

Tue

Wed

Thu

Fri

Sat

Sun

☐

☐

☐

☐

☐

☐

☐

Back

OK

Here you may define whether the activity of the rule set should be restricted to a certain time window.

Starting and ending time must be in HH:MM format. You must also select the days of week on which the rule set is supposed to be active.

**Caution:** If you do not check at least one day the rule set will not be activated at all!

Figure 13: Time limitations on filter rule-sets

Set time and date limitations for the rule-set.



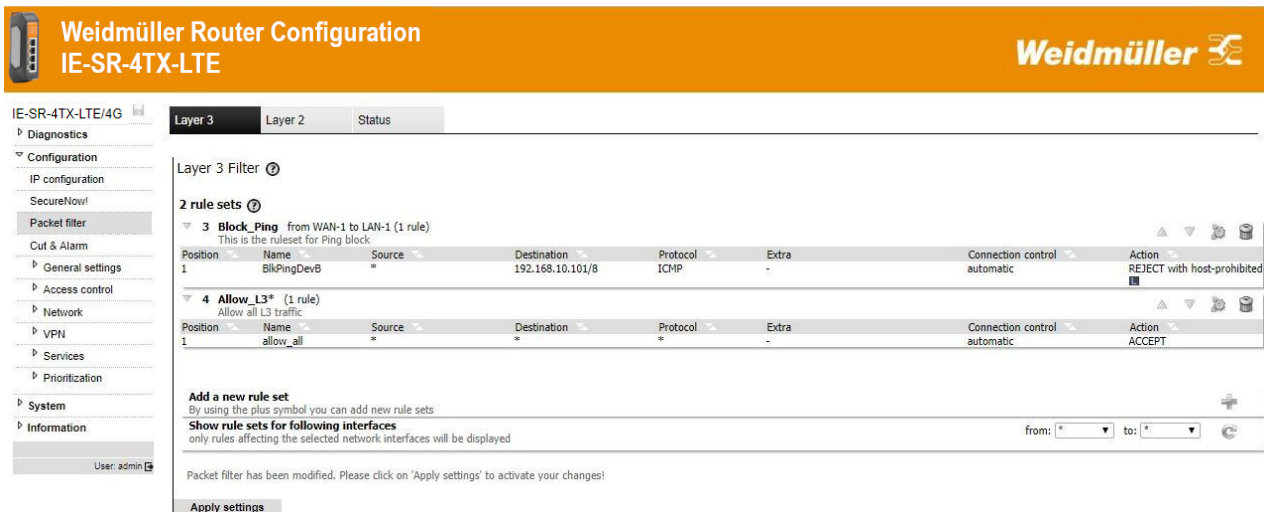


Figure 14: Overview of Packet filter rules

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”.

	<b>Note</b>
	<ol style="list-style-type: none"> <li>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.</li> <li>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)</li> </ol>



## A4 – 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.

Example network topology: Switched network with IP address range 192.168.99.0/ 255.255.255.0

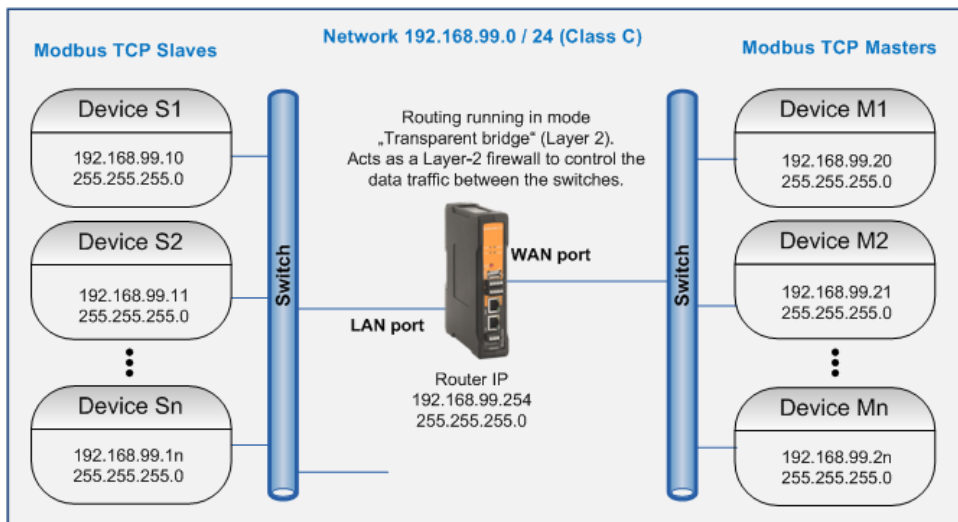


Figure 15: Example network topology

### 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 16: Display of initial web page after login (Menu System state)



## A5-1 Configuration of initial parameters

► Goto menu Configuration → IP configuration

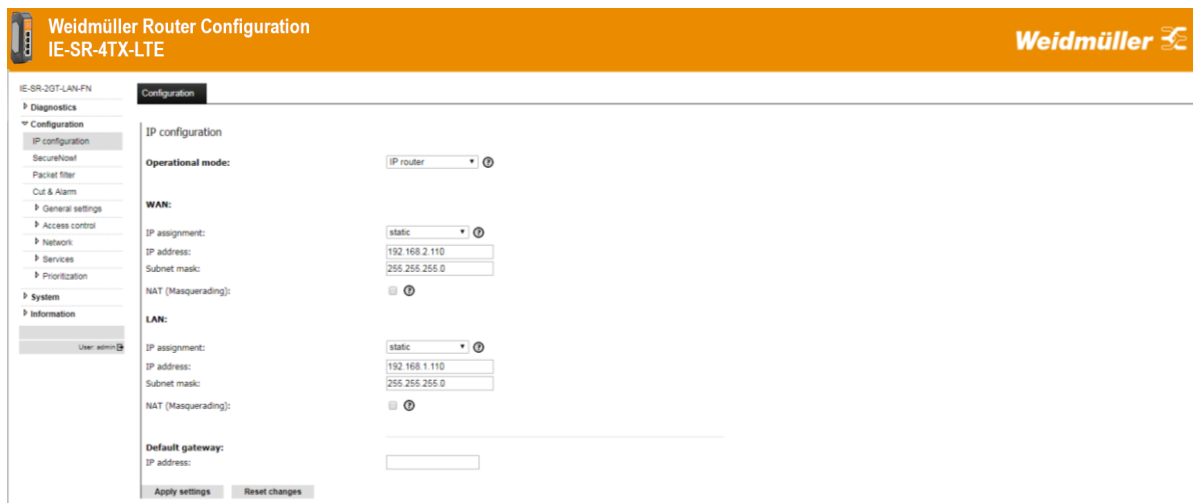


Figure 17: IP configuration factory defaults

- 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”

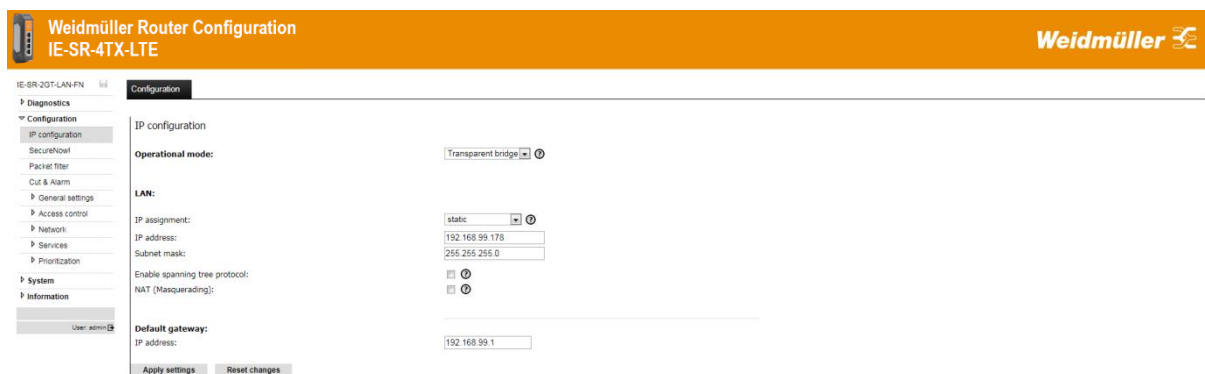
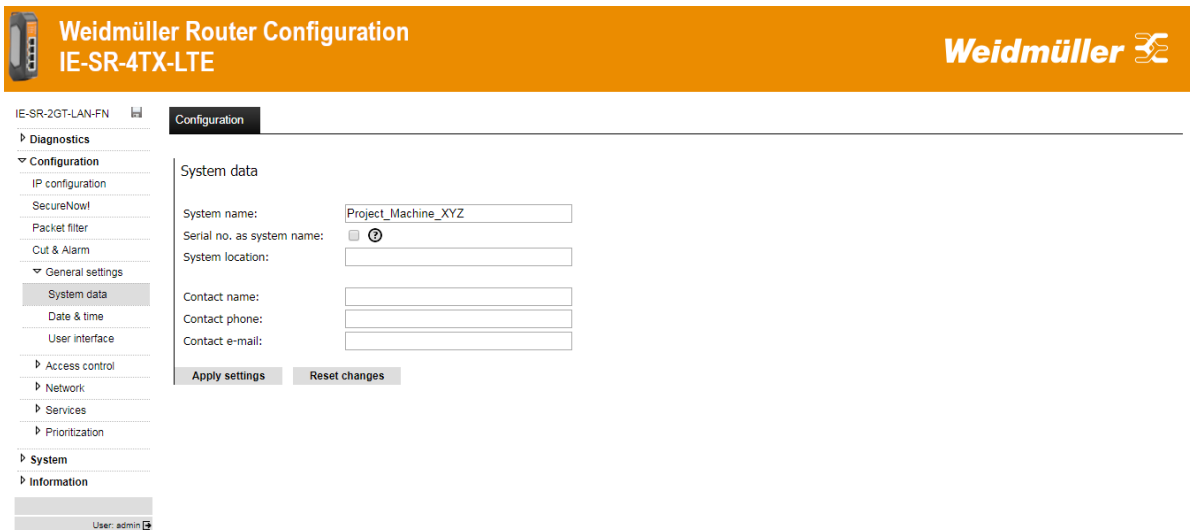


Figure 18: New IP configuration running as “Transparent bridge” (Layer 2)

### 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”.






**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Configuration**

System data

System name:

Serial no. as system name: ☐ 

System location:

Contact name:

Contact phone:

Contact e-mail:


User: admin 

Figure 19: 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".



**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Configuration** **State**

DNS

Hostname:  

Serial no. as hostname: ☒ 

Domain name (search suffix):  

1st DNS server:  

2nd DNS server:

3rd DNS server:

Register hostname at DHCP server: ☒ 

Use all servers concurrently: ☐ 

Enable DNS proxy: ☒ 


DNS proxy interfaces: ☒ LAN ☒ WAN


Figure 20: First DNS server (or DNS server relay) is 192.168.99.1

### Configuration of date / time settings (Optional step)

- ▶ Go to 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".




**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Weidmüller** 

IE-SR-2GT-LAN-FN

Diagnostics

Configuration

IP configuration

SecureNow!

Packet filter

Cut & Alarm

General settings

System data

Date & time

User interface

Access control

Network

Services

Prioritization

System

Information

User: admin

Configuration

State

### Date & time

Date & time: Fri Jun 15 10:28:29 CEST 2018

Time zone: Region: Europe City: Berlin

Enable timeserver synchronization (NTP): ☒ ⓘ

Primary NTP server: pool.ntp.org

Secondary NTP server: de.pool.ntp.org

Tertiary NTP server: ptbtime1.ptb.de

Enable NTP time server relay: ☐

Manual setting of date & time :


Date (day/month/year): 15 / 06 / 2018


Time (hour/minute/second): 10 / 28 / 29

Apply settings
Reset changes

Figure 21: Date & Time settings

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


**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**

**Weidmüller** 

IE-SR-2GT-LAN-FN

Diagnostics

Configuration

IP configuration

SecureNow!

Packet filter

Cut & Alarm

General settings

System data

Date & time

User interface

Access control

Network

Services

Prioritization

System

Information

User: admin

Configuration

State

### NTP Server Statistics

Server IP	Reference ID	Stratum	Type	Age of last response (s)	Polling Interval (s)	Success - Failure count	Roundtrip Time (ms)	Offset (ms)	Jitter (ms)
94.130.231.116	131.168.3.220	2	u	4	64	1	43.043	21.523	0.061
*85.214.58.202	124.216.164.14	2	u	6	64	1	25.257	19.852	0.061
192.53.103.108	PTB	1	u	6	64	1	38.539	26.428	0.061

Reload

Figure 22: Tab “State” – showing NTP server statistics



## A4-2 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).

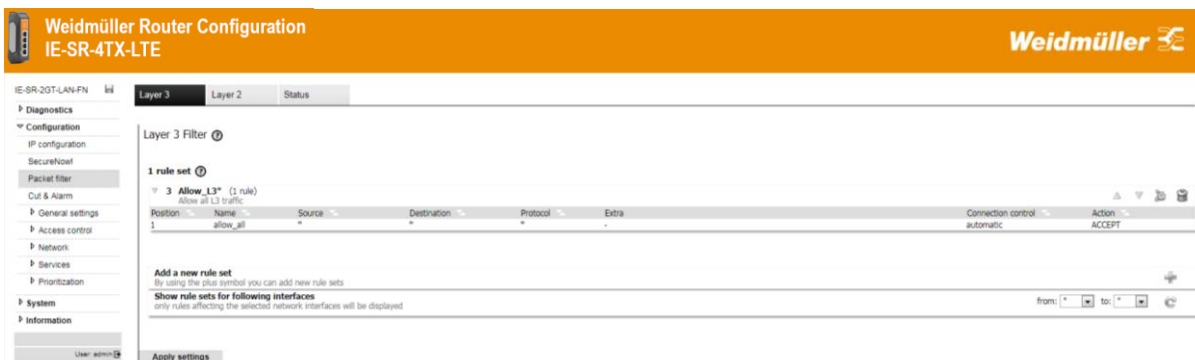


Figure 23: Factory default settings of Layer-3 Packet filter (firewall), valid for operation mode “IP Router”

#### 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).

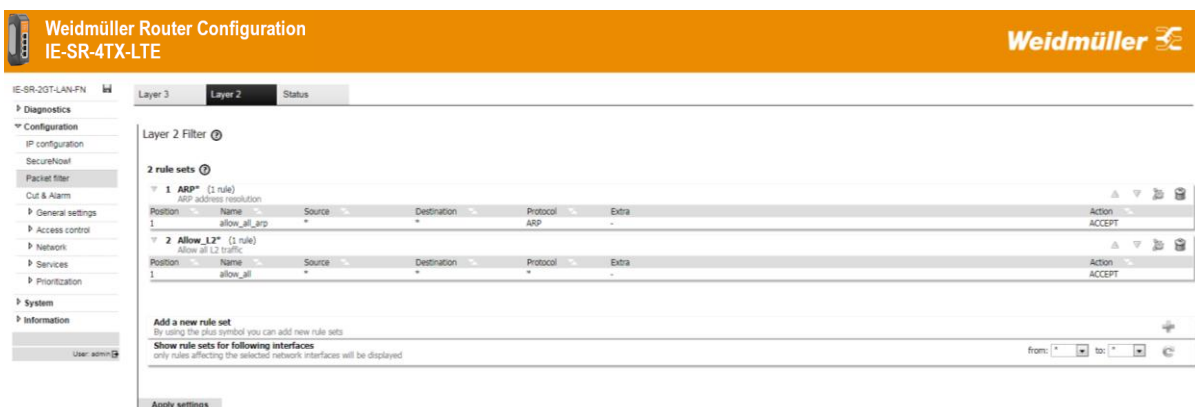


Figure 24: Factory default settings of Layer-2 Packet filter (firewall), valid for operation mode “Transparent bridge”



## 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.

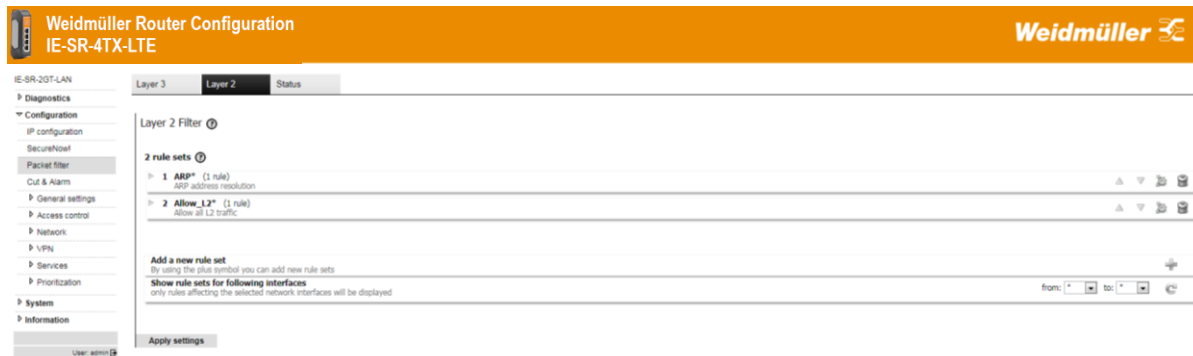
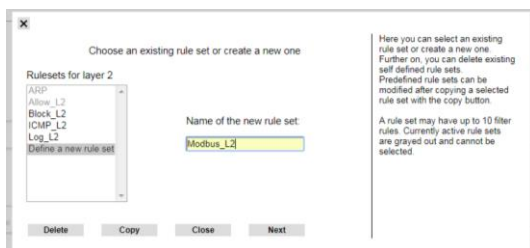
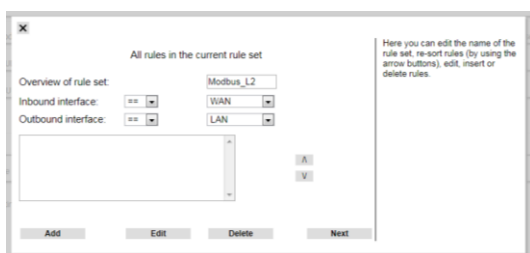


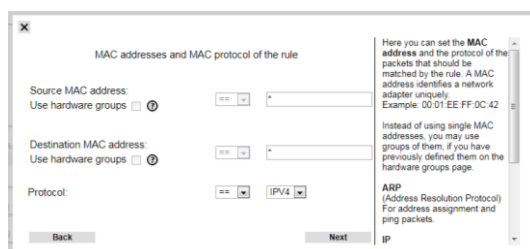
Figure 25: Factory default settings of Layer-2 Packet filter (firewall)



- Add a name for new rule-set (here Modbus\_L2).
- Click ‘Next’.

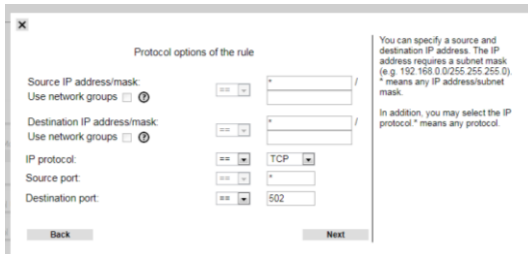


- Select Inbound interface (here WAN) and outbound interface (here LAN).
- Click Add to add a new rule inside of this rule-set named Modbus\_L2.



- Enter wild character \* for source and destination MAC addresses
- Select protocol IPv4 to be checked inside of the Ethernet frame.
- Click ‘Next’.





Protocol options of the rule

You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). \* means any IP address/subnet mask.

In addition, you may select the IP protocol. \* means any protocol.

Source IP address/mask:  /

Use network groups: ☐

Destination IP address/mask:  /

Use network groups: ☐

IP protocol:  TCP

Source port:  \*

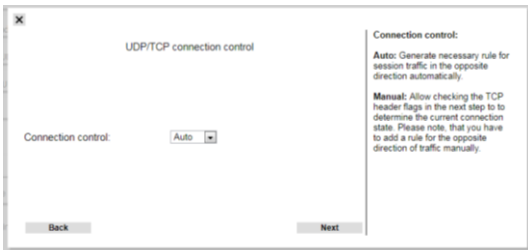
Destination port:  502

Back 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'.



UDP/TCP connection control

Connection control:  Auto

Back Next

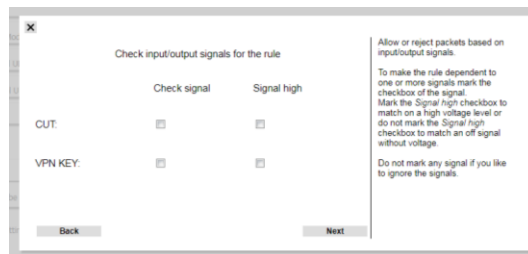
Connection control:

Auto: Generate necessary rule for session traffic in the opposite direction automatically.

Manual: Allow checking the TCP header flags in the next step to determine the current connection state. Please note that you have to add a rule for the opposite direction of traffic manually.

► 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'.



Check input/output signals for the rule

Check signal Signal high

CUT: ☐ ☐

VPN KEY: ☐ ☐

Back Next

Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal. Mark the Signal high checkbox to match on a high voltage level or do not mark the Signal high checkbox to match an off signal without voltage.

Do not mark any signal if you like to ignore the signals.

Additionally, a log entry could be generated or an alarm could be generated.

► No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action:  Allow

Reject reason:  net-unreachable

Log: ☐

Alarm: ☐

Max. packets/s:

Rule name:  Modbus\_Allow

Back Next

Action:

Tells how to handle a packet that passed all criteria.

Allow:

The packet will be forwarded.

Drop:

The packet will be silently discarded.

Cut:

The network link will be cut at hardware level.

Reject:

The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

Additionally, a log entry could be generated or an alarm could be generated.

► 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.



Description of the rule set

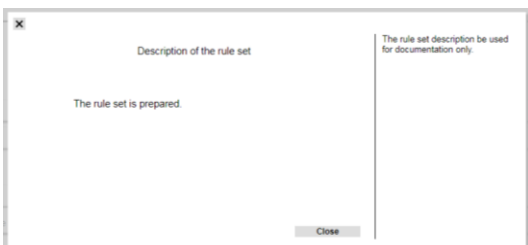
The rule set description be used for documentation only.

Allows any TCP traffic with destination port 502 ModbusTCP Incoming at WAN port. By setting Connection Control to AUTO the packet filter automatically recognizes and allows ModbusTCP responses incoming at LAN port.

Back Next

► Add a description text for this rule-set.

► Click 'Next'.



Description of the rule set

The rule set description be used for documentation only.

The rule set is prepared.

Close

► 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.

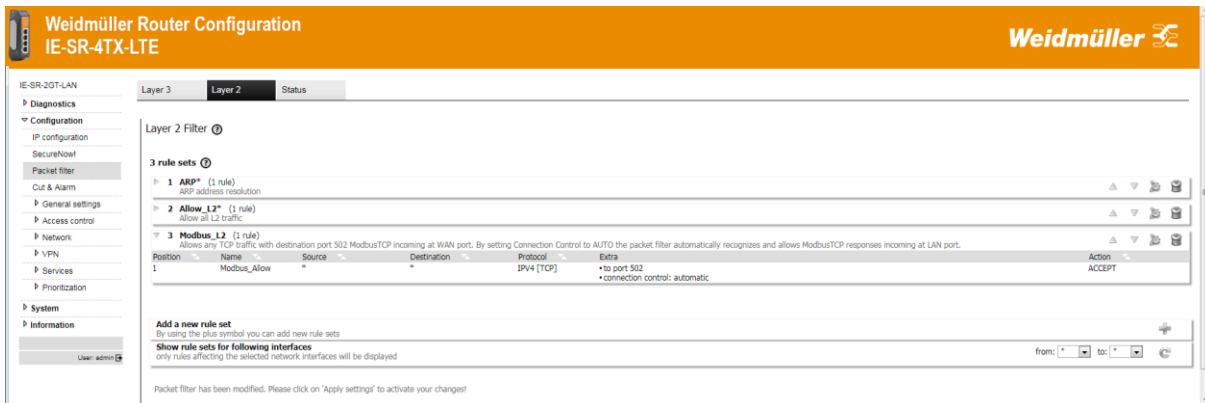
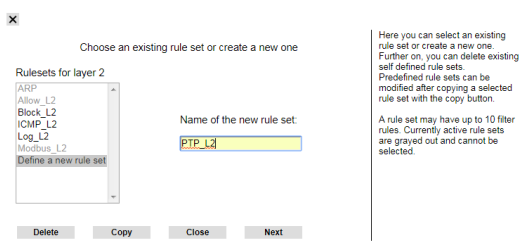


Figure 11: Layer-2 filter list containing new rule-set “Modbus\_L2”

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.

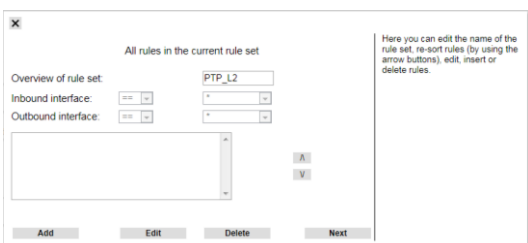
## 2.2 Configuration of a rule-set containing 2 rules which allow any PTP communication based on protocol UDP, ports 319 and 320, either initially incoming at WAN port or LAN port.

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



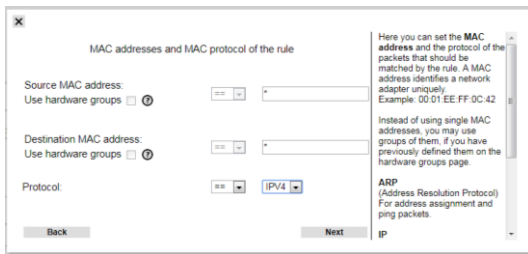
► Add a name for the new rule-set (here PTP\_L2).

► Click Next.



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





MAC addresses and MAC protocol of the rule

Source MAC address:  
Use hardware groups ☐  \*

Destination MAC address:  
Use hardware groups ☐  \*

Protocol:  
 IPv4

Back Next

Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely. Example: 00 01 EE FF 0C 42

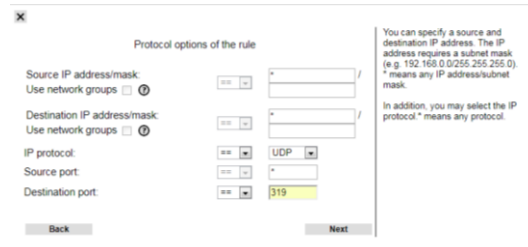
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

ARP (Address Resolution Protocol) For address assignment and ping packets.

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

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

► Click Next.



Protocol options of the rule

Source IP address/mask:  
Use network groups ☐  \*

Destination IP address/mask:  
Use network groups ☐  \*

IP protocol:  
 UDP

Source port:  
 \*

Destination port:  
 319

Back Next

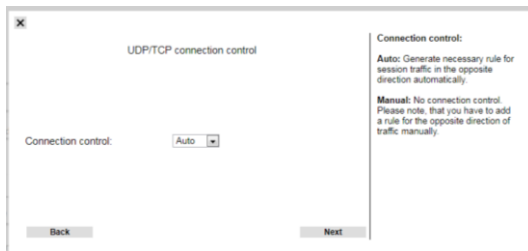
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). \* means any IP address/subnet mask.

In addition, you may select the IP protocol. \* means any protocol.

► 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'.



UDP/TCP connection control

Connection control:  
Auto

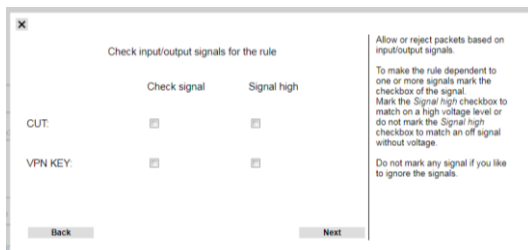
Back Next

Connection control:  
Auto: Generate necessary rule for session traffic in the opposite direction automatically.  
Manual: No connection control. Please note, that you have to add a rule for the opposite direction of traffic manually.

► 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'.



Check input/output signals for the rule

Check signal Signal high

CUT: ☐ ☐

VPN KEY: ☐ ☐

Back Next

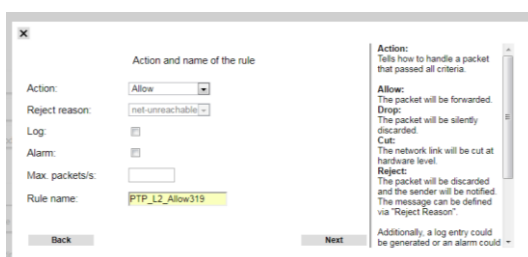
Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal. Mark the Signal/high checkbox to match on a high voltage level or do not mark the Signal/high checkbox to match an off signal without voltage.

Do not mark any signal if you like to ignore the signals.

► No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action:  
Allow

Reject reason:  
net-unreachable

Log:  
☐

Alarm:  
☐

Max. packets/s:

Rule name:  
PTP\_L2\_Allow319

Back Next

Action:  
Tells how to handle a packet that passed all criteria.

Allow:  
The packet will be forwarded.

Drop:  
The packet will be silently discarded.

Cut:  
The network link will be cut at hardware level.

Reject:  
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

Additionally, a log entry could be generated or an alarm could be triggered.

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

► Add a name for this rule (here PTP\_L2\_Allow319).

► Click 'Next'.



All rules in the current rule set

Overview of rule set:  
Inbound interface:  \*  
Outbound interface:  \*

PTP\_L2\_Allow319

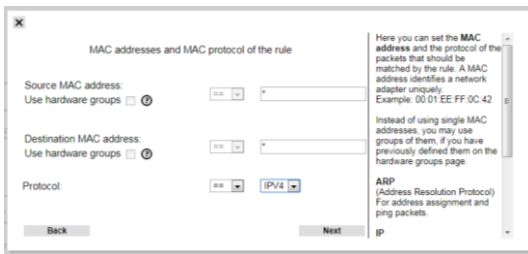
Add Edit Delete Next

Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

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.





MAC addresses and MAC protocol of the rule

Source MAC address:  
Use hardware groups ☐

Destination MAC address:  
Use hardware groups ☐

Protocol: IPv4

Back Next

Here you can set the MAC address and the protocol of the packets that should be matched by the rule. A MAC address identifies a network adapter uniquely. Example: 00:01:EE:FF:0C:42

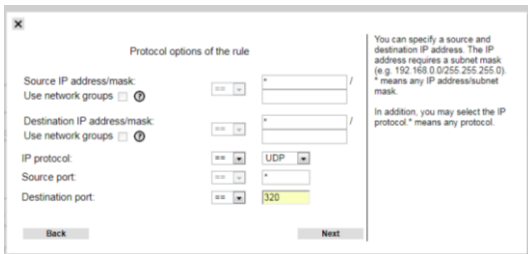
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

ARP (Address Resolution Protocol) For address assignment and ping packets.

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

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

► Click 'Next'.



Protocol options of the rule

Source IP address/mask:  
Use network groups ☐

Destination IP address/mask:  
Use network groups ☐

IP protocol: UDP

Source port:  
Destination port: 320

Back Next

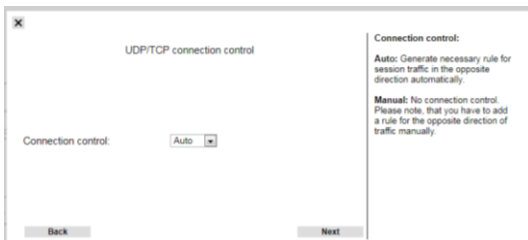
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). \* means any IP address/subnet mask.

In addition, you may select the IP protocol. \* means any protocol.

► 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'.



UDP/TCP connection control

Connection control: Auto

Back Next

Connection control:

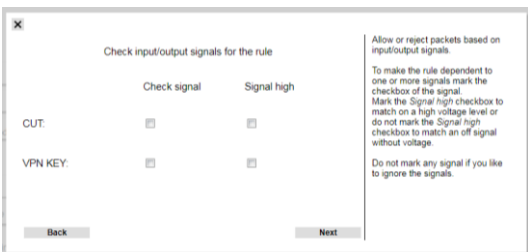
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

Manual: No connection control. Please note, that you have to add a rule for the opposite direction of traffic manually.

► 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'.



Check input/output signals for the rule

Check signal Signal high

CUT: ☐ ☐

VPN KEY: ☐ ☐

Back Next

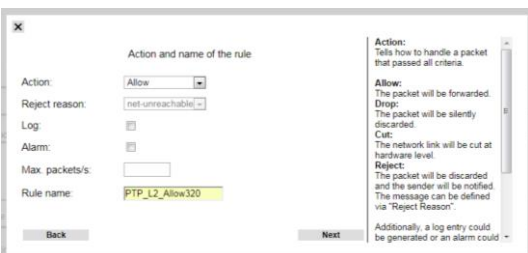
Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal. Mark the Signal high checkbox to match on a high voltage level or do not mark the Signal high checkbox to match on an off signal without voltage.

Do not mark any signal if you like to ignore the signals.

No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action: Allow

Reject reason: net-unreachable

Log: ☐

Alarm: ☐

Max. packets/s:

Rule name: PTP\_L2\_Allow320

Back Next

Action:

Tells how to handle a packet that passed all criteria.

Allow:

The packet will be forwarded.

Drop:

The packet will be silently discarded.

Cut:

The network link will be cut at hardware level.

Reject:

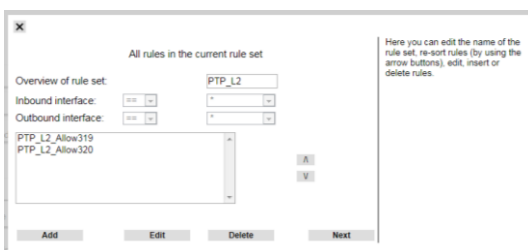
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

Additionally, a log entry could be generated or an alarm could be triggered.

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

► Add a name for this rule (here PTP\_L2\_Allow320).

► Click 'Next'.



All rules in the current rule set

Overview of rule set: PTP\_L2

Inbound interface: \*

Outbound interface: \*

PTP\_L2\_Allow319

PTP\_L2\_Allow320

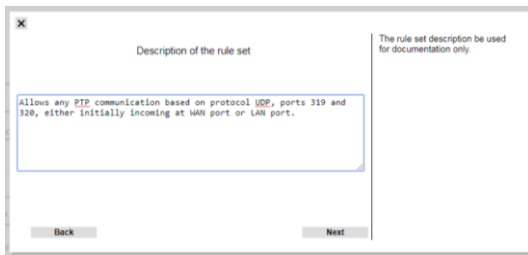
Add Edit Delete Next

Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

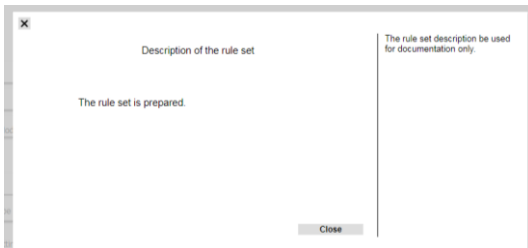
Now both necessary rules are configured.

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





- Enter the description text.
- Click 'Next'.



- The rule-set is prepared.
- Click 'Close'.

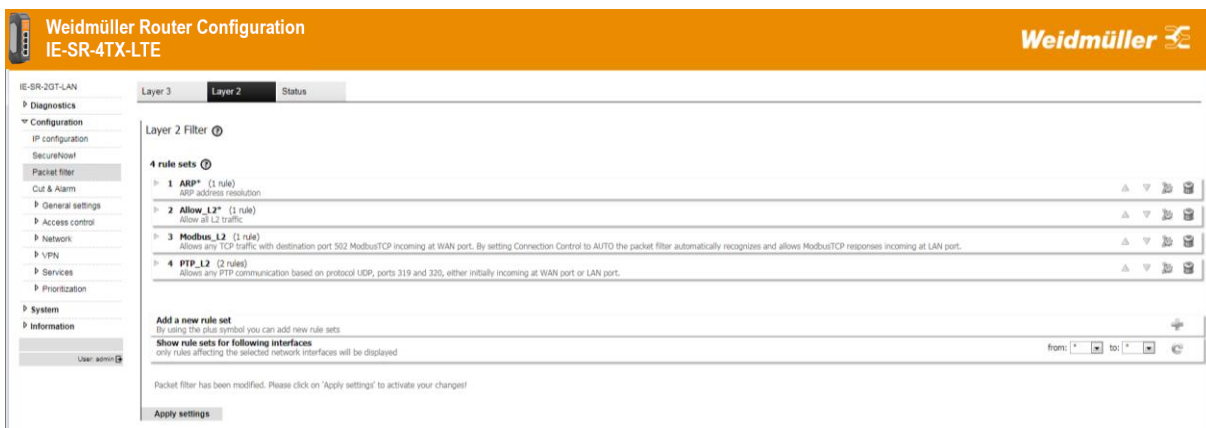
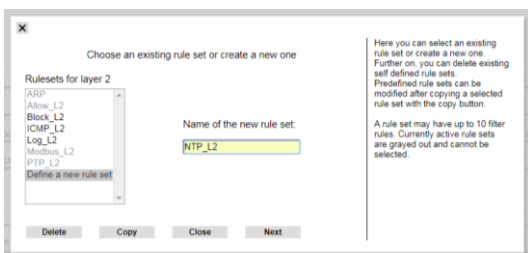


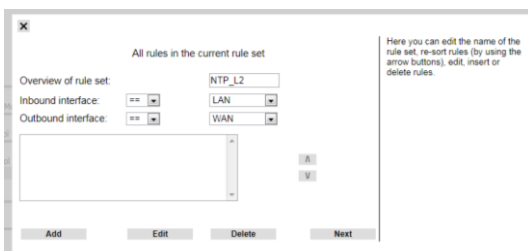
Figure 12: Layer-2 filter list containing new rule-set “PTP\_L2”

## 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.

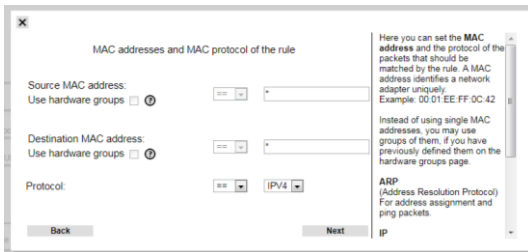


- Add a name for the new rule-set (here NTP\_L2).
- Click 'Next'.



- Select inbound and outbound interface.
- Click 'Add' to add a new rule.
- Click 'Next'.

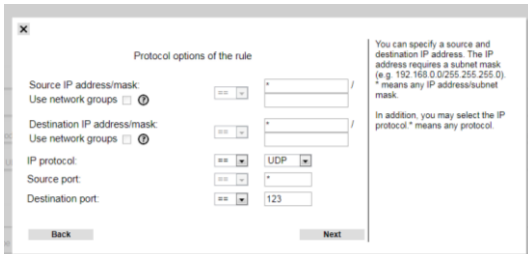




► Enter wild character \* for source and destination MAC addresses

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

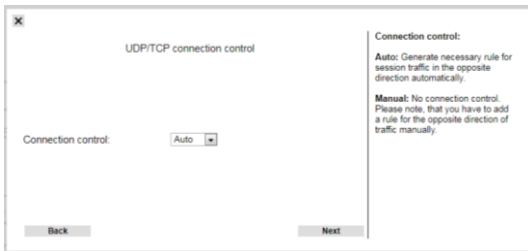
► Click 'Next'.



► 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).

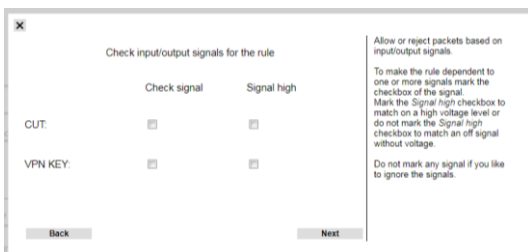
► Click 'Next'.



► Select auto for Connection control.

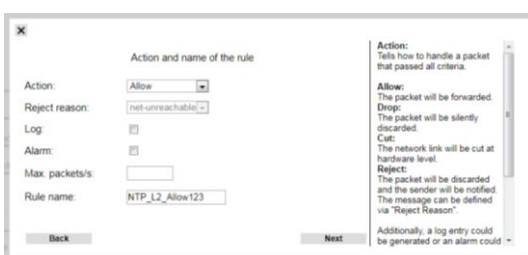
(Packet filter acts as an stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

► Click 'Next'.



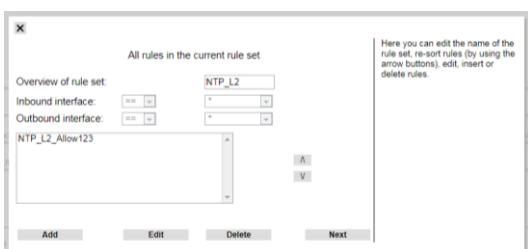
No signal check and setting.

► Click 'Next'.



► Select action (allow) related to the previous defined rules. ► Add a name for this rule (here NTP\_L2\_Allow123).

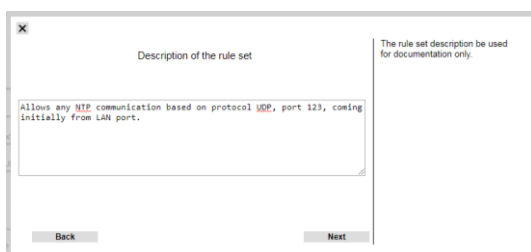
► Click 'Next'.



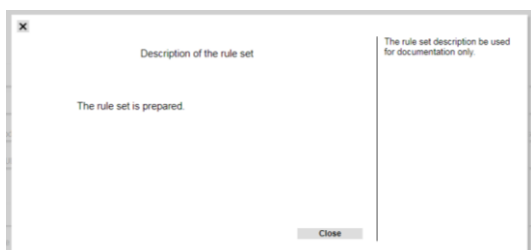
Now the necessary rule is configured.

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







- Enter the description text.
- Click 'Next'.



- Click 'Close'.


**Weidmüller Router Configuration**  
**IE-SR-4TX-LTE**



IE-SR-20T-LAN-FN

Layer 3
Layer 2
Status

► Diagnostics

▼ Configuration

  IP configuration

  SecureView

Packet filter

  Cut & Alarm

  General settings

  Access control

  Network


  Services

  Prioritization

► System

  Information

### Layer 2 Filter

5 rule sets 

Position	Name	Source	Destination	Protocol	Extra	Action	
1	allow_all_arp	*	*	ARP		ACCEPT	
1	allow_all	*	*	*		ACCEPT	
3	Modbus_L2 from WAN to LAN (1 rule)	Allows any TCP traffic with destination port 502 ModbusTCP incoming at WAN port. By setting Connection Control to AUTO the packet filter automatically recognizes and allows ModbusTCP responses incoming at LAN port.					
1	Modbus_Allow	*	*	IPv4 [TCP]	• to port 502 • connection control: automatic	ACCEPT	
4	PTP_L2 (2 rules)	Allows any PTP communication based on protocol UDP, ports 319 and 320, either initially incoming at WAN port or LAN port.					
1	PTP_L2_Allow319	*	*	IPv4 [UDP]	• to port 319 • connection control: automatic	ACCEPT	
2	PTP_L2_Allow320	*	*	IPv4 [UDP]	• to port 320 • connection control: automatic	ACCEPT	
5	NTP_L2 from LAN to WAN (1 rule)	Allows any NTP communication based on protocol UDP, port 123, coming initially from LAN port.					
1	NTP_L2_Allow123	*	*	IPv4 [UDP]	• to port 123 • connection control: automatic	ACCEPT	

**Add a new rule set**

By using the plus symbol you can add new rule sets

**Show rule sets for following interfaces**


only rules affecting the selected network interfaces will be displayed

from:

\*

to:

\*



Packet filter has been modified. Please click on 'Apply settings' to activate your changes!

Apply settings

Figure 26: 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.



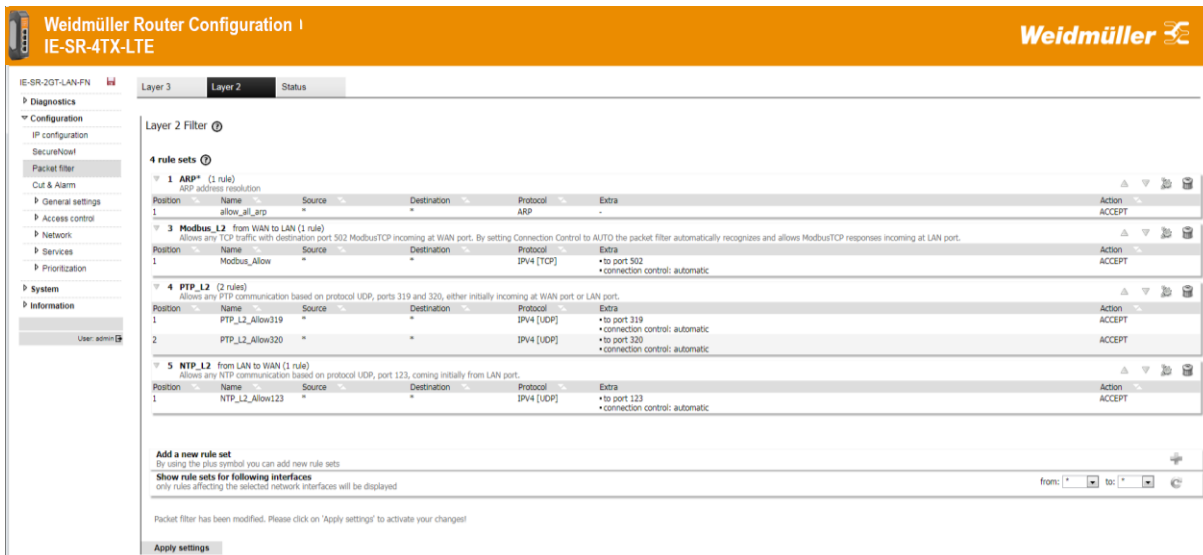
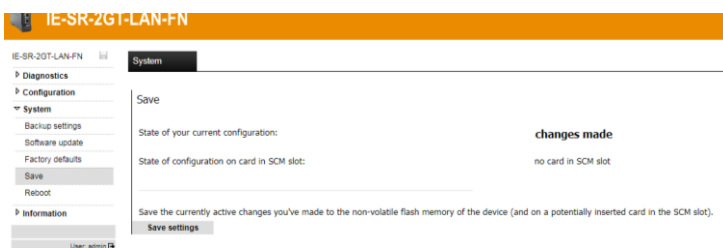


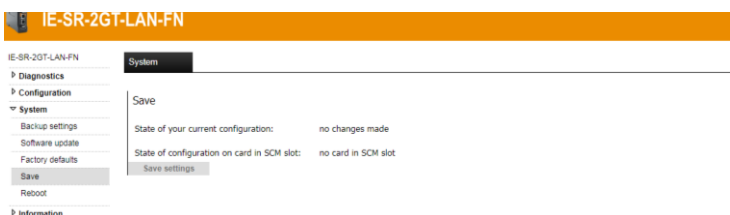
Figure 27: Final list of Layer-2 filter

**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).

### A4-3 Save the configuration

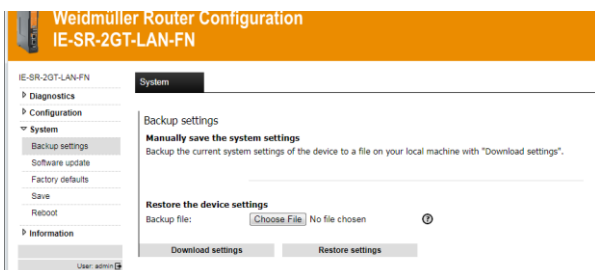


- Goto menu System → Save.
- Click ‘Save settings’.

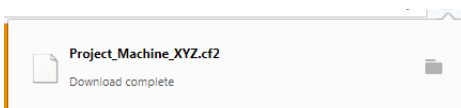


Now the settings are saved in the flush memory.

### 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 restoring select this file via button ‘Choose file’ and click button ‘Restore settings’.



## A5 - 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 Dynamic routing of the menu:**

→ **Configure the below described parameters for all Routers 1 and 2 and all used interfaces**

Interfaces Router 1: LAN 1, LAN 2, WAN, 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 <b>LAN/WAN</b> port (other Routers)

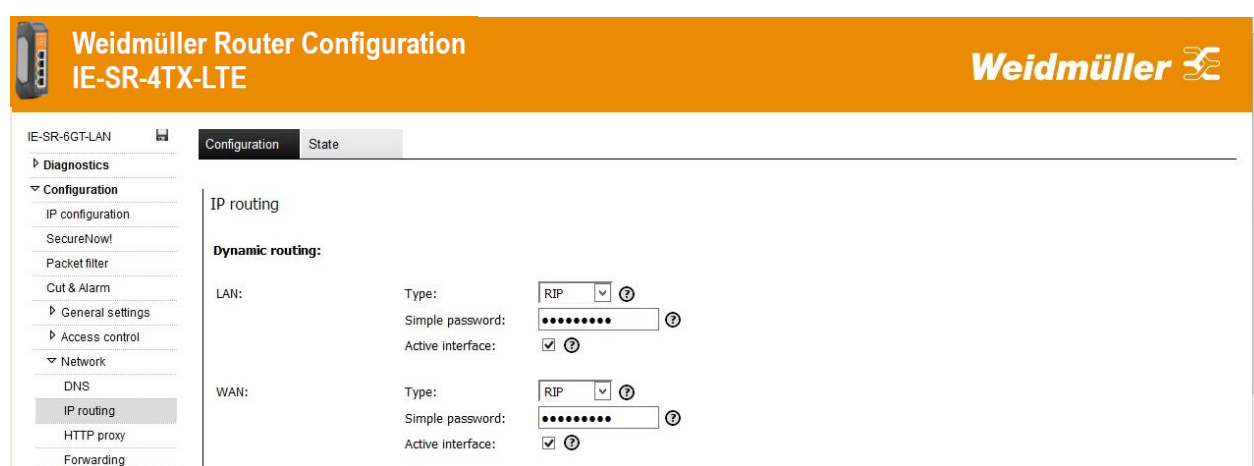



Figure 28: Configuration of dynamic routing using RIP



	Note
	<ol style="list-style-type: none"> <li>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.</li> <li>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 <b>not</b> announce (outgoing WAN port) the configured network connected to its LAN port.</li> </ol>

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
	<ol style="list-style-type: none"> <li>1. If you perform the ping test using PC’s please check your firewall configuration to ensure that ping requests and echoes are allowed.</li> <li>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).</li> </ol>




## 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.



## Weidmüller Router Configuration

### IE-SR-4TX-LTE

IE-SR-4TX-LTE/4G

▼ Diagnostics

- System State
- Eventlog
- WAN
- LAN
- WWAN
- Ping test
- Remote capture

Configuration

### Remote capture

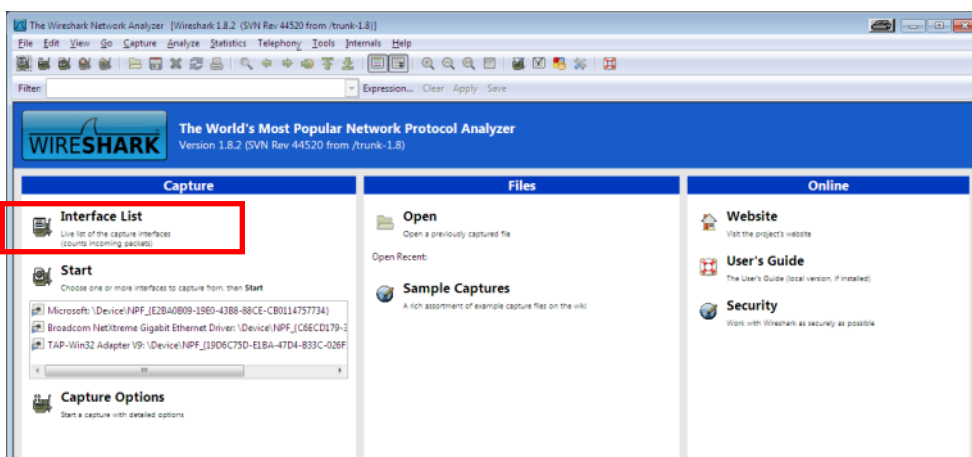
Enable remote capture server: ☒ ?

Client address:  ?

Apply settings
Reset changes

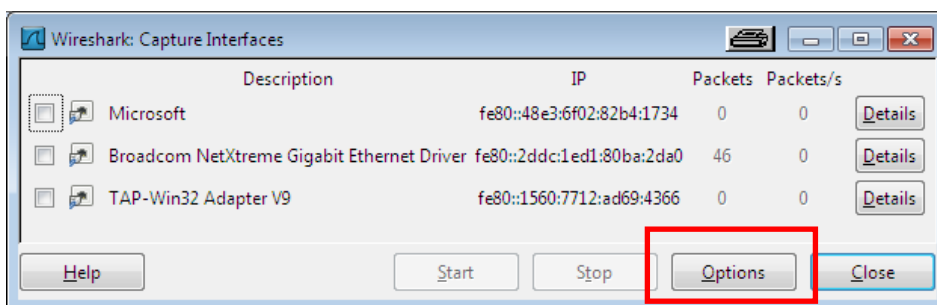
Activate the checkboxes and enter the IP address of the remote Wireshark-PC. Then click button Apply settings

2. Start Wireshark at your PC
3. Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”

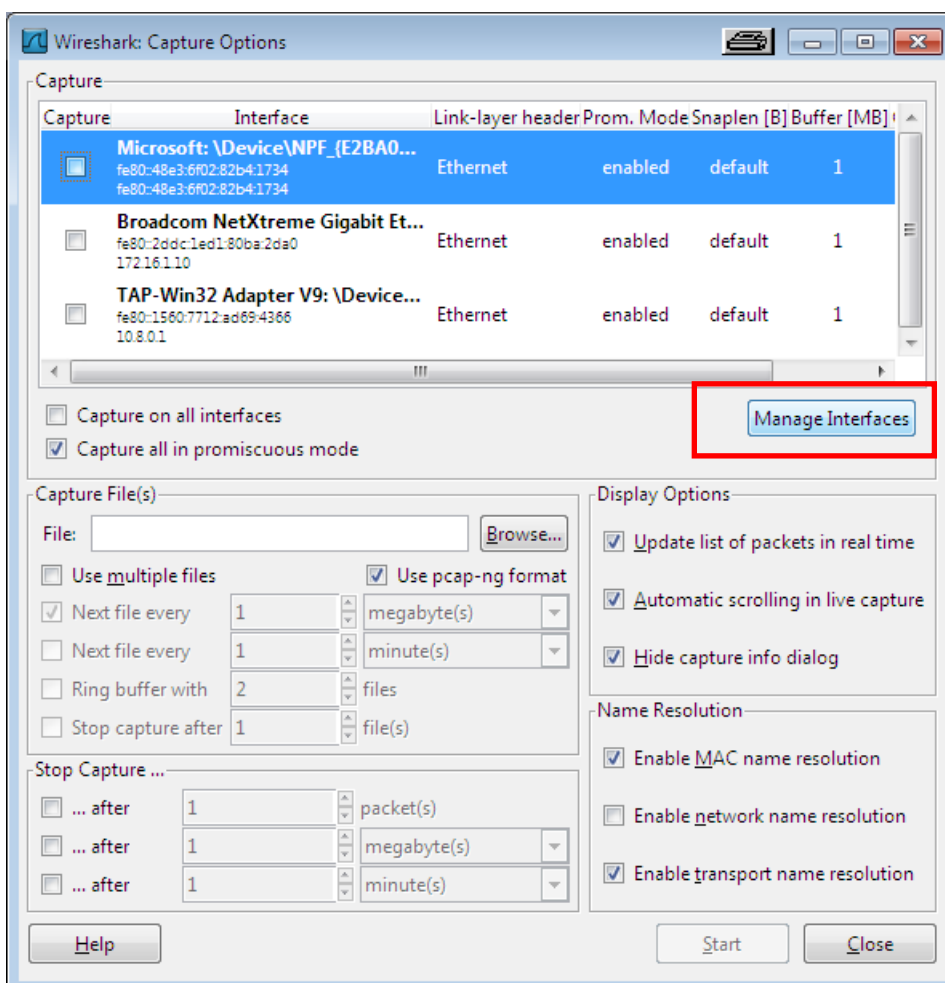


The local Ethernet Interfaces of the computer will be displayed.

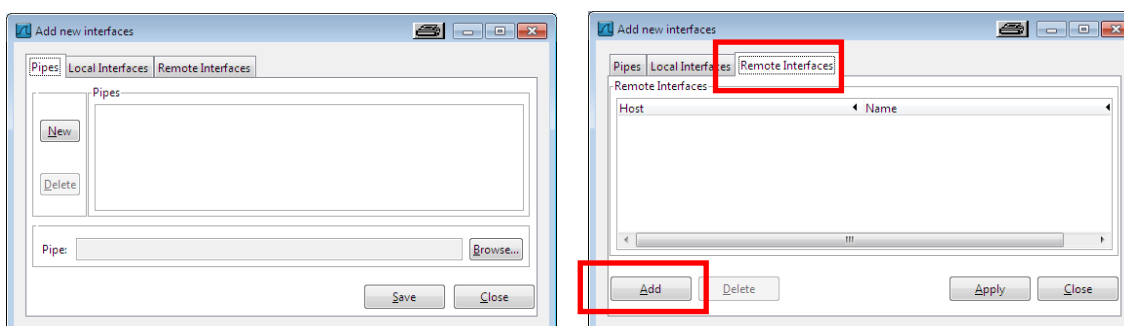




4. Click button “Options”

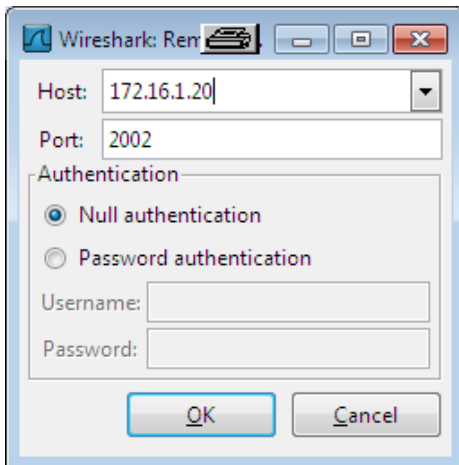


5. Click button “Manage Interfaces” and change to tab “Remote Interfaces”



6. Click button “Add”



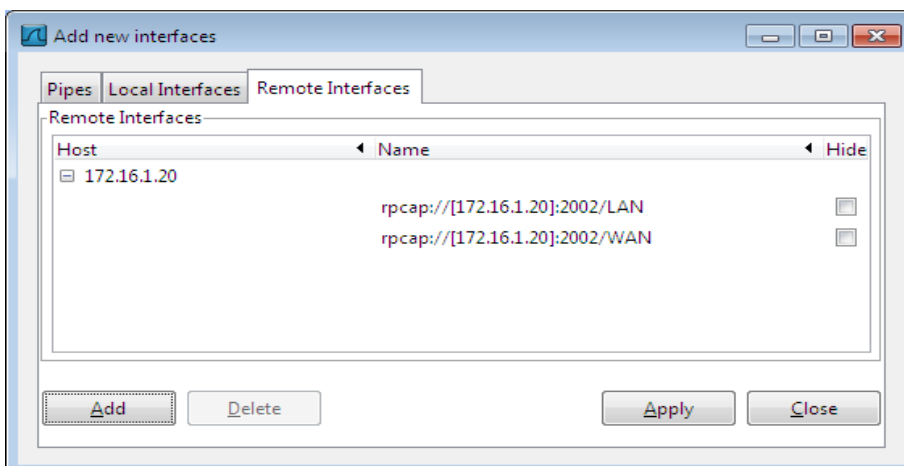


7. Enter the IP address of the Router to field "Host"

Note: You can enter either the IP address of LAN or WAN port. The important fact is that the Router's 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

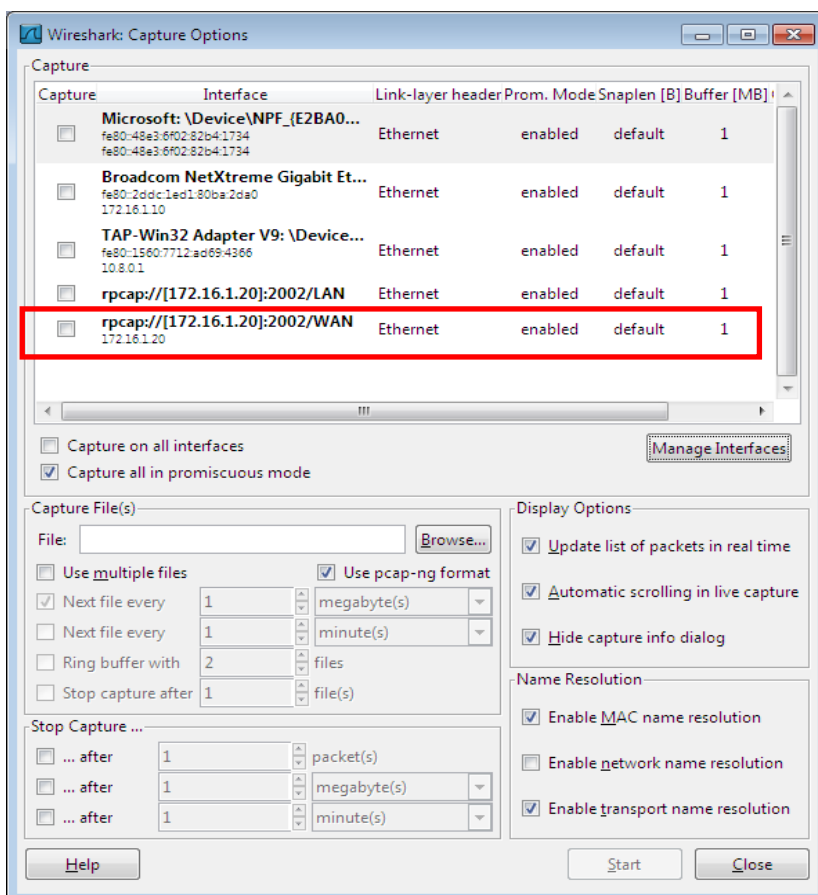
Now both Interfaces of the Router (= Host 172.16.1.20) should be displayed.



10. Click button Close

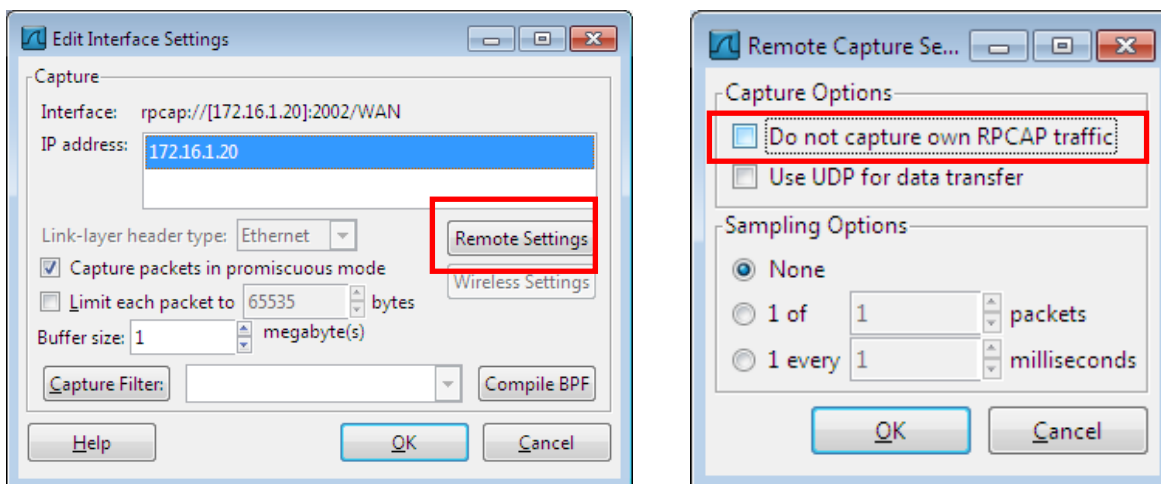
The "remote capture interfaces" will be displayed in the list of selectable interfaces.





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

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



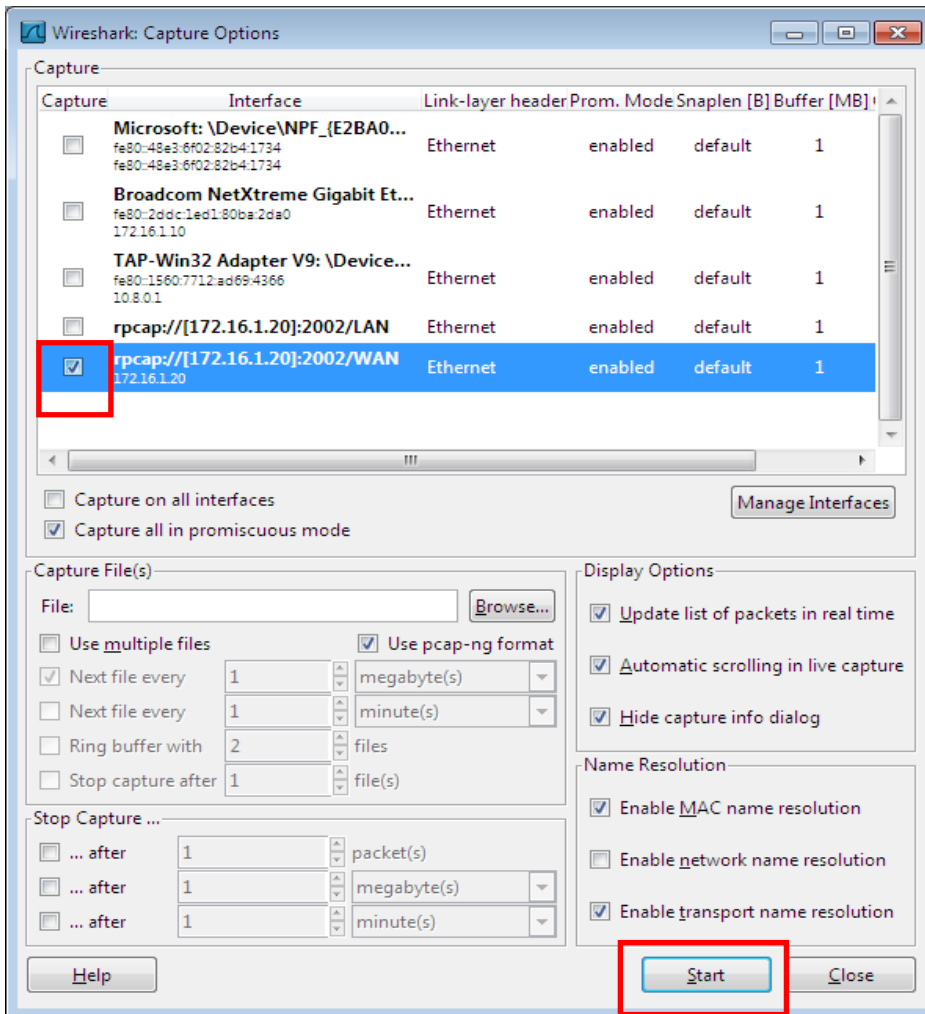
12. Click button “Remote Settings”

13. **Clear** the checkbox “Do not capture own RPCAP traffic”

14. Click button “OK”

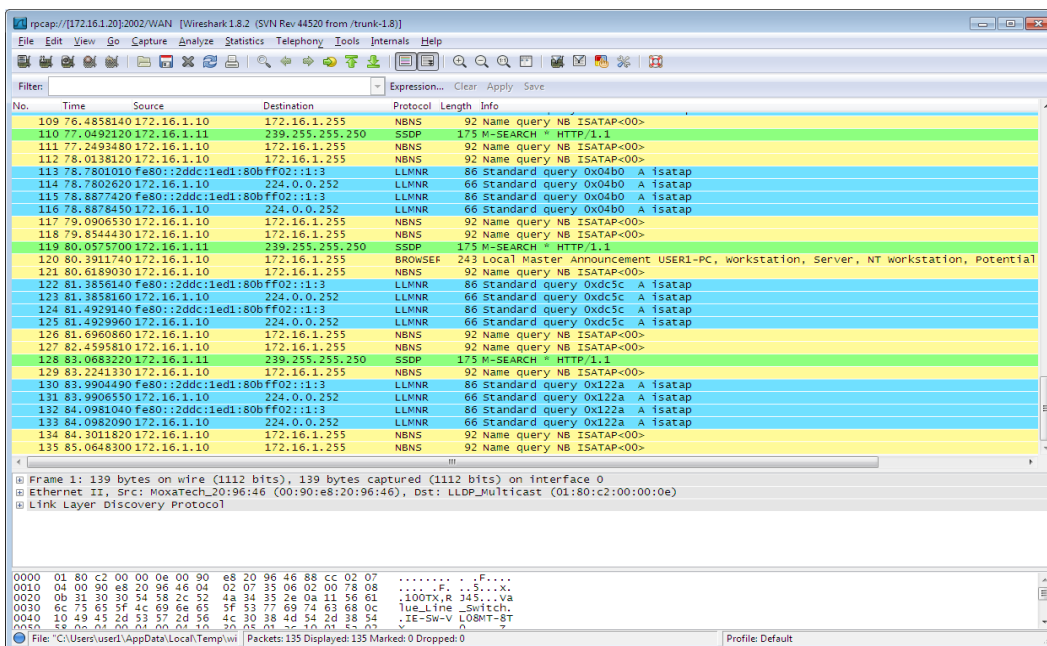
15. Again click button “OK” to close the window “Edit Interface Settings”





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

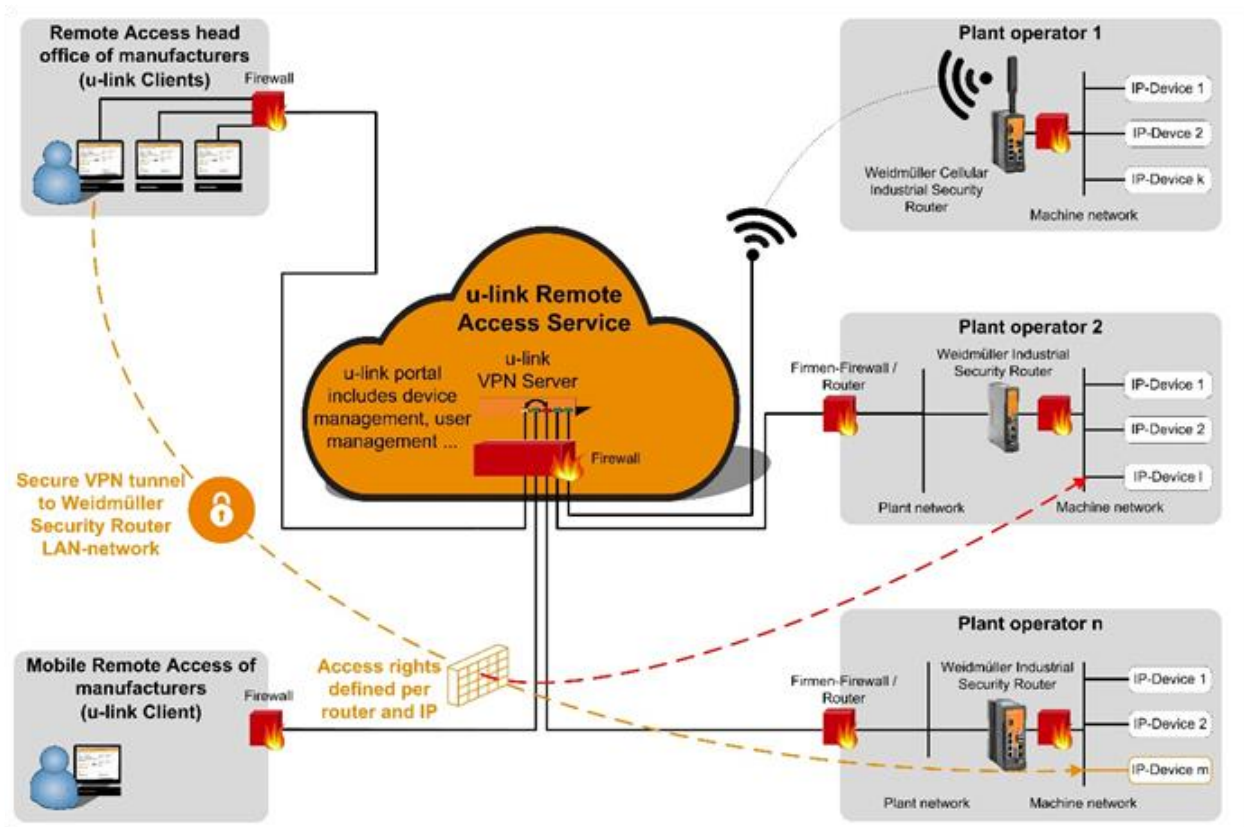




## A7 - u-link Remote Access Service → VPN based connection to remote locations

### 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 (redundantly hosted in a German data center).

### 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](#)