

Industrial Security Router / Firewall

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



Manual

Version 1.3

August 2020

Important notes:

This document will be updated continuously.

This version refers to Router firmware version 1.0.7 and above.

This document, new firmware or additional product information can be downloaded using following link:

<https://catalog.weidmueller.com>

- ▶ Select „Active Industrial Ethernet “
- ▶ Select „Industrial Security Router“
- ▶ Select a product model of the IE-SR-4TX-Family
- ▶ Click and expand section „Downloads “
- Download needed documentation or 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 © 2020 Weidmüller Interface GmbH & Co. KG
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

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

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

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

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

Contact Information

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

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

Table of Contents

INDUSTRIAL SECURITY ROUTER / FIREWALL	1
1. INTRODUCTION.....	5
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
2. HARDWARE RELATED FUNCTIONAL DESCRIPTIONS.....	13
2.1 DESCRIPTION OF LED STATUS INDICATORS	13
2.2 INTERFACES.....	14
2.3 PIN ASSIGNMENTS	15
Pin assignment of 4-pin connector for „VPN initiate“ and „VPN active“	15
Pin assignment of power supply connector.....	15
Pin assignment of RJ45 Ethernet ports (LAN and WAN).....	15
Pin assignment of Smartcard Reader (ISO 7816 Standard).....	15
3. INITIAL START-UP / GETTING STARTED	16
3.1 Configuration of the Router by using an Internet browser	16
3.2 Starting the Web interface	16
3.3 Default factory settings of the Router:.....	18
3.4 Reset to factory default settings by external push button.....	18
3.5 Using the Weidmüller Router-Search-Utility.....	19
3.6 Basic description of Router's configuration interface (menu items)	20
4. WEB CONFIGURATION	21
4.1 SECTION DIAGNOSTICS.....	21
4.1.1 Diagnostics → System State	21
4.1.2 Diagnostics → Event Log (Tab State)	22
4.1.3 Diagnostics → Event Log (Tab Configuration)	22
4.1.4 Diagnostics → WAN.....	23
4.1.5 Diagnostics → LAN.....	23
4.1.6 Diagnostics → WWAN.....	24
4.1.7 Diagnostics → Ping test.....	24
4.1.8 Diagnostics → Remote capture	25
4.2 SECTION CONFIGURATION	26
4.2.1 Configuration → Config Wizard.....	26
4.2.1 Configuration → IP Configuration.....	30
IP Configuration → Operational mode "IP Router"	30
4.2.3 Configuration → Packet filter (Firewall).....	32
4.2.5 Configuration → General settings.....	34
General settings → System data.....	34
General settings → Date & Time	34
General settings → User Interface.....	35
General settings → Certificates	36
General settings → SCEP (Tab Configuration)	37
General settings → SCEP (Tab State)	37
4.2.6 Configuration → Access Control	38
Access Control → User accounts	38
Access Control → Permissions.....	38
Access Control → Web access	39
4.2.7 Configuration → Network	39
Network → DNS (Tab Configuration)	39
Network → IP Routing (Tab Configuration).....	41

Network → IP Routing (Tab State)	43
Network → HTTP proxy	43
Network → Forwarding	44
Network → 1:1 NAT	46
Network → Network Groups	47
Network → Hardware Groups	47
4.2.8 Configuration → VPN	49
VPN → u-link (Tab Configuration)	49
VPN → u-link (Tab State)	50
VPN → u-link (Tab Registration)	51
VPN → OpenVPN (Tab Configuration)	51
VPN → OpenVPN (Tab VPN1)	52
VPN → OpenVPN (Tab State)	54
VPN → IPsec (Tab Configuration)	54
VPN → IPsec (Tab State)	57
4.2.9 Configuration → Services	58
Services → DHCP Server (Tab Configuration)	58
Services → DHCP Server (Tab State)	59
Services → Web server	59
Services → SNMP	60
4.3 SECTION SYSTEM	61
4.3.1 System → Backup settings	61
4.3.2 System → Software update	61
4.3.3 System → Factory defaults	62
4.3.4 System → Save	63
4.3.5 System → Reboot	63
4.4 SECTION INFORMATION	64
4.4.1 Information → General	64
4.4.2 Information → Sitemap	64
5. APPENDIX A (CONFIGURATION EXAMPLES)	65
A1 – BASIC ROUTER CONFIGURATION TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES	65
A2 - CONNECTING 2 ETHERNET NETWORKS WITH ACTIVATED NAT MASQUERADING AND USING IP ADDRESS FORWARDING	69
A3 - CONFIGURING THE ROUTER TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES AND ADDITIONAL FIREWALL RULES	74
A4 – FIREWALL APPLICATION EXAMPLE: SECURING THE ACCESS TO MODBUS TCP DEVICES BY LAYER-2 FIREWALL RULES	81
A5 - USING DYNAMIC IP ROUTING ALTERNATIVELY TO MANUALLY CONFIGURED STATIC ROUTES (REFERS TO EXAMPLE A6)	95
A6 - HOW TO USE FEATURE “REMOTE CAPTURE” WITH WIRESHARK TO ANALYSE ROUTER’S LAN/WAN TRAFFIC	97
A7 - U-LINK REMOTE ACCESS SERVICE → VPN BASED CONNECTION TO REMOTE LOCATIONS	102

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).

The Router has implemented extensive security standards to enable different networks to work together smoothly.

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

	Warning
	<ul style="list-style-type: none">- Using the selected device for purposes other than those specified or failure to observe the operating instructions and warning notes can lead to serious malfunctions that may result in personal injury or damage to property.- If this product malfunctions, it is no longer possible to predict the behavior of neighboring networked facilities and their connected devices. Personal injury and property damage can occur because of malfunctions. Only carry out changes to the settings when you are certain of the consequences such changes will have on all connected networks, facilities and devices.- Personal injury and property damage can occur if this product is used improperly. Adjustments and setting changes to this product should only be carried out by sufficiently qualified personnel.


	Caution
	<ul style="list-style-type: none"> - 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. - The Security Router does not have an on/off switch. The operating voltage must be switched on by the facility in which the device is integrated.


	Caution
	<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"> - The default system access information for the Security Router is included in this document. Unauthorized individuals can use this access data to gain access to the Router's web browser and cause damage. Be sure to change these system default access settings. - Some services may be blocked by a firewall. You may need to deactivate the firewall. By deactivating the firewall, the PC is no longer protected against viruses or other attacks. Only deactivate the firewall when your PC is sufficiently protected by other measures. - A single port can only properly execute one service. If multiple services are assigned to a port, the port can no longer execute any service. Be sure to assign only one service to any port.

	Note
	<ul style="list-style-type: none"> - The IP protocol reserves certain IP address ranges for special purposes (such as multicasting). Do not assign IP addresses in the range from 127.0.0.0 – 127.255.255.255 or 224.0.0.0 – 255.255.255.255. - This device is intended for use in applications as described in the operating instructions only. Using this device in non-approved applications will lead immediately to the expiration of all guarantee and warranty claims on the part of the operator against the manufacturer.

1.4 Mounting the device

	Caution
	<ul style="list-style-type: none"> - 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. - Connecting plugs should never be connected or disconnected from electrical devices if they are carrying a live load. Be sure to first disconnect all poles of the plug. Remember to disconnect all plugs from the Router before it is installed or removed. - Electrical devices should not be installed or removed during operations. Never install or remove the Router while it is running.

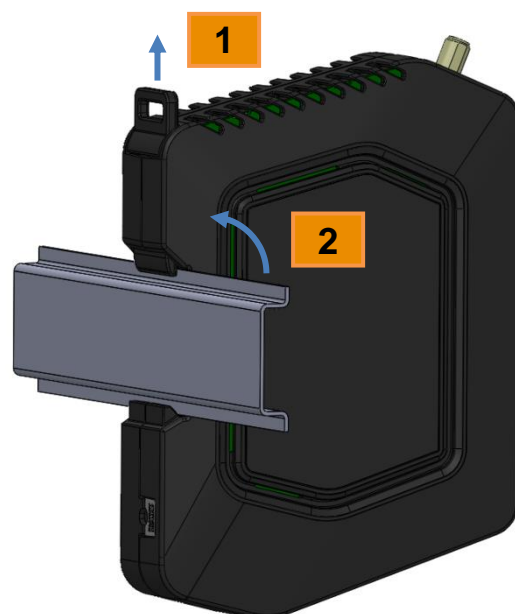
	Caution
	<ul style="list-style-type: none"> - It is important to provide sufficient clearance between devices which cause strong electromagnetic interference (such as frequency converters, transformers or motor regulators). The clearance gap between such devices and the Router should be as wide as possible. The Router can be further shielded by using a mu-metal partition. - The Router is designed to be mounted on a top-hat rail that is compliant with the EN 50022 standard. This Router will not have a secure mount if any other type of rail is used. Use a top-hat rail that complies with the EN 50022 standard. Be sure to observe the mounting information provided by the manufacturer.

	Note
	<ul style="list-style-type: none"> - 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. - The top-hat rail should be in a horizontal position along the vertical rear wall of the electrical cabinet. This ensures that the Router can be adequately ventilated from below to above.

DIN-rail mounting:

Insert the bottom of the DIN-rail clip behind the lower edge of the DIN-rail. Then open the latch at top of the device by using a flatbladed screwdriver (1) and fix the device on 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"> • IPv4-Routing between the interfaces (LAN ports / WAN port / optional 4G modem). LAN-Ports behave as unmanaged switch. • Static or dynamic routing according to RIPv2 or OSPF protocol.
Network Services	<ul style="list-style-type: none"> • DHCP Server / DHCP Relay • DNS-Relay • NTP-Client • DynDNS (DHCP-Client according to RFC 2136)
Firewall	<ul style="list-style-type: none"> • IPv4 Stateful inspection Firewall • NAT-Masquerading, 1:1 NAT, Port forwarding • Layer-2/3-Filter (VLAN ID, VLAN QoS Tag, MAC address based, Ethertype Frame)

OpenVPN	<ul style="list-style-type: none"> • Configurable as OpenVPN server or client (Layer 2 and Layer 3) • Authentication with X.509 Certificates • Tunnel support via HTTP-Proxy • A maximum of 10 different server configurations • Unlimited number of client connections in server mode
IPsec	<ul style="list-style-type: none"> • Can be configured as an IPsec server or client. • Authentication with PSK (user ID, password) or X.509 certificates. • Hardware encryption for faster data flow rate. • A maximum of 64 simultaneous connections (subnet with subnet or as IPsec server) • Encryption algorithms DES-56, 3DES-168, AES 128, AES 192, AES-256
u-link	<ul style="list-style-type: none"> • Based on certificate-secured OpenVPN technology • To be used with the Weidmüller Remote Access Service • Simplifies VPN connections and management • Fast and easy connections • Free of charge • Visit https://u-link.weidmueller.com for further information.

Configuration

Management	<ul style="list-style-type: none"> • Configuration with web interface (HTTP/HTTPS) • Web interface selectable in English or German language • Configuration support through wizard • Configuration support through detailed help information (tooltip) • Configurable Multi-user access with definable rights • Support for SNMP v1/v3/v3 • Event log / syslog
------------	---

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"> • Cut & Alarm: Get status / Set acknowledgment • IPsec /OpenVPN/u-link: Switch configured VPN connections on or off *
Diagnosis	<ul style="list-style-type: none"> • „Remote Capture“ - feature for network diagnostics via a connected PC (Wireshark)

Interfaces

RJ45-Ports	<ul style="list-style-type: none"> • 4 x 10/100 BaseT(X)
RS 485	<ul style="list-style-type: none"> • Interface for Modbus RTU communication
SCM card reader	<ul style="list-style-type: none"> • 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)
SIM card slot* ¹	<ul style="list-style-type: none"> • Insert SIM card for mobile communication
LED displays	<ul style="list-style-type: none"> • Signaling the status for power, device status, active VPN connection and an active cellular connection*¹
Digital Inputs	<ul style="list-style-type: none"> • 1 DI to trigger different functions as VPN, Firewall or CUT
Reset-Button	<ul style="list-style-type: none"> • Restore to the factory settings

*¹ for LTE/4G models only

Power

Input Voltage	<ul style="list-style-type: none"> • 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
Current consumption	<ul style="list-style-type: none"> • Max. 500 mA @ 24 VDC for IE-SR-4TX • Max. 800 mA @ 24 VDC for IE-SR-4TX-4G*

Technical data (housing)

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

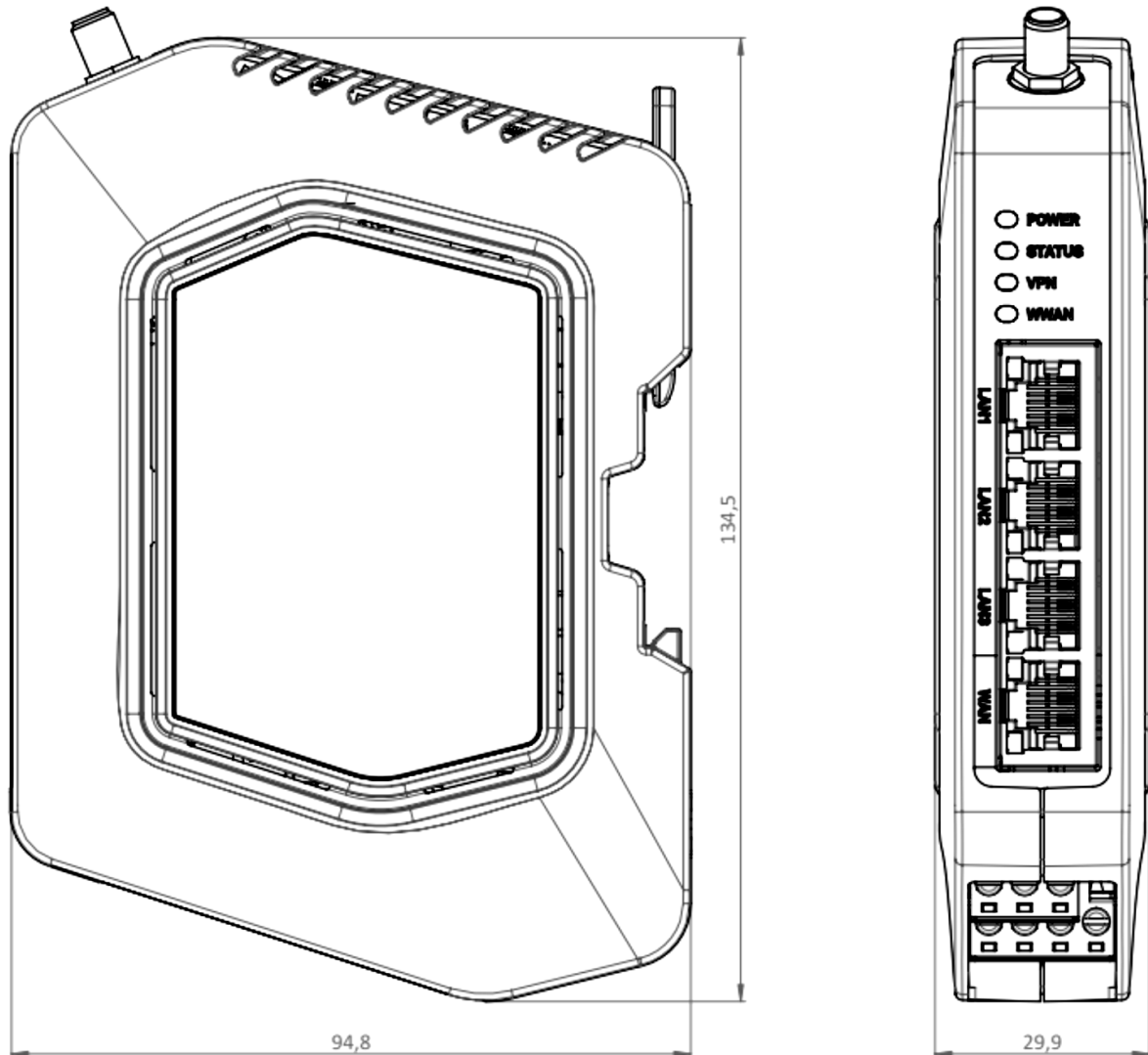


Figure 1: Dimensional drawings

Environmental conditions

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

DSL and 4G/LTE

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

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"> • 1 dBi @ 698-960 MHz • 2 dBi @ 1710-1990 MHz • 2 dBi @ 2300-2400 MHz • 3 dBi @ 2500-2700 MHz • Polarisation: vertical 	
-----------	---	--

* Only 4G models

Approvals

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

Warranty

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

Order Information

	Model name	Order number
2-Port LAN/WAN Router with VPN features	IE-SR-4TX	2751270000
2-Port LAN / WAN Router with VPN features and additional integrated LTE/4G modem	EU: IE-SR-4TX-4G-EU	2751280000
	US: IE-SR-4TX-4G-US-VZ	Coming soon
	EU: IE-SR-4TX-4G-USEMEA	2739630000

2. Hardware related functional descriptions

2.1 Description of LED status indicators



Description of LED status indicators

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

* not available for IE-SR-2GT-LAN-FN

2.2 Interfaces



Description of device interfaces at top and front side

Connectors for LTE/4G antennas at top side; Connector type: **SMA female** (Only model IE-SR-6GT-LTE/4G)

3 x RJ45-Connector LAN (10/100BaseTX)

1 x RJ45-Connector WAN (10/100BaseTX)

3-pin connector for RS485 interface

4-pin connector for 24 V DC power supply and digital input

Description of device interfaces at rear side



SIM1 slot / socket

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

SCM/SIM2 slot / socket

SIM memory card reader for external backup and restore of the Router configuration.

A second SIM-card currently is not supported!



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

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



External antennas:

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

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

Use coaxial cable with nominal impedance of 50 ohms.

2.3 Pin assignments

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

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



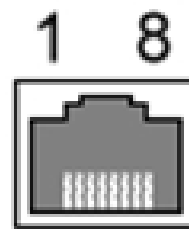
Pin assignment of RS485 interface

Pin number	Description
GND	Reference potential
D-	Inverted data signal
D+	Non-inverted data signal



Pin assignment of RJ45 Ethernet ports (LAN and WAN)

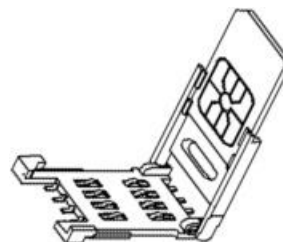
Pin number	SIGNAL NAME (MDI)	
	10/100Base T(x)	1000Base T
1	TX +	BI_DA+
2	TX -	BI_DA-
3	RX +	BI_DB+
4	NC	BI_DC+
5	NC	BI_DC-
6	RX -	BI_DB-
7	NC	BI_DD+-
8	NC	BI_DD-



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 autonegotiation.

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



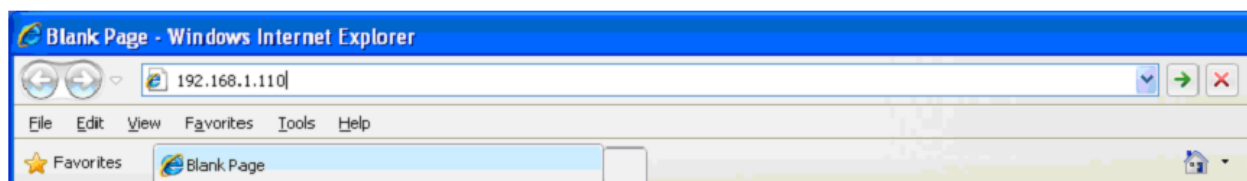
Important note

The Router's Web server **partly** is using Java script for parameter settings (e.g. if you want to apply or deleting a configured Open VPN session).

Please ensure that the Web browser you are using can run Java script. For Router configuration. You do NOT need to install Java runtime software (for executable Java applets) because only Java script will be used. Standard Web browsers by default can run Java script code.

If some "Apply" buttons are not working (seems to be without function) and if you are using Internet Explorer 10 please verify that you are using Bowser Mode IE10 to ensure that Java script is running properly. To validate the browser mode press key F12 and activate – if not set – mode Internet Explorer 10 as shown in the screenshot below.

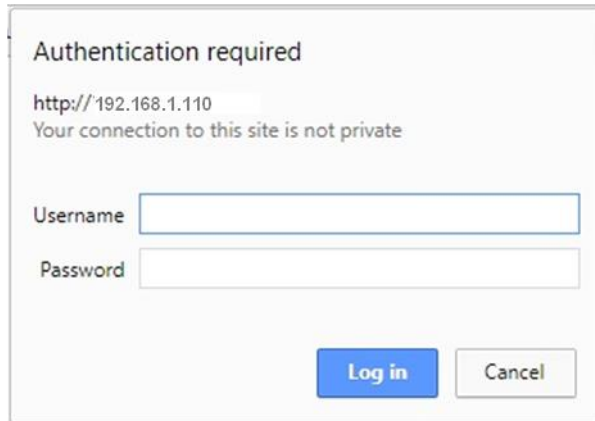
1. Start your Web browser and enter the IP address of the connected Router port into the browser's address line. (i.e. when connected to a LAN-Port 192.168.1.110)



- Now the login prompt of the Router should appear for input User name and Password.

Default values (factory settings) for Login:

User name: admin
Password: Detmold



Authentication required

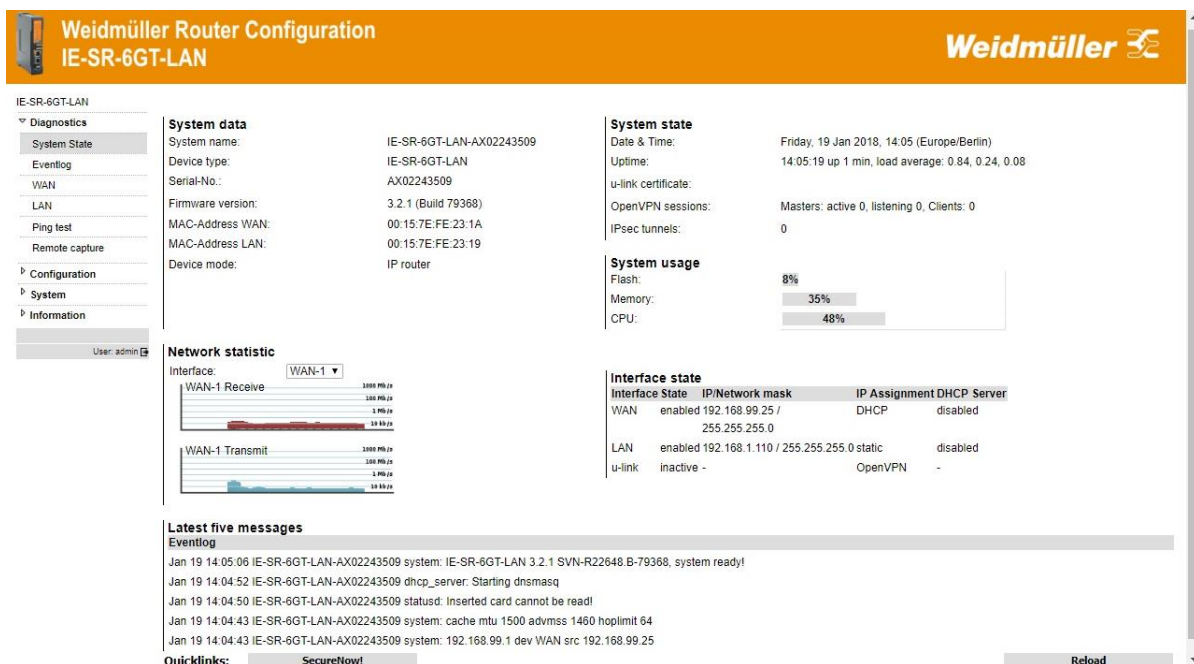
http://192.168.1.110
 Your connection to this site is not private

Username

Password

Confirm your input by pressing the Log in button.

Now the Router homepage is displayed. This page corresponds to the menu item "Diagnostics → System State." On this page the most important configuration and status information are summarized.



Weidmüller Router Configuration
 IE-SR-6GT-LAN

System data

System name:	IE-SR-6GT-LAN-AX02243509
Device type:	IE-SR-6GT-LAN
Serial-No.:	AX02243509
Firmware version:	3.2.1 (Build 79368)
MAC-Address WAN:	00:15:7E:FE:23:1A
MAC-Address LAN:	00:15:7E:FE:23:19
Device mode:	IP router

System state

Date & Time:	Friday, 19 Jan 2018, 14:05 (Europe/Berlin)
Uptime:	14:05:19 up 1 min, load average: 0.84, 0.24, 0.08
u-link certificate:	
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	8%
Memory:	35%
CPU:	48%

Network statistic

Interface: WAN-1

WAN-1 Receive: 1000 MB/s, 1 MB/s, 10 KB/s

WAN-1 Transmit: 1000 MB/s, 1 MB/s, 10 KB/s

Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.99.25 / 255.255.255.0	DHCP	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled
u-link	inactive	-	OpenVPN	-

Latest five messages

Eventlog

Jan 19 14:05:06 IE-SR-6GT-LAN-AX02243509 system: IE-SR-6GT-LAN 3.2.1 SVN-R22648 B-79368, system ready!

Jan 19 14:04:52 IE-SR-6GT-LAN-AX02243509 dhcp_server: Starting dnsmasq

Jan 19 14:04:50 IE-SR-6GT-LAN-AX02243509 statusd: Inserted card cannot be read!

Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: cache mtu 1500 advmss 1460 hoplimit 64

Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: 192.168.99.1 dev WAN src 192.168.99.25

Quicklinks: [SecureNow!](#)



Note

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

3.3 Default factory settings of the Router:



Note

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

Language	English
Operation Mode	IP Router
IP address LAN Port(s)	192.168.1.110 (static value)
Subnet Mask	255.255.255.0
NAT (Masquerading) on LAN Port	Not activated
IP address WAN Port	DHCP 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 and Layer 3. For that the packet filter contains two default rules, called "Allow_L2" and "Allow_L3" (allow traffic at Layer 2 and 3) which allows as "white lists" all network traffic.
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

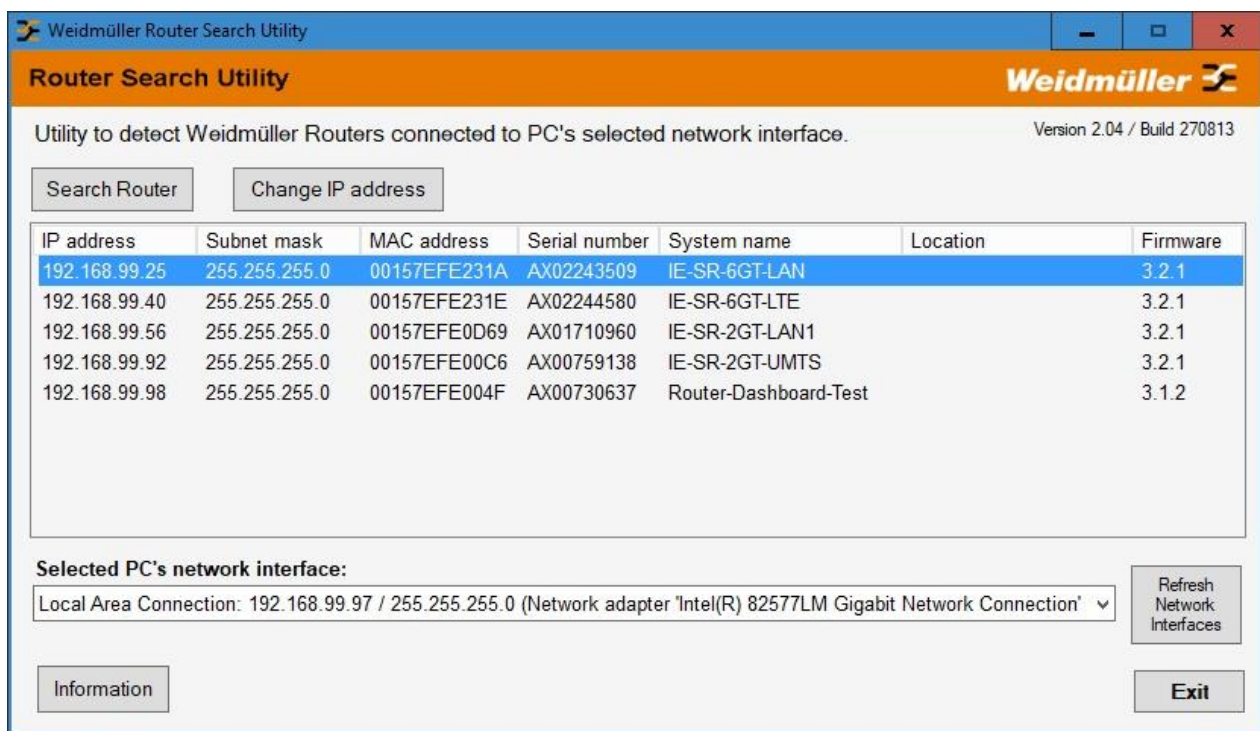
The software tool Weidmüller Router-Search-Utility can be used to find Weidmüller Routers and detect their IP addresses within a switched network. This software is very helpful if you don't know the current IP address of a Router. This can e.g. happen in cases that you have forgotten the current IP configuration 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
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
- Displays current interface parameters (LAN/WAN/4G)
- Feature for testing the data communication between the Router and other Ethernet devices (Ping test)

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
- User administration (assignment of rights)
- IP-Routing (static, dynamic) and IP address management (Masquerading, 1:1 NAT, Portforwarding)
- Configuration of u-link Remote Access Service / OpenVPN / IPsec connections
- Configuration of general network services (e.g. DHCP, DBS, SNMP)

Section system

- Backup and restore of device configuration
- Update firmware, Reboot


Section Information

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


4. Web Configuration

4.1 Section Diagnostics

4.1.1 Diagnostics → System State



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

Diagnostics

- System State
- Eventlog
- WAN
- LAN
- Ping test
- Remote capture
- Configuration
- System
- Information

User: admin

System data

System name: IE-SR-6GT-LAN-AX02243509

Device type: IE-SR-6GT-LAN

Serial-No.: AX02243509

Firmware version: 3.2.1 (Build 79368)

MAC-Address WAN: 00:15:7E:FE:23:1A

MAC-Address LAN: 00:15:7E:FE:23:19

Device mode: IP router

System state

Date & Time: Friday, 19 Jan 2018, 14:05 (Europe/Berlin)

Uptime: 14:05:19 up 1 min, load average: 0.84, 0.24, 0.08

u-link certificate:

OpenVPN sessions: Masters: active 0, listening 0, Clients: 0

IPsec tunnels: 0

System usage

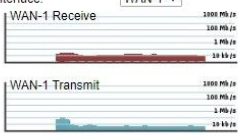
Flash: 8%

Memory: 35%

CPU: 48%

Network statistic

Interface: WAN-1



Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.99.25 / 255.255.255.0	DHCP	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled
u-link	inactive	-	OpenVPN	-

Latest five messages

Eventlog

Jan 19 14:05:06 IE-SR-6GT-LAN-AX02243509 system: IE-SR-6GT-LAN 3.2.1 SVN-R22648-B-79368, system ready!

Jan 19 14:04:52 IE-SR-6GT-LAN-AX02243509 dhcp_server: Starting dnsmasq

Jan 19 14:04:50 IE-SR-6GT-LAN-AX02243509 statusd: Inserted card cannot be read!

Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: cache mtu 1500 advmss 1460 hoplimit 64

Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: 192.168.99.1 dev WAN src 192.168.99.25

Quicklinks: [SecureNow!](#)


[Reload](#)

Menu	Diagnostics → System State	
Function	Startup screen of the web interface after login. Displays current configuration and status data.	
	System name	Name of the device, default "<Device Type>-<Serial No.>"
	Device type	Article Name
	Serial No.	Unique Number of this product
	Firmware version	Actual used Firmware and Build
	MAC-Address WAN	Registered MAC-address of the WAN-Ports
	MAC-Address LAN	Registered MAC-address of the LAN-Ports
	Device mode	Displays actual device mode
	Network statistics	Displays current network traffic on selected interface
	Date & Time	Date and time of the router
	Uptime (see screenshot)	Actual time (14:05:19) followed by Time the router is running continuously (1 min) followed by average system usage in order CPU (0,84), 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, Memory and CPU
	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-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN

▼ Diagnostics

System State

Eventlog

WAN

LAN

Ping test

Remote capture

▶ Configuration

▶ System

▶ Information

User: admin

State

Configuration

Eventlog


```

Jan 19 14:05:06 IE-SR-6GT-LAN-AX02243509 system: IE-SR-6GT-LAN 3.2.1 SVN-R22648.B-79368, system ready!
Jan 19 14:04:52 IE-SR-6GT-LAN-AX02243509 dhcp_server: Starting dnsmasq
Jan 19 14:04:50 IE-SR-6GT-LAN-AX02243509 statusd: Inserted card cannot be read!
Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: cache mtu.1500 advmss 1460 hoplimit 64
Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: 192.168.99.1 dev WAN src 192.168.99.25
Jan 19 14:04:43 IE-SR-6GT-LAN-AX02243509 system: running /etc/init.d/S41routing
Jan 19 14:04:42 IE-SR-6GT-LAN-AX02243509 dhcpclient: bound to 192.168.99.25 -- renewal in 423911 seconds.
Jan 19 14:04:41 IE-SR-6GT-LAN-AX02243509 dhcp_server: Starting dnsmasq
Jan 19 14:04:41 IE-SR-6GT-LAN-AX02243509 dhcp_server: Stopping dnsmasq
Jan 19 14:04:40 IE-SR-6GT-LAN-AX02243509 dhcpclient: dnsmasq not running. Restarting...
Jan 19 14:04:40 IE-SR-6GT-LAN-AX02243509 dhcpclient: DHCPACK from 192.168.99.1
Jan 19 14:04:40 IE-SR-6GT-LAN-AX02243509 dhcpclient: DHCPREQUEST on WAN to 255.255.255.255 port 67
Jan 19 14:04:40 IE-SR-6GT-LAN-AX02243509 dhcpclient: DHCPDISCOVER on WAN to 255.255.255.255 port 67 interval 11
Jan 19 14:04:40 IE-SR-6GT-LAN-AX02243509 dhcpclient: DHCPDISCOVER on WAN to 255.255.255.255 port 67 interval 11
Jan 19 14:04:34 IE-SR-6GT-LAN-AX02243509 dhcpclient: DHCPDISCOVER on WAN to 255.255.255.255 port 67 interval 6


```

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

4.1.3 Diagnostics → Event Log (Tab Configuration)



Weidmüller Router Configuration
IE-SR-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN

▼ Diagnostics

System State

Eventlog

WAN

LAN

Ping test

Remote capture

▶ Configuration

▶ System

▶ Information

User: admin

State

Configuration

Eventlog

Enable remote syslog: ☐ ?

Address of syslog server:


UDP port of syslog server:

Apply settings

Reset changes

Menu	Diagnostics → Event Log → Tab Configuration	
Function	Event and error messages can be sent to a syslog server (PC on the network) or sent as emails.	
	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 → WAN



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN
 ▾ Diagnostics
 System State
 Eventlog
 WAN
 LAN
 Ping test
 Remote capture
 ▸ Configuration
 ▸ System
 ▸ Information
 User: admin

WAN-1

WAN-2

WAN-1

MAC-Address: 00:15:7E:FE:23:1A


Link: yes
 Speed: 100Mb/s
 Duplex: Full

Received bytes: 2323638
 Received packets: 9926
 Received dropped packets: 0
 Received overrun packets: 0
 Transmitted bytes: 1557482
 Transmitted packets: 2711
 Transmitted dropped packets: 0
 Transmitted overrun packets: 0
 Collisions: 0


Reload

Menu	Diagnostics → WAN
Function	Displays the current status of the WAN ports Diagnose the WAN-port.

4.1.5 Diagnostics → LAN



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN
 ▾ Diagnostics
 System State
 Eventlog
 WAN
 LAN
 Ping test
 Remote capture
 ▸ Configuration
 ▸ System
 ▸ Information
 User: admin

LAN-1

LAN-2

LAN-3

LAN-4

LAN-1

MAC-Address:

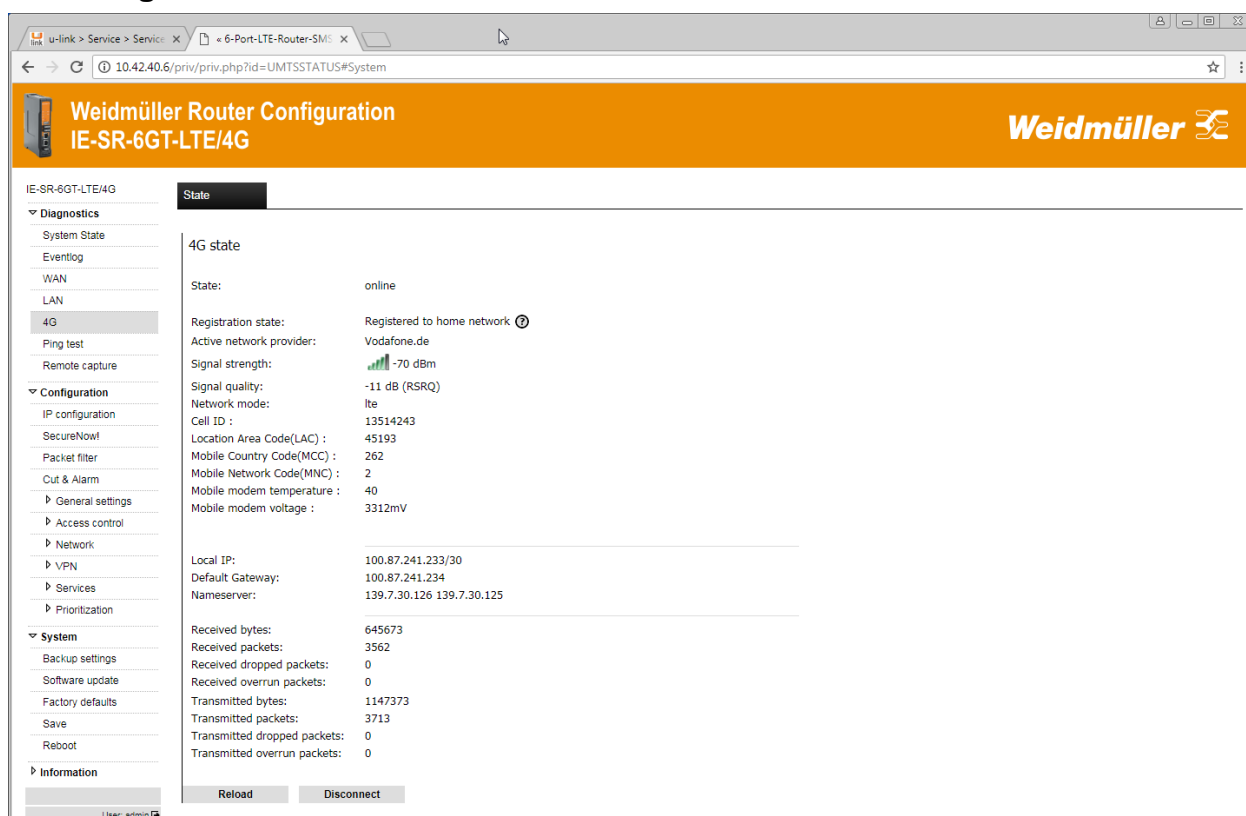
Link: no
 Speed: 10Mb/s
 Duplex: Half

Received bytes: 0
 Received packets: 0
 Received dropped packets: 0
 Received overrun packets: 0
 Transmitted bytes: 0
 Transmitted packets: 0
 Transmitted dropped packets: 0
 Transmitted overrun packets: 0
 Collisions: 0

Reload

Menu	Diagnostics → LAN
Function	Displays the current status of the LAN ports. Diagnose the LAN-port.

4.1.6 Diagnostics → WWAN



Weidmüller Router Configuration
IE-SR-6GT-LTE/4G

4G state

State: online

Registration state: Registered to home network

Active network provider: Vodafone.de

Signal strength: -70 dBm

Signal quality: -11 dB (RSRQ)

Network mode: lte

Cell ID : 13514243

Location Area Code(LAC) : 45193

Mobile Country Code(MCC) : 262

Mobile Network Code(MNC) : 2

Mobile modem temperature : 40

Mobile modem voltage : 3312mV

Local IP: 100.87.241.233/30

Default Gateway: 100.87.241.234

Nameserver: 139.7.30.126 139.7.30.125

Received bytes: 645673

Received packets: 3562

Received dropped packets: 0

Received overrun packets: 0

Transmitted bytes: 1147373

Transmitted packets: 3713

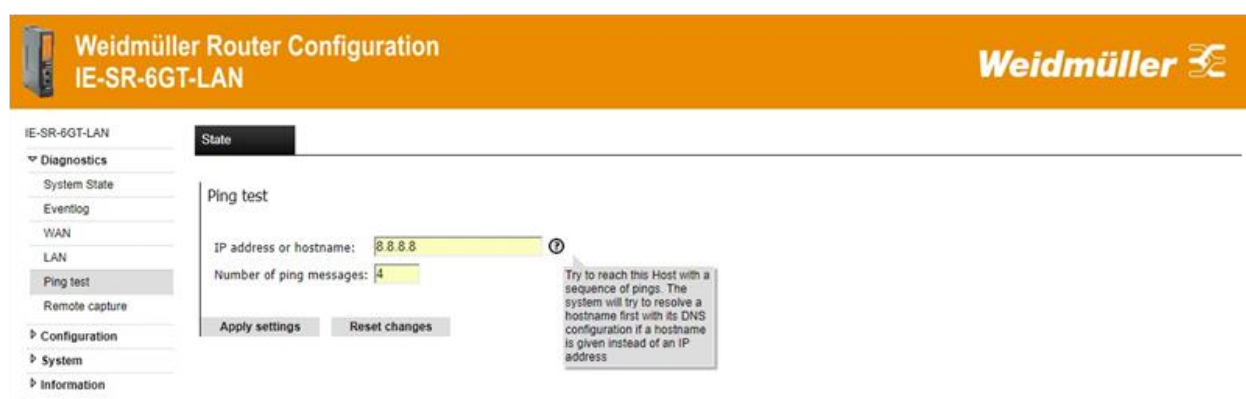
Transmitted dropped packets: 0

Transmitted overrun packets: 0

Buttons: Reload, Disconnect

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

4.1.7 Diagnostics → Ping test



Weidmüller Router Configuration
IE-SR-6GT-LAN

Ping test

IP address or hostname: 8.8.8.8


Number of ping messages: 4

Buttons: Apply settings, Reset changes


Try to reach this Host with a sequence of pings. The system will try to resolve a hostname first with its DNS configuration if a hostname is given instead of an IP address

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

Example of result of a ping test:



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

- Diagnostics
- Configuration
- System
- Information

User: admin

Result


```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=58 time=25.628 ms
64 bytes from 8.8.8.8: seq=1 ttl=58 time=24.694 ms
64 bytes from 8.8.8.8: seq=2 ttl=58 time=24.919 ms
64 bytes from 8.8.8.8: seq=3 ttl=58 time=24.716 ms


--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 24.694/24.989/25.628 ms
                
```

Continue...

4.1.8 Diagnostics → Remote capture



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

- ▾ Diagnostics
 - System State
 - Eventlog
 - WAN
 - LAN
 - Ping test
 - Remote capture**
- Configuration
- System
- Information

User: admin

Configuration

Remote capture


Enable remote capture server: ☒ ?

Client address: ?

Enable hub mode on LAN-out: ☐ ?




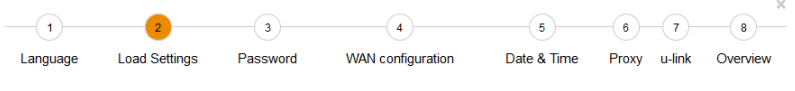
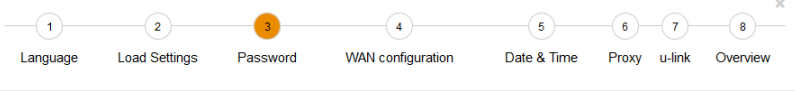
Verbose logging: ☐ ?

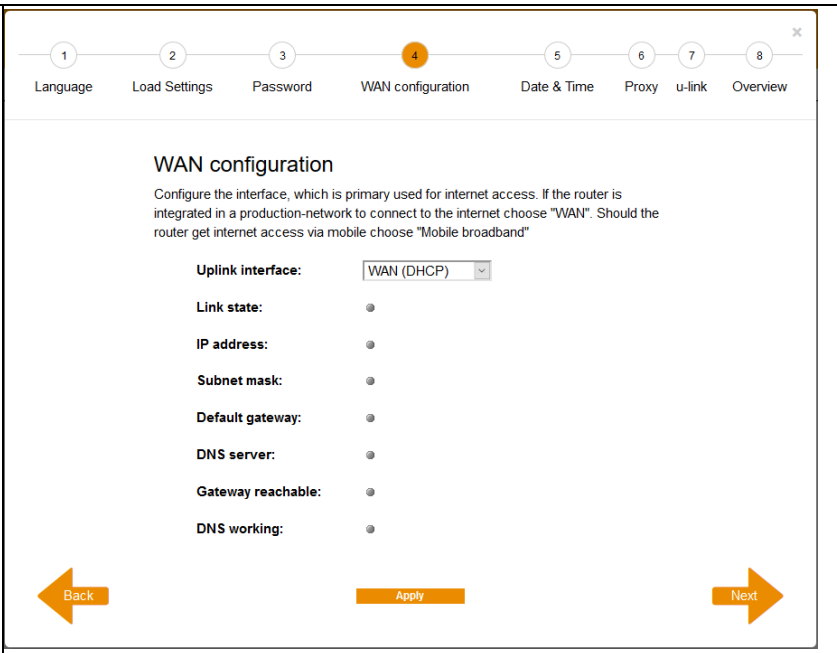
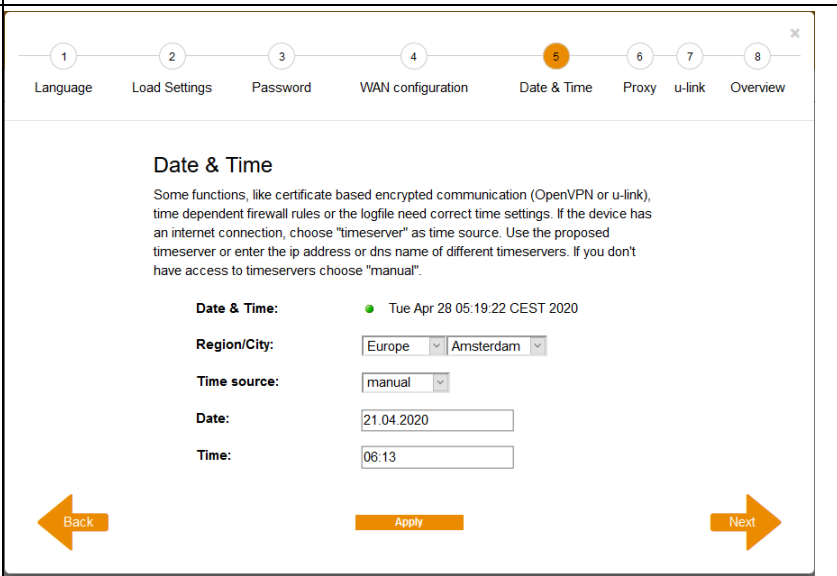
Menu	Diagnostics → Remote capture	
Function	By using the "remote capture" function data packets on both the LAN and the WAN port of the Router can be recorded for diagnostic purposes. The receiver of the diagnostic data is a PC/Server which must have installed the tool "Wireshark" listening on Port 2002. How to use please refer to application note in Appendix A .	
	Enable remote capture server	Enables the function
	Client address	IP address of permitted remote capture client (e.g. your service pc)
	Verbose logging	By default only access violations are logged (wrong client IP address or second connection attempt). With this option information about connections and requests are also logged.

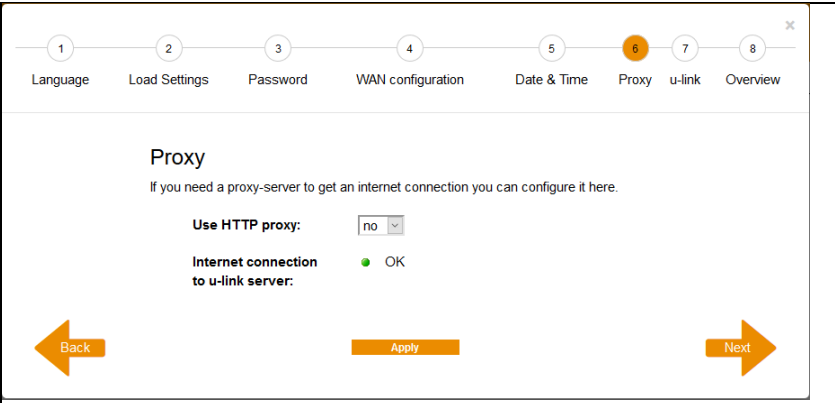
	Note
	No authentication is possible for remote capture. Therefore, this feature should only be activated for a limited time during diagnosis.

4.2 Section Configuration

4.2.1 Configuration → Config Wizard

Menu	Configuration → Config Wizard
Function	<p>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.</p> <div> <div> Language </div> <div>  </div> <div> <p>Language</p> <p>Please choose the language of the user interface</p> <div>   </div> </div> <div> <p>Setting the language of the Router Web interface</p> </div> </div> <div> <div> Load settings </div> <div>  </div> <div> <p>Load Settings</p> <p>If you have an existing settings file you can provide it here. Otherwise proceed the wizard by clicking "Next".</p> <p>Settings file: <input type="text" value="Durchsuchen..."/> Keine Datei ausgewählt.</p> <div> Back Apply Next </div> </div> <div> <p>Load a configuration file created before.</p> </div> </div> <div> <div> Password </div> <div>  </div> <div> <p>Password</p> <p>Please enter a secure password for the user "admin". It should contain at least 8 characters and consists of a combination of upper and lower case letters, numbers and special characters</p> <p>Enter new password: <input type="text"/></p> <p>Confirm password: <input type="text"/></p> <div> Back Apply Next </div> </div> <div> <p>Change the default password to a new one. It is recommended to change default passwords for security reasons.</p> </div> </div>

	<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 & 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>

	<h2>Proxy</h2>	 <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>
	<h2>u-link</h2>	www.u-link.weidmueller.com and create a router-object to get a Registration code.' Below this, there is a 'Registration code:' input field containing 'TMENHTAUTJXZ'. There are four status indicators: 'Internet connection to u-link server:' (green dot, OK), 'Registration state:' (green dot, registered), 'u-link Heartbeat:' (green dot, Connected), and 'u-link VPN connection state:' (green dot, Connected to u-link VPN server). At the bottom, there are 'Back', 'Apply', and 'Next' buttons." data-bbox="366 312 892 571"/> <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 www.u-link.weidmueller.com and create a router-object to get a Registration code.</p> <p>The status LED's will turn green, if settings work.</p>

Overview

1

Language

2

Load Settings

3

Password

4

WAN configuration

5

6

7

8

Overview

Link state:

● WAN: 100Mb/s

IP address:

● 192.168.43.222

World-wide heartbeat connectivity:

● OK

u-link Heartbeat:

● Connected

u-link VPN connection state:

● Connected to u-link VPN server.

Disconnect

Back

Download settings


Save settings

Summarizes your settings. Download Settings to store the configuration or to load this configuration into another router. Save settings to activate the settings on this router.

The status LED's will turn green, if settings work.

4.2.1 Configuration → IP Configuration

IP Configuration → Operational mode “IP Router”



Weidmüller Router Configuration
IE-SR-2GT-LTE/4G

W

IE-SR-2GT-LTE/4G

▸ Diagnostics

▾ Configuration

IP configuration

SecureNow!

Packet filter

Cut & Alarm

▸ General settings

▸ Access control

▸ Network

▸ VPN

▸ Services

▸ Prioritization

▸ System

▸ Information

User: admin

Configuration

IP configuration

Operational mode: IP router

WAN:

IP assignment: DHCP

☒ DNS via DHCP

☒ Gateway via DHCP

IP address:

Subnet mask:

NAT (Masquerading): ☒

LAN:

IP assignment: static

IP address:

Subnet mask:

NAT (Masquerading): ☒

4G:

Dialmode: permanent

PIN:

Provider APN:

Username:

Password:

DNS via 4G: ☐

NAT (Masquerading): ☒

Gateway via 4G: ☐

Default gateway:

IP address:

Apply settings
Reset changes

Screenshot shows factory default operation mode ‘IP Router’.

At factory default all 2-Port Routers do have configured static IP 192.168.2.110 at WAN port.

At factory default all 6-Port Routers do have configured the DHCP mode for getting an IP address.

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

Section 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.

Menu	Configuration → IP configuration	
Function	This is the main configuration window for setting the operating mode and the network configuration (Assignment of IP data on LAN / WAN ports and optional 4G interface).	
Operational mode	<p>IP Router: Supports routing functions (Layer 3) between WAN and LAN port(s). For 6-port models, the two WAN-Ports and the four LAN-ports act each as unmanaged switch. The IP address ranges of WAN and LAN side must not be the same.</p> <p>Transparent bridge: The device is acting like a layer 2 bridge and is transparent within a switched network. All Ethernet ports (LAN and WAN) behave like a common unmanaged Ethernet Switch. Only 1 IP address will be configured for accessing the web interface. This mode typically will be used for Layer 2 firewall application based on Ethernet frames (including IP packet control).</p>	
LAN / WAN IP assignment	<p>All interfaces can be configured with static or dynamic (DHCP) IP addresses.</p> <p>Static: Assign a static IP address and subnet mask to the interface.</p> <p>DHCP: Request an IP address from a DHCP (Dynamic Host Configuration Protocol) server.</p> <p>DHCP + fallback: First, try to request an IP address by DHCP and if it fails use the static one.</p> <p>PPPoE: The IP address will be assigned by the provider.</p>	
4G (optional)	Configuration of 4G network connection	

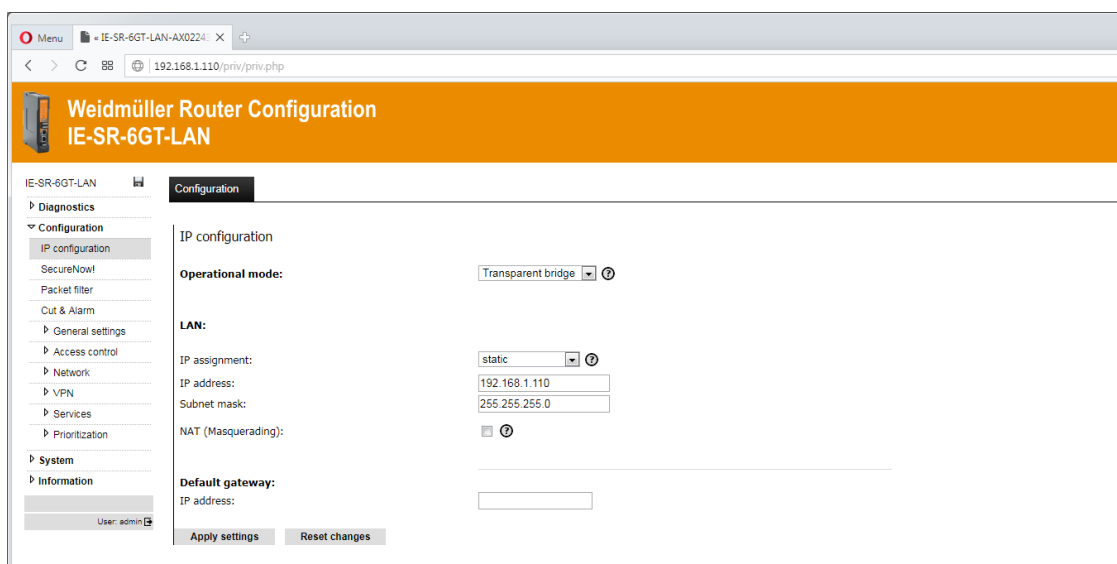
Dialmode	<p>Disabled: Do not use 4G modem.</p> <p>Manual: Dialing can be triggered manually from 4G status page.</p> <p>Permanent: The 4G link will be established automatically on system boot.</p> <p>Fallback: The 4G link will go online if the monitoring on the given interface "Fallback for interface" 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. NAT is always activated for 4G modem.
Gateway via 4G	If activated as soon as mobile connection is active (Online) it will be used as the Router's default gateway.
Default gateway	<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>

IP Configuration → Operational mode "Transparent bridge"

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

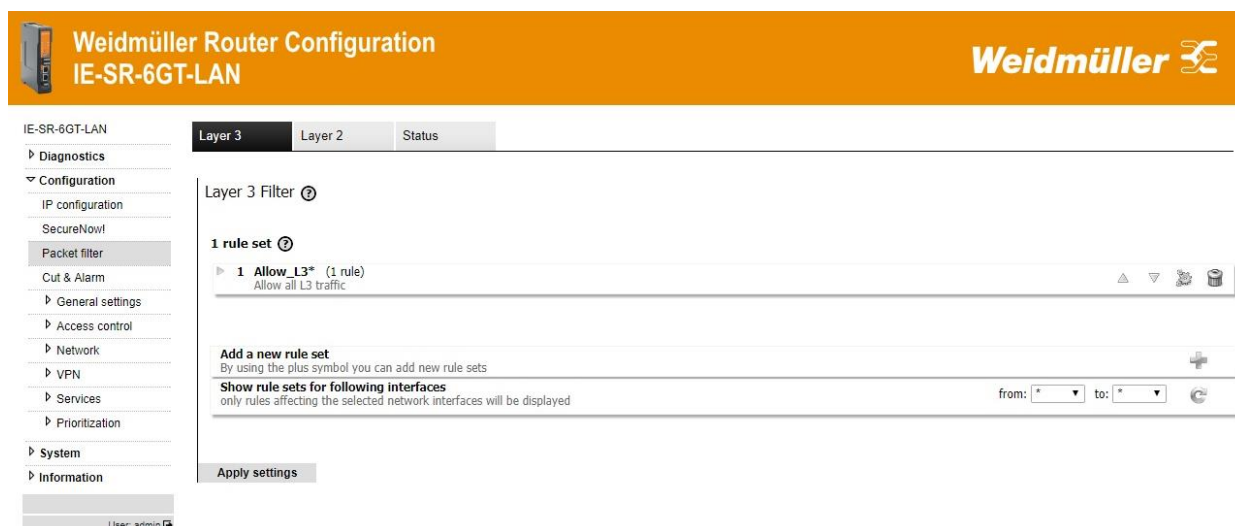
Only 1 IP address will be configured for accessing the web interface independent of the Ethernet port to which the configuration PC is connected.

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



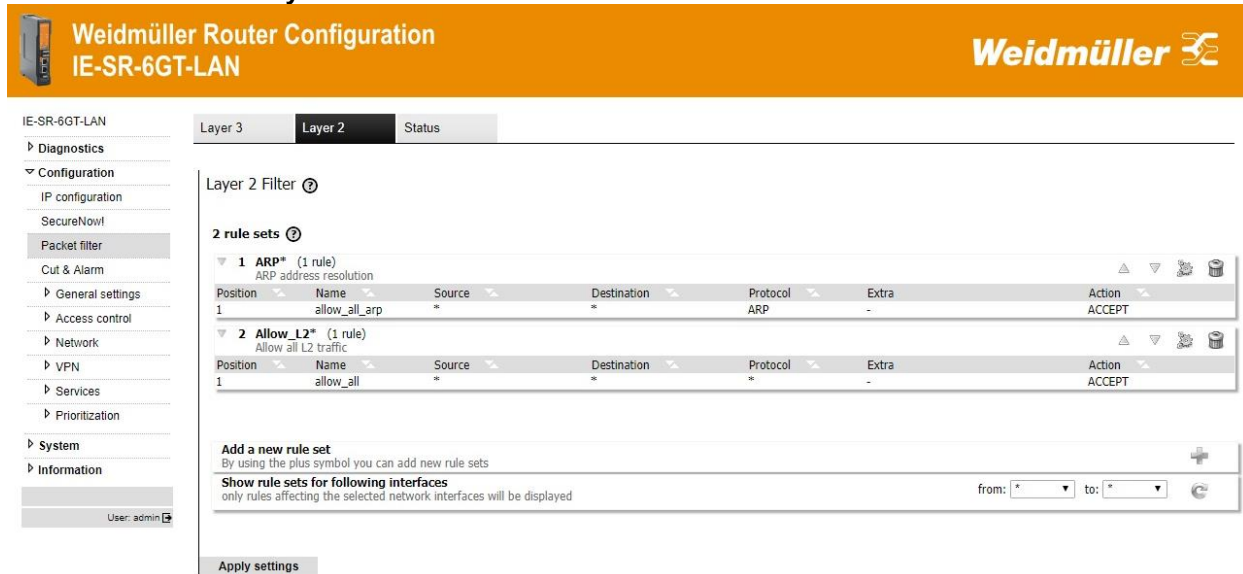
4.2.3 Configuration → Packet filter (Firewall)

Packet filter → Tab Layer 3



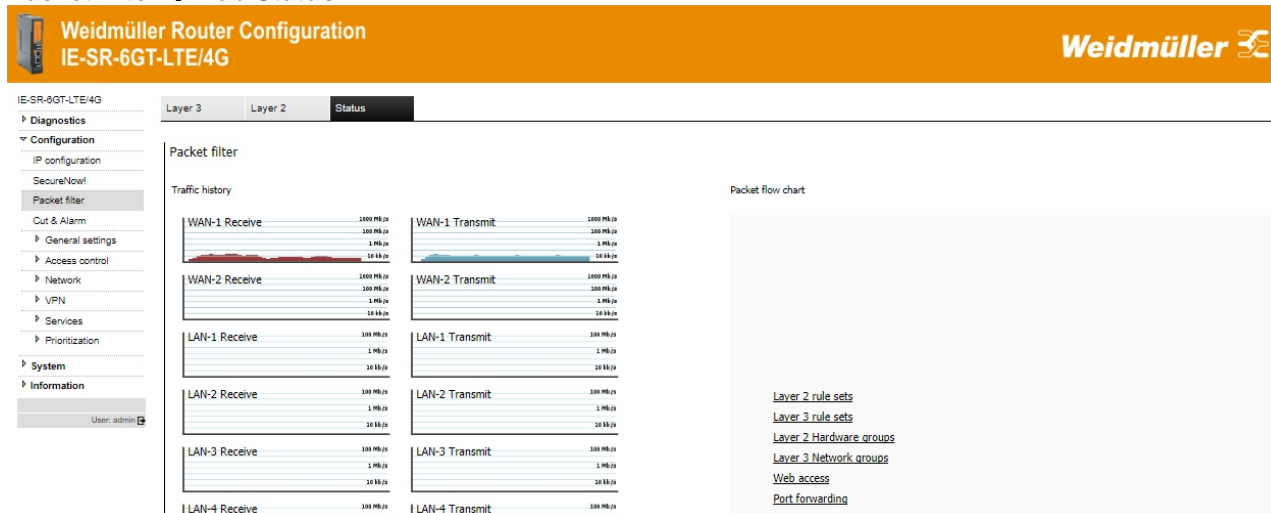
Menu	Configuration → Packet filter → Tab „Layer 3“
Function	<p>This is the window for the manual configuration of firewall filter rules based on Layer 3 (IP layer). The screenshot shows the firewall settings as delivered with the default rule "Allow_L3*". This rule says that any IP protocol (*) and any 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



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

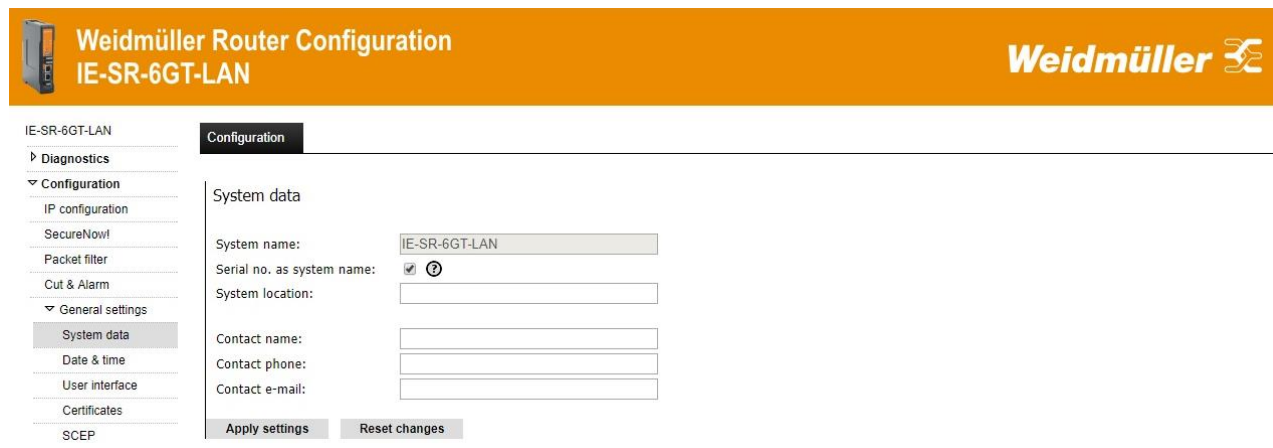
Packet filter → Tab Status



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

4.2.5 Configuration → General settings

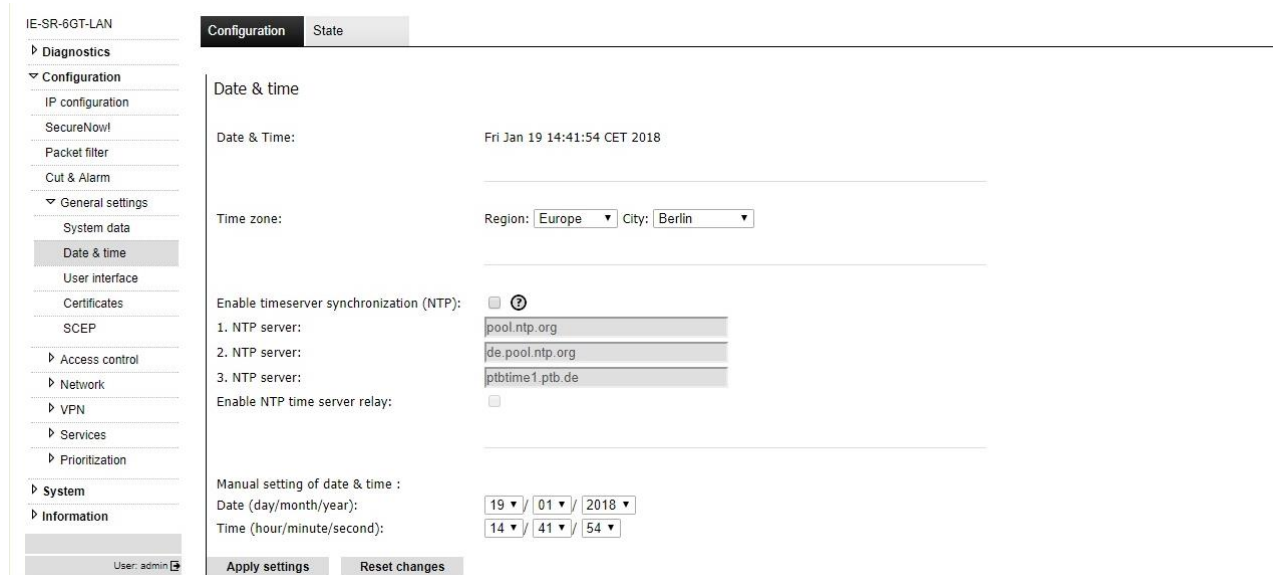
General settings → System data




Menu	Configuration → General settings → System data	
Function	Configuring application-related data of the Router (free text).	
	System name	Name of the router (by default the Router model name). Can be edited if checkbox 'Serial no. as system name' is disabled. <u>Note:</u> 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-2GT-LAN-AX02254366).

General settings → Date & Time


Date & Time → Tab Configuration




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.	

Note
 <ol style="list-style-type: none"> The Router has no battery-buffered, but a capacity-buffered system clock. <u>General behavior of date/time settings:</u> During operation the Router will save its current date/time (either based on manual input or by NTP update) each hour into the flash memory. After next power-up the Router will restore the internal system clock with the date/time value last saved into the flash memory. If no NTP update is enabled then the system clock will run based on the last stored date/time.

Date & Time → Tab State


Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

Configuration
State

Diagnostics
Configuration
IP configuration
SecureNow!
Packet filter
Cut & Alarm
General settings
System data
Date & time
User interface
Certificates
SCEP

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)
5.9.110.236	131.188.3.222	2	u	3	64	1	42.806	22.174	0.061
78.46.93.106	126.94.231.148	2	u	3	64	1	39.714	23.561	0.061
*192.53.103.108	.PTB.	1	u	3	64	1	34.984	29.299	0.061

Reload

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

General settings → User Interface


Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

Configuration

Diagnostics
Configuration
IP configuration
SecureNow!
Packet filter
Cut & Alarm
General settings
System data
Date & time
User interface

User interface


Choose language and apply mode:

Language: English
Save and apply: apply immediately & do not save


Apply settings
Reset changes

Menu		Configuration → General settings → User interface
Function	Language Save and apply: <ul style="list-style-type: none"> Apply immediately and do not save Save only and do not apply 	Setting the language (German or English) of the Web interface. Changes will be immediately activated but not saved. The new activated changes have to be saved explicitly in menu System → Save. Using this mode all changes will only be saved but not activated. The changes come into effect after a restart.

General settings → Certificates



Weidmüller Router Configuration
IE-SR-6GT-LAN

Weidmüller 



IE-SR-6GT-LAN
 ▸ Diagnostics
 ▾ Configuration
 IP configuration
 SecureNow!
 Packet filter
 Cut & Alarm
 ▾ General settings
 System data
 Date & time
 User interface
 Certificates
 SCEP
 ▸ Access control
 ▸ Network
 ▸ VPN
 ▸ Services
 ▸ Prioritization
 ▸ System
 ▸ Information

User: admin







Configuration

Certificates

Trusted root certification authorities:

Certificate	CRL status ?	validity
▸ DEMO-CN (demoCA.pem)	CRL not found	invalid ? 
▸ Big-LinX Signing Certificate (idascepcapca.pem)	CRL not found	valid 

Device certificates:

Certificate	validity
▸ DEMO-CN1 (demo-client1.pem)	invalid ? 
▸ DEMO-CN2 (demo-client2.pem)	invalid ? 
▸ DEMO-CN3 (demo-client3.pem)	invalid ? 
▸ DEMO-CN4 (demo-client4.pem)	invalid ? 
▸ DEMO-CN5 (demo-client5.pem)	invalid ? 
▸ IE-SR-6GT-LAN-AX02243509 (identity.pem)	valid 

Upload local certificate file for authentication or CRL:

Filename (*.p12 / *.pfx / *.pem / *.crt):
 Certificate password for validation:

Choose File

No file chosen

?

Upload certificate

Apply settings

Reset changes

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.	

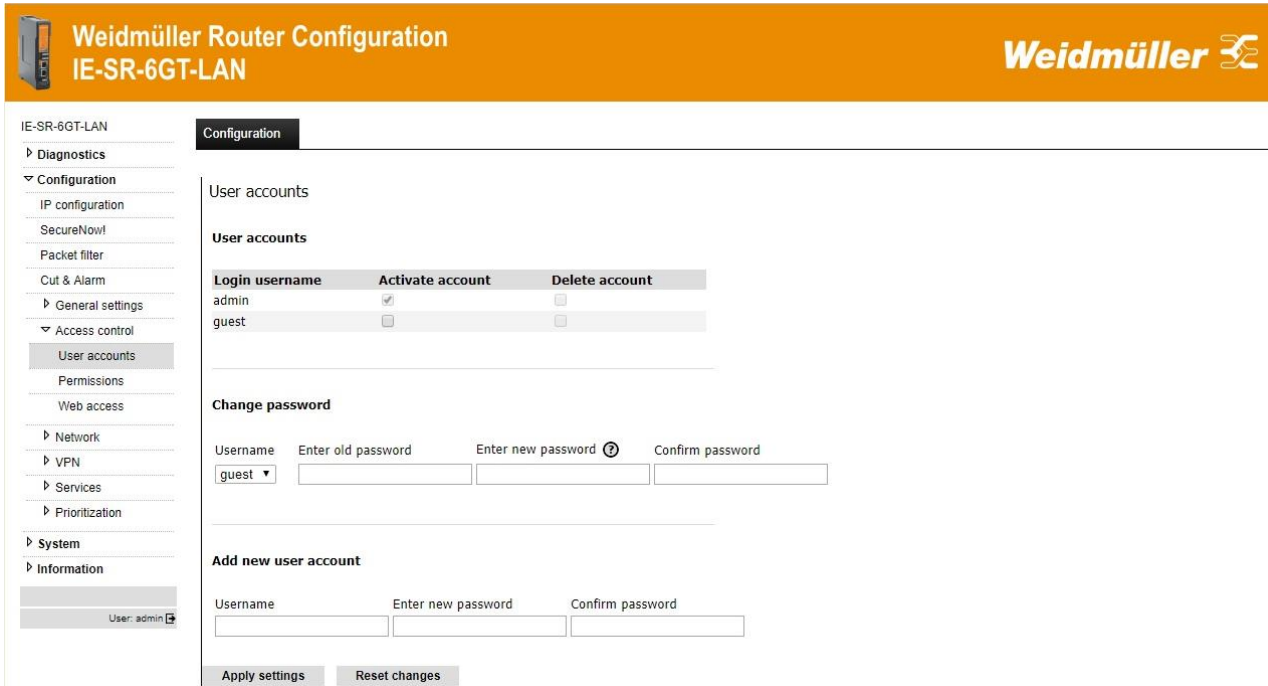
General settings → SCEP (Tab State)



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

4.2.6 Configuration → Access Control

Access Control → User accounts



Weidmüller Router Configuration
IE-SR-6GT-LAN

Configuration

IE-SR-6GT-LAN

- Diagnosics
- Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - User accounts**
 - Permissions
 - Web access
 - Network
 - VPN
 - Services
 - Prioritization
- System
- Information

User: admin

User accounts

Login username	Activate account	Delete account
admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>
guest	<input type="checkbox"/>	<input type="checkbox"/>

Change password

Username: Enter old password: Enter new password: Confirm password:

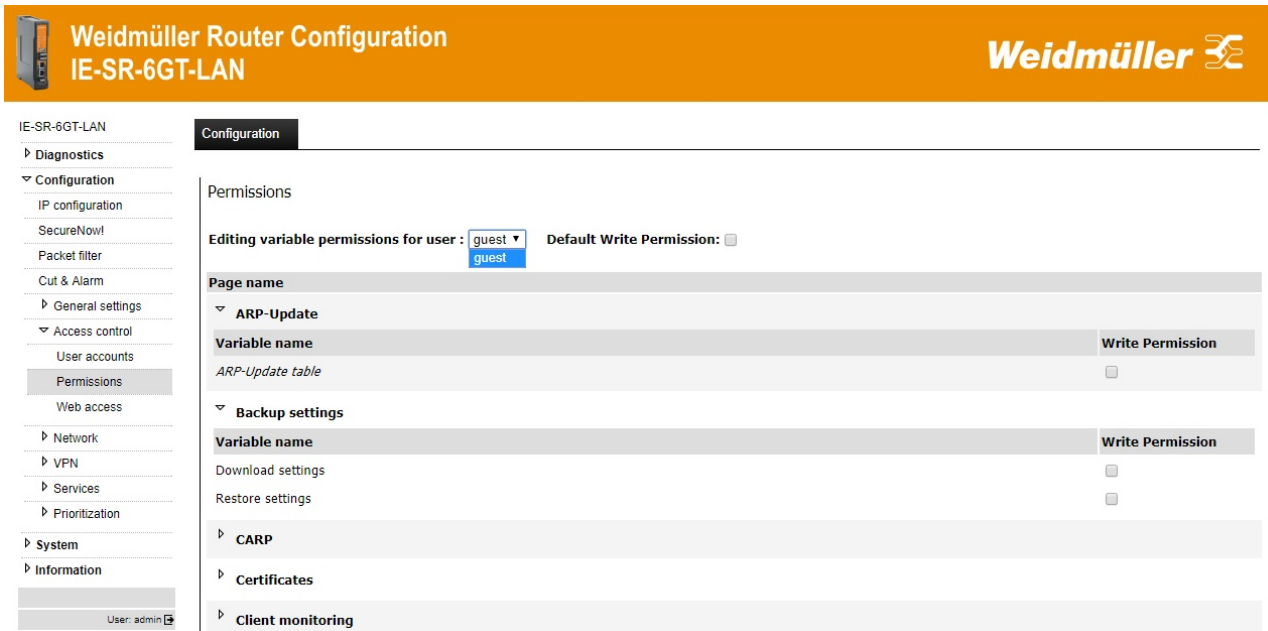
Add new user account

Username: Enter new password: Confirm password:

Apply settings Reset changes

Menu	Configuration → Access control → User accounts
Function	Create and delete other user accounts Note: The Administrator account always has full access. It cannot be deleted.

Access Control → Permissions



Weidmüller Router Configuration
IE-SR-6GT-LAN

Configuration

IE-SR-6GT-LAN

- Diagnosics
- Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - User accounts
 - Permissions**
 - Web access
 - Network
 - VPN
 - Services
 - Prioritization
- System
- Information

User: admin

Permissions

Editing variable permissions for user: Default Write Permission: ☐

Page name

ARP-Update

Variable name	Write Permission
ARP-Update table	<input type="checkbox"/>

Backup settings

Variable name	Write Permission
Download settings	<input type="checkbox"/>
Restore settings	<input type="checkbox"/>


CARP

Certificates


Client monitoring

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-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN
Diagnostics
Configuration
IP configuration
SecureNow!
Packet filter
Cut & Alarm
General settings
Access control
User accounts
Permissions
Web access

Configuration

Web access

Allow protocol access on interface

	WAN-1	WAN-2	LAN	u-link
HTTP:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HTTPS:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


Report access violations using syslog ☒

Apply settings Reset changes


Menu	Configuration → Access control → Web access
Function	<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>

4.2.7 Configuration → Network

Network → DNS (Tab Configuration)



Weidmüller Router Configuration IE-SR-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN
Diagnostics
Configuration
IP configuration
SecureNow!
Packet filter
Cut & Alarm
General settings
Access control
Network
DNS
IP routing
HTTP proxy
Forwarding
1:1 NAT
Network groups
Hardware groups
Ethernet

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: ☒ WAN-1 ☒ WAN-2 ☒ LAN ☒ u-link

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 st , 2 nd , 3 rd 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.
	Enable DNS proxy	Device acts as DNS server and will forward DNS requests to the configured DNS servers. Please ensure that the DNS proxy is only running on the required (internal) interfaces.
	DNS proxy interfaces	Select which interfaces shall forward DNS requests to defined DNS server

Network → DNS (Tab State)




IE-SR-6GT-LAN

- Diagnostics
- ▼ Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - ▼ Network
 - DNS**

Configuration

State

DNS

Current DNS configuration

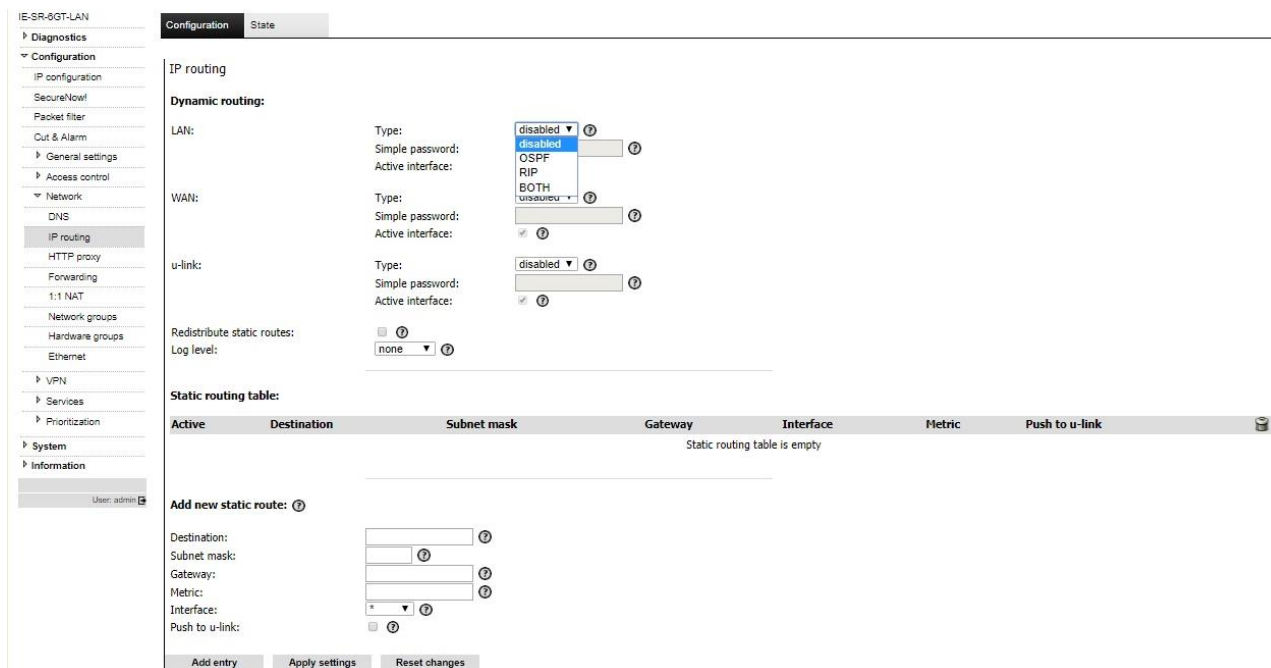
Domain suffix: fritz.box

Nameserver: 192.168.99.1

[Reload](#)

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

Network → IP Routing (Tab Configuration)



IP routing

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 ⓘ

Static routing table:

Active	Destination	Subnet mask	Gateway	Interface	Metric	Push to u-link
Static routing table is empty						

Add new static route: ⓘ

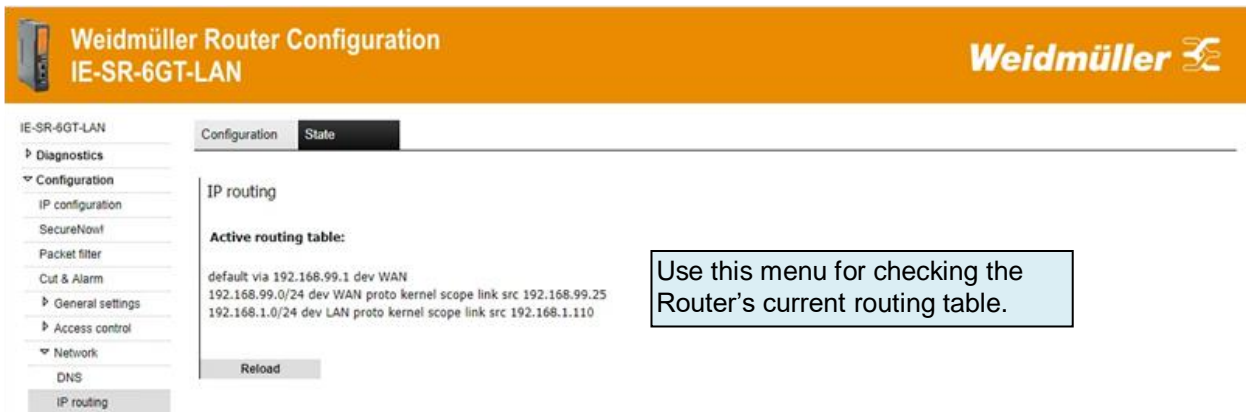
Destination: ⓘ
Subnet mask: ⓘ
Gateway: ⓘ
Metric: ⓘ
Interface: ⓘ
Push to u-link: ☐ ⓘ

Add entry 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">- RIP the Routing Information Protocol is frequently used and helps routers to dynamically adapt to changes- OSPF Open Shortest Path First is newer and make RIP obsolete- Both Select this if you want to use both protocols at a time	
	Dynamic Routing Simple Password	This field is optional. The OSPF/RIP simple password authentication will protect all packets with this password. Note that this password will be send as clear text! It is only meant to prevent misconfigured routers to be placed on the network.	
	Dynamic Routing Active interface	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	

	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 Subnet mask	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 In- terface	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 State)



Weidmüller Router Configuration
IE-SR-6GT-LAN

Weidmüller

IE-SR-6GT-LAN

Configuration State

IP routing

Active routing table:

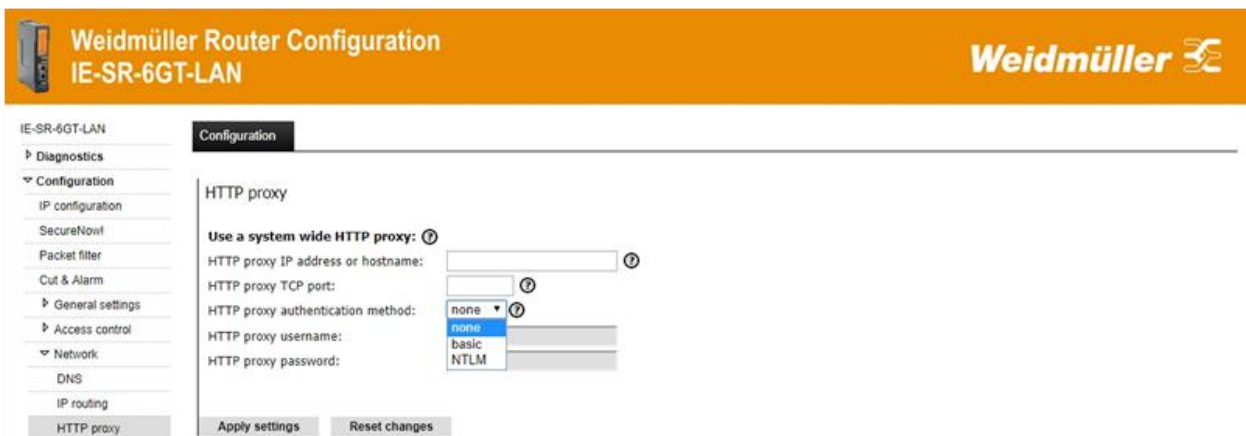
default via 192.168.99.1 dev WAN
192.168.99.0/24 dev WAN proto kernel scope link src 192.168.99.25
192.168.1.0/24 dev LAN proto kernel scope link src 192.168.1.110

Reload

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

Menu	Configuration → Network → IP Routing → Tab „State“
Function	<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><Target Network> dev <interface> proto kernel scope link src <interface IP address ></p> <p>Means: <Target Network> is accessible via <IP address> of device <interface></p>

Network → HTTP proxy



Weidmüller Router Configuration
IE-SR-6GT-LAN

Weidmüller

IE-SR-6GT-LAN

Configuration

HTTP proxy

Use a system wide HTTP proxy:

HTTP proxy IP address or hostname:

HTTP proxy TCP port:

HTTP proxy authentication method:

HTTP proxy username:

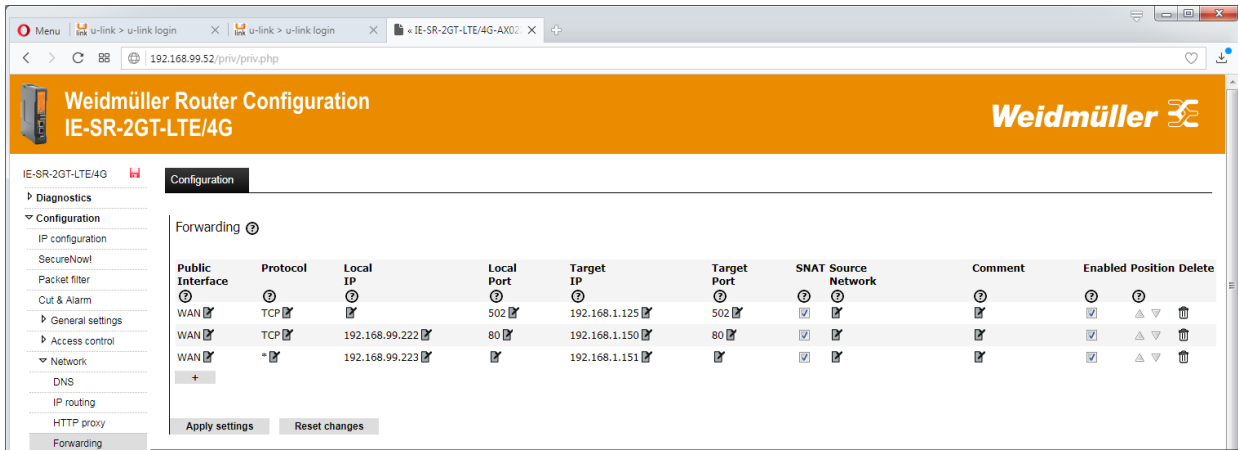
HTTP proxy password:

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



Forwarding

Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT Source Network	Comment	Enabled	Position	Delete
WAN	TCP		502	192.168.1.125	502	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	▲ ▼	🗑
WAN	TCP	192.168.99.222	80	192.168.1.150	80	<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 3 defined Forwardings. Current Router IP settings: LAN IP 192.168.1.110 / 24, WAN IP 192.168.99.52 / 24

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

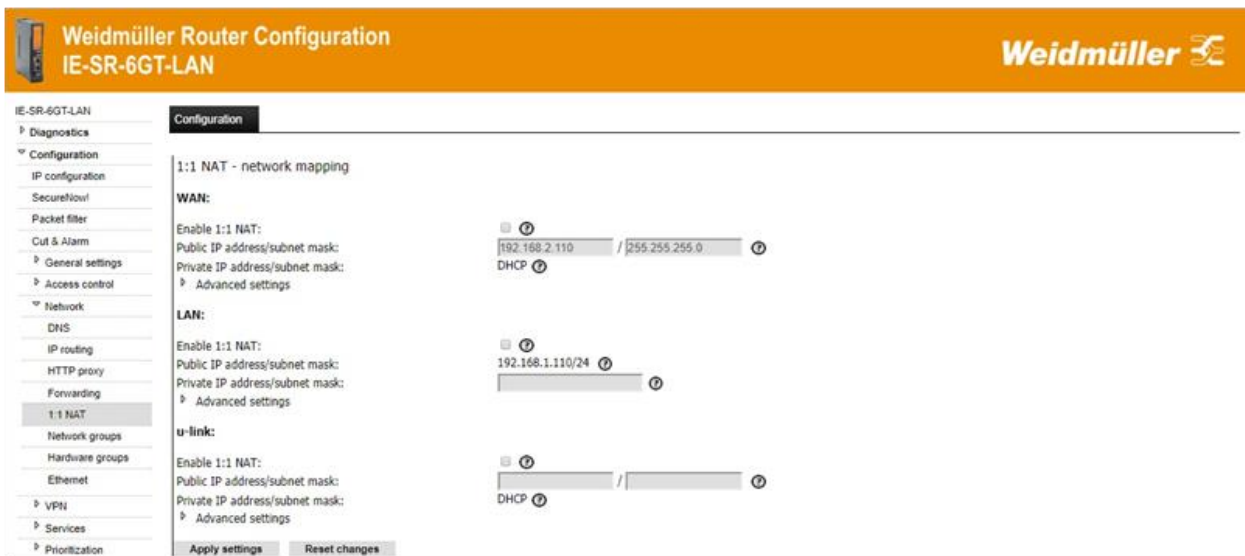
Entry 2: Router will accept and forward any IP packet - addressed to **virtual** WAN IP 192.168.99.222 with protocol TCP and port 80 – to IP 192.168.1.150 with protocol TCP and port 80 (outgoing via LAN port).

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

Menu	Configuration → Network → Forwarding	
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. Please take care of the position of each row, as the table is progressed from the top to the bottom for each packet until a match is found. If you run a restricting packet filter you must open the data paths there too. The packet filter will see the forwarding target as destination and always the original source independent of the SNAT checkbox.</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	Enter a free available IP address which will behave as an additional (virtual) IP address of the selected “Public Interface” (mostly WAN). In case of physical interfaces this address is most likely one of the public interface range. In case of OpenVPN or IPsec interfaces it should be one of the VPN address range. The device will take this additional IP address as its own and will forward the traffic - addressed to this IP – to defined Target IP. This option cannot be used on 4G or DSL links. If you leave it empty, the current IP address of the defined (incoming) interface will be used as ‘Local IP’.
	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.
	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	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. <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. 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.
Note after editing a value, press accept ✓ or delete x, otherwise the message “Syntax error applying data” will appear.		

Network → 1:1 NAT




Menu	Configuration → Network → 1:1 NAT	
Function	<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. 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>For more detailed information about using 1:1 NAT please refer to application notes in appendix A.</p>	
Enable 1:1 NAT	Enable 1:1 NAT for this interface.	Note: 1:1 NAT only can be activated if NAT (masquering) is not enabled for this interface
Public IP address	This is the public interface IP address and subnet mask as defined in menu 'IP Configuration', e.g. 192.168.1.110/24. If DHCP is enabled, you must define a network to which the IP addresses received via DHCP will be mapped.	
Private IP address	The definition of the private subnet is the private device IP with the subnet mask appended. E.g. 192.168.0.110/24 means, that the device itself is reachable as 192.168.0.110 from the private subnet 192.168.0.0/24	
Enable double sided network mapping	With this extension, (private) IP address conflicts can be solved if public hosts use IP addresses from the same subnet as the 1:1 NAT private subnet. Where possible, you should not use such a subnet for 1:1 NAT private subnet, but sometimes the private subnet is already defined through the according network components. This conflict will be solved by using a further subnet that is not used anywhere else, neither on public nor on private subnets.	
Substitute with IP address/subnet mask	A subnet, preferably of the same size as the according private 1:1 NAT subnet. Will be used for translating private IP addresses on public interfaces to a subnet of IP addresses that is otherwise not used. Therefore, only IP source address for packets going to the according private subnet will be changed. This option is not necessary if the private subnet is not used on public interfaces.	

Network → Network Groups



Weidmüller Router Configuration
IE-SR-6GT-LTE/4G



IE-SR-6GT-LTE/4G

- Diagnostics
- ▼ Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - ▼ Network
 - DNS
 - IP routing
 - HTTP proxy
 - Forwarding
 - 1:1 NAT
 - Network groups**
 - Hardware groups
 - Ethernet

Configuration

Network groups

▼ **Machine1** used in 0 rules

192.168.2.100/32 ✕
 192.168.2.102/32 ✕
 192.168.2.104/32 ✕

▼ **Machine2** used in 0 rules

192.168.2.101/32 ✕
 192.168.2.103/32 ✕

Group name:

Machine2 ?


Network address:

192.168.2.105/32 ?


Apply settings
Reset changes

Menu	Configuration → Network → Network groups	
Function	<p>Creating groups with "speaking" names for ranges of IP addresses (Layer 3). A network group always contains a range of IP addresses with specified subnet (e.g. 192.168.1.0/24). A network group can contain a set of single IP addresses and complete IP address ranges. Network groups can be used instead of IP address ranges if you will create firewall filtering rules (See menu Configuration → Packet filters → Layer 3). To add several IP address (ranges) to a group insert the same group name.</p>	
	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 <Apply settings> is triggered (or <Save settings> respectively)</p>

Network → Hardware Groups



Weidmüller Router Configuration
IE-SR-6GT-LAN



IE-SR-6GT-LAN

- Diagnostics
- ▼ Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - ▼ Network
 - DNS
 - IP routing
 - HTTP proxy
 - Forwarding
 - 1:1 NAT
 - Network groups
 - Hardware groups**

Configuration

Hardware groups

▸ no groups have been stored yet

add groups by using the form below

Group name:

?

Hardware address:

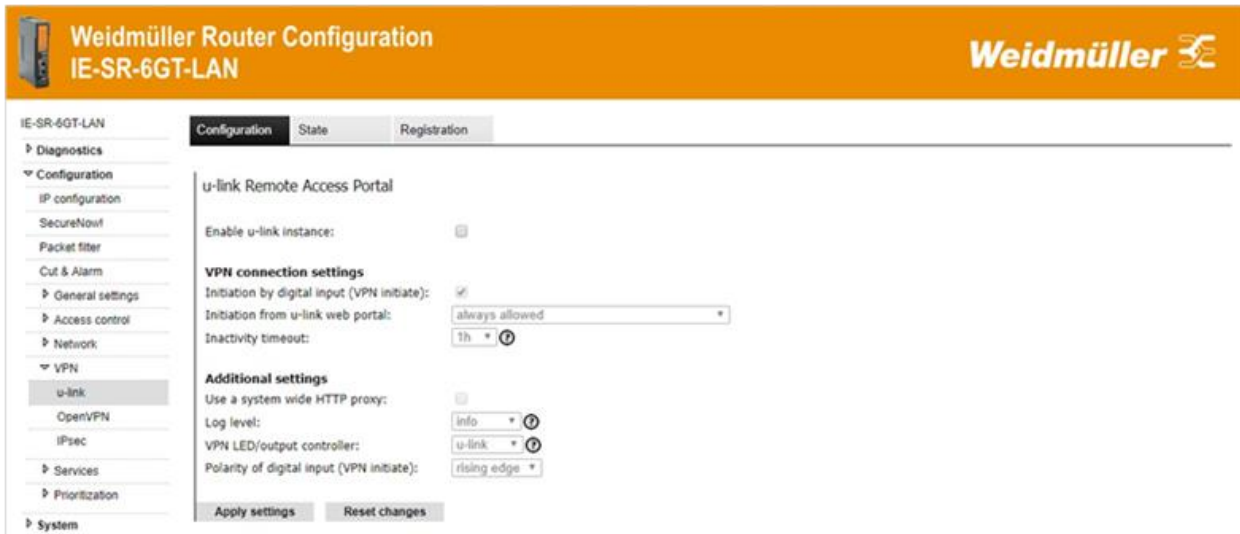
?

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)

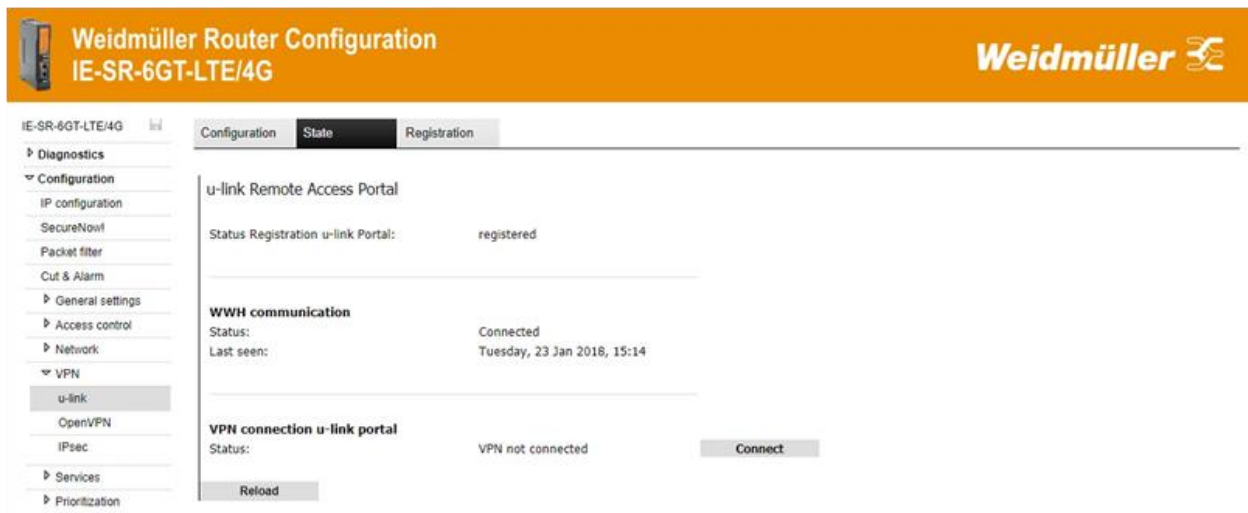
4.2.8 Configuration → VPN

VPN → u-link (Tab Configuration)



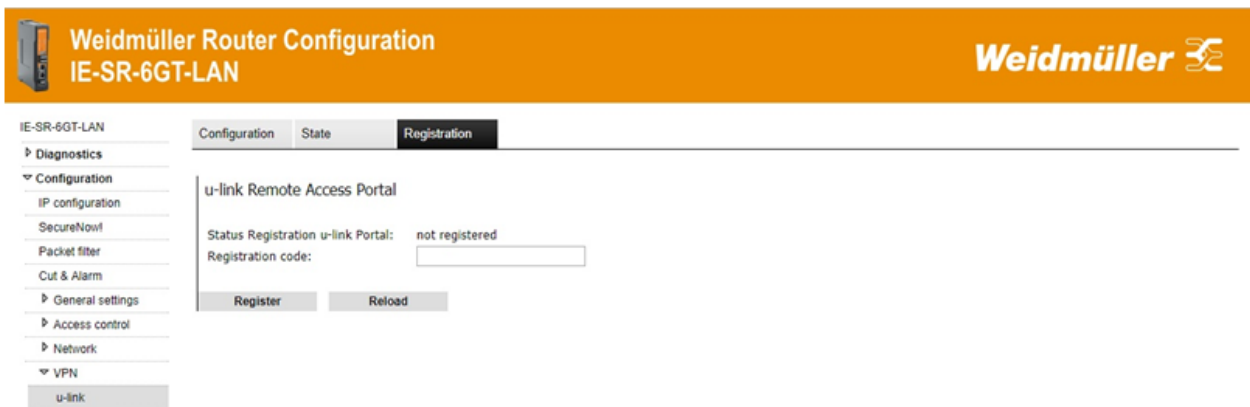
Menu	Configuration → VPN → u-link → Tab “Configuration”	
Function	Enable u-link instance	Enables the routers connectivity service to be used for the Weidmüller u-link Remote Access Service.
	Initiation by digital input (VPN initiate):	Allows/Denies to establish a VPN connection to the u-link platform by setting 24 VDC on digital input “VPN initiate”.
	Initiation from u-link web portal	<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 only if the external digital input (‘VPN initiate’ set to 24 VDC) is active.</p>
	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	<p><u>None:</u> Will log no messages through the Event Log</p> <p><u>Info:</u> Log only some information and critical errors</p> <p><u>Debug:</u> Log state information too</p> <p><u>Verbose:</u> Log all possible messages</p>
	VPN LED/output controller	<p><u>Disabled:</u> The LED and digital output are not used by u-link.</p> <p><u>u-link:</u> LED is <u>blinking</u> during connecting and <u>on</u> during connection, digital output “VPN active” is set to ON as long as the VPN tunnel is established.</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 → u-link (Tab State)




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

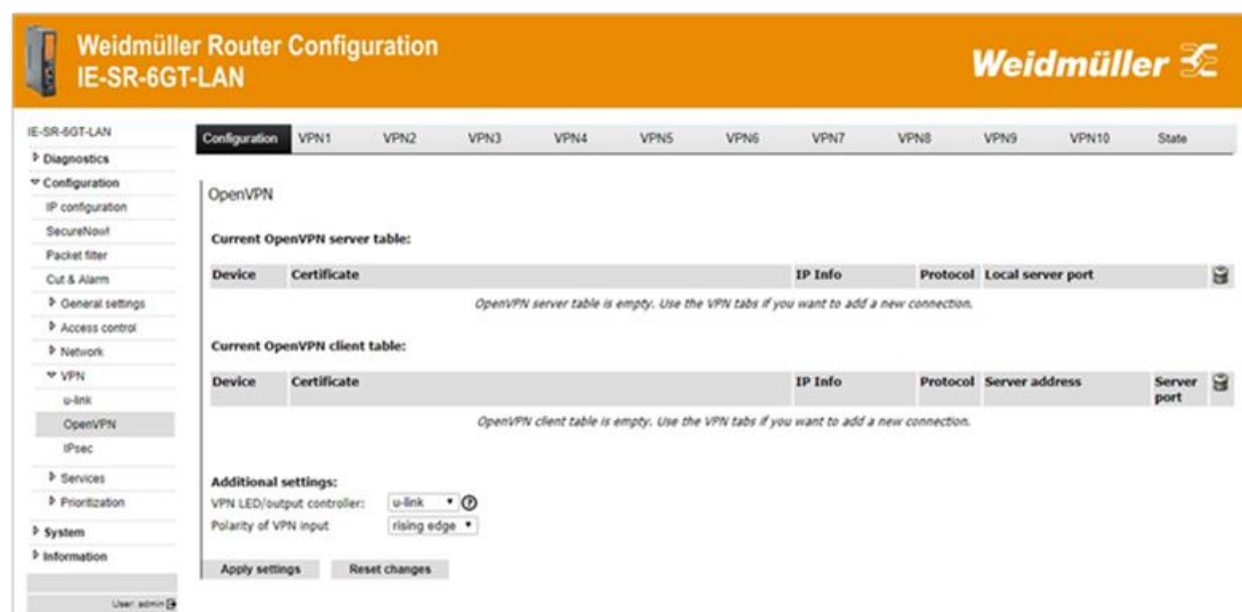
VPN→ u-link (Tab Registration)



Menu	Configuration → VPN → u-link → Tab “Registration”
Function	<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 (https://u-link.weidmueller.com) by adding a new router-item or the code of a previously used router-item in section Administration → Device management.</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 (u-link-support@weidmueller.com).</p>

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


VPN→ OpenVPN (Tab Configuration)




Menu	Configuration → VPN → OpenVPN → Tab „Configuration“
-------------	---

Function	<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/output controller	<p>Disabled: The LED and digital output are not used by u-link</p> <p>u-link: LED is blinking during connecting and on during connection, digital output is triggered by u-link</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-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN

- Diagnostics
- ▾ Configuration
 - IP configuration
 - Secureflow
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - Network
 - ▾ VPN
 - u-link
 - OpenVPN**
 - IPsec
 - Services
 - Prioritization
 - 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:
Server port:
Protocol: TCP
Certificate: scp-cert.pem
Authenticate with username and password: ☐
Username:
Password:
Pull routes from server: ☐
Use HTTP proxy: ☐

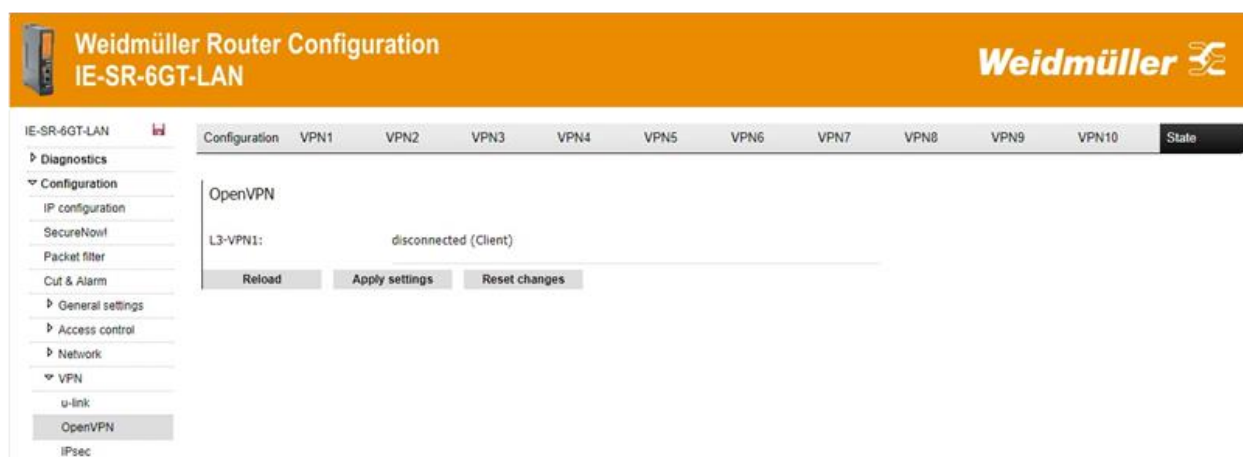
Additional settings
Log level: info
LZO compression: adaptive
Cipher: BF-CBC

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	<p>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.</p>

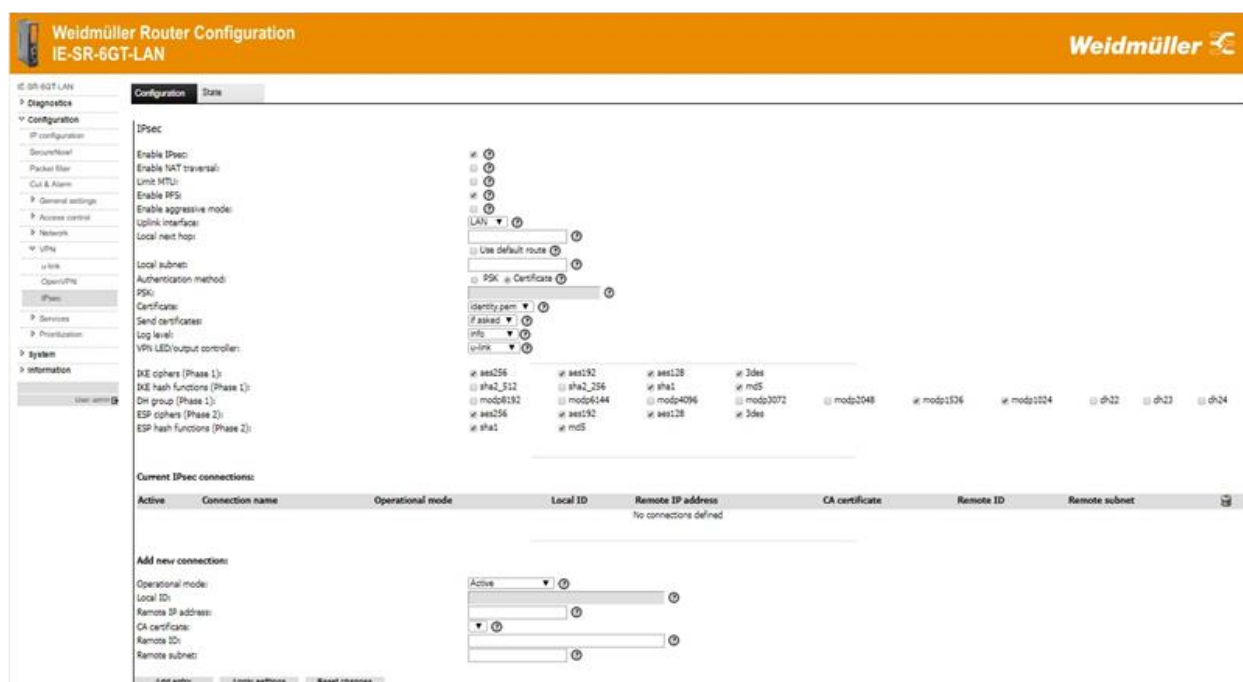
	Layer	The OpenVPN interface may operate on two different layers: Ethernet Layer (Layer 2), i.e. will be bridged with >LAN (interface)< IP Layer (Layer 3) with its own IP address which must be configured on the IP configuration page.
	OpenVPN device type	L3 interfaces can either be run as TUN or TAP devices. The latter 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
	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 providers 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).
	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
	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.

VPN → OpenVPN (Tab State)



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

VPN → IPsec (Tab Configuration)




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

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

	Remote ID	<p>The peer will identify (not authenticate) itself with this ID depending on the chosen 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
	<p>By default, the Router uses the parameters AES128, MD5, DH group 2 for Main-Mode and AES128, SHA1 for Quick-Mode.</p> <p>Authentication by „Aggressive-Mode is due to security reasons not supported!</p>

VPN → IPsec (Tab State)

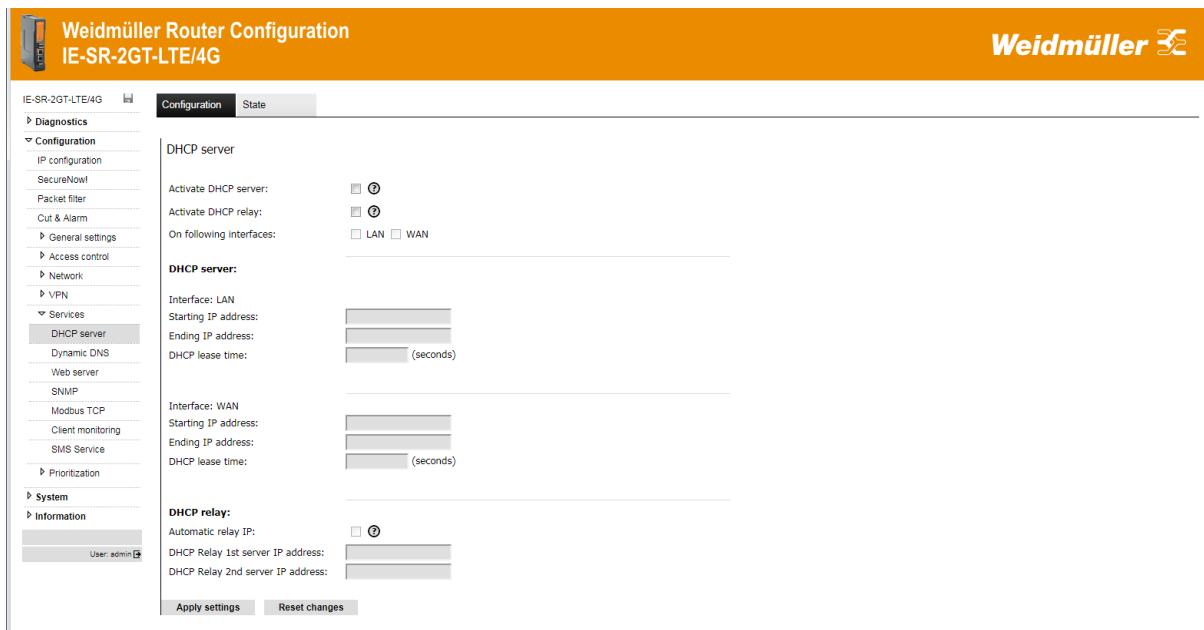


The screenshot shows the Weidmüller Router Configuration interface for the IE-SR-6GT-LAN model. The left sidebar contains a navigation menu with options like Diagnostics, Configuration, IP configuration, SecureNow!, Packet filter, Cut & Alarm, General settings, Access control, Network, VPN, u-link, OpenVPN, and IPsec. The main content area is titled 'IPsec' and shows the 'State' tab. It displays 'Current IPsec tunnels:' with a table header: 'Packets sent Local subnet Local endpoint Remote endpoint Remote subnet'. Below the header, it indicates 'No IPsec tunnels'. There is also a 'Detailed debug state' link and a 'Reload' button.

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

4.2.9 Configuration → Services

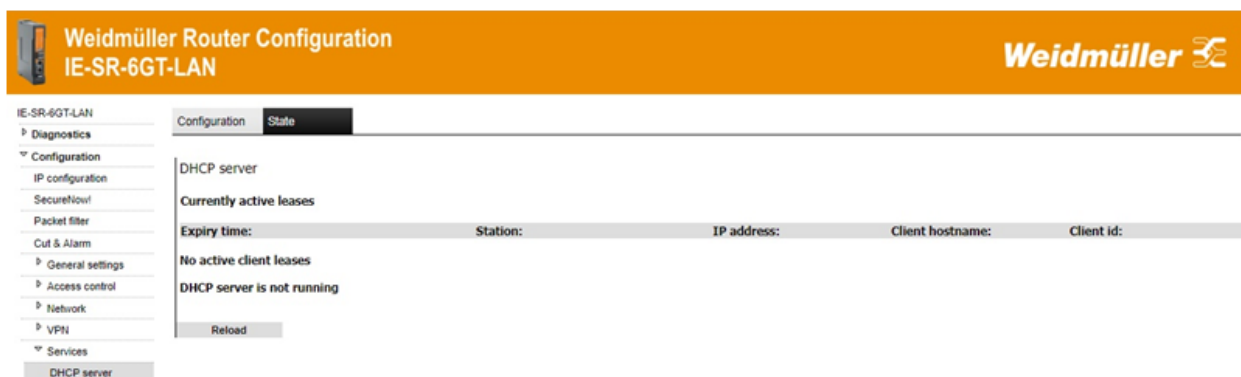
Services → DHCP Server (Tab Configuration)



The screenshot shows the 'Weidmüller Router Configuration' interface for the 'IE-SR-2GT-LTE/4G' model. The 'Configuration' tab is active, and the 'DHCP server' configuration page is displayed. The left sidebar shows a navigation menu with categories like 'Diagnostics', 'Configuration', 'Access control', 'Network', 'VPN', 'Services', 'System', and 'Information'. The 'DHCP server' configuration page includes sections for 'DHCP server' and 'DHCP relay'. The 'DHCP server' section has checkboxes for 'Activate DHCP server' and 'Activate DHCP relay', and a section for 'On following interfaces' with checkboxes for 'LAN' and 'WAN'. Below these are input fields for 'Interface: LAN', 'Starting IP address', 'Ending IP address', and 'DHCP lease time' (in seconds). The 'DHCP relay' section has a checkbox for 'Automatic relay IP' and input fields for 'DHCP Relay 1st server IP address' and 'DHCP Relay 2nd server IP address'. At the bottom, there are 'Apply settings' and 'Reset changes' buttons.

Menu	Configuration → Services → DHCP Server → Tab "Configuration"	
Function	In operating mode "IP Router", the built-in DHCP server can be used for allocating IP addresses on both LAN-side and WAN side. By default, the DHCP server is switched off.	
	Activate DHCP server	Enables the DHCP service. The device will answer to DHCP requests on the selected interfaces with the supplied IP address range and name server configuration. Note: The IP address range must be in the same IP subnet as the IP of the selected interface itself.
	Activate DHCP relay	Enables the DHCP relay service. The device will forward all incoming DHCP requests to the given DHCP server. Please ensure that the internal network (i.e. the network that is served by the relay) is reachable from the DHCP server.
	On following interfaces	Select the Interfaces that should use DHCP server or relay. Displayed interfaces depending on routing mode, integrated modem and virtual interfaces.
	Starting IP address	First IP address that can be assigned via DHCP
	Ending IP address	Last IP address that can be assigned via DHCP Note: Must be in the same IP subnet as Starting IP address.
	DHCP lease time	Value between 3.000 s and 700.000 s
	DHCP Relay	
	Alternatively, the Router can be configured as a DHCP relay. DHCP requests from clients which require an IP address are then forwarded to the "real" DHCP server.	
	Automatic relay IP	Use the DHCP server of the DHCP lease of the device itself. To make this option work at least one interface of the device itself must be configured as DHCP client.
	DHCP relay 1 st server IP address	IP address to which DHCP requests will be forwarded to.
	DHCP relay 2 st server IP address	IP address to which DHCP requests will be forwarded to if first DHCP server is not available.

Services → DHCP Server (Tab State)



The screenshot shows the 'Weidmüller Router Configuration' interface for device 'IE-SR-6GT-LAN'. The left sidebar contains a navigation menu with categories like 'Diagnostics', 'Configuration', 'General settings', 'Access control', 'Network', 'VPN', and 'Services'. Under 'Services', 'DHCP server' is selected. The main content area has two tabs: 'Configuration' and 'State', with 'State' being the active tab. The 'State' tab displays the DHCP server status, including 'Currently active leases' (none shown), 'No active client leases', and 'DHCP server is not running'. A 'Reload' button is visible at the bottom.

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

Services → Web server



The screenshot shows the 'Weidmüller Router Configuration' interface for device 'IE-SR-6GT-LAN'. The left sidebar is the same as in the previous screenshot, but 'Web server' is selected under the 'Services' category. The main content area has a 'Configuration' tab active, showing the 'Web server' settings. It includes a section for 'HTTPS web server certificate' with options to 'Enable HTTPS server' (checked) and 'Authentication certificate' (set to 'identity.pem'). At the bottom, there are 'Apply settings' and 'Reset changes' buttons.

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

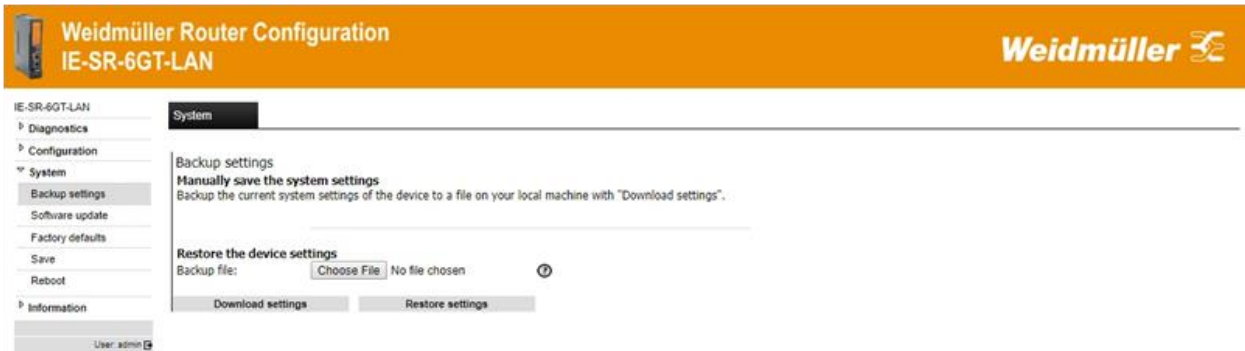
Services → SNMP



Menu	Configuration → Services → SNMP	
Function	Activation / deactivation of the SNMP protocol (Simple Network Management Protocol). 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 alphanumeric characters are required.
	Password	SNMPv3 only: Password for SNMPv3. Authentication Protocol: MD5. More than 8 alphanumeric characters are required.
	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


4.3 Section System

4.3.1 System → Backup settings

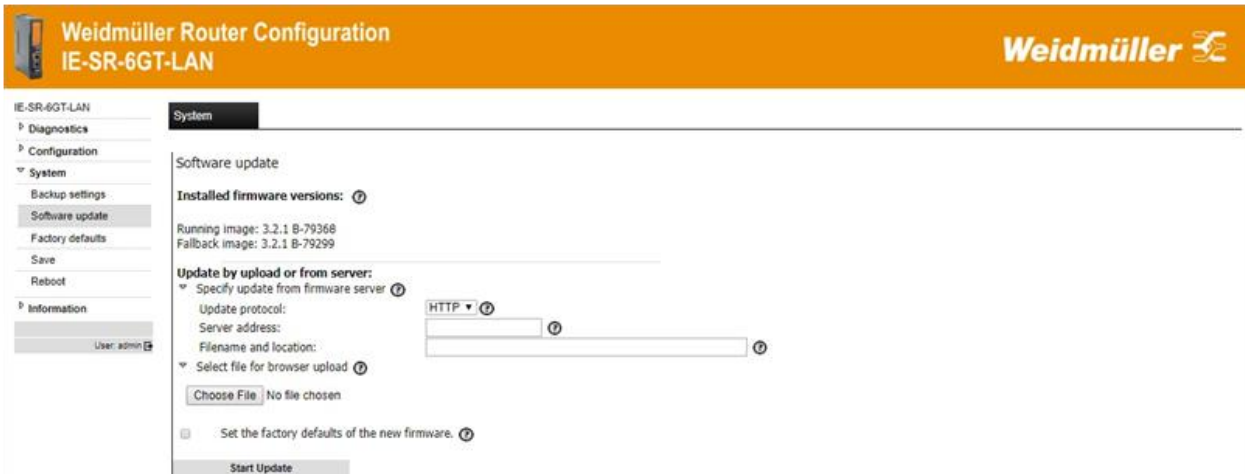


The screenshot shows the 'Weidmüller Router Configuration' web interface for an 'IE-SR-6GT-LAN' router. The left sidebar contains a navigation menu with 'System' selected. The main content area is titled 'System' and contains the 'Backup settings' section. It includes a 'Manually save the system settings' section with a 'Download settings' button, and a 'Restore the device settings' section with a 'Choose File' button and a 'Restore settings' button. The user is logged in as 'admin'.

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

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

4.3.2 System → Software update



The screenshot shows the 'Weidmüller Router Configuration' web interface for an 'IE-SR-6GT-LAN' router. The left sidebar contains a navigation menu with 'System' selected. The main content area is titled 'System' and contains the 'Software update' section. It displays 'Installed firmware versions' (Running image: 3.2.1 B-79368, Fallback image: 3.2.1 B-79299) and options to 'Update by upload or from server'. The 'Update by upload or from server' section includes a 'Specify update from firmware server' section with fields for 'Update protocol' (HTTP), 'Server address', and 'Filename and location', and a 'Select file for browser upload' section with a 'Choose File' button. There is also a checkbox for 'Set the factory defaults of the new firmware' and a 'Start Update' button. The user is logged in as 'admin'.

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>The easiest way to update the Router with a new firmware is to use the function „Update by browser upload“.</p>

	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 ftp.fw-server.net.</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>

4.3.3 System → Factory defaults






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

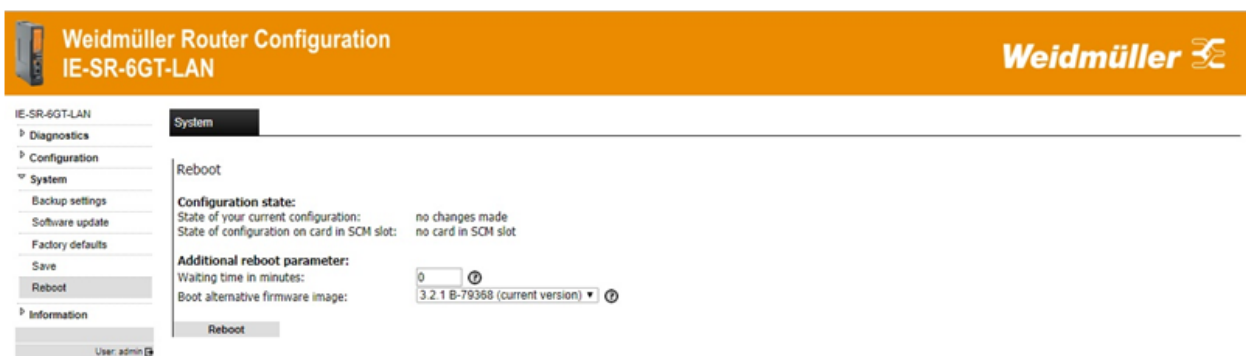
4.3.4 System → Save



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

Note		
		
		<p>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)</p>

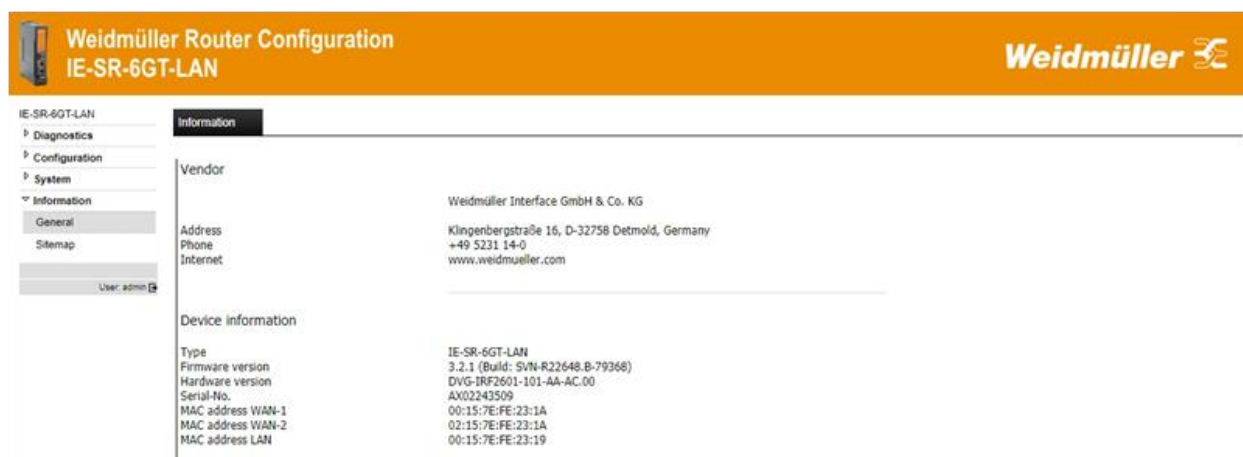
4.3.5 System → Reboot



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

4.4 Section Information

4.4.1 Information → General

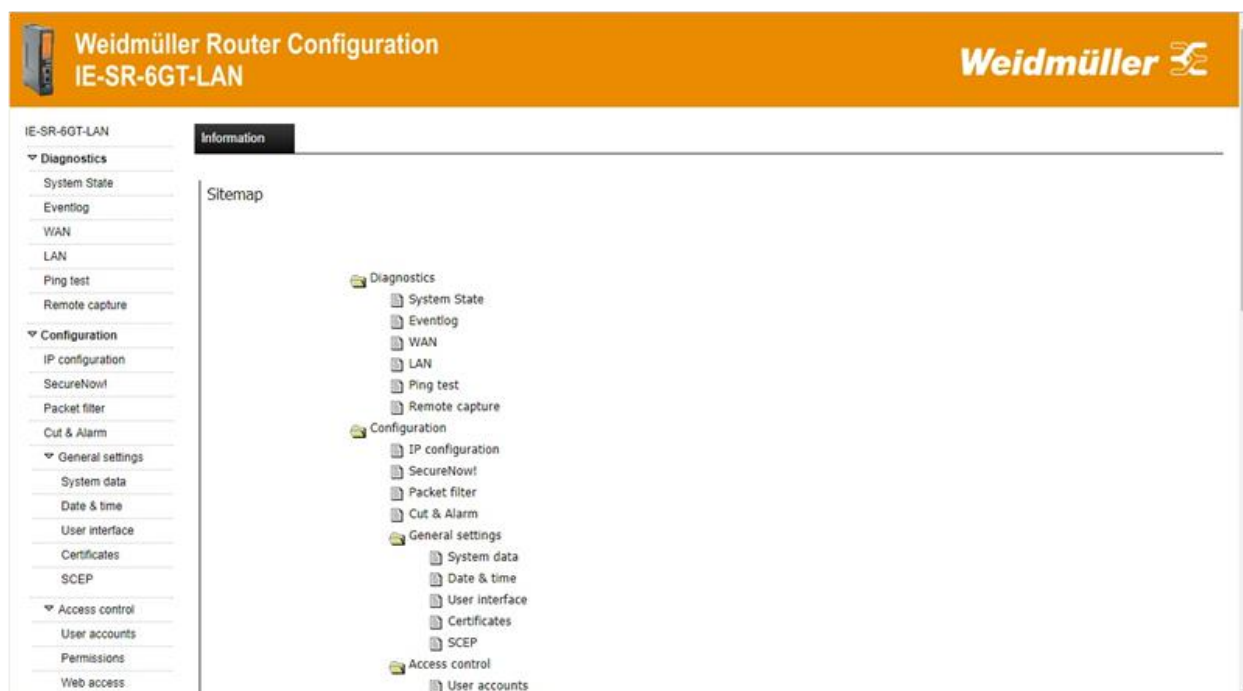


The screenshot shows the 'Weidmüller Router Configuration' interface for the 'IE-SR-6GT-LAN' device. The 'Information' tab is selected, and the 'General' sub-tab is active. The interface displays the following information:

- Vendor:** Weidmüller Interface GmbH & Co. KG
- Address:** Klingenbergstraße 16, D-32758 Detmold, Germany
- Phone:** +49 5231 14-0
- Internet:** www.weidmueller.com
- Device information:**
 - Type: IE-SR-6GT-LAN
 - Firmware version: 3.2.1 (Build: SVN-R22648.B-79368)
 - DVG-IRF2601-101-AA-AC.00
 - Serial-No.: AX02243509
 - MAC address WAN-1: 00:15:7E:FE:23:1A
 - MAC address WAN-2: 02:15:7E:FE:23:1A
 - MAC address LAN: 00:15:7E:FE:23:19

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

4.4.2 Information → Sitemap



The screenshot shows the 'Weidmüller Router Configuration' interface for the 'IE-SR-6GT-LAN' device. The 'Information' tab is selected, and the 'Sitemap' sub-tab is active. The interface displays a hierarchical tree structure of the configuration options:

- Diagnostics**
 - System State
 - Eventlog
 - WAN
 - LAN
 - Ping test
 - Remote capture
- Configuration**
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings**
 - System data
 - Date & time
 - User interface
 - Certificates
 - SCEP
 - Access control**
 - User accounts
 - Permissions
 - Web access

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

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

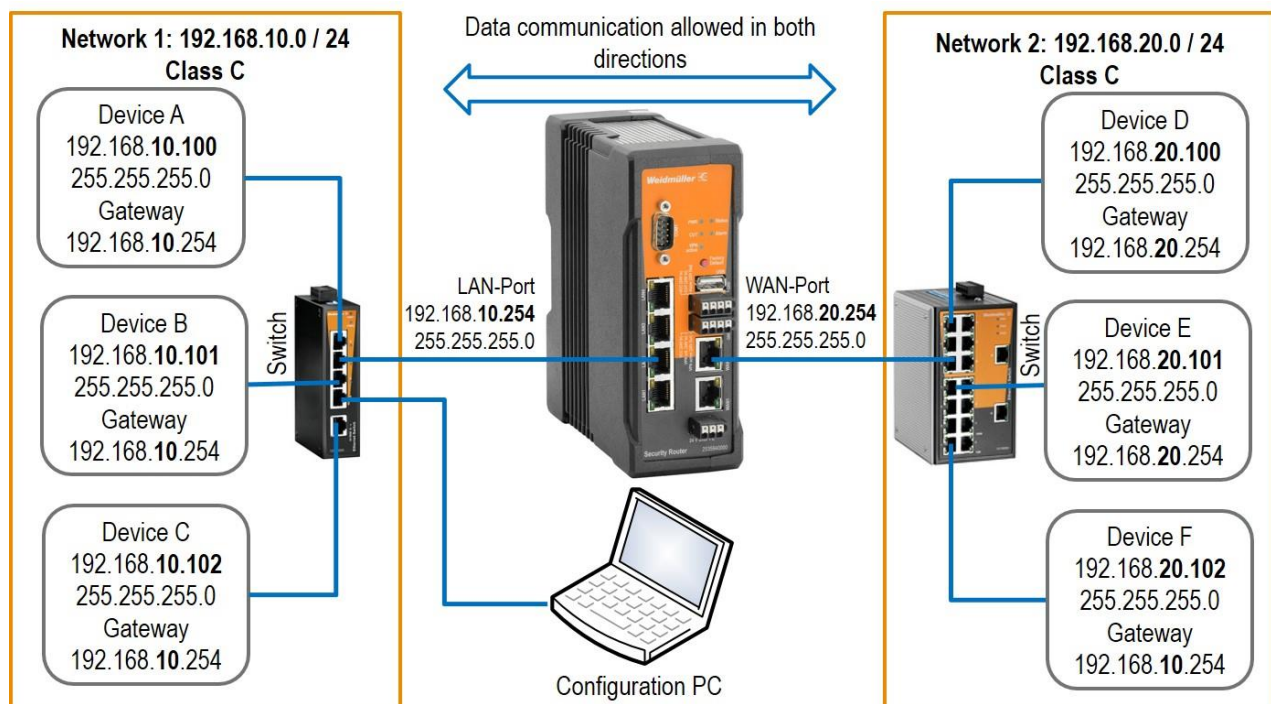
192.168.20.0 / 255.255.255.0 for Network 2

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

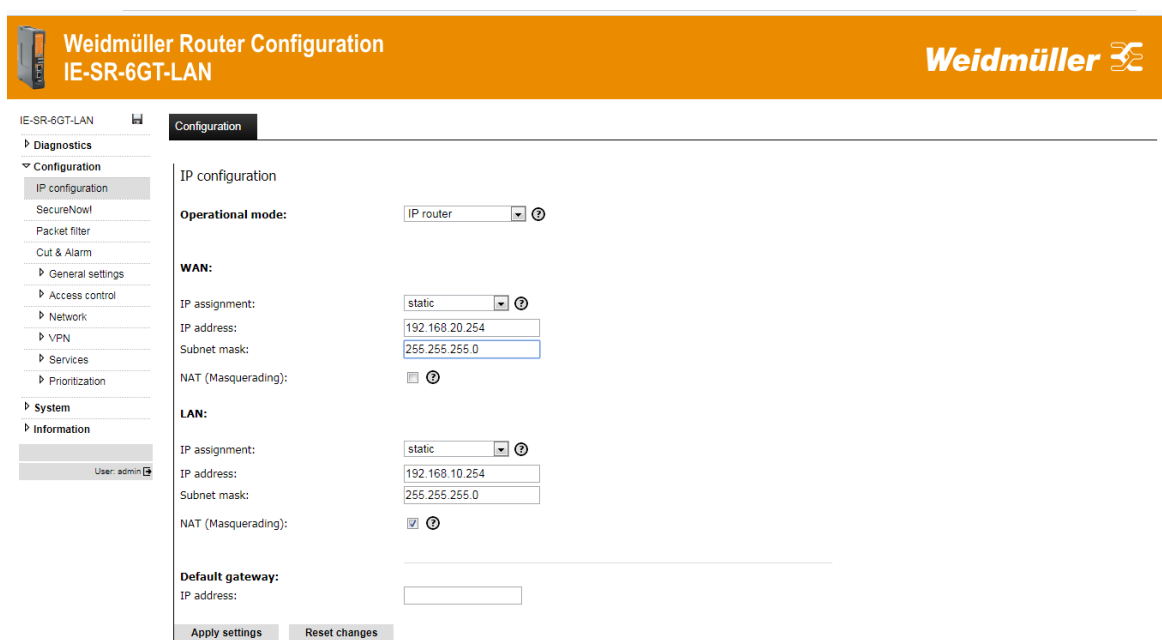
3. Start a web browser and login into the web Interface of Router (<http://192.168.1.110>)

User: admin
 Password: Detmold

4. Set the basic IP configuration

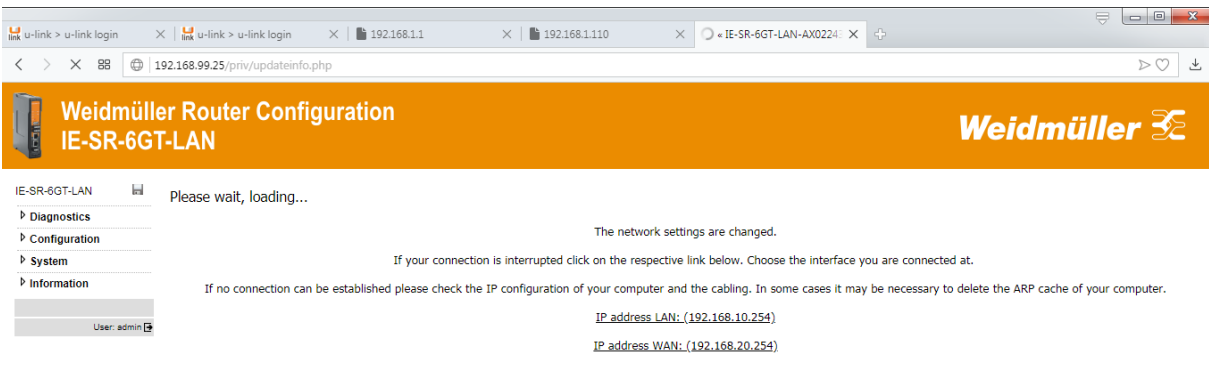
- ▶ Select menu **Configuration → IP configuration**
- ▶ Configure the menu entries as following shown

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



- ▶ Click button “Apply settings” to activate the new settings.

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



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

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

IP address: 192.168.10.99

Subnet mask: 255.255.255.0

Standard-Gateway: 192.168.10.254

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

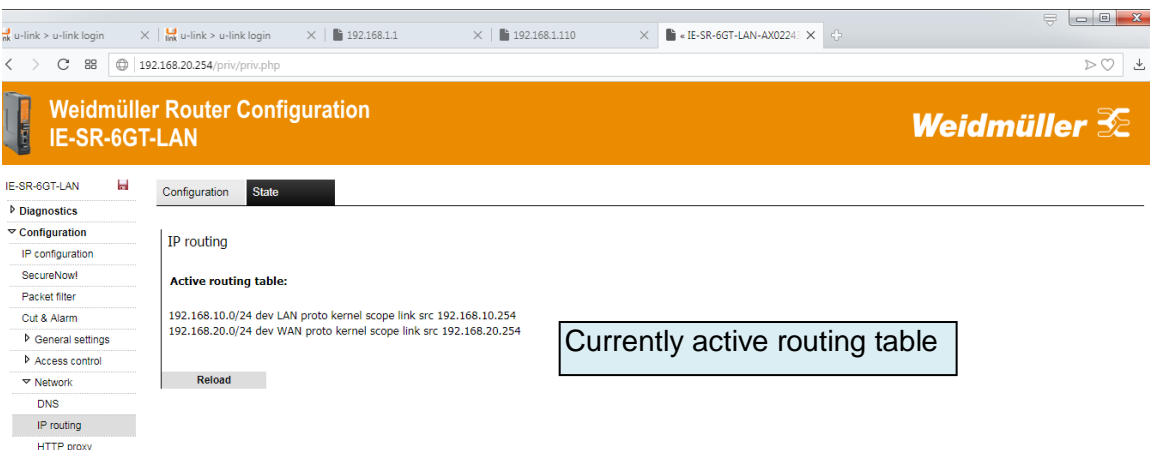
Use IP address 192.168.10.254 (http://192.10.1.254) on LAN port

User: admin

Password: Detmold

6. Check the currently active “routes”

- Select menu Configuration → Network → IP routing → Tab “State”



7. Saving the new configuration

- Select menu System → Save or Click on the Disk icon in the upper left corner of the web interface

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

- Select menu **System → Backup settings**

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

Now the configuration of the Router is finished!

Testing the accessibility between Ethernet Devices of both networks

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

- ping 192.168.20.100
- ping 192.168.20.101
- ping 192.168.20.102

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

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

- ping 192.168.10.100
- ping 192.168.10.101
- ping 192.168.10.102

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



Note

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

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.

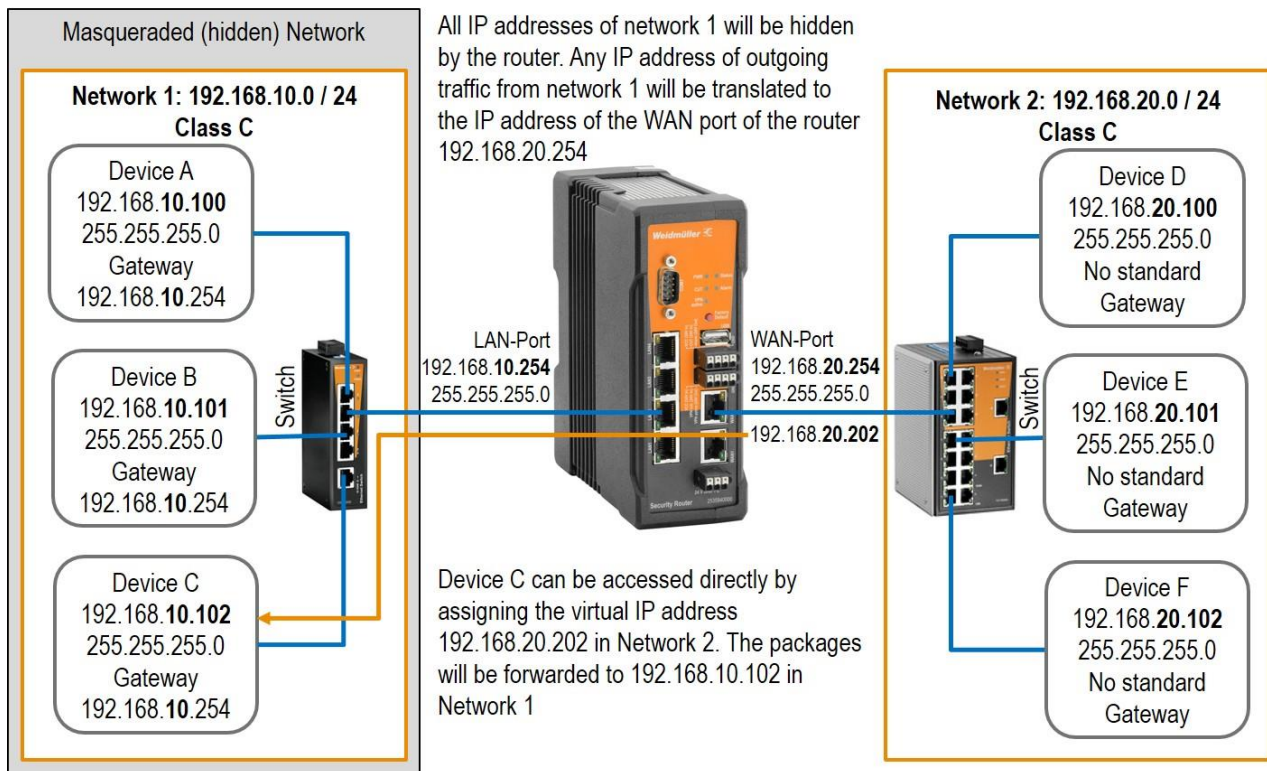
In this example the IP address ranges are set to

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

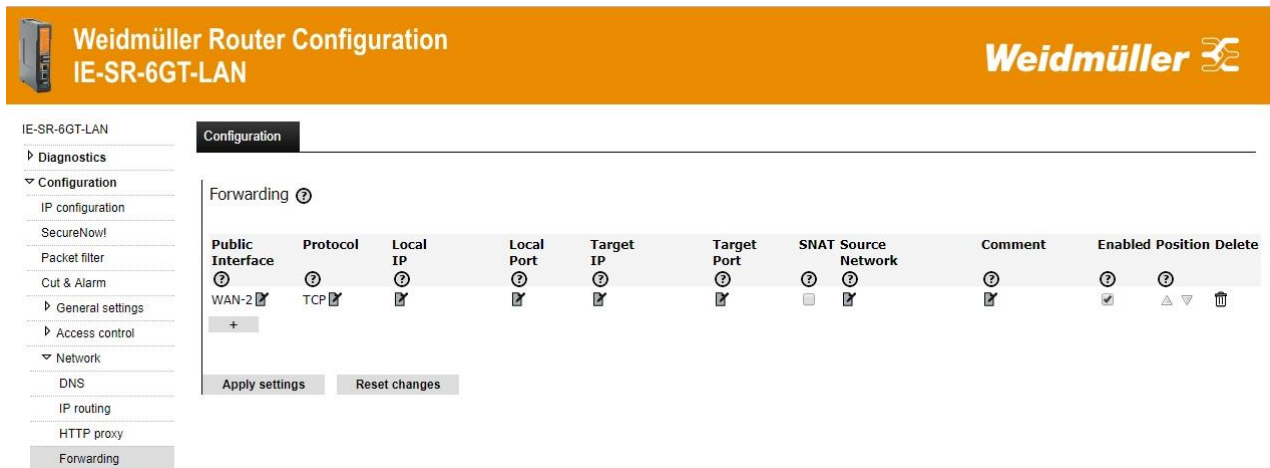



Figure 2: Empty IP forwarding table

- ▶ 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”

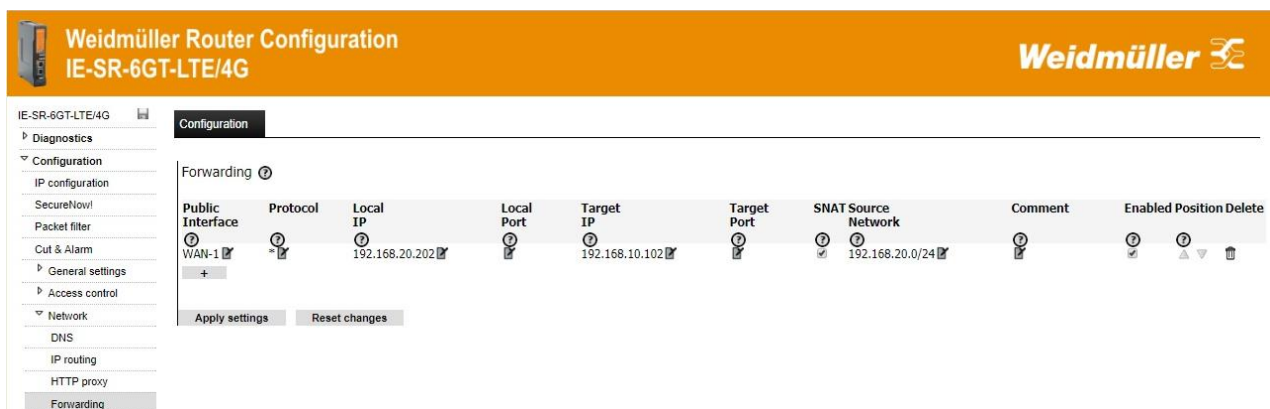


Figure 3: IP forwarding

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

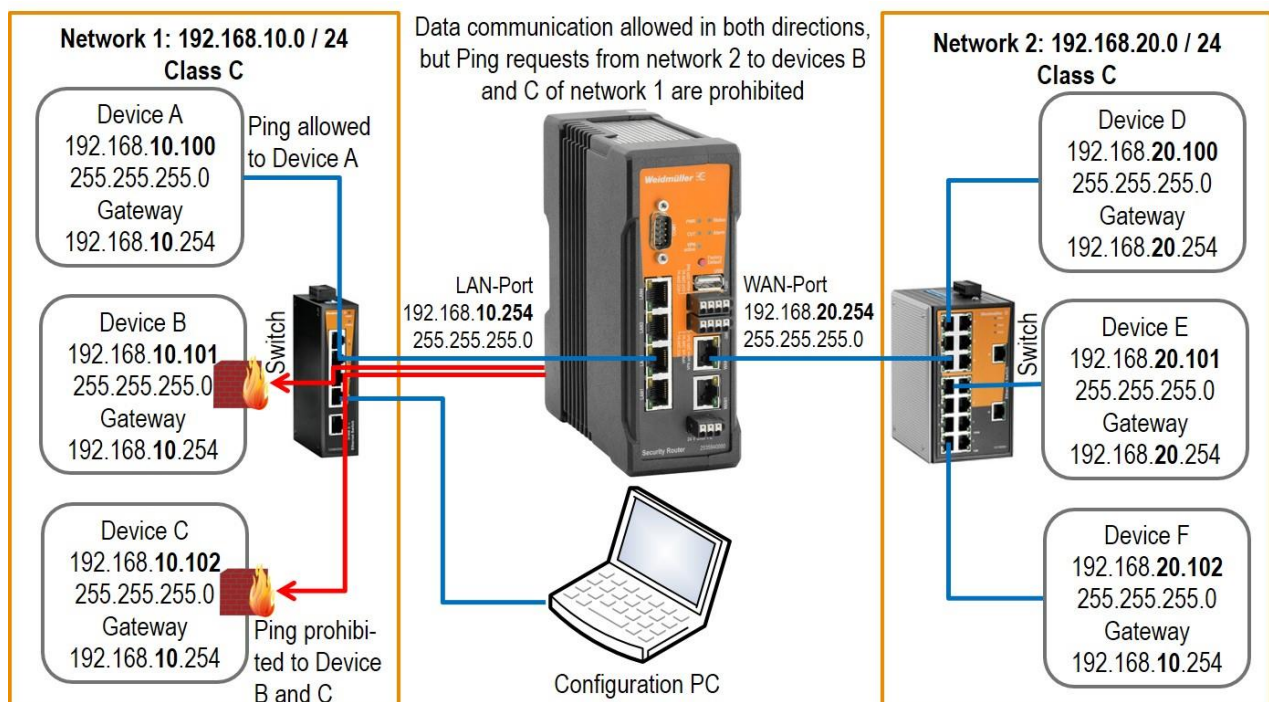
192.168.10.0 / 255.255.255.0 for Network 1 and

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

- ▶ Click button “Apply settings” to activate the new settings.

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

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

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

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

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

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

General description of the Packet filter

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

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

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

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

Application method of defined rule-sets

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

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

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

7. Setup the firewall rules

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

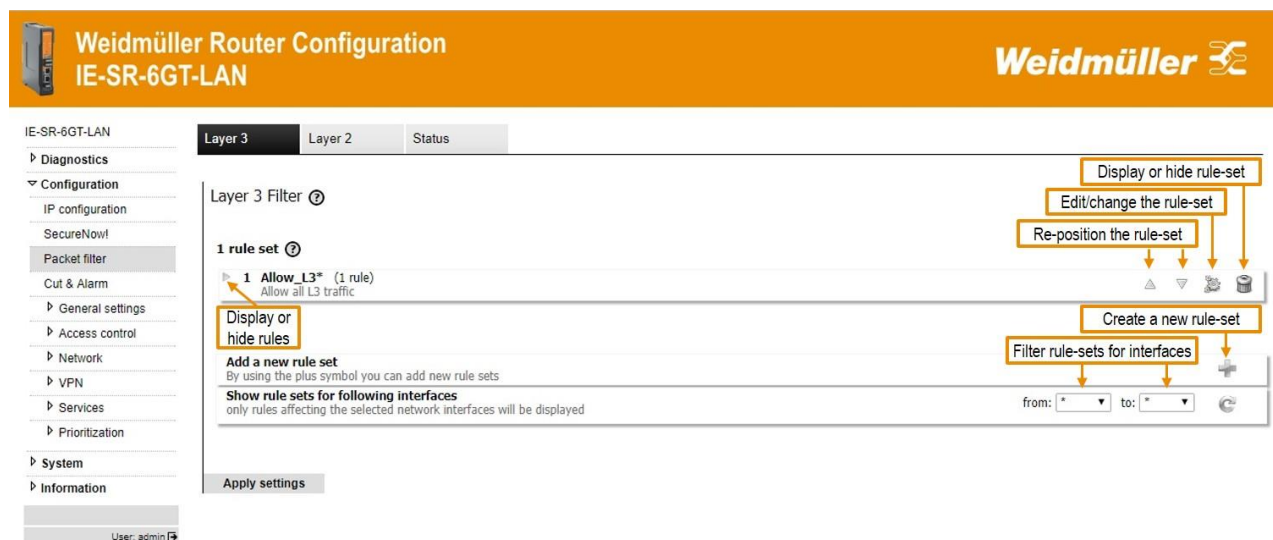


Figure 4: Packet filter

- 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)

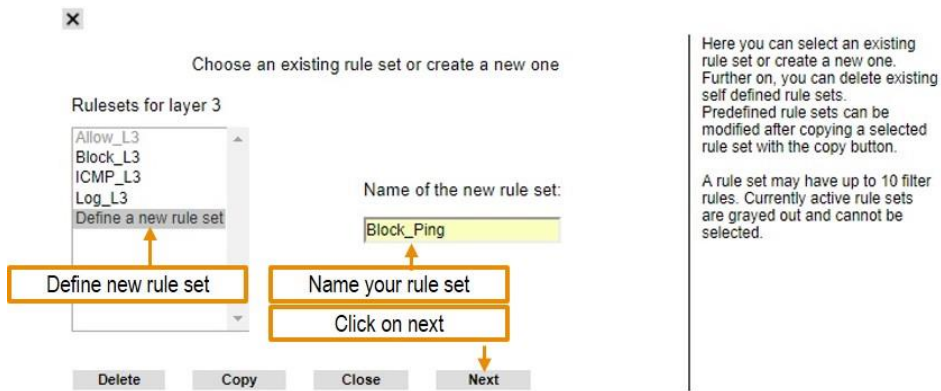


Figure 5: Create a new rule-set

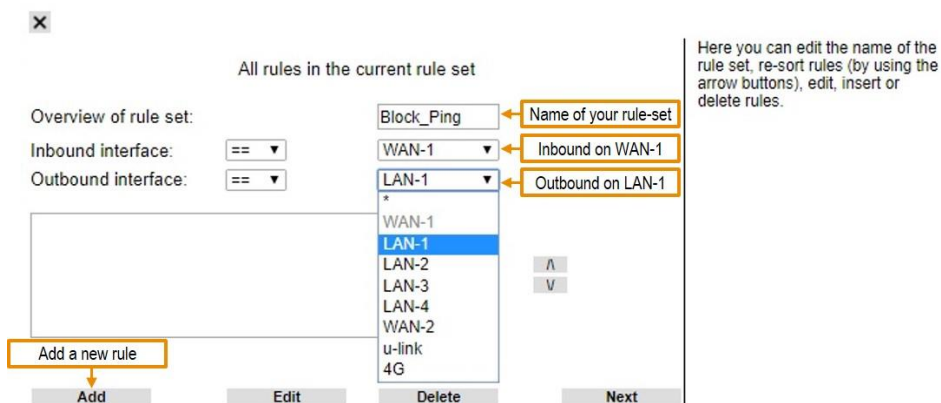


Figure 6: Define additional parameters of the new rule-set

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.

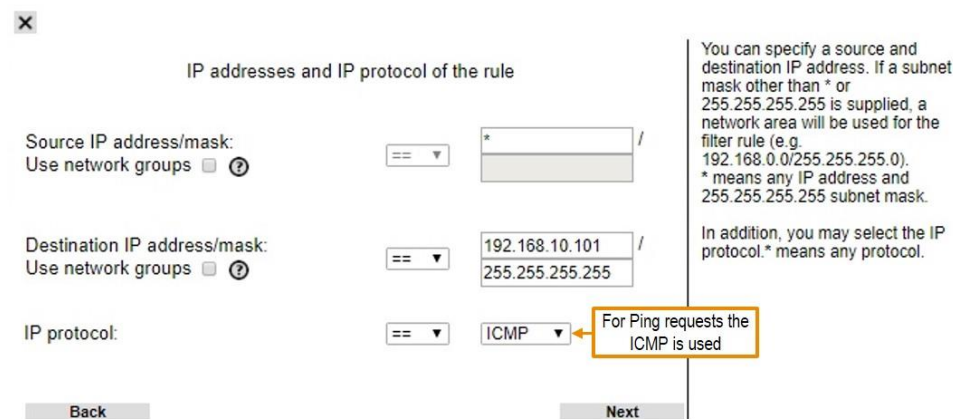


Figure 7: Define the first rule

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.

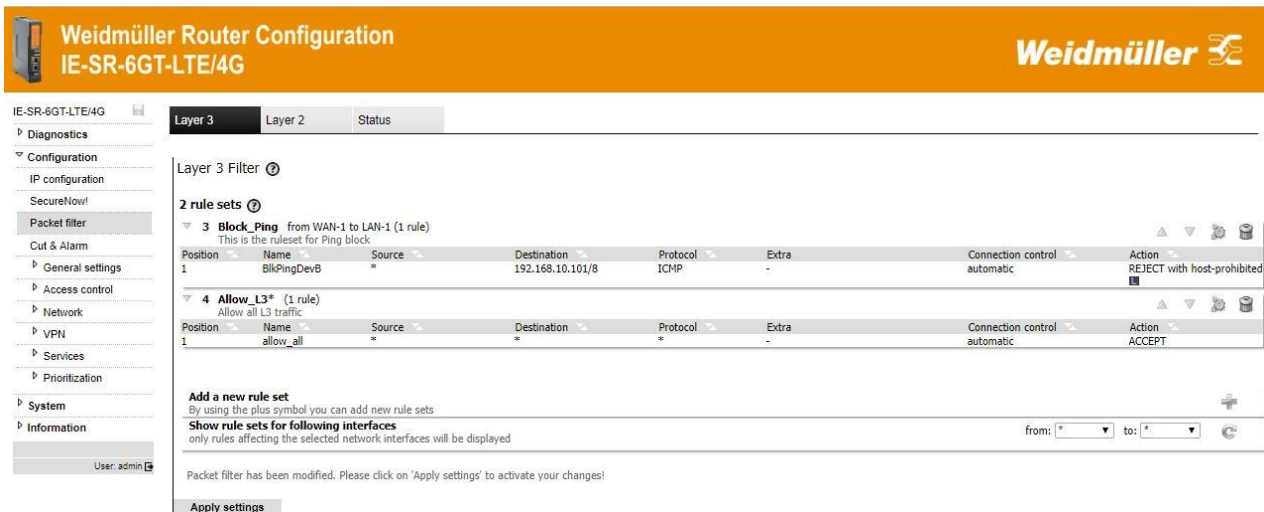


Figure 14: Overview of Packet filter rules

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”.

	<p>Note</p> <ol style="list-style-type: none"> 1. If you perform the ping test using a PC please check the PC's firewall configuration to ensure that ping requests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gateway (IP address is pointing to the Router of the PC's network)
---	---

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

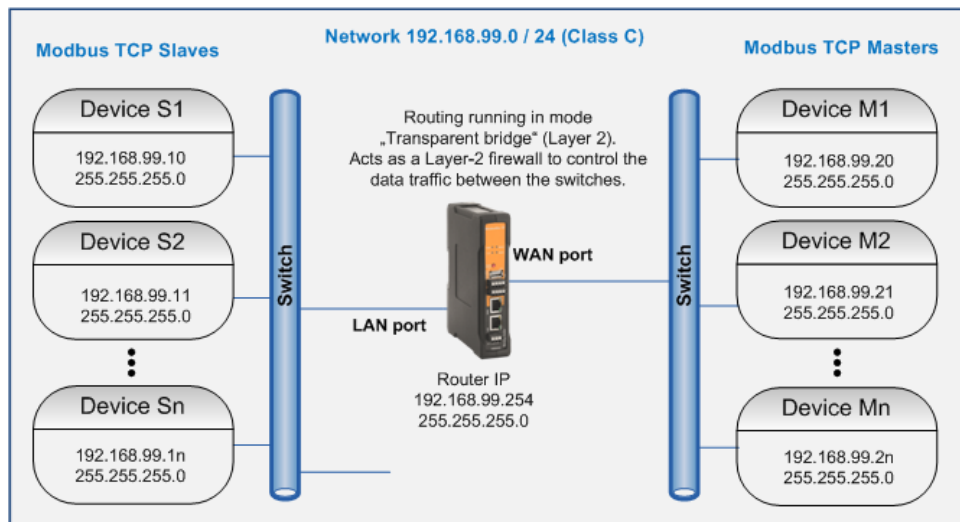


Figure 15: Example network topology

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).

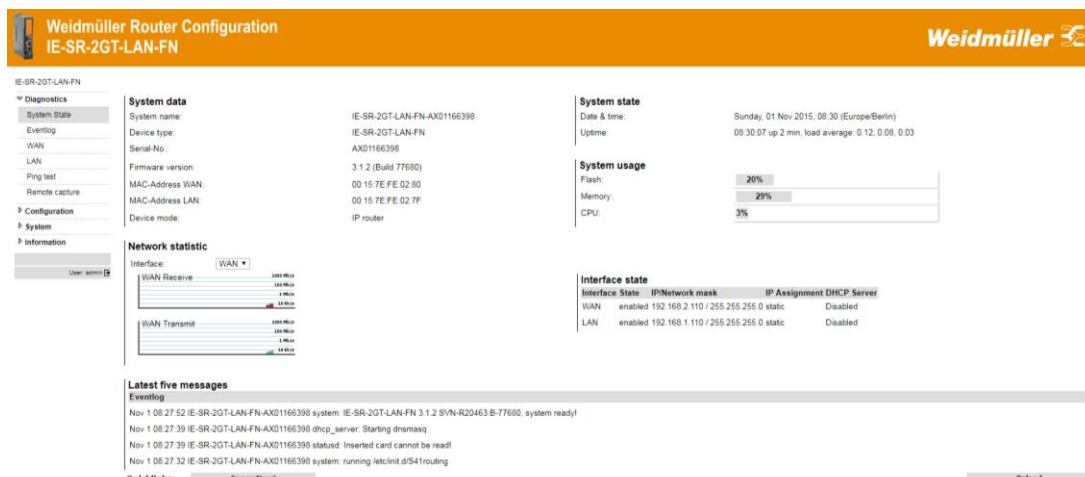


Figure 16: Display of initial web page after login (Menu System state)

A5-1 Configuration of initial parameters

► Goto menu Configuration → IP configuration

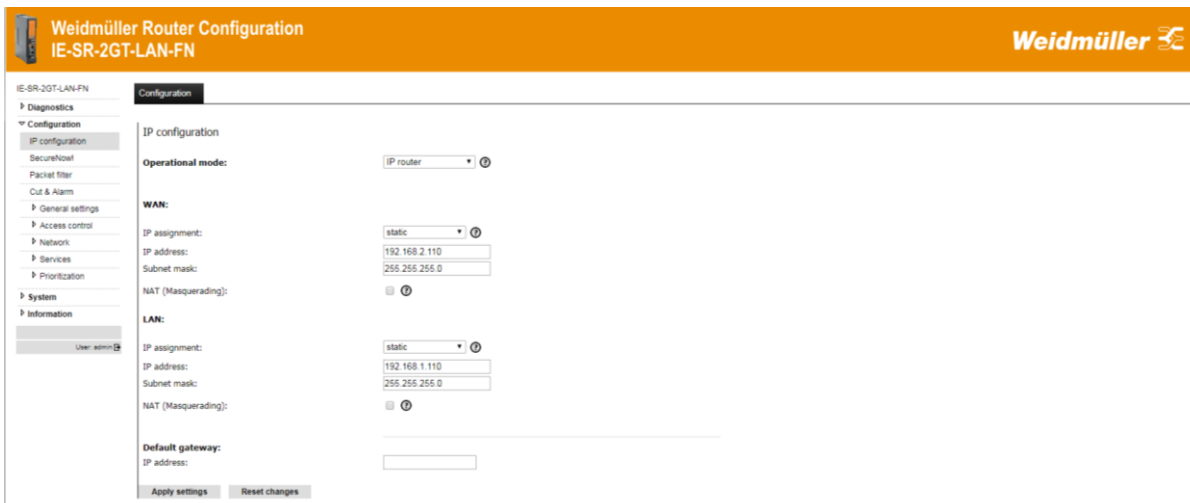


Figure 17: IP configuration factory defaults

- 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”

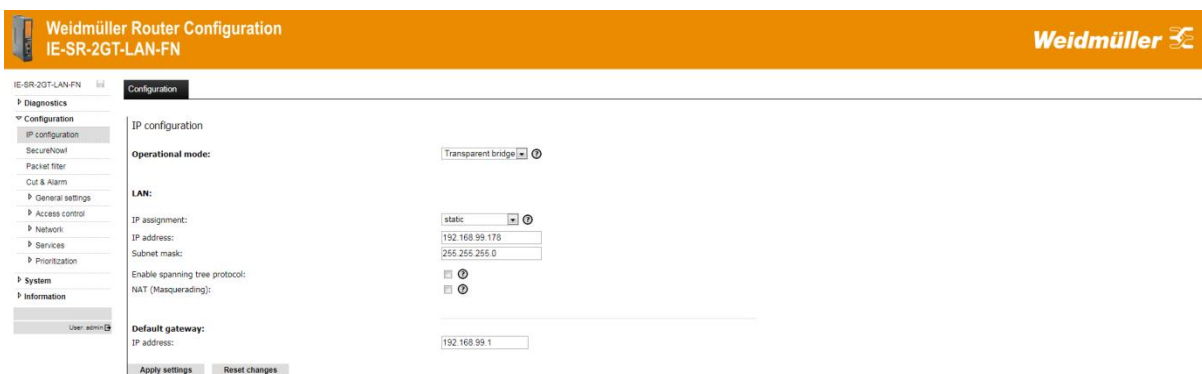
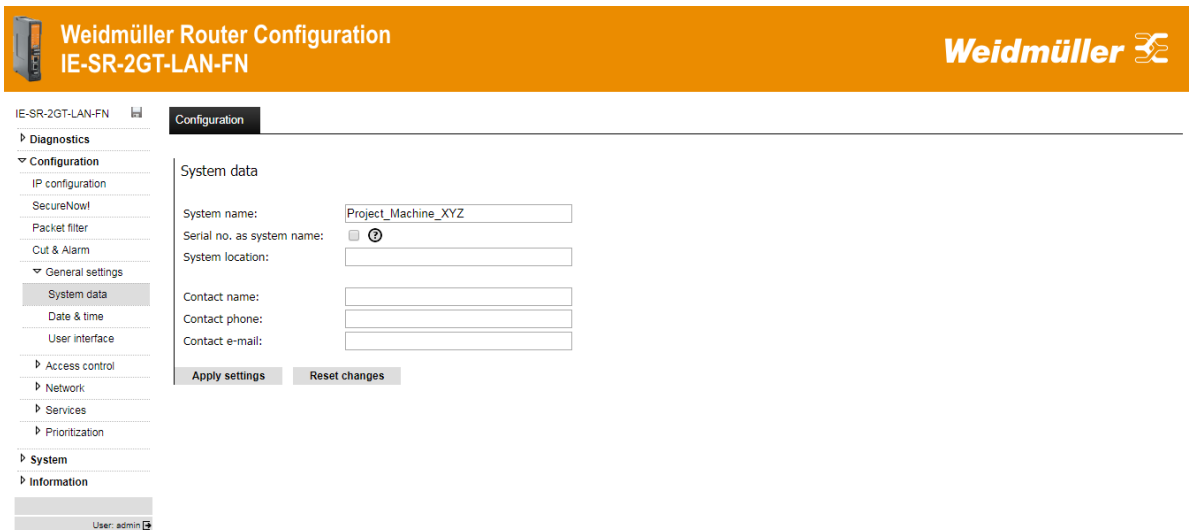


Figure 18: New IP configuration running as “Transparent bridge” (Layer 2)

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-2GT-LAN-FN

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-2GT-LAN-FN

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)

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


Weidmüller Router Configuration
IE-SR-2GT-LAN-FN

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-2GT-LAN-FN

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).

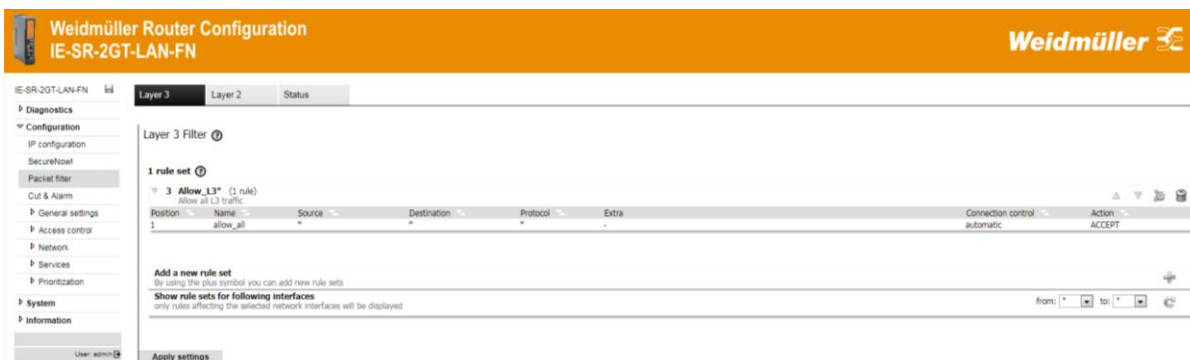


Figure 23: Factory default settings of Layer-3 Packet filter (firewall), valid for operation mode “IP Router”

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).

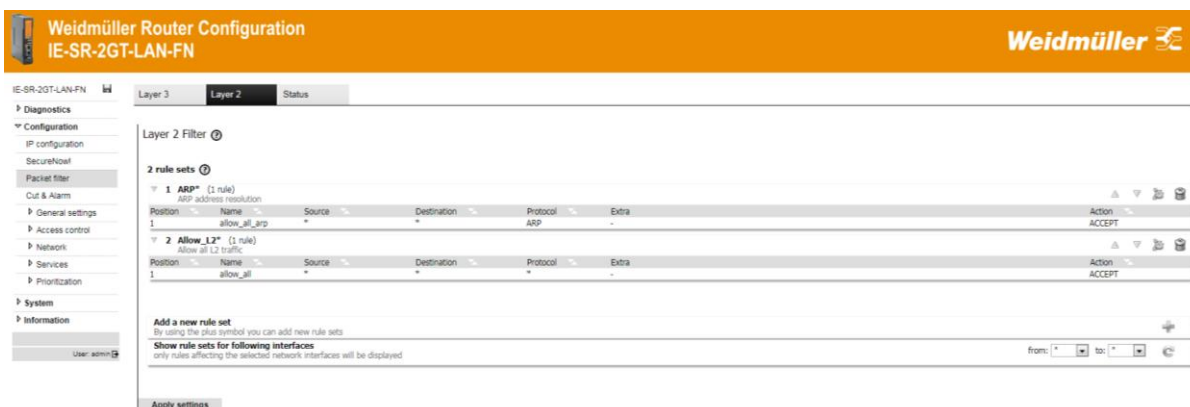


Figure 24: Factory default settings of Layer-2 Packet filter (firewall), valid for operation mode “Transparent bridge”

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.

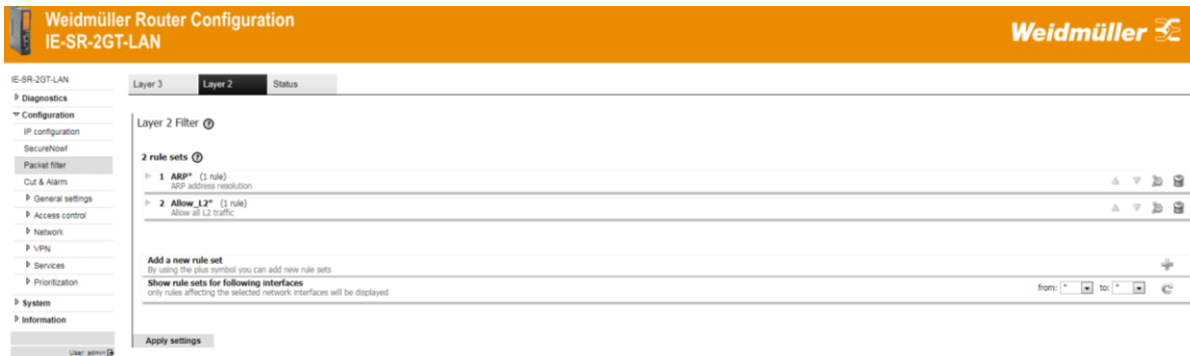
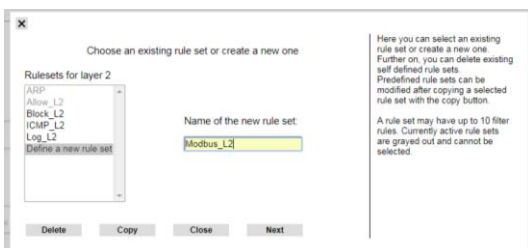
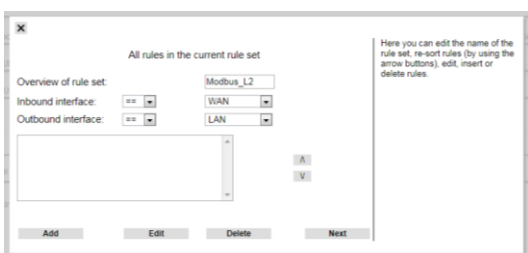


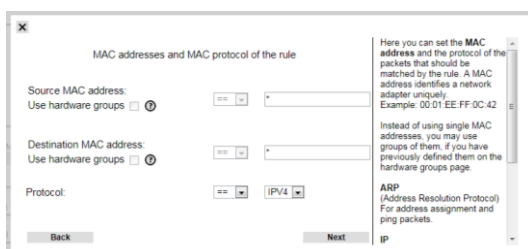
Figure 25: Factory default settings of Layer-2 Packet filter (firewall)



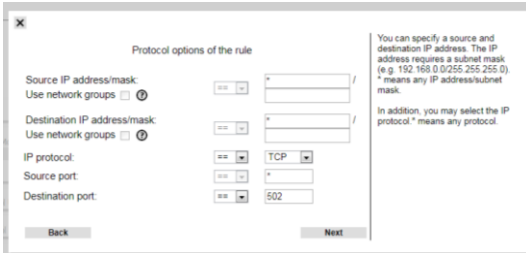
- ▶ Add a name for new rule-set (here Modbus_L2).
- ▶ Click ‘Next’.



- ▶ 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: *

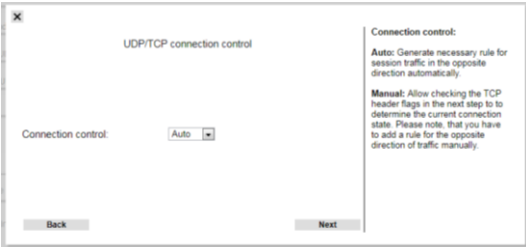
Destination port: 502

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

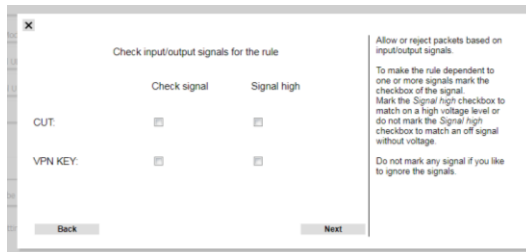
Connection control:

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.

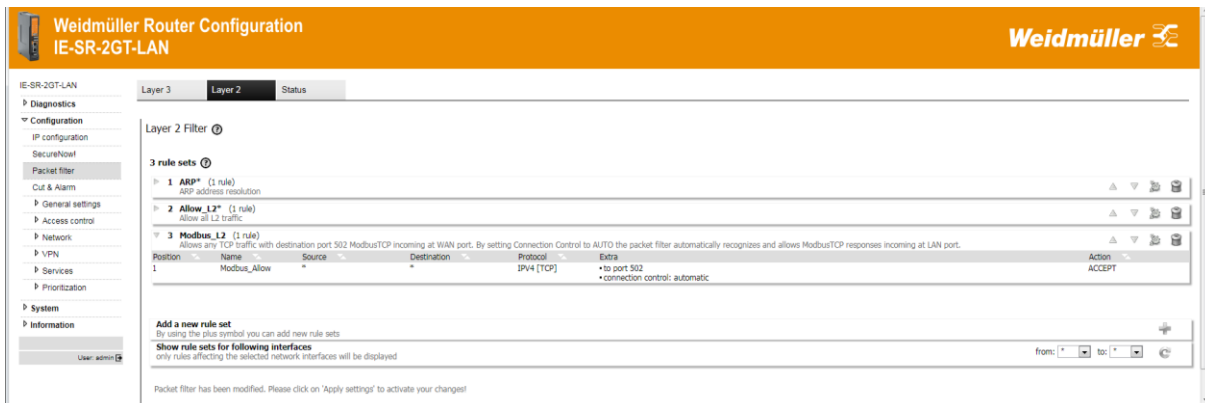
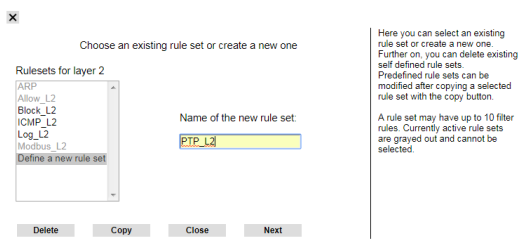


Figure 11: Layer-2 filter list containing new rule-set “Modbus_L2”

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.

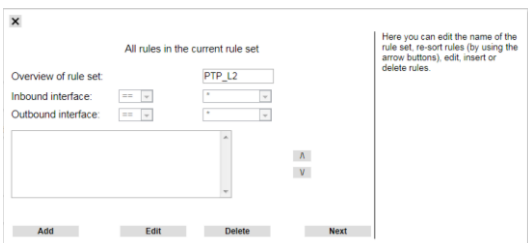
2.2 Configuration of a rule-set containing 2 rules which allow any PTP communication based on protocol UDP, ports 319 and 320, either initially incoming at WAN port or LAN port.

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

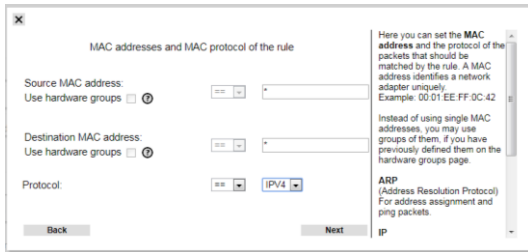


► Add a name for the new rule-set (here PTP_L2).

► 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:

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

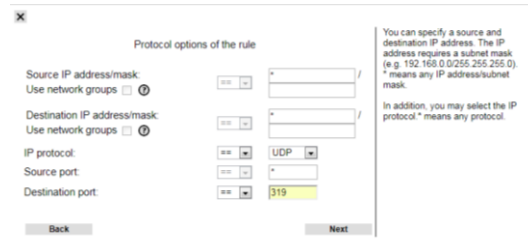
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

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:

Source port:

Destination port:

Back Next

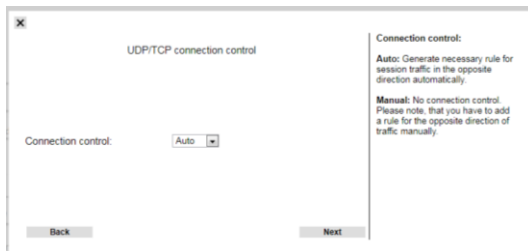
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.

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:

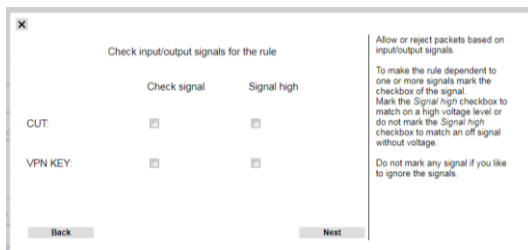
Back Next

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:	<input type="checkbox"/>	<input type="checkbox"/>
VPN KEY:	<input type="checkbox"/>	<input type="checkbox"/>

Back Next

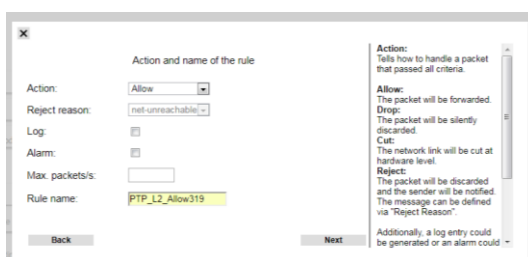
Allow or reject packets based on input/output signals.

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.

► No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action:

Reject reason:

Log:
☐

Alarm:
☐

Max. packets/s:

Rule name:

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:

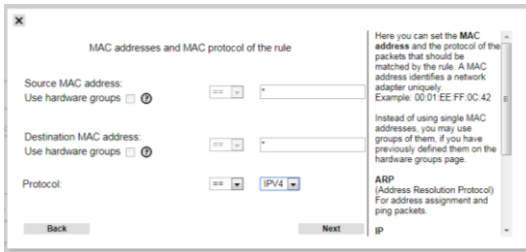
PTP_L2_Allow319

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

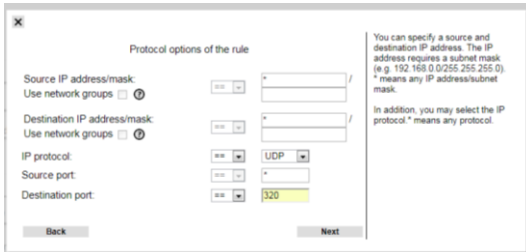
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

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

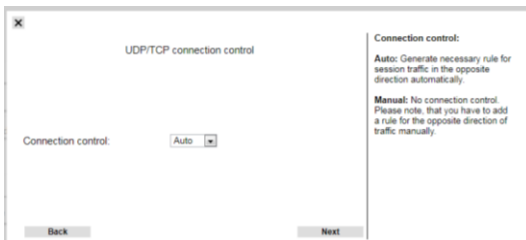
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.

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:

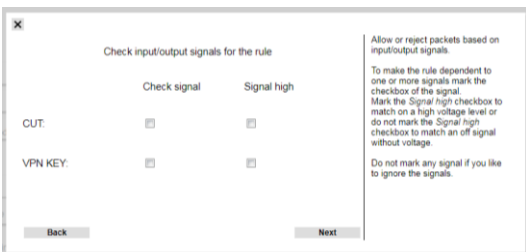
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

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

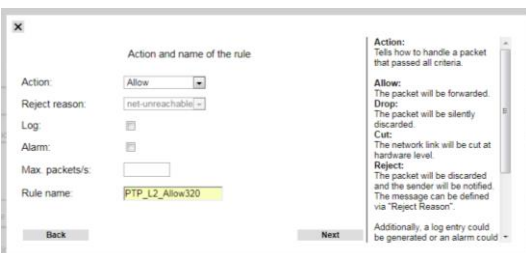
Allow or reject packets based on input/output signals.

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:

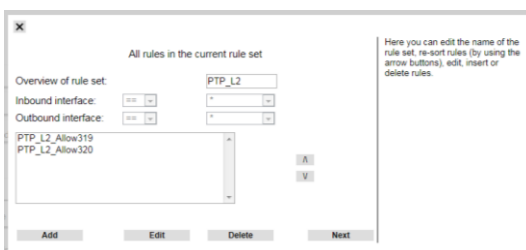
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

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

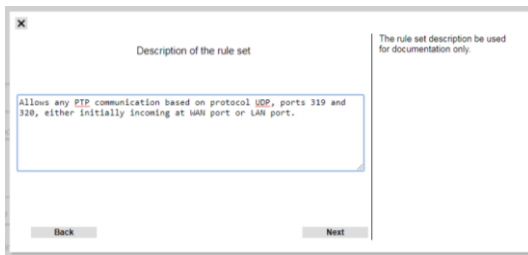
PTP_L2_Allow320

Add Edit Delete Next

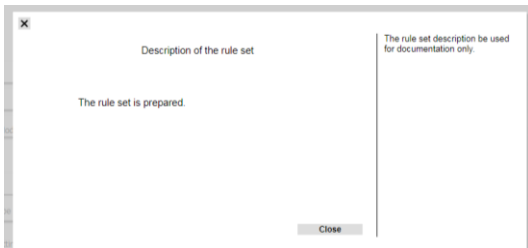
Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

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'.

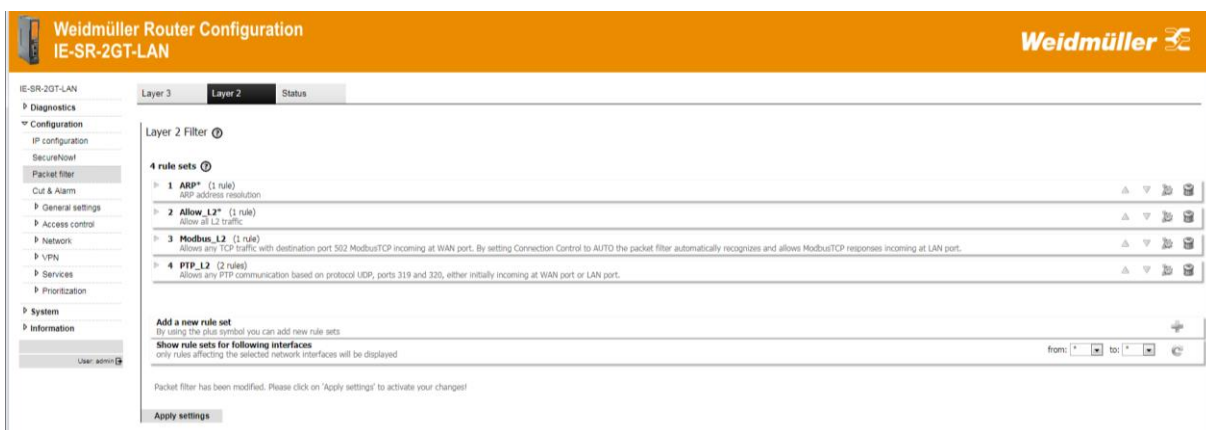
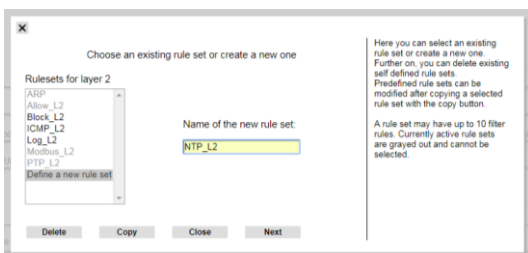


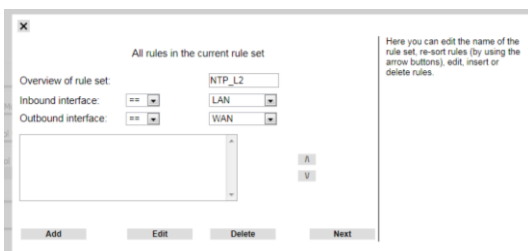
Figure 12: Layer-2 filter list containing new rule-set “PTP_L2”

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).

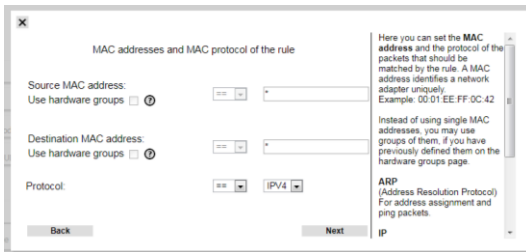
- Click '+' icon to add a new rule-set.



- Add a name for the new rule-set (here NTP_L2).
- Click 'Next'.



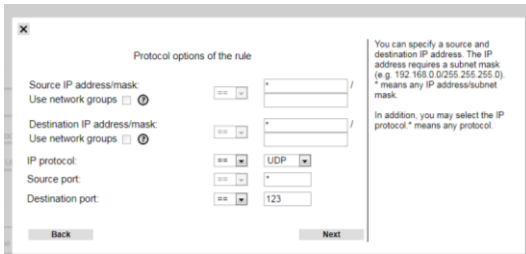
- Select inbound and outbound interface.
- Click 'Add' to add a new rule.
- Click 'Next'.



► Enter wild character * for source and destination MAC addresses

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

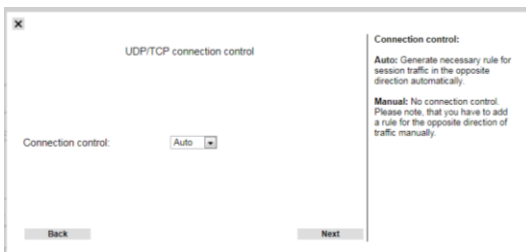
► Click 'Next'.



► 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).

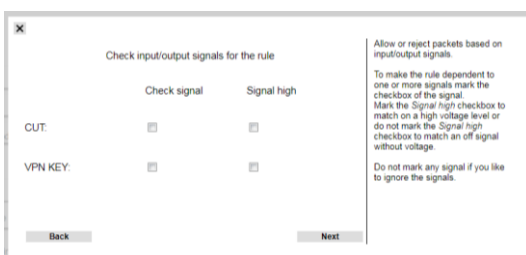
► Click 'Next'.



► Select auto for Connection control.

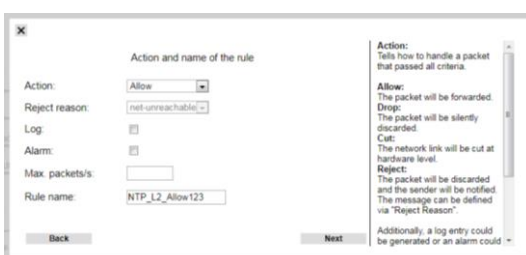
(Packet filter acts as an stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

► Click 'Next'.



No signal check and setting.

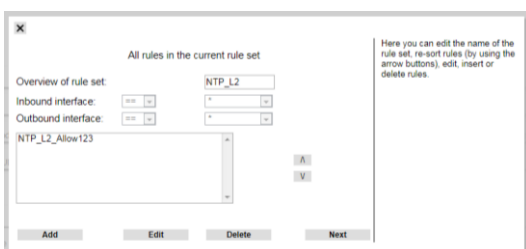
► Click 'Next'.



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

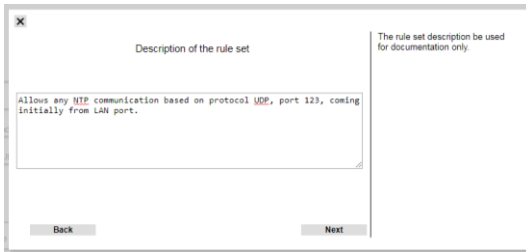
► Add a name for this rule (here NTP_L2_Allow123).

► Click 'Next'.

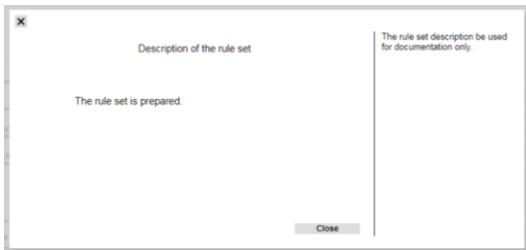


Now the necessary rule is configured.

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



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



- Click 'Close'.

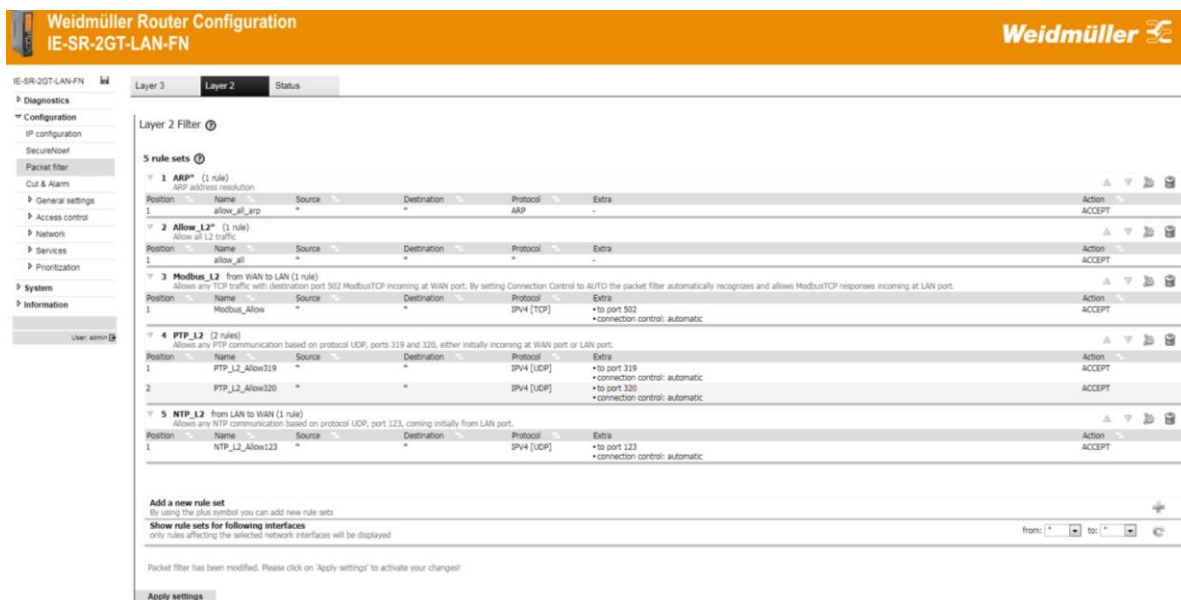


Figure 26: Layer-2 filter list containing new rule-set “NTP_L2”

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.

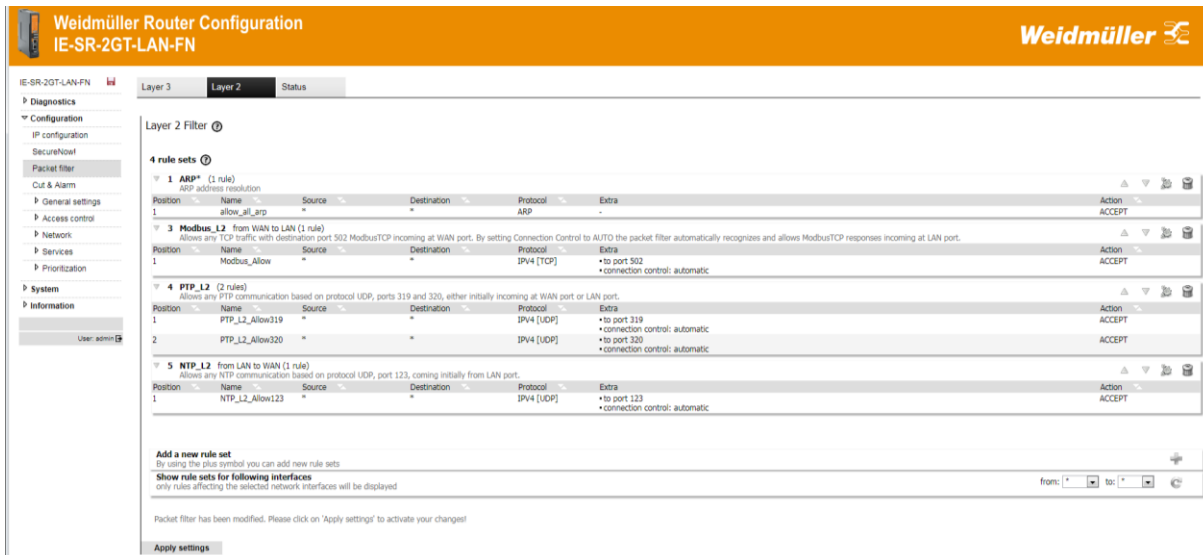
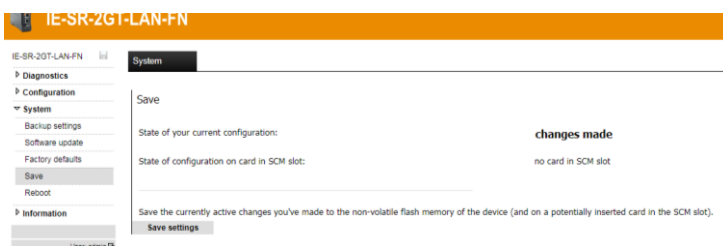


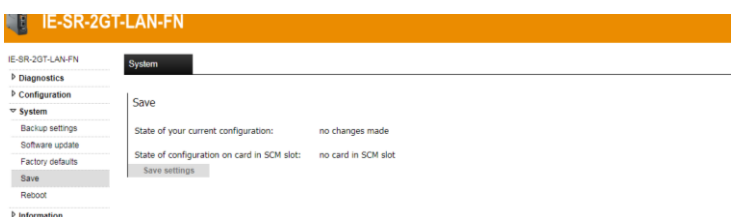
Figure 27: Final list of Layer-2 filter

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

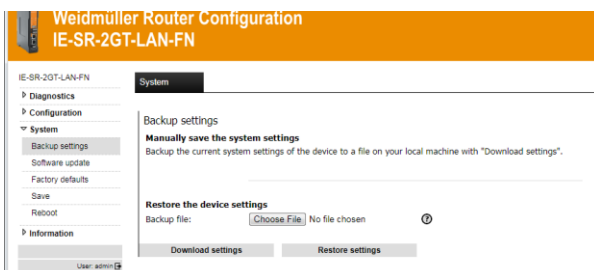


- Goto menu System → Save.
- Click ‘Save settings’.

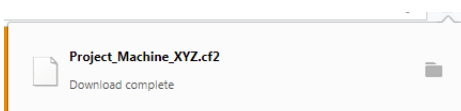


Now the settings are saved in the flush memory.

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 LAN/WAN port (other Routers)

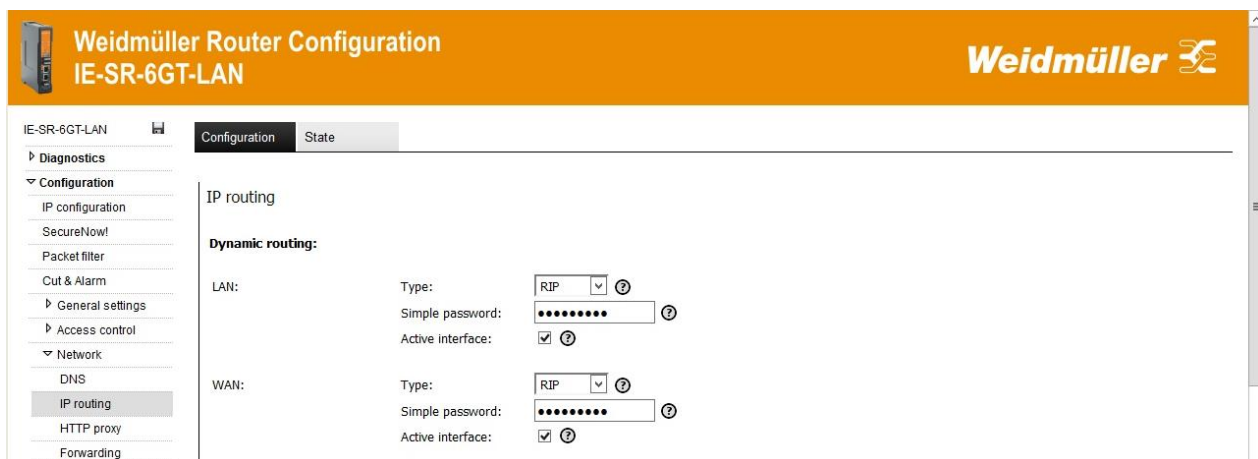



Figure 28: Configuration of dynamic routing using RIP

	Note
	<ol style="list-style-type: none"> 1. If there are several Routers with activated RIP but only the Routers 1 and 2 should exchange their routing tables, then you must use the same password for each Router. 2. You should always use the same value for “Type” on both ports (LAN and WAN). For example, if you leave Type=disabled on LAN port and you activate only the parameters Type=RIP and Active interface=set on WAN port, then the Router will not announce (outgoing WAN port) the configured network connected to its LAN port.

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

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

Now Router configuration is finished!

Testing the accessibility between Ethernet Devices of network 1 and 2

1. Send a ping request from Machine A to Machine D

Send “ping 192.168.11.101”


Note: This is the public IP address of Machine 1 of Network 2, translated 1:1 NAT from 192.168.1.101 to from 192.168.11.101

2. Send a ping request from Machine D to Machine A

Send “ping 192.168.10.101”

Note: This is the public IP address of Machine 1 of Network 1, translated by 1:1 NAT from 192.168.1.101 to from 192.168.10.101

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

	Note
	<ol style="list-style-type: none"> 1. If you perform the ping test using PC’s please check your firewall configuration to ensure that ping requests and echoes are allowed. 2. Keep in mind that every device which will be used for ping testing needs an entry for the standard gateway (IP address is pointing to the Router of the PC’s network).

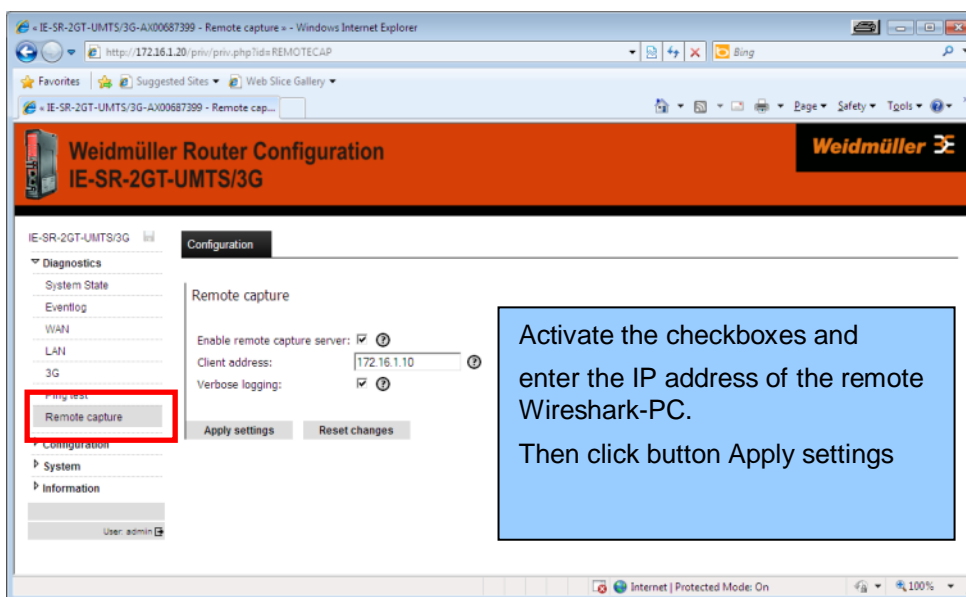
A6 - How to use feature “Remote Capture” with Wireshark to analyse Router’s LAN/WAN traffic

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

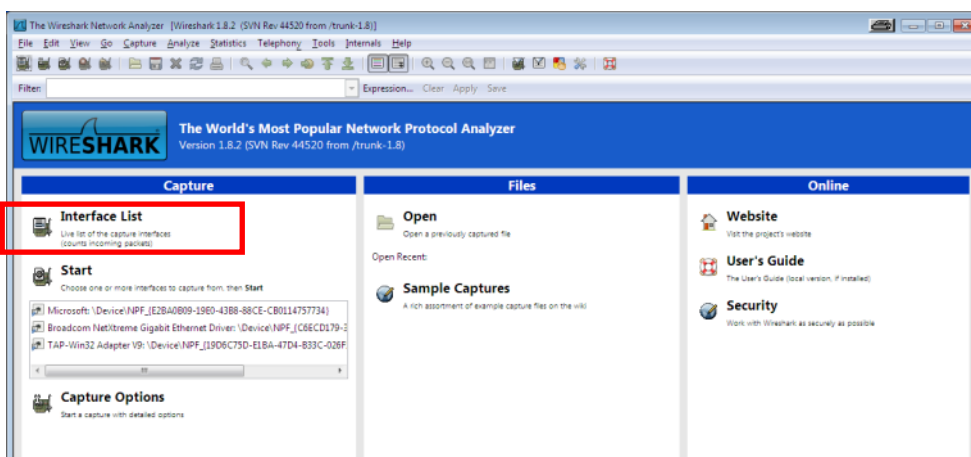
Step-by-step guidance

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

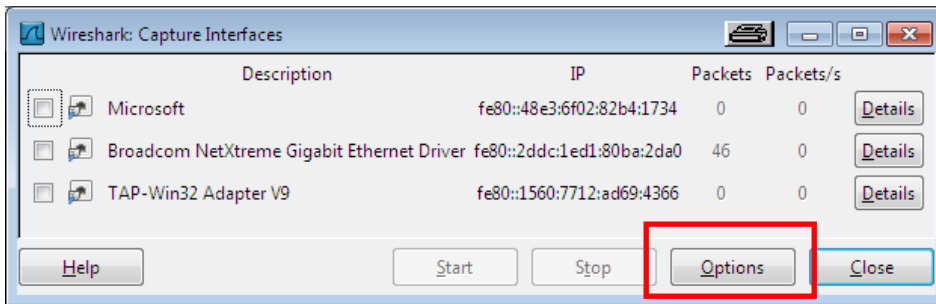
Note: Only one Wireshark-Client-PC (here 172.16.1.10) can be used at the same time record the traffic by Wireshark. Please deactivate this feature if you no longer need to analyse the traffic because it has an impact on the performance of the Router.



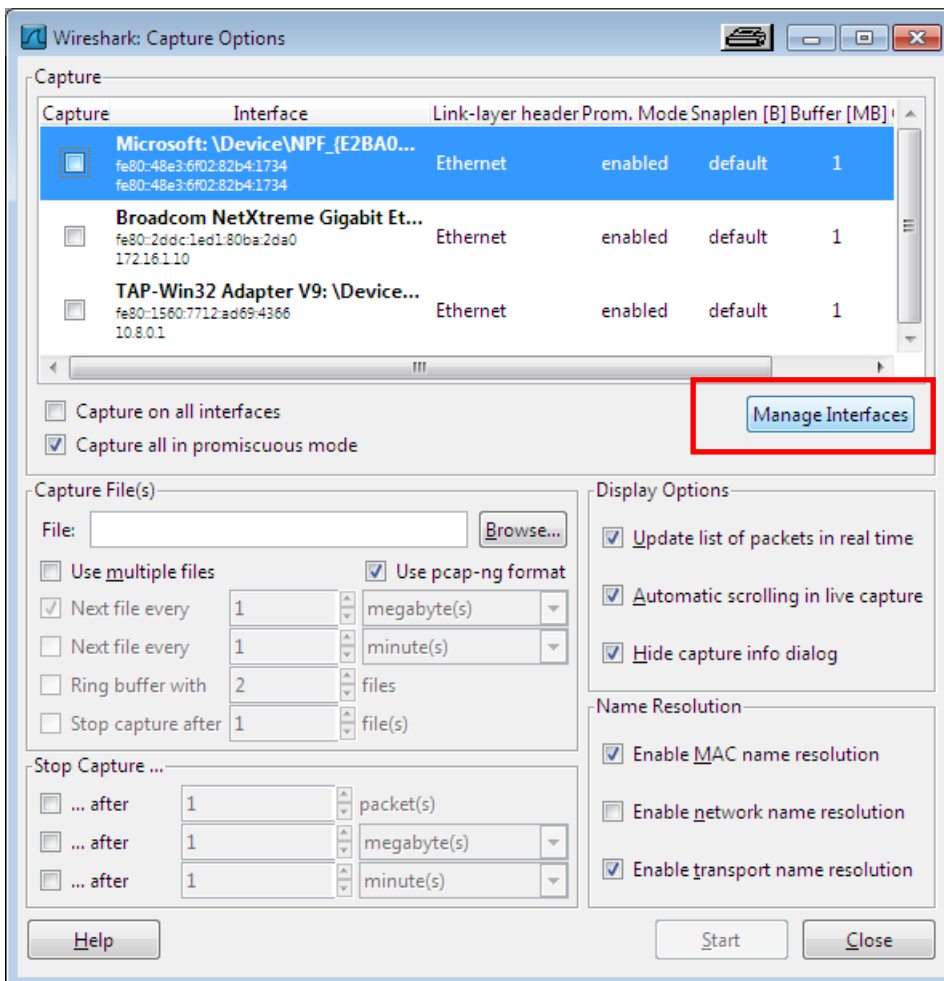
2. Start Wireshark at your PC
3. Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”



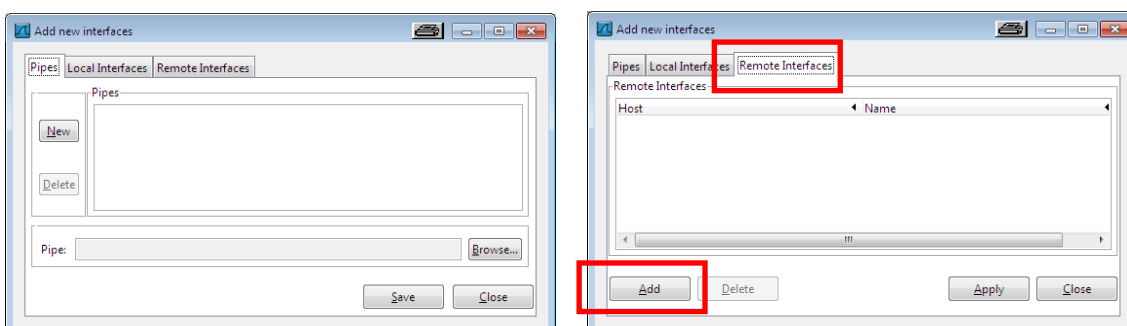
The local Ethernet Interfaces of the computer will be displayed.



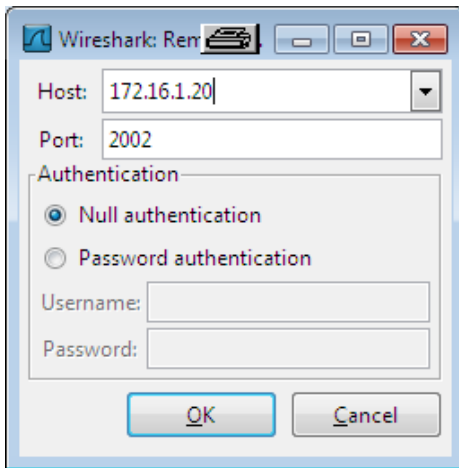
4. Click button “Options”



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



6. Click button “Add”

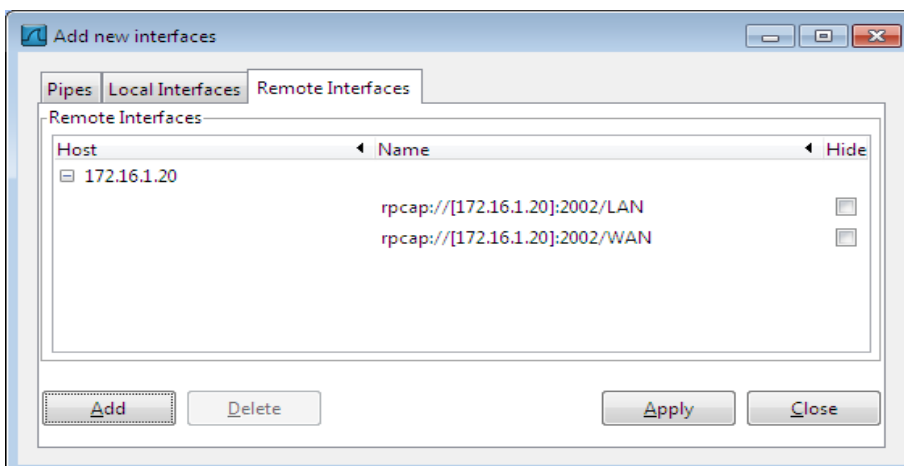


7. Enter the IP address of the Router to field "Host"

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

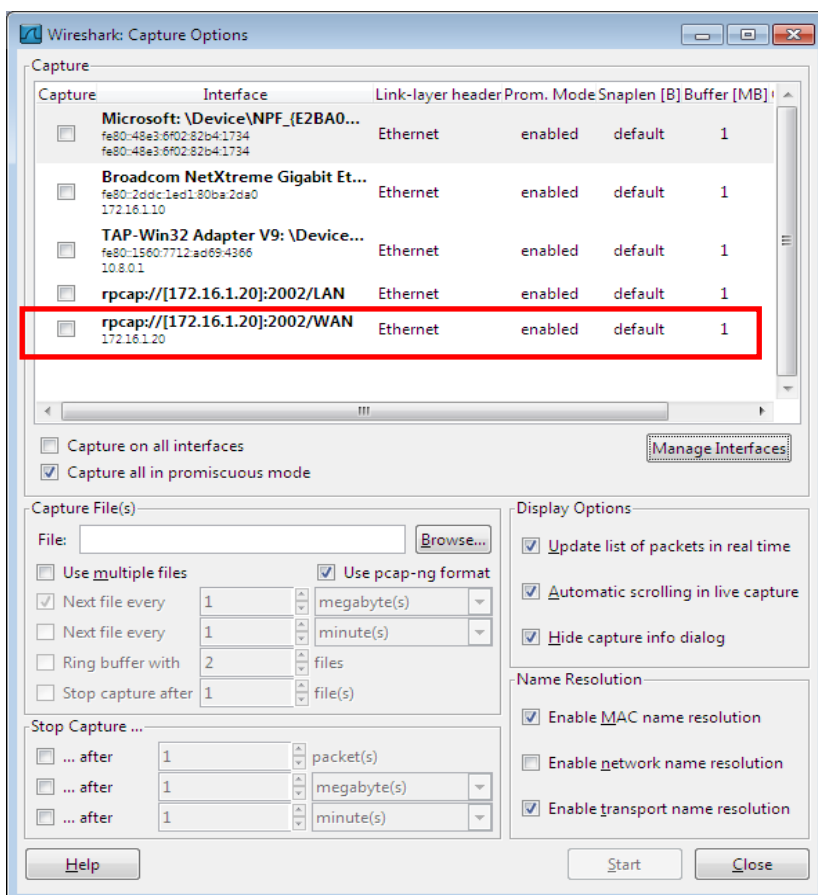
8. Enter into field "Port" the value 2002 (will be filled automatically if you enter an IP address)
9. Click button OK

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



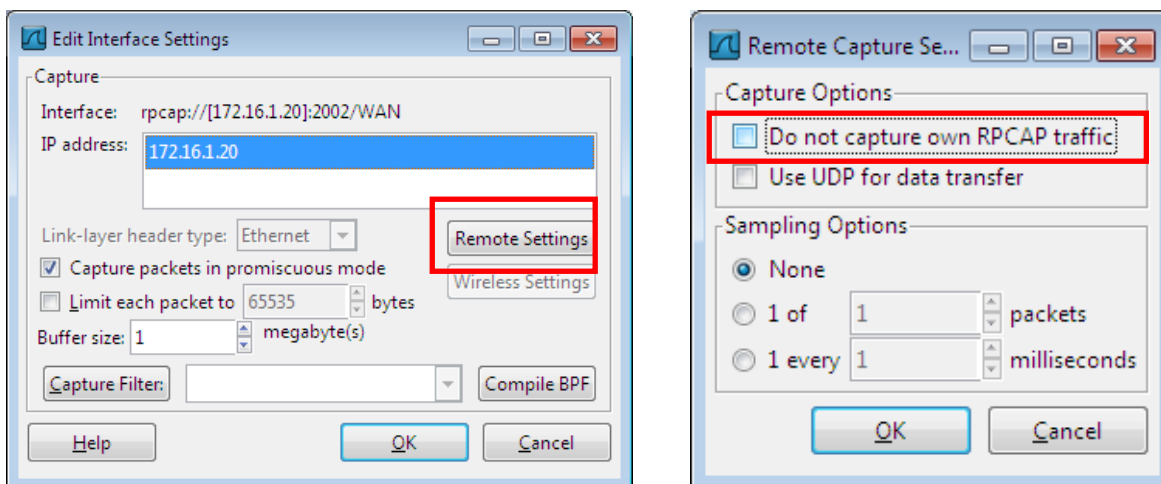
10. Click button Close

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**

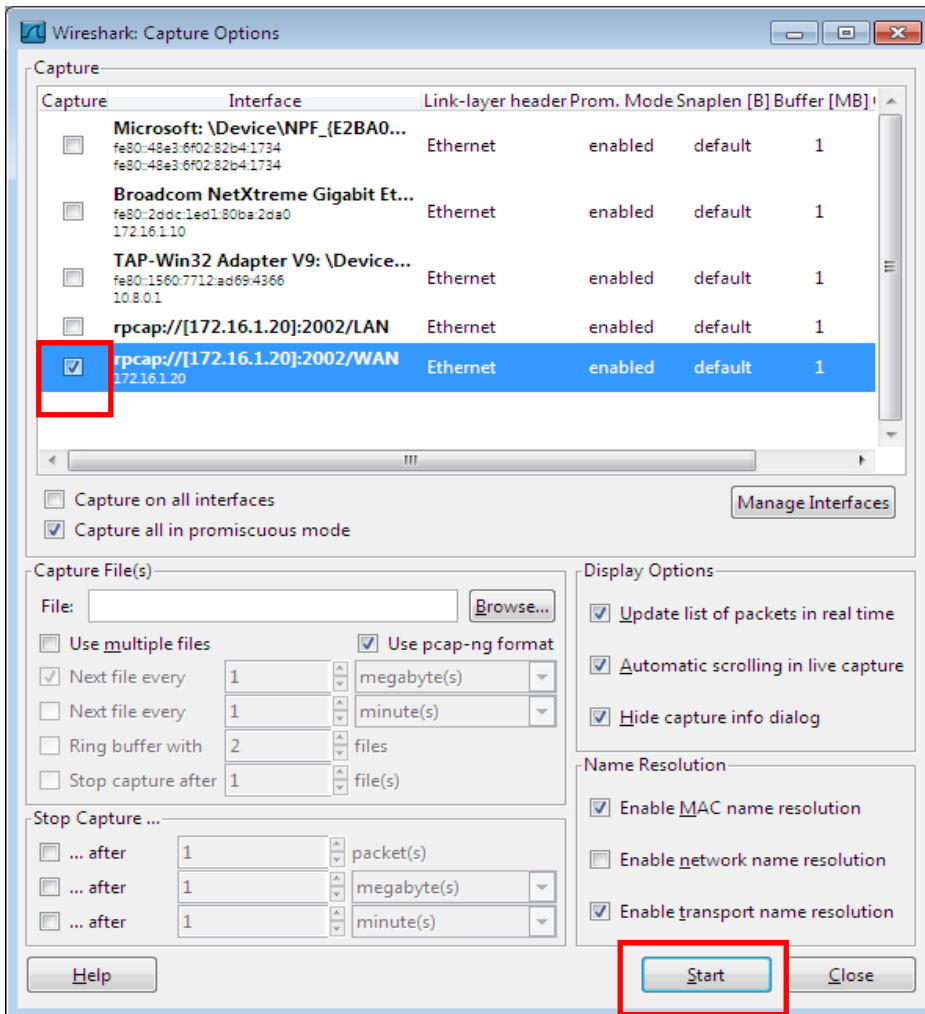


12. Click button “Remote Settings”

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

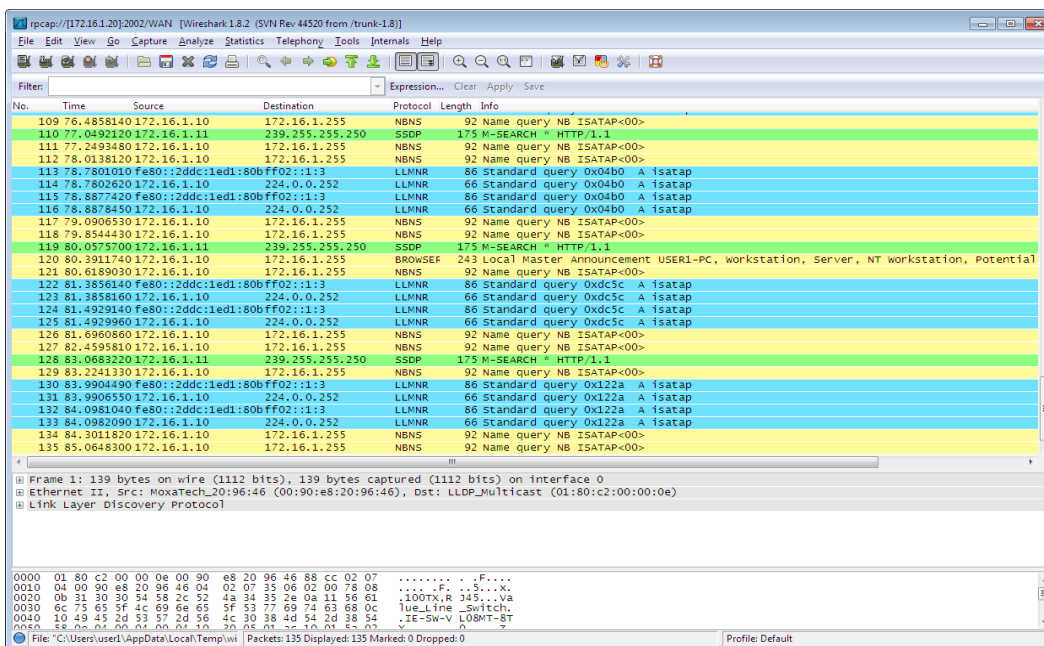
14. Click button “OK”

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**

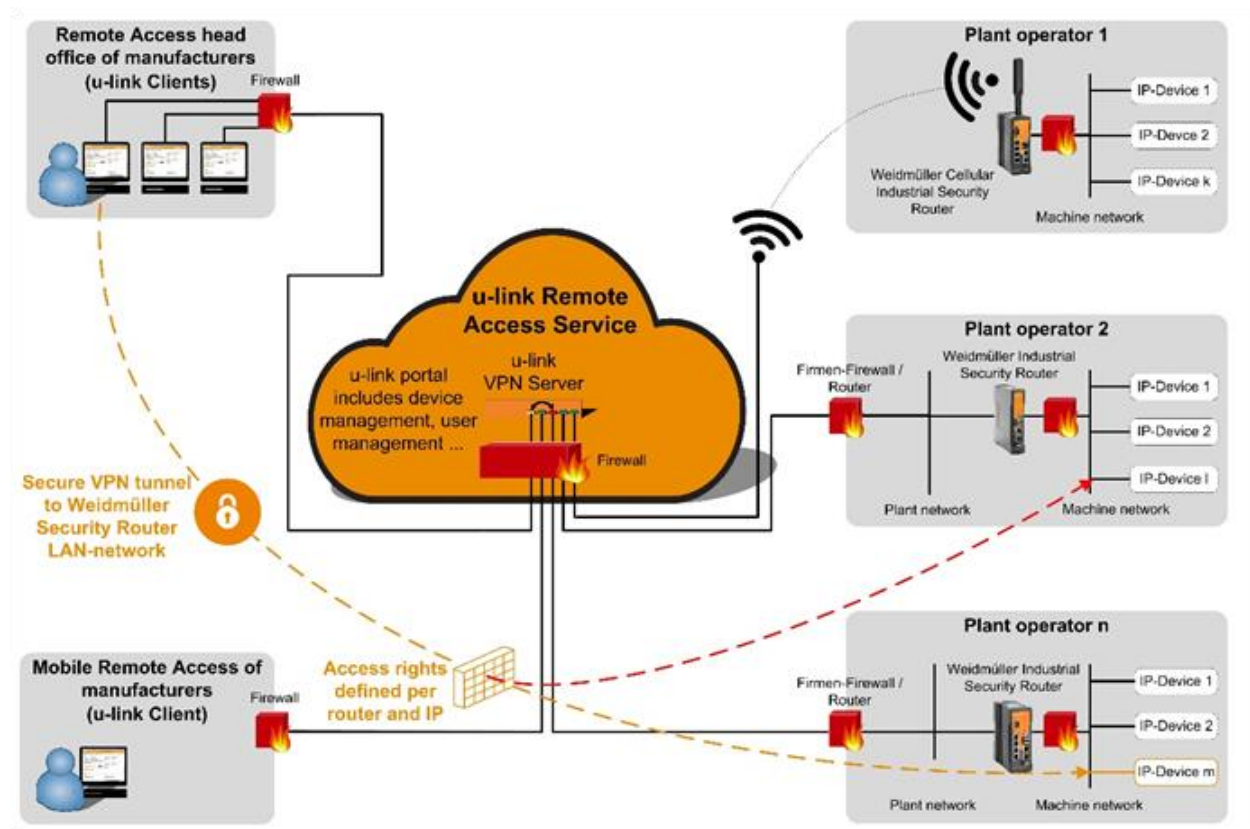
17. Click button “Start” to record the traffic at Routers WAN port



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.


Available u-link versions

Entry Version

- Can be used free of charge and timely unlimited.
- Max. configuration of 50 Routers (Access point to remote network).
- Unlimited configuration of user accounts (Service user).
- All defined users belong to same group "Service group".
- All defined Routers are members of the same "Device container" and can be accessed from all Service users.
- Any connected service user always can access the complete remote IP network connected to Router LAN port (No Filtering or selective access).
- At a time max. 2 service users may establish a pass-through connection to a Router/Remote network via u-link.
- Data performance:
 - Max. 500 kBit/sec per service user up to a data volume <= 1 GB/Month (Cumulative value, valid for all service users)
 - Bandwidth reduction to max. 64 kBit/sec for a data volume > 1GB/Month
- Integrated reporting- und status information.
- No guaranteed system availability.

Standard Version(s) 150, 300, 500 und unlimited

- Payable versions with a term of 1 year (Extension of a license by purchase of a new license key).
- Dependent on license max. configuration of 150, 300, 500 or unlimited numbers of Routers.
- Variable organization of Routers in different device containers (e.g. Locations, groups, etc.).
- Unlimited configuration of user accounts (Service user).
- Creation of additional user groups for access to selected devices and/or device containers.
- Configurable access of service users to defined IP addresses of a target network (Network filter).
- At a time max. 3 service users may establish a pass-through connection to a Router/Remote network via u-link.
- Option for booking additional VPN tunnels to be used concurrently.
- Data performance:
 - 1 MBit/sec per service user up to a data volume <= 5 GB/Month (Cumulative value, valid for all service users).
 - Bandwidth reduction to max. 512 kBit/sec for a data volume > 5 GB/Month.
 - Each additional booked VPN tunnel provides for an additional data volume of 1 GB/Month the bandwidth of 1 MBit/sec.
- Extended reporting- und status information.
- Guaranteed system availability: ≥ 99,6%

	Note
	<p>For more details about u-link please download documents</p> <ul style="list-style-type: none"> • u-link Introduction and Overview and • u-link Technical User Guide <p>from web page "Maintenance and cloud service" (using below link).</p> <p>http://www.weidmueller.com/int/products/electronics-and-automation/maintenance-and-cloud-service</p>