

Industrial Security Router / Firewall

IE-SR-2GT-LAN
IE-SR-2GT-LAN-FN
IE-SR-2GT-LTE/4G (EU/US)
IE-SR-6GT-LAN
IE-SR-6GT-LTE/4G (EU/US)
IE-SR-2GT-LTE/4G-EU-M
IE-SR-2GT-LAN-M



Manual

Version 2.0.4

March 2020

Important notes:

This document will be updated continuously.

This version refers to Router firmware version 3.5.0 and above.

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

<http://www.weidmueller.com>

- ▶ Select **Product Catalogue**
- ▶ Select „Active Industrial Ethernet “
 - ▶ Select „Industrial Security Router“
 - ▶ Select any product model
 - ▶ 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 OF 2-PORT MODELS	14
2.3 INTERFACES OF 6-PORT MODELS	14
2.3 PIN ASSIGNMENTS	16
Pin assignment of power supply connector.....	16
Pin assignment of RJ45 Ethernet ports (LAN and WAN).....	16
Pin assignment of 4-pin connector for „VPN initiate“ and „VPN active“	16
Pin assignment of 4-pin connector for „Cut WAN port“ and „Signalize Alarm“	16
Pin assignment of USB 2.0 connector	16
Pin assignment of Smartcard Reader (ISO 7816 Standard).....	17
Pin assignment serial interface COM (RS232)*	17
3. INITIAL START-UP / GETTING STARTED	18
3.1 Configuration of the Router by using an Internet browser	18
3.2 Starting the Web interface	18
3.3 Default factory settings of the Router:.....	20
3.4 Reset to factory default settings by external push button.....	20
3.5 Using the Weidmüller Router-Search-Utility.....	21
3.6 Basic description of Router's configuration interface (menu items)	22
4. WEB CONFIGURATION	23
4.1 SECTION DIAGNOSTICS.....	23
4.1.1 Diagnostics → System State	23
4.1.2 Diagnostics → Event Log (Tab State)	24
4.1.3 Diagnostics → Event Log (Tab Configuration)	24
4.1.4 Diagnostics → WAN.....	25
4.1.5 Diagnostics → LAN.....	25
4.1.6 Diagnostics → 4G.....	26
4.1.7 Diagnostics → Ping test.....	28
4.1.8 Diagnostics → Remote capture	29
4.2 SECTION CONFIGURATION	30
4.2.1 Configuration → IP Configuration.....	30
IP Configuration → Operational mode “IP Router”	30
IP Configuration → Operational mode “IP Router (Extended)”	33
IP Configuration → Operational mode “Transparent bridge”	34
4.2.2 Configuration → SecureNow! (Learning Firewall).....	35
4.2.3 Configuration → Packet filter (Firewall).....	37
4.2.4 Configuration → Cut & Alarm.....	38
4.2.5 Configuration → General settings.....	39
General settings → System data.....	39
General settings → Date & Time	40
General settings → User Interface.....	41
General settings → Certificates	41
General settings → SCEP (Tab Configuration)	42
General settings → SCEP (Tab State)	42

4.2.6 Configuration → Access Control	43
Access Control → User accounts	43
Access Control → Permissions	43
Access Control → Web access	44
4.2.7 Configuration → Network	44
Network → DNS (Tab Configuration)	44
Network → IP Routing (Tab Configuration)	46
Network → IP Routing (Tab State)	48
Network → HTTP proxy	48
Network → Forwarding	49
Network → 1:1 NAT	51
Network → Network Groups	52
Network → Hardware Groups	52
Network → Ethernet Interfaces	53
4.2.8 Configuration → VPN	54
VPN → u-link (Tab Configuration)	54
VPN → u-link (Tab State)	55
VPN → u-link (Tab Registration)	56
VPN → OpenVPN (Tab Configuration)	56
VPN → OpenVPN (Tab VPN1)	57
VPN → OpenVPN (Tab State)	59
VPN → IPsec (Tab Configuration)	59
VPN → IPsec (Tab State)	62
4.2.9 Configuration → Services	63
Services → DHCP Server (Tab Configuration)	63
Services → DHCP Server (Tab State)	64
Services → Dynamic DNS	64
Services → Web server	65
Services → SNMP	65
Services → Modbus TCP	66
Services → Client Monitoring	70
Services → SMS Service	71
Services → COM port server	73
4.2.10 Configuration → Prioritization	74
Prioritization → LAN	74
Prioritization → LAN	76
Prioritization → 4G	76
4.3 SECTION SYSTEM	77
4.3.1 System → Backup settings	77
4.3.2 System → Software update	77
4.3.3 System → Factory defaults	78
4.3.4 System → Save	79
4.3.5 System → Reboot	79
4.4 SECTION INFORMATION	80
4.4.1 Information → General	80
4.4.2 Information → Sitemap	80
5. APPENDIX A (CONFIGURATION EXAMPLES)	81
A1 – RESTORE CONFIGURATION FROM USB STICK	81
A2 – BASIC ROUTER CONFIGURATION TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES	83
A3 - CONNECTING 2 ETHERNET NETWORKS WITH ACTIVATED NAT MASQUERADING AND USING IP ADDRESS FORWARDING	87
A4 - CONFIGURING THE ROUTER TO CONNECT 2 NETWORKS WITH DIFFERENT IP ADDRESS RANGES AND ADDITIONAL FIREWALL RULES	92
A5 – FIREWALL APPLICATION EXAMPLE: SECURING THE ACCESS TO MODBUS TCP DEVICES BY LAYER-2 FIREWALL RULES	99
A6 - CONNECTING 2 NETWORKS WITH SAME IP RANGES TO ANOTHER NETWORK USING 1:1 NAT AND IP ROUTING (EXTENDED)	113
A7 - USING DYNAMIC IP ROUTING ALTERNATIVELY TO MANUALLY CONFIGURED STATIC ROUTES (REFERS TO EXAMPLE A6)	119
A8 - HOW TO USE FEATURE “REMOTE CAPTURE” WITH WIRESHARK TO ANALYSE ROUTER’S LAN/WAN TRAFFIC	121
A9 - U-LINK REMOTE ACCESS SERVICE → VPN BASED CONNECTION TO REMOTE LOCATIONS	126

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-xGT-LAN or IE-SR-xGT-LTE/4G)
- 1 x 3-pin connector for power supply
- 2 x 4-pin connectors for special digital inputs and output signals (Alarm, CUT, VPN)
- 1 x Ethernet cable (Length 1 m)
- 2 x antennas 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
	- Using the selected device for purposes other than those specified or failure to observe the operating instructions and warning notes can lead to serious malfunctions that may result in personal injury or damage to property. - If this product malfunctions, it is no longer possible to predict the behavior of neighboring networked facilities and their connected devices. Personal injury and property damage can occur because of malfunctions. Only carry out changes to the settings when you are certain of the consequences such changes will have on all connected networks, facilities and devices. - Personal injury and property damage can occur if this product is used improperly. Adjustments and setting changes to this product should only be carried out by sufficiently qualified personnel.

	Caution
	- This device is designed only for an operating voltage range from 7 to 36 V DC. Do not use a higher voltage; this could destroy the Router and other devices. - The Security Router does not have an on/off switch. The operating voltage must be switched on by the facility in which the device is integrated.

	Caution
	You should activate and synchronize the time server or set the system time manually if you are using certificates in virtual private networks (VPNs) or simple network management protocol (SNMP). An inaccuracy in the system time can cause the virtual private network (VPN) to malfunction. You should synchronize the system time with a time server after each Router reboot and after you load the default settings. Or you can set the system time manually.

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

	Note
	- The IP protocol reserves certain IP address ranges for special purposes (such as multicasting). Do not assign IP addresses in the range from 127.0.0.0 – 127.255.255.255 or 224.0.0.0 – 255.255.255.255. - This device is intended for use in applications as described in the operating instructions only. Using this device in non-approved applications will lead immediately to the expiration of all guarantee and warranty claims on the part of the operator against the manufacturer.

1.4 Mounting the device

	Caution
	- This device is designed only for an operating voltage range from +7 to 36 VDC. Do not use a higher voltage; this could destroy the Router and other devices. - Connecting plugs should never be connected or disconnected from electrical devices if they are carrying a live load. Be sure to first disconnect all poles of the plug. Remember to disconnect all plugs from the Router before it is installed or removed. - Electrical devices should not be installed or removed during operations. Never install or remove the Router while it is running.

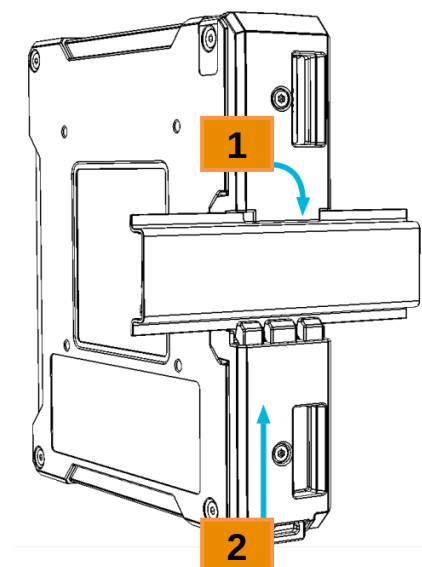
	Caution
	- It is important to provide sufficient clearance between devices which cause strong electromagnetic interference (such as frequency converters, transformers or motor regulators). The clearance gap between such devices and the Router should be as wide as possible. The Router can be further shielded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

	Note
	- A minimum of 2-inch (5 cm) gap should be kept between the Router and neighboring devices <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 top of the DIN-rail clip behind the upper edge of the DIN-rail (1). Then open the latch (2) at bottom of the device by using a flat-bladed screwdriver and fix the device on the DIN-rail by gently pressing on the bottom.

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



1.5 Technical data

Operation mode

IP-Router	• 2-Port-Variants: IPv4-Routing between the interfaces (LAN port / WAN port / optional 4G modem). • 6-Port-Variants: IPv4-Routing between LAN ports (group), WAN ports (group) and 4G modem (optional). LAN-Ports 1..4 and WAN-Ports 1..2 behave each as an unmanaged switch. • Static or dynamic routing according to RIPv2 or OSPF protocol.
IP-Router (extended)*	• Each RJ45 port can be configured individually as an IPv4 network. • IPv4-Routing between all available RJ45 ports (LAN 1..4, WAN 1..2) and 4G modem (optional). • A maximum of 6 individual subnets (using LAN/WAN ports) can be configured. • Static or dynamic routing according to RIPv2 or OSPF protocol.
Transparent Bridge	• Running as 2/6-Port-Switch with additional Layer-2 (MAC) or Layer-3 (IP-based) filter.
Network Services	• DHCP Server / DHCP Relay • DNS-Relay • NTP-Client • DynDNS (DHCP-Client according to RFC 2136)
Firewall	• IPv4 Stateful inspection Firewall • NAT-Masquerading, 1:1 NAT, Port forwarding • Layer-2/3-Filter (VLAN ID, VLAN QoS Tag, MAC address based, Ethernet Frame) • "Auto-Learning"-function (SecureNow) to create new packet filter rules (Analysis of the network traffic). • Layer 2/3 packet prioritization (Ethernet Frame, IP Header, VLAN Tag)

* available for IE-SR-6GT-LAN and IE-SR-6GT-LTE/4G only

VPN (not available for model IE-SR-2GT-LAN-FN)

OpenVPN	• Configurable as OpenVPN server or client (Layer 2 and Layer 3) • Authentication with X.509 Certificates • Tunnel support via HTTP-Proxy • A maximum of 10 different server configurations • Unlimited number of client connections in server mode
IPsec	• Can be configured as an IPsec server or client. • Authentication with PSK (user ID, password) or X.509 certificates. • Hardware encryption for faster data flow rate. • A maximum of 64 simultaneous connections (subnet with subnet or as IPsec server) • Encryption algorithms DES-56, 3DES-168, AES 128, AES 192, AES-256
u-link	• Based on certificate-secured OpenVPN technology • To be used with the Weidmüller Remote Access Service • Simplifies VPN connections and management • Fast and easy connections • Free of charge • Visit https://u-link.weidmueller.com for further information.

Configuration

Management	• Configuration with web interface (HTTP/HTTPS) • Web interface selectable in English or German language • Configuration support through wizard • Configuration support through detailed help information (tooltip) • Configurable Multi-user access with definable rights • Support for SNMP v1/v3/v3 • Event log / syslog
------------	---

Other features

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

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

Interfaces

RJ45-Ports	• 2 x 10/100/1000BaseT(X)*¹ • 6 x 10/100/1000BaseT(X)*²
USB-Port	• Useable for automatic configuration restore from backup file (*.cf2) or firmware upgrade via USB stick at boot process
RS 232* ²	• Interface for COM-port server function
SCM card reader	• 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* ³	• Insert SIM card for mobile communication
LED displays	• Signaling the status for power, device status, Cut, Alarm, active VPN connection*⁴ and an active cellular connection*³
Digital Outputs	• "Alarm" -> Indicates a configurable network status or error (24V out) • "VPN-active" -> Indicates an active VPN connection (24 V out)*⁴
Digital Inputs	• "Cut" -> Disconnects physically (link down) the WAN port (24 V In) • "VPN-initiate" -> Enables a pre-configured VPN connection (24 V In)*⁴
Reset-Button	• Restore to the factory settings

*¹ IE-SR-2GT-LAN, IE-SR-2GT-LTE/4G, -M Models and IE-SR-2GT-LAN-FN

*² IE-SR-6GT-LAN and IE-SR-6GT-LTE/4G

*³ for LTE/4G models only

*⁴ not available for model IE-SR-2GT-LAN-FN

Power

Input Voltage	• 1* 24 VDC (7 to 36 Volt) Use a power supply according to NEC Class 2 for use according to UL certification
Current consumption	• Max. 600 mA @ 24 VDC (2-Port models) • Max. 800 mA @ 24 VDC (6-Port models)

Technical data (housing)

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

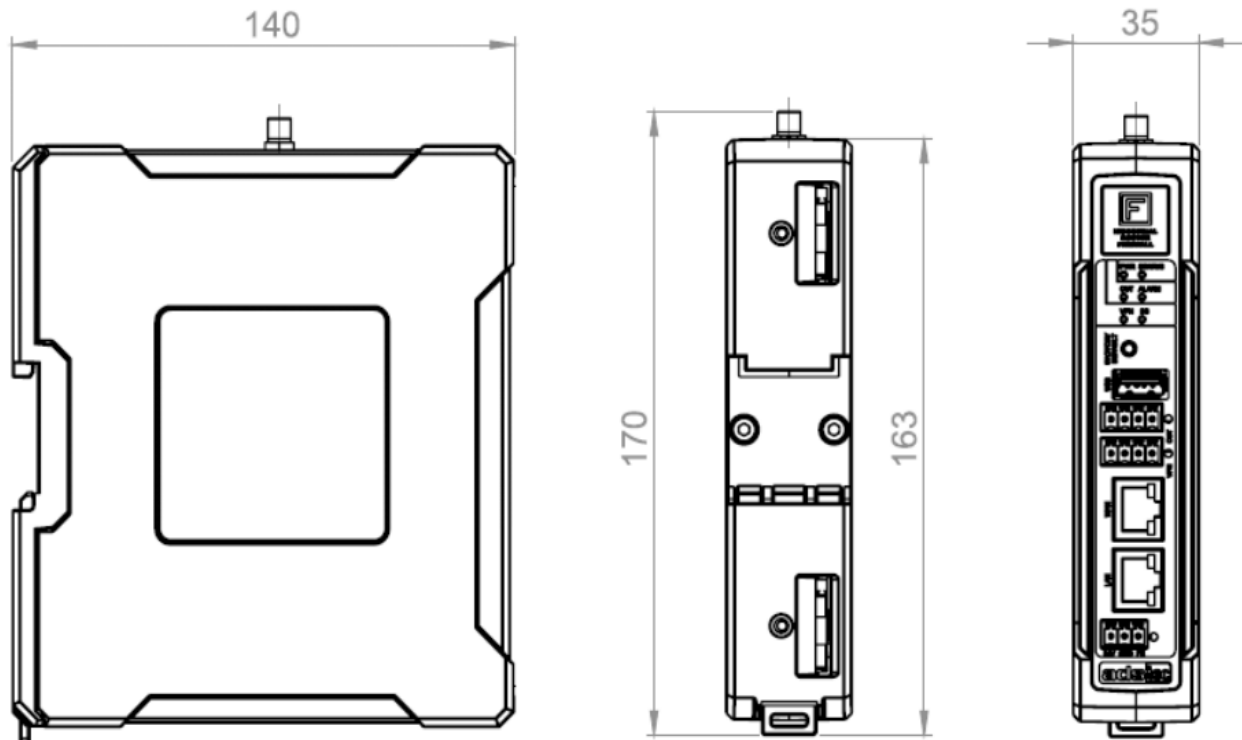


Figure 1: Dimensional drawings (cm) of 2-Port models

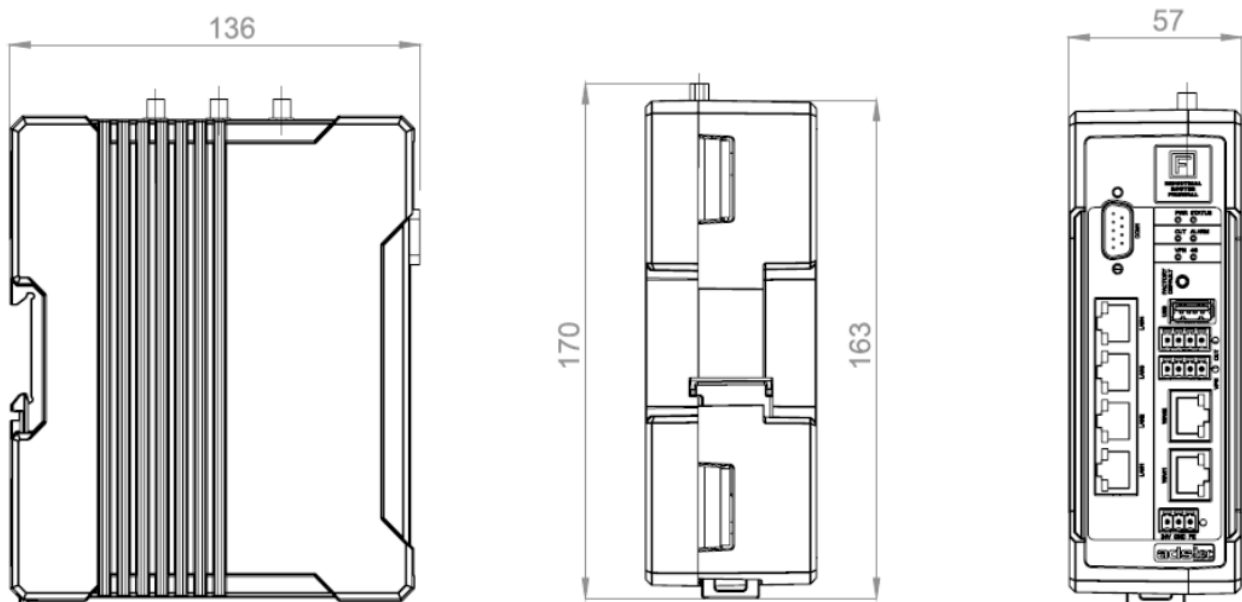
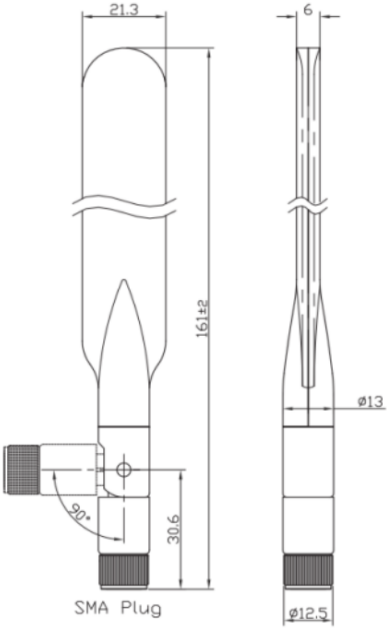


Figure 2: Dimensional drawings (cm) of 6-Port models

Environmental conditions

Operating Temperature	-20°C to +70°C
Storage Temperature	-20°C to + 85°C
Ambient Humidity	5 to 90% non-condensing

DSL and 4G/LTE

DSL	- DSL Internet access by connecting to an external DSL modem via LAN or WAN port - Free configuration of the PPPoE login
DynDNS	Support for automatic DNS registration (DynDNS.org)
LTE/4G*	- Built-in 4G/LTE modem with 300 Mbps peak downlink and 50 Mbps peak uplink - FCC, CE, FCC, IC, NCC, PTCRB, Bell, AT&T
Standards*	- LTE: 3GPP Release 11 - UMTS: 3GPP Releases 9
Frequency bands US, EMEA and Australia*	LTE: B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B29, B30, B41reduced data rates UMTS: B1, B2, B3, B4, B5, B8
Transmit power*	- LTE Bands 1, 2, 3, 4, 5, 8, 13, 17, 20, 25, 26: +23 dBm ± 1 dB - LTE Bands 7, 30, 41: +22 dBm ± 1 dB - UMTS Bands 1, 2, 3, 4, 5, 8: +23 dBm ± 1 dB
Antennas*	Antenna gain and frequencies: 0 dBi @ 790-960 MHz 1 dBi @ 1710-2170 MHz 3 dBi @ 2500-2700 MHz - Polarisation: linear 

* Only models IE-SR-2GT-LTE/4G, IE-SR-6GT-LTE/4G and IE-SR-2GT-LTE/4G-M

Approvals

Safety	cULus (UL508)
EMC	- FCC Part 15 Class A, - EN61000-6-2 Immunity for industrial environments - EN61000-6-4 Emission Standard for industrial environments

	• IEC 60945, DNVGL sec. 5/14/15 electrical discharge, fast transients (burst), conducted radio/audio frequency, electromagnetic fields, voltage drops and fluctuations, compass safe distance*
Shock	• DIN EN 60068-2-27 • IEC 60945, DNVGL-CG-0339*
Vibration	• DIN EN 60068-2-6 • IEC 60945, DNVGL-CG-0339*

* Only models IE-SR-2GT-LAN-M and IE-SR-2GT-LTE/4G-M

Warranty

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

Order Information

	Model name	Order number
2-Port LAN/WAN Router with VPN features	IE-SR-2GT-LAN	1345270000
2-Port LAN/WAN Router without VPN features	IE-SR-2GT-LAN-FN	1489940000
2-Port LAN / WAN Router with VPN features and additional integrated LTE/4G modem	EU: IE-SR-2GT-LTE/4G-EU US: IE-SR-2GT-LTE/4G-US	2535930000 2535780000
6-Port LAN/WAN Router with VPN features	IE-SR-6GT-LAN	2535940000
6-Port LAN / WAN Router with VPN features and additional integrated LTE/4G modem	EU: IE-SR-6GT-LTE/4G-EU US: IE-SR-6GT-LTE/4G-US	2535960000 2535950000

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

2.2 Interfaces of 2-Port models



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)
USB 2.0 connector
4-pin connector („Cut WAN port“ and „Signalize Alarm“) - 24 VDC input for Cut signal (Disabling WAN interface) and - 24 VDC output for signaling an alarm event
4-pin connector („VPN initiate“ and „VPN active“) - 24 VDC input for initiating a predefined VPN tunnel - 24 VDC output for signaling an active VPN tunnel
1 x RJ45-Connector WAN (10/100/1000BaseTX)
1 x RJ45-Connector LAN (10/100/1000BaseTX)
3-pin connector for 24V DC power supply (Socket connector is included)

2.3 Interfaces of 6-Port models



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)
USB 2.0 connector for configuration restore
4-pin connector („Cut WAN port“ and „Signalize Alarm“) - 24 VDC input for Cut signal (Disabling WAN interface) and - 24 VDC output for signaling an alarm event
4-pin connector („VPN initiate“ and „VPN active“) - 24 VDC input for initiating a predefined VPN tunnel - 24 VDC output for signaling an active VPN tunnel
2 x RJ45-Connector WAN (10/100/1000BaseTX)
4 x RJ45-Connector LAN (10/100/1000BaseTX)
3-pin connector for 24V DC power supply (Socket connector is included)
RS232 Interface (Sub-D9) to be used as COM port server

Description of device interfaces at rear side for 2-Port models



SCM slot / socket

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

4G slot / socket

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



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.

Description of device interfaces at rear side for 6-Port models



SCM slot / socket

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

4G slot / socket

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



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

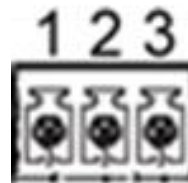
Use coaxial cable with nominal impedance of 50 ohms.

2.3 Pin assignments

Pin assignment of power supply connector

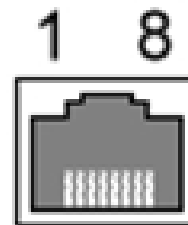
Note: Allowed input voltage range from 7 to 36 VDC (24 VDC typical)

Pin number	SIGNAL NAME
1	24V DC
2	GND
3	PE



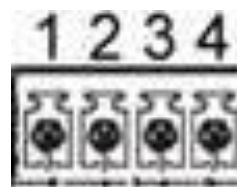
Pin assignment of RJ45 Ethernet ports (LAN and WAN)

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-



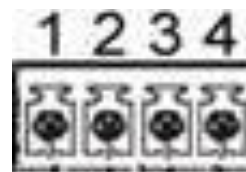
Pin assignment of 4-pin connector for „VPN initiate“ and „VPN active“

Pin number	SIGNAL NAME
1	24V DC (VCC)
2	Initiate VPN (24 V In)
3	VPN active (24 V Out)
4	GND



Pin assignment of 4-pin connector for „Cut WAN port“ and „Signalize Alarm“

Pin number	SIGNAL NAME
1	24V DC (VCC)
2	Cut (Disabling WAN-Port, 24 V In)
3	Signalize Alarm (24 V Out)
4	GND



Pin assignment of USB 2.0 connector

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

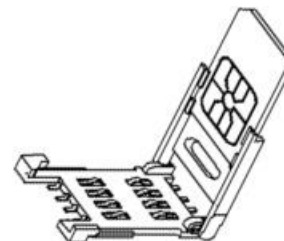
Pin number	SIGNAL NAME
1	VDC
2	D -
3	D+
4	GND



Pin assignment of Smartcard Reader (ISO 7816 Standard)

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

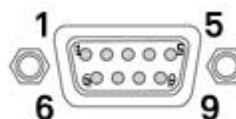
Pin number	SIGNAL NAME
1	VCC 5 Volt
2	RESET
3	CLOCK
4	n/c
5	GND
6	n/c
7	I/O
8	n/c



Pin assignment serial interface COM (RS232)*

The serial interface is used for digital data transmission. The RS232 interface can be connected by using a commercially available 9-pin SUB-D cable.

Pin number	SIGNAL NAME
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI



* 6-Port models only

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 (3-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 to 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 ports at 2-Port models: 192.168.2.110 / 255.255.255.0

WAN ports at 6-Port models: DHCP

3.2 Starting the Web interface



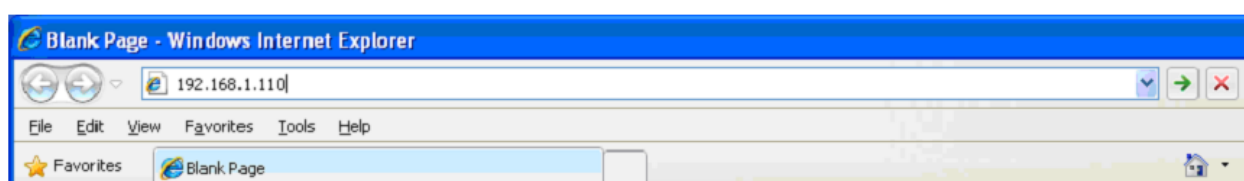
Important note

The Router's Web server **partly** is using Java script for parameter settings (e.g. if you want to apply or 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.

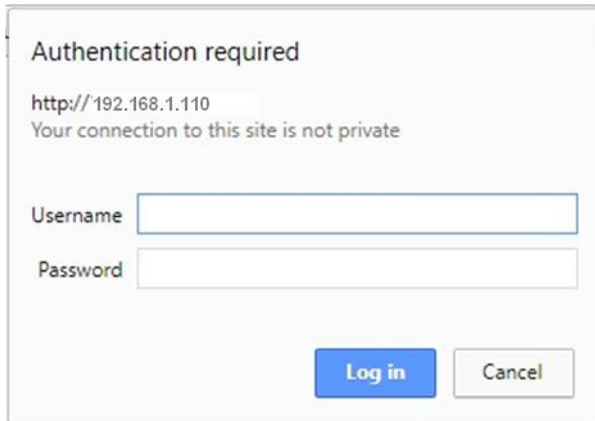
1. Start your Web browser and enter the IP address of the connected Router port into the browser's address line. (i.e. when connected to a LAN-Port 192.168.1.110)



- 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

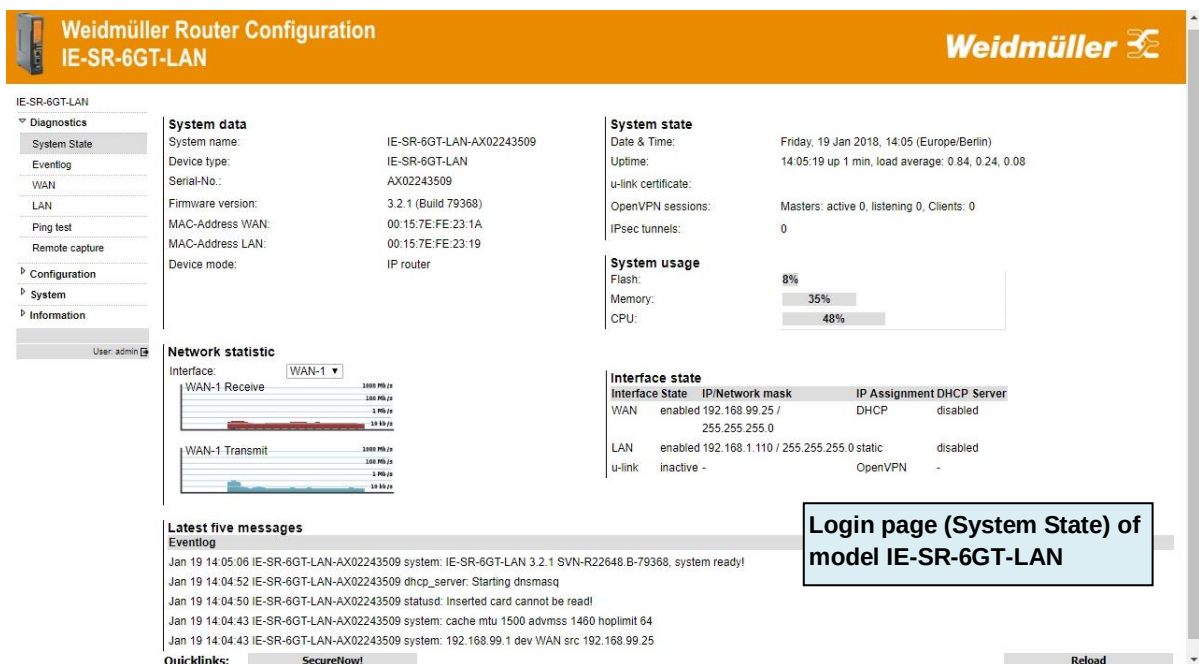
http://192.168.1.110
 Your connection to this site is not private

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 Pkts/s, 100 Pkts/s, 10 Pkts/s, 1 Pkts/s, 0.15 K/s

WAN-1 Transmit: 1000 Pkts/s, 100 Pkts/s, 10 Pkts/s, 1 Pkts/s, 0.15 K/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!](#)

Login page (System State) of model IE-SR-6GT-LAN



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	2-Port variants: 192.168.2.110 (static value) 6-Port variants: DHCP
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 (not for IE-SR-2GT-LAN-FN)	Disabled
Data prioritization	Disabled
4G Modem (for IE-SR-6GT-LTE/4G and IE-SR-6GT-LTE/4G 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

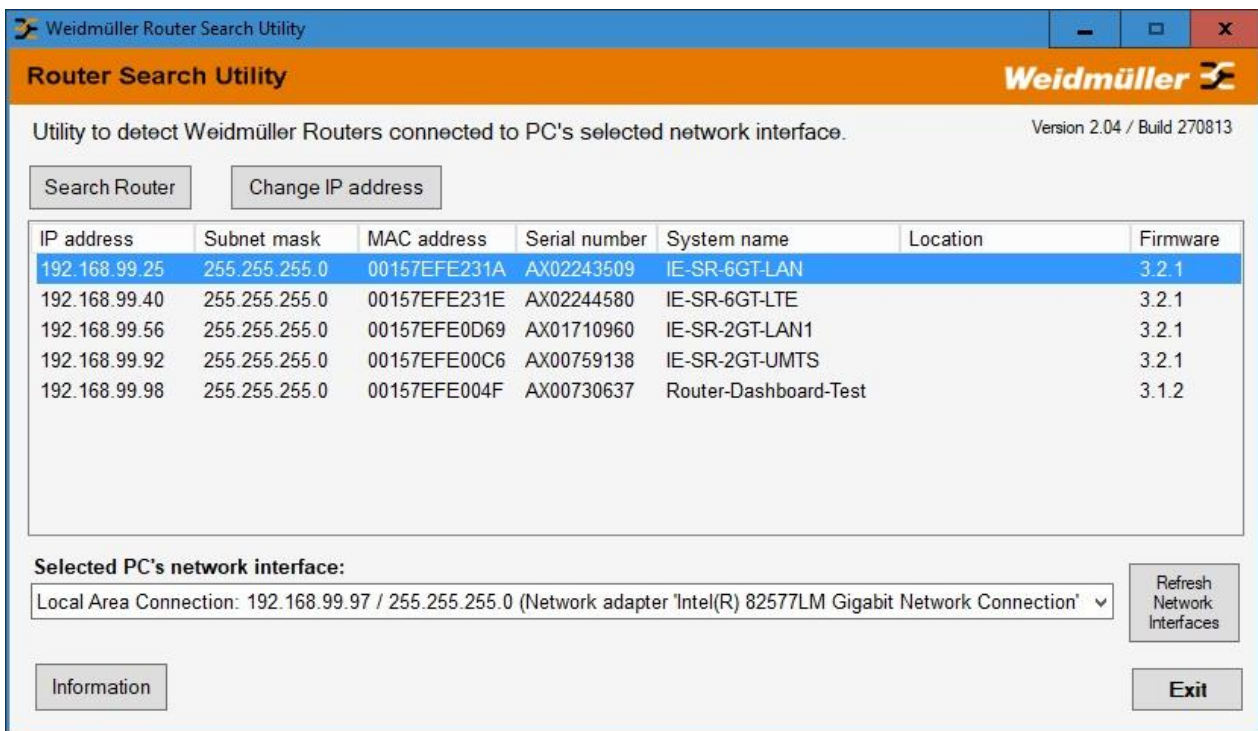
The software tool Weidmüller Router-Search-Utility can be used to find Weidmüller Routers and detect their IP addresses within a switched network. This software is very helpful if you don't know the current IP address of a Router. This can e.g. happen in cases that you have forgotten the current IP configuration, 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.weidmueller.com/IE
2. Select section "Industrial Ethernet" → „Software“
3. Select category "Additional Software (Configuration utilities, Drivers and MIB-files)"
4. Download from section *Industrial Security Router (Firmware and Software)*



Alternatively, you can download this software from this web page:

1. Open www.weidmueller.com
2. Select Service → Online support and downloads → Product software → Industrial Ethernet
3. Download from section *Industrial Security Router (Firmware and Software)*

Alternatively, you can download this software from the online catalog:

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 operation mode (*IP Router*, *IP Router (extended)* or *Transparent Bridge*) and basic network parameters (IP addresses, Default gateway)
- Setting of firewall rules (Packet filter and an additional auto learning feature called „SecureNow!“ to assist the creation of packet filtering rules)
- Configuration of general system data (name, location, contact person, date / time, language interface, etc.)
- Certificate Management for VPN connections (not available for model IE-SR-2GT-LAN-FN)
- User administration (assignment of rights)
- IP-Routing (static, dynamic) and IP address management (Masquerading, 1:1 NAT, Port forwarding)
- Configuration of u-link Remote Access Service / OpenVPN / IPsec connections (not available for model IE-SR-2GT-LAN-FN)
- Configuration of general network services (e.g. DHCP, DBS, SNMP)
- Prioritization of network traffic (Layer-2 and Layer-3 level)

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

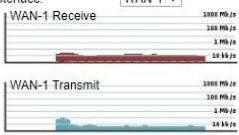
Flash: 8%

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

State

Configuration

Diagnostics

System State

Eventlog

WAN

LAN

Ping test

Remote capture

Configuration

System

Information

User: admin

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 from 192.168.99.1
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

State

Configuration

Diagnostics

System State

Eventlog

WAN

LAN

Ping test

Remote capture

Configuration

System

Information

User: admin

Eventlog

Enable remote syslog: ☒ 

Send all log messages to a remote machine.

Address of syslog server:

UDP port of syslog server:

Enable syslog to e-mail: ☐

E-mail server:

E-mail address:

Line threshold:

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
	Enable syslog to e-mail	Send syslog files to an e-mail address
	E-mail server	Local syslog-server address
	E-mail address	E-mail address of the syslog-receiver
	Line threshold	Amount of code lines in an email

4.1.4 Diagnostics → 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. At the 6-Port routers in extended router mode you can choose the WAN interface via the tabs (WAN-1 and WAN-2) at the top of the web interface.

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. At the 6-Port routers in extended router mode you can choose the WAN interface via the tabs (LAN-1 to LAN-4) at the top of the web interface.

4.1.6 Diagnostics → 4G



Weidmüller Router Configuration

IE-SR-6GT-LTE/4G



IE-SR-6GT-LTE/4G

State

Diagnostics
System State
Eventlog
WAN
LAN
4G
Ping test
Remote capture
Configuration
IP configuration
SecureNow!
Packet filter
Cut & Alarm
General settings
Access control
Network
VPN
Services
Prioritization
System
Backup settings
Software update
Factory defaults
Save
Reboot
Information
General
Sitemap

4G state

Modem Vendor: Sierra Wireless, Incorporated
Model: MC7304
Revision: SWI9X15C_05.05.16.02 r21040 carmd-fvbuild1 2014/03/17 23:49:48
IMEI SV: 11
Firmware version: 05.05.16.02
Config version: GENEU-4G_005.006_001
Carrier name: GENEU-4G

State: online

Registration state: Registered to home network ⓘ
Active network provider:
Signal strength:  -77 dBm
Signal quality:  -10 dB (RSRQ) ⓘ
Network mode: LTE
Mobile Country Code (MCC): 262
Mobile Network Code (MNC): 3
Tacking Area Code (TAC): 14570
Band: B3
Cell ID: 11157273
Roaming: off
Mobile modem temperature: 34 °C
Mobile modem voltage: 3309 mV

Local IP: 10.40.45.181/30

Received bytes: 664
Received packets: 2
Received dropped packets: 0
Received overrun packets: 0
Transmitted bytes: 684
Transmitted packets: 2
Transmitted dropped packets: 0
Transmitted overrun packets: 0

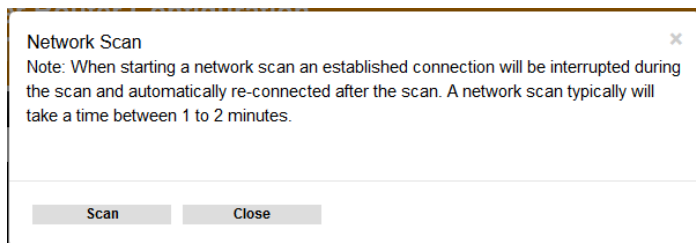
Reload
Reconnect
Network Scan

User: admin

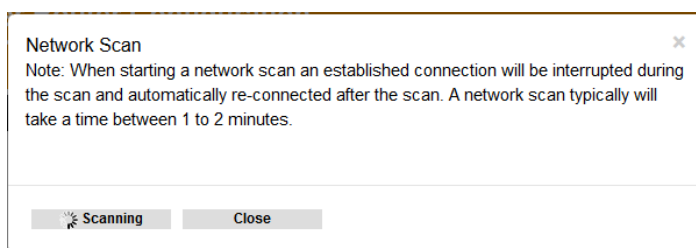
Menu	Diagnostics → 4G	
Function	Displays the current status of the 4G mobile connection.	
	Menu available for IE-SR-2GT-LTE/4G and IE-SR-6GT-LTE/4G only.	
	Reload	Refreshes the page with actual values
	(Re)Connect	(Re)establishes the 4G connection.
	Network Scan	Performs a scan of networks available

Network Scan

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



Klick "Scan":



Scan result:

Network Scan				
Note: The shown data is provided by the mobile network. Therefore some network providers will be displayed with their short name (e.g. TDG = Deutsche Telekom).				
MCC	MNC	Network provider	Network mode	Status Network mode
262	1	TDG	GSM	available, roaming, forbidden, not_preferred
262	1	TDG	LTE	available, roaming, forbidden, not_preferred
262	1	TDG	UMTS	available, roaming, forbidden, not_preferred
262	2	Vodafone	GSM	available, roaming, forbidden, not_preferred
262	2	Vodafone	LTE	available, roaming, forbidden, not_preferred
262	2	Vodafone	UMTS	available, roaming, forbidden, not_preferred
262	3	E-Plus	GSM	available, home, not_forbidden, preferred
262	3	E-Plus	LTE	available, home, not_forbidden, preferred
262	3	E-Plus	UMTS	available, home, not_forbidden, preferred
Scan Close				

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

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

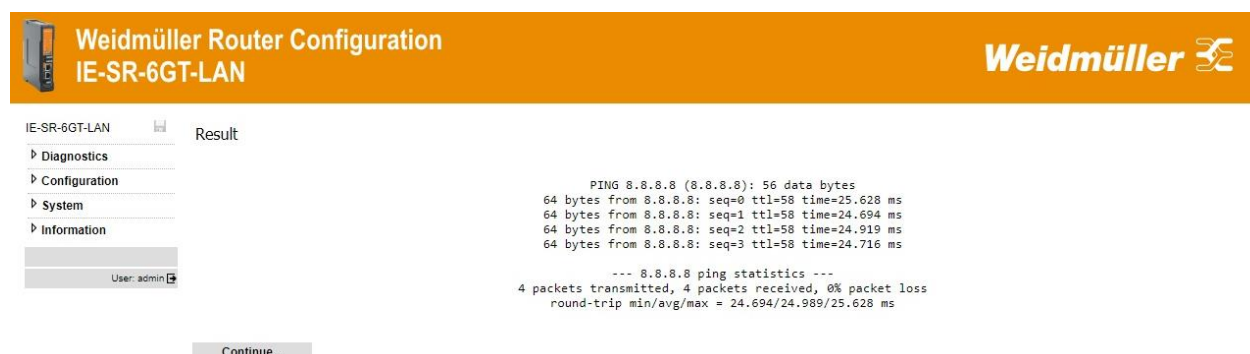
4.1.7 Diagnostics → Ping test



The screenshot shows the 'Ping test' configuration page in the Weidmüller Router Configuration interface. The left sidebar contains a menu with options: IE-SR-6GT-LAN, Diagnostics (selected), System State, Eventlog, WAN, LAN, Ping test (highlighted), Remote capture, Configuration, System, and Information. The main content area is titled 'Ping test' and includes input fields for 'IP address or hostname' (set to 8.8.8.8) and 'Number of ping messages' (set to 4). Below these fields are 'Apply settings' and 'Reset changes' buttons. A tooltip on the right explains: '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:



The screenshot shows the 'Result' of a ping test in the Weidmüller Router Configuration interface. The left sidebar is the same as in the previous screenshot. The main content area displays the following text:

```

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
  
```

At the bottom of the result area, there is a 'Continue...' button. The user is identified as 'User: admin'.

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: ☐ 

Apply settings

Reset changes

Menu	Diagnostics → Remote capture	
Function	By using the "remote capture" function data packets on both the LAN and the WAN port of the Router can be recorded for diagnostic purposes. The receiver of the diagnostic data is a PC/Server which must have installed the tool "Wireshark" listening on Port 2002. How to use please refer to application note in Appendix A .	
	Enable remote capture server	Enables the function
	Client address	IP address of permitted remote capture client (e.g. your service pc)
	Enable hub mode on LAN-port	Puts LAN-out interfaces into hub mode to allow capturing traffic between the ports. This option is ignored for IP-routing (extended) or VLAN use.
	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 → 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: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒ ⓘ

4G:

Dialmode: fallback ⓘ

PIN: ⓘ

Provider APN: ⓘ

Username: ⓘ

Password: ⓘ

Fallback for interface: LAN ⓘ

Fallback for IP address: ⓘ

DNS via 4G: ☒ ⓘ

NAT (Masquerading): ☒ ⓘ

Gateway via 4G: ☒ ⓘ

Preferred Network Mode: 4G ⓘ

Home Network only (no Roaming): ☐

Connect to specific provider/operator: ☒

Mobile Country Code(MCC): 000 ⓘ

Mobile Network Code(MNC): 00 ⓘ

Manual band selection: ☒

2G ☒ any ☒ G1900 ☒ G850 ☒ G900P ☒ G900 ☒ G1800

3G ☒ any ☒ B8 ☒ B5 ☒ B2 ☒ B1

4G ☒ any ☒ B20 ☒ B8 ☒ B7 ☒ B3 ☒ B1

Default gateway:

IP address:

Apply settings
Reset changes

Screenshot shows factory default operation mode ‘IP Router’.

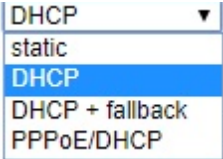
At factory default all 2-Port Routers do have configured static IP 192.168.2.110 at WAN port.

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	<u>Transparent bridge</u>: The device is acting like a layer 2 bridge and is transparent within a switched network. All Ethernet ports (LAN and WAN) behave like a common unmanaged Ethernet Switch. Only 1 IP address will be configured for accessing the web interface. This mode typically will be used for Layer 2 firewall application based on Ethernet frames (including IP packet control). <u>IP Router</u>: 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. <u>IP router (extended)*</u>: Supports flexible routing functions between WAN and LAN ports. In this mode each port WAN 1...2 and LAN 1...4 can be configured as an individual subnet with its own IP address range. The IP address ranges must not be the same for the ports.
	LAN / WAN IP assignment 	All interfaces can be configured with static or dynamic (DHCP) IP addresses. <u>Static</u>: Assign a static IP address and subnet mask to the interface. <u>DHCP</u>: Request an IP address from a DHCP (Dynamic Host Configuration Protocol) server. <u>DHCP + fallback</u>: First, try to request an IP address by DHCP and if it fails use the static one. <u>PPPoE</u>: The IP address will be assigned by the provider.
	4G (optional)	Configuration of 4G network connection
	Dialmode	Disabled: Do not use 4G modem. Manual: Dialing can be triggered manually from 4G status page. Permanent: The 4G link will be established automatically on system boot. Fallback: The 4G link will go online if the monitoring on the given interface "Fallback for interface" fails. The system will actively monitor the given IP addresses on the given interface. After a failure of at least 30 seconds the 4G link will be established.
	PIN	The Pin of your SIM-Card.
	Provider APN	Access point name (APN) of your provider for packet based services.
	Username	Username needed to authenticate at the APN (Access Point Name).
	Password	Password needed to authenticate at the APN (Access Point Name).
	Fallback for interface	Selection of the interface (LAN/WAN) 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.

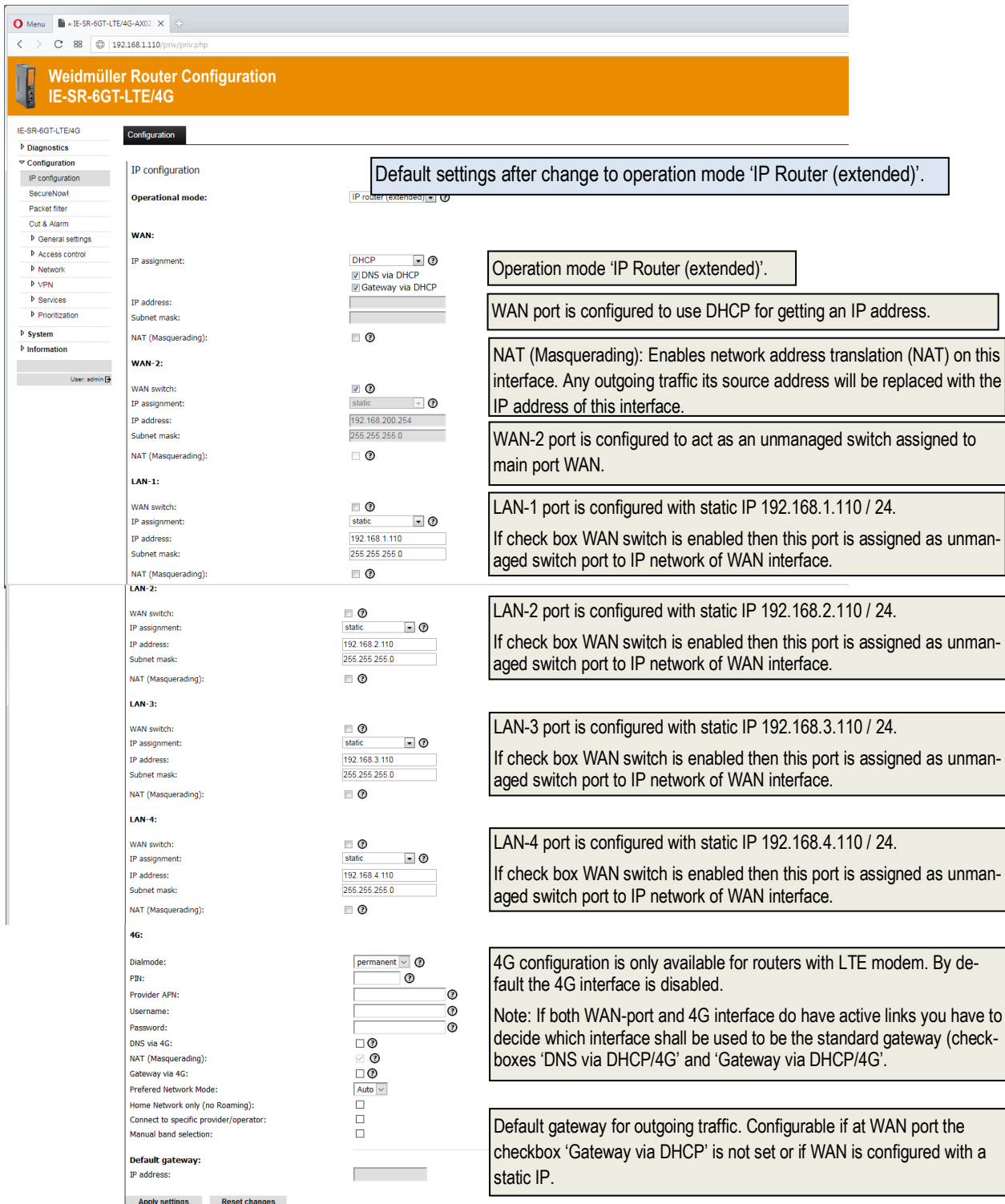
NAT (Masquerading)	Enable network address translation (NAT) on this interface. Any outgoing traffic, it's source address will be replaced with the IP address of this interface. NAT is always activated for 4G modem.
Gateway via 4G	If activated as soon as mobile connection is active (Online) it will be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

* for 6-Port models only

IP Configuration → Operational mode “IP Router (Extended)”

The extended routing mode is only available for 6-Port Router variants. Each interface (LAN 1...4, WAN 1..2, optional 4G modem) can be configured as individual IP network (Static, DHCP, DHCP + fallback or PPPoE). When using this mode then generally each router function (Firewall, Forwarding, NAT, etc.) can be applied to each interface same as it can be done to the standard LAN/WAN ports of a 2-Port Router.

Alternatively to an individual IP configuration of a LAN port each LAN port and port WAN-2 can be set as an unmanaged switch port assigned to IP address of main port WAN.



Default settings after change to operation mode 'IP Router (extended)'.

Operation mode 'IP Router (extended)'.

WAN:
 IP assignment: DHCP
☒ DNS via DHCP
☒ Gateway via DHCP

WAN-2:
 WAN switch: ☒
 IP assignment: static
 IP address: 192.168.200.254
 Subnet mask: 255.255.255.0
 NAT (Masquerading): ☐

LAN-1:
 WAN switch: ☐
 IP assignment: static
 IP address: 192.168.1.110
 Subnet mask: 255.255.255.0
 NAT (Masquerading): ☐

LAN-2:
 WAN switch: ☐
 IP assignment: static
 IP address: 192.168.2.110
 Subnet mask: 255.255.255.0
 NAT (Masquerading): ☐

LAN-3:
 WAN switch: ☐
 IP assignment: static
 IP address: 192.168.3.110
 Subnet mask: 255.255.255.0
 NAT (Masquerading): ☐

LAN-4:
 WAN switch: ☐
 IP assignment: static
 IP address: 192.168.4.110
 Subnet mask: 255.255.255.0
 NAT (Masquerading): ☐

4G:
 Dialmode: permanent
 PIN:
 Provider APN:
 Username:
 Password:
 DNS via 4G:
☒ NAT (Masquerading):
☐ Gateway via 4G:
 Preferred Network Mode: Auto
☐ Home Network only (no Roaming):
☐ Connect to specific provider/operator:
☐ Manual band selection:
Default gateway:
 IP address:

Callouts:

- Operation mode 'IP Router (extended)'.
- WAN port is configured to use DHCP for getting an IP address.
- NAT (Masquerading): Enables network address translation (NAT) on this interface. Any outgoing traffic its source address will be replaced with the IP address of this interface.
- WAN-2 port is configured to act as an unmanaged switch assigned to main port WAN.
- LAN-1 port is configured with static IP 192.168.1.110 / 24. If check box WAN switch is enabled then this port is assigned as unmanaged switch port to IP network of WAN interface.
- LAN-2 port is configured with static IP 192.168.2.110 / 24. If check box WAN switch is enabled then this port is assigned as unmanaged switch port to IP network of WAN interface.
- LAN-3 port is configured with static IP 192.168.3.110 / 24. If check box WAN switch is enabled then this port is assigned as unmanaged switch port to IP network of WAN interface.
- LAN-4 port is configured with static IP 192.168.4.110 / 24. If check box WAN switch is enabled then this port is assigned as unmanaged switch port to IP network of WAN interface.
- 4G configuration is only available for routers with LTE modem. By default the 4G interface is disabled. Note: If both WAN-port and 4G interface do have active links you have to decide which interface shall be used to be the standard gateway (checkboxes 'DNS via DHCP/4G' and 'Gateway via DHCP/4G').
- Default gateway for outgoing traffic. Configurable if at WAN port the checkbox 'Gateway via DHCP' is not set or if WAN is configured with a static IP.

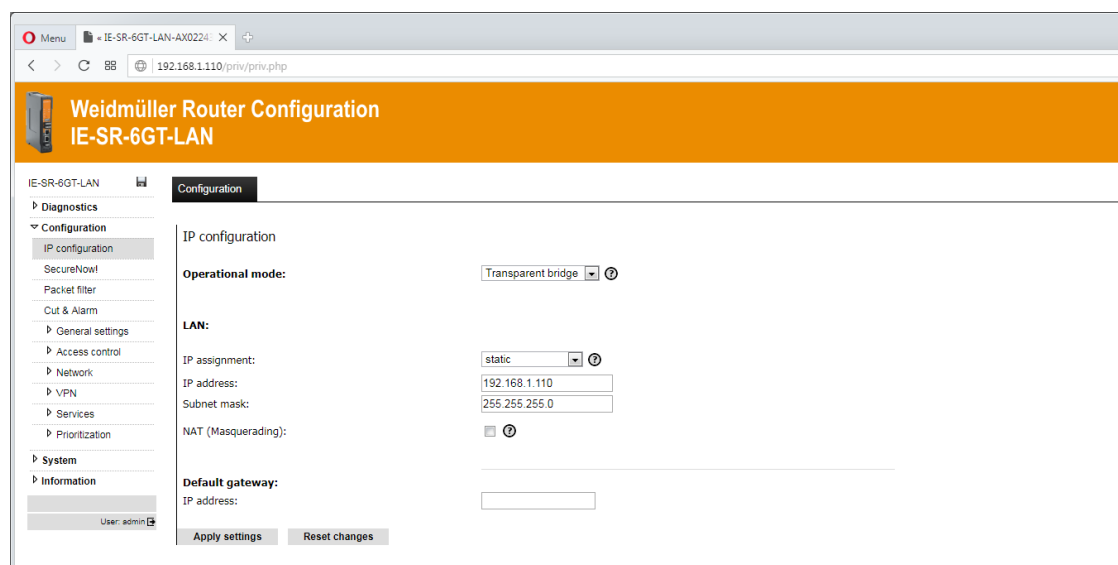
Screenshot of 6-Port LTE-Router with operation mode 'IP Router (extended)'

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).



Menu IE-SR-6GT-LAN-AX0224 X

192.168.1.110/priv/priv.php

Weidmüller Router Configuration IE-SR-6GT-LAN

IE-SR-6GT-LAN Configuration

- Diagnostics
- Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - General settings
 - Access control
 - Network
 - VPN
 - Services
 - Prioritization
- System
- Information

User: admin

IP configuration

Operational mode: Transparent bridge ?

LAN:

IP assignment: static ?

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): ☐ ?

Default gateway:

IP address:

Apply settings Reset changes

Screenshot of 6-Port LAN/WAN-Router with operation mode ‘Transparent bridge’

4.2.2 Configuration → SecureNow! (Learning Firewall)

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

Configuration

SecureNow!

IE-SR-6GT-LTE/4G

Diagnosics

Configuration

IP configuration

SecureNow!

Packet filter

Cut & Alarm

General settings

Access control

Network

VPN

Services

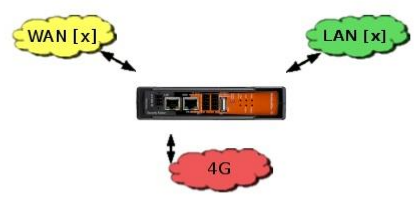
Prioritization

System

Information

User: admin

SecureNow!



Click on a cloud to change security setting.

capture mode: layer 3 ?

start analysis

On this page you can start the automatic network traffic analysis. Click on the clouds to assign security zones to network areas. The meaning of the colors is as follows:

green: high security. Example: production network.

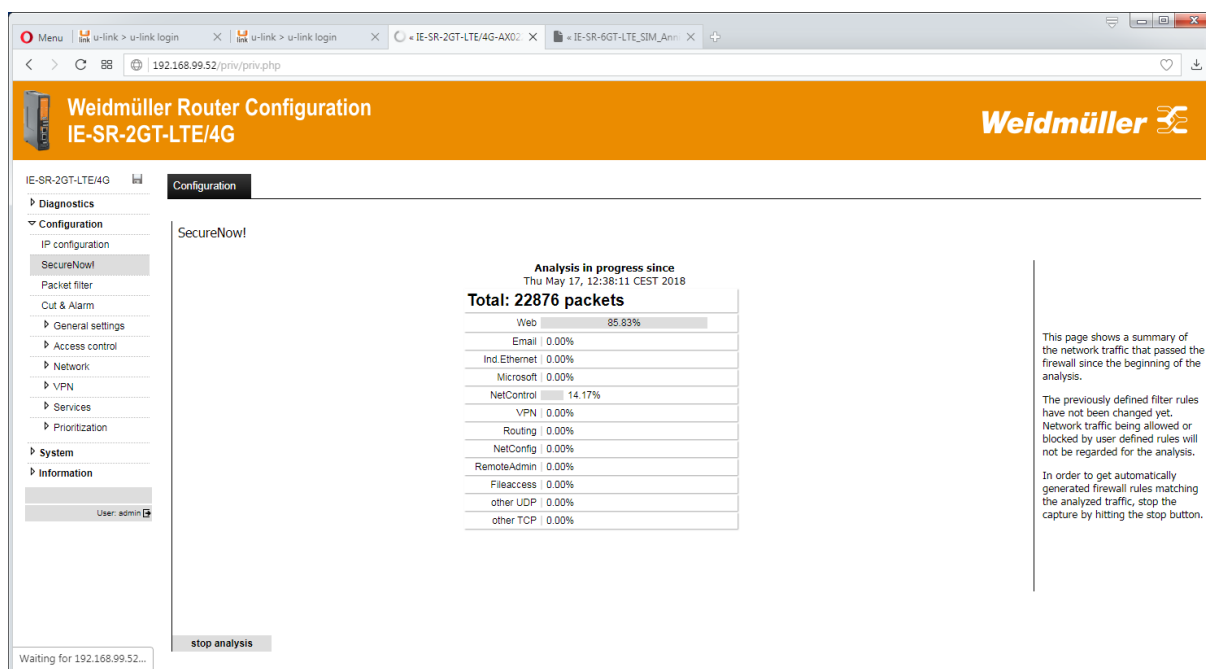
yellow: moderate security. Compromise between moderate security requirement and unrestricted data flow. Example: office network.

red: low security. The zone has no security requirement. Example: Internet.

Menu	Configuration → SecureNow!
Function	This is an auxiliary function for "independent learning" firewall rules based on temporary re- cording of data traffic. Depending on your model and operation mode you can choose the security levels for each group of interfaces. IP-Routing mode: • LAN is valid for LAN port • WAN is valid for WAN port • 4G is available for cellular router only IP-Routing mode (extended)*: • LAN [x] is valid for all 4 LAN ports • WAN [x] is valid for all 2 WAN ports • 4G is available for cellular router only As shown in the example normally the interfaces connected to bigger networks, such as the internet, tend to have lower security settings as the local networks. The Stateful Package Inspection (SPI) Firewall captures the protocols either on layer 2 (MAC) or layer 3 (IP)

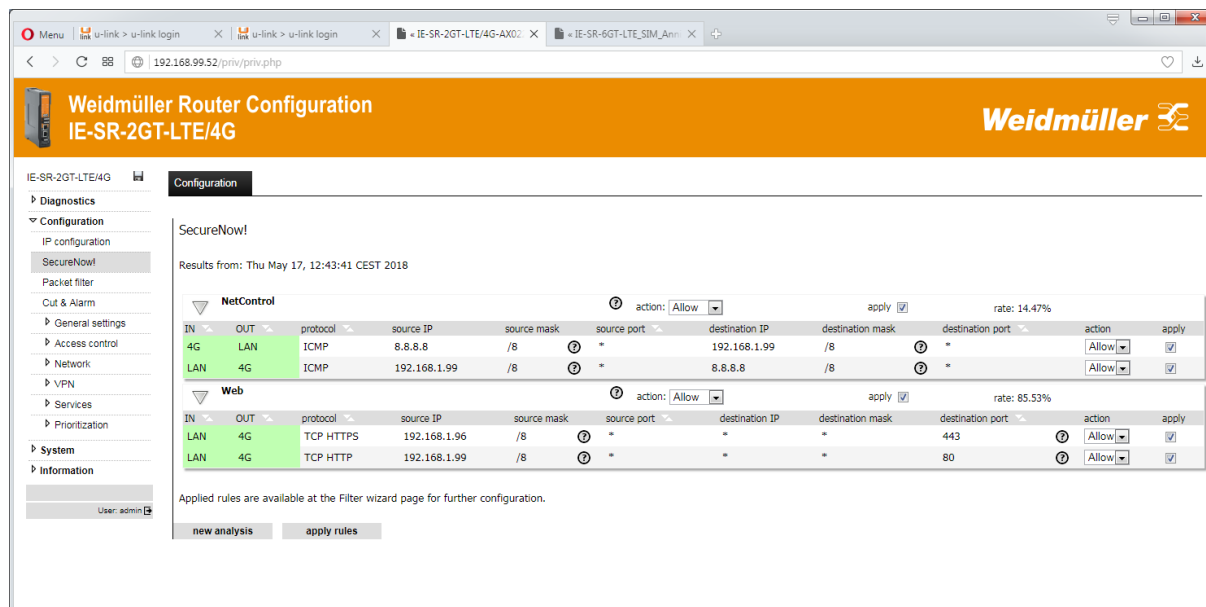
* for 6-Port models only

Screenshot of a started traffic analysis:



Menu	Configuration → SecureNow! (started analysis)
Function	By pressing the button "Start Analysis" the Router begins to analyze the network traffic (ports LAN, WAN and opt. LTE/4G) until "Stop Analysis" is triggered.

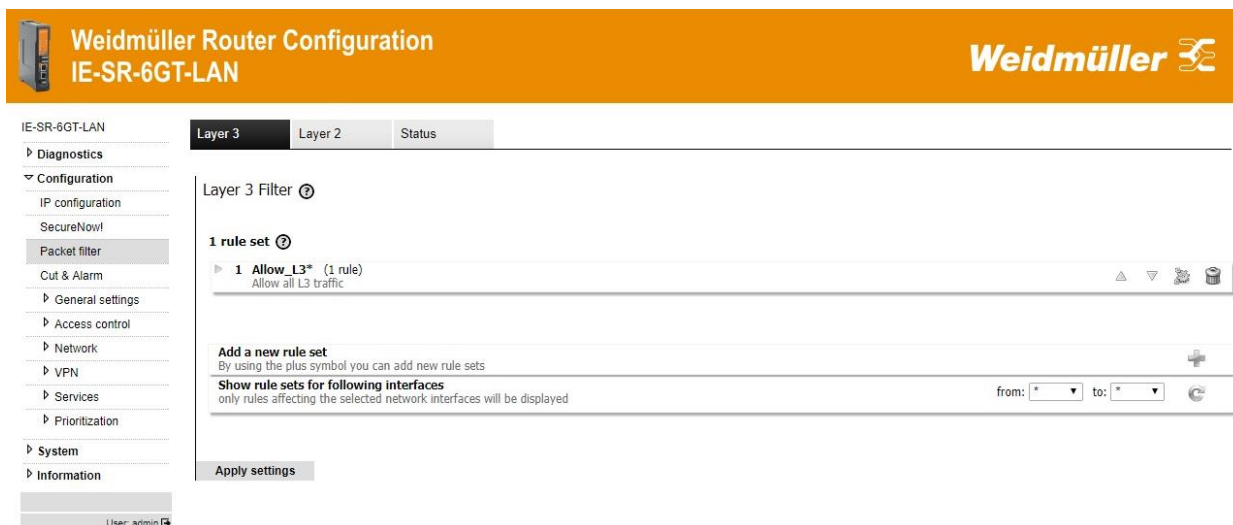
Screenshot after stopped traffic analysis (showing a proposal for firewall rules based on analyzed traffic):



Menu	Configuration → SecureNow! (stopped analysis)
Function	Thus, the Router will provide a table showing the recorded TCP packets and protocols as well as a proposal for the setting of firewall filtering rules. Window after exiting the network analysis with a proposed indication of firewall filtering rules. If you click the button "apply rules", the firewall will be updated with the proposed rules and immediately activated. The changes are not saved automatically, so that e.g. "wrong" filter rules can be removed by a Router restart. Previous filter rules will then be valid again.

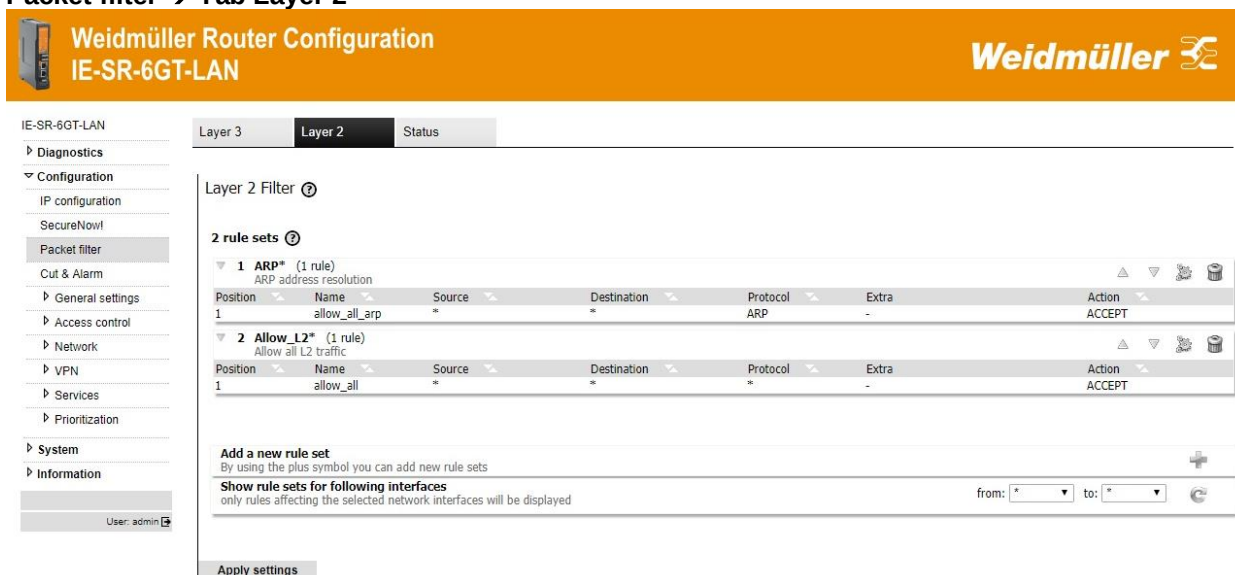
4.2.3 Configuration → Packet filter (Firewall)

Packet filter → Tab Layer 3



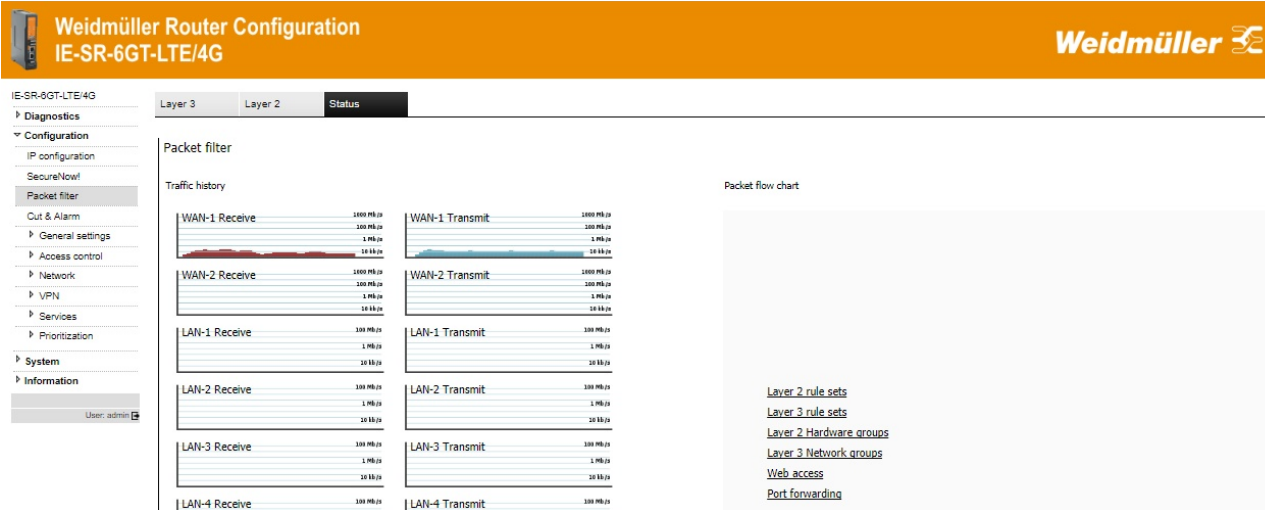
Menu	Configuration → Packet filter → Tab „Layer 3“
Function	This is the window for the manual configuration of firewall filter rules based on Layer 3 (IP layer). The screenshot shows the firewall settings as delivered with the default rule "Allow_L3*". This rule says that any IP protocol (*) and any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

Packet filter → Tab Layer 2



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

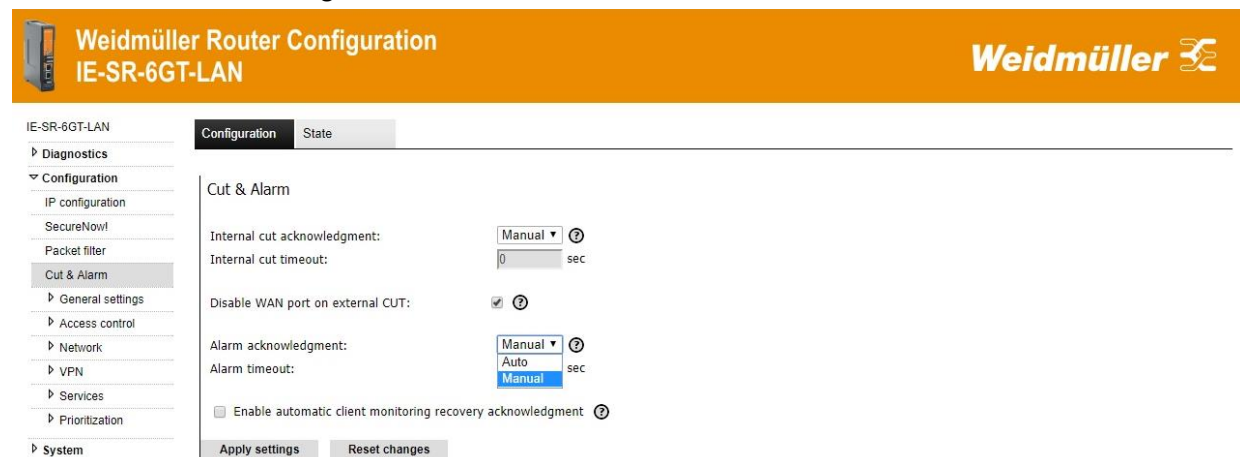
Packet filter → Tab Status



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

4.2.4 Configuration → Cut & Alarm

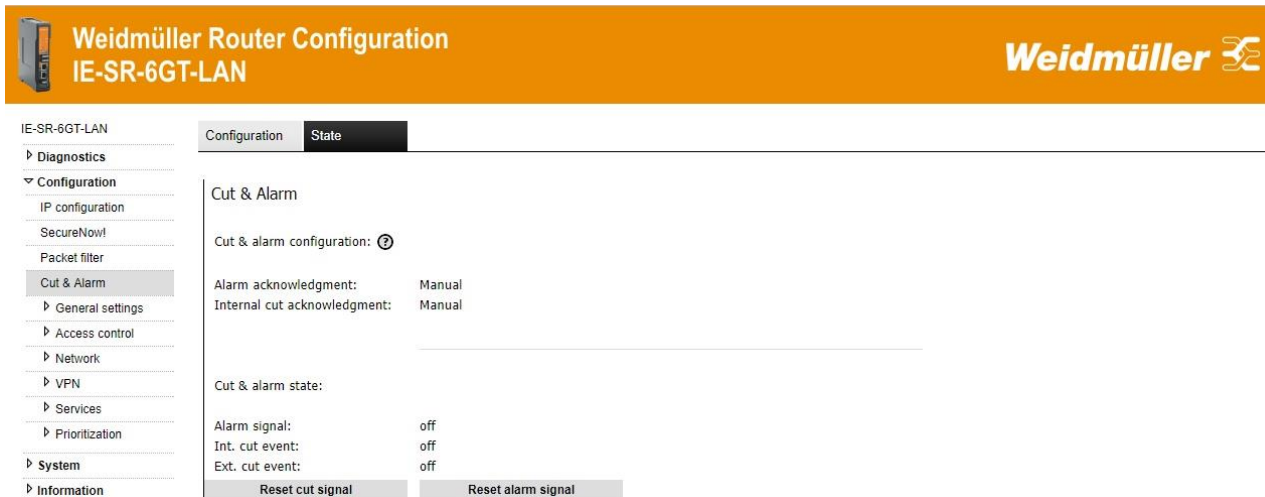
Cut & Alarm → Tab Configuration



The screenshot shows the 'Cut & Alarm' configuration page for a Weidmüller router. 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, Services, Prioritization, System, and Information. The main content area is titled 'Cut & Alarm' and shows configuration options for internal cut acknowledgment, internal cut timeout, disable WAN port on external CUT, alarm acknowledgment, alarm timeout, and enable automatic client monitoring recovery acknowledgment. The 'Internal cut acknowledgment' is set to 'Manual', 'Internal cut timeout' is 0 seconds, 'Disable WAN port on external CUT' is checked, 'Alarm acknowledgment' is set to 'Manual', 'Alarm timeout' is 0 seconds, and 'Enable automatic client monitoring recovery acknowledgment' is unchecked. There are 'Apply settings' and 'Reset changes' buttons at the bottom.

Menu	Configuration → Cut & Alarm → Tab „Configuration“	
Function	In this menu, it can be configured how the events "Cut" and "Alarm" - after they have been triggered – will be reset.	
	Acknowledgements	Manual: Cut must be reset manually by button on the tab "State" Auto: Cut will be reset automatically after the given timeout in seconds
	Disable WAN port on external cut	By default, an external CUT signal will disable the WAN Ethernet ports. You can disable the feature if you like to use CUT signal for switching packet filter rules only. The behavior of the internal CUT signal is not affected by this option
	Enable automatic client monitoring recovery acknowledgment	If enabled, a recovery event of the client monitoring system will acknowledge a previously triggered Alarm or CUT signal through a communication failure. In this case the cut or alarm acknowledgment should be set to manual to prevent an acknowledge through the automatic timer

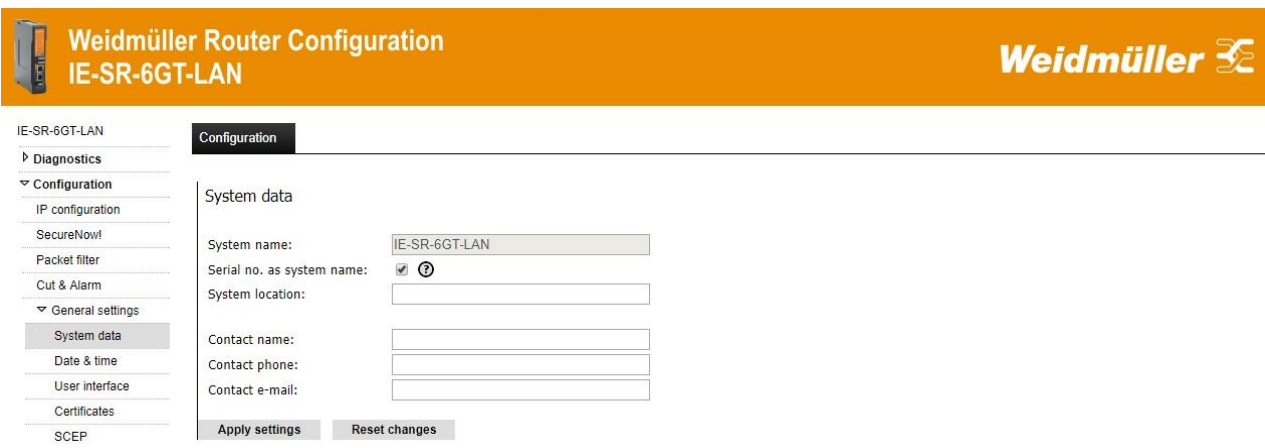
Cut & Alarm → Tab State



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

4.2.5 Configuration → General settings

General settings → System data



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

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

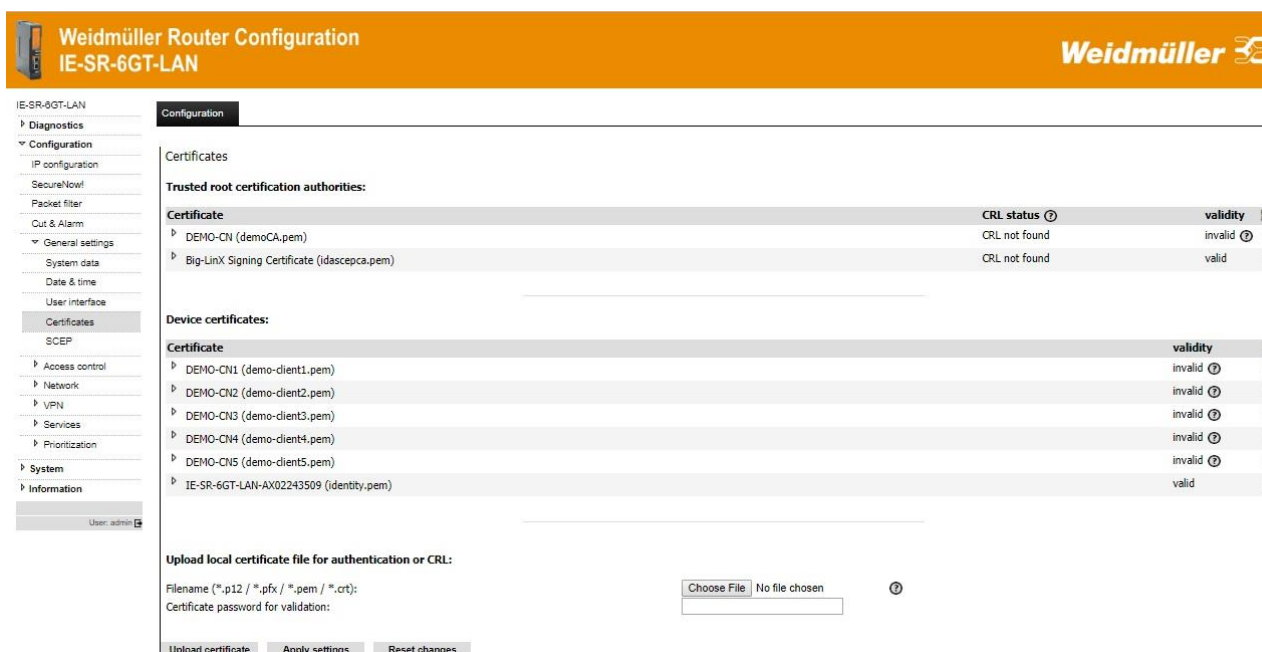
Menu	Configuration → General settings → Date & time → Tab "State"
Function	Shows the states of the used NTP servers. Please use tooltips for further information.

General settings → User Interface



Menu	Configuration → General settings → User interface
Function	Language Save and apply: • 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



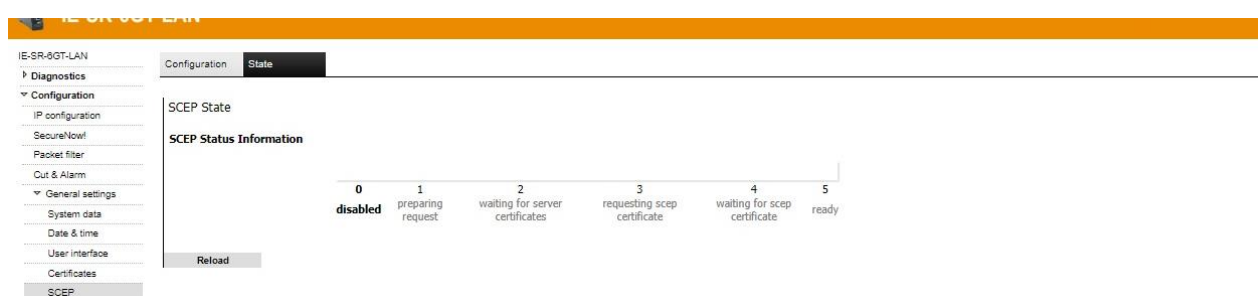
Menu	Configuration → General settings → Certificates
Function	Adding or deleting of certificates for VPN applications (used for both IPsec and OpenVPN).

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.	

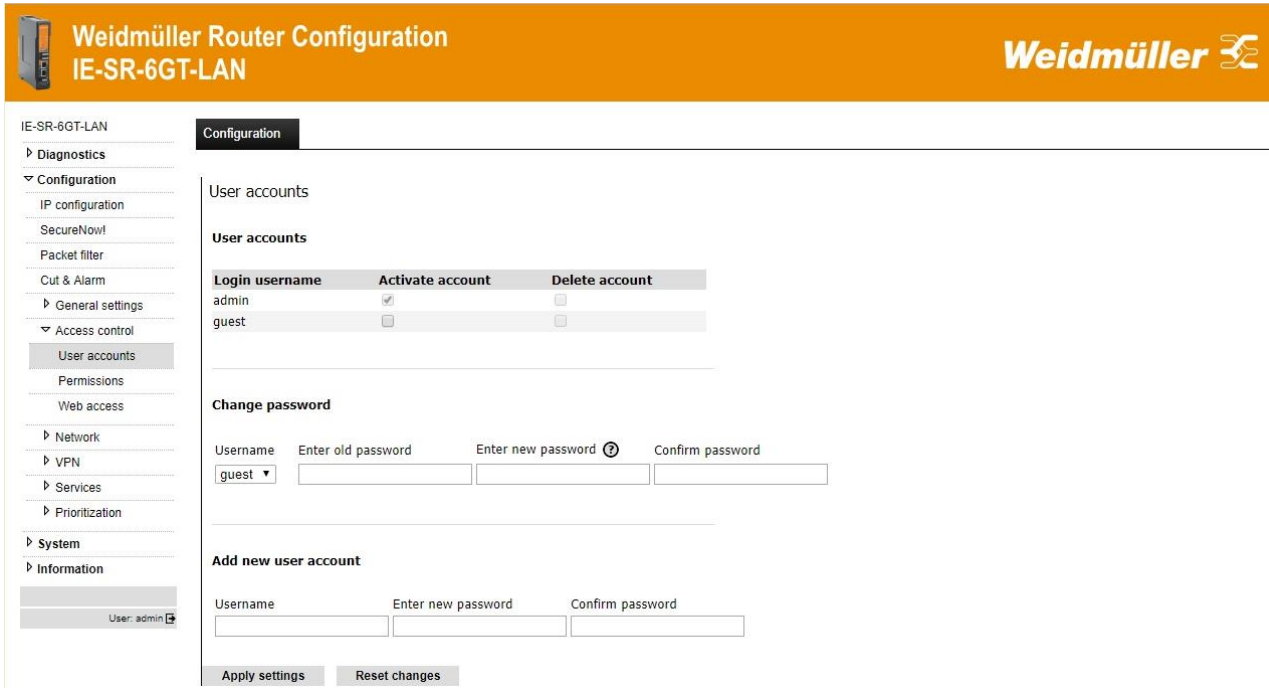
General settings → SCEP (Tab State)



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	☒	☐
guest	☐	☐

Change password

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

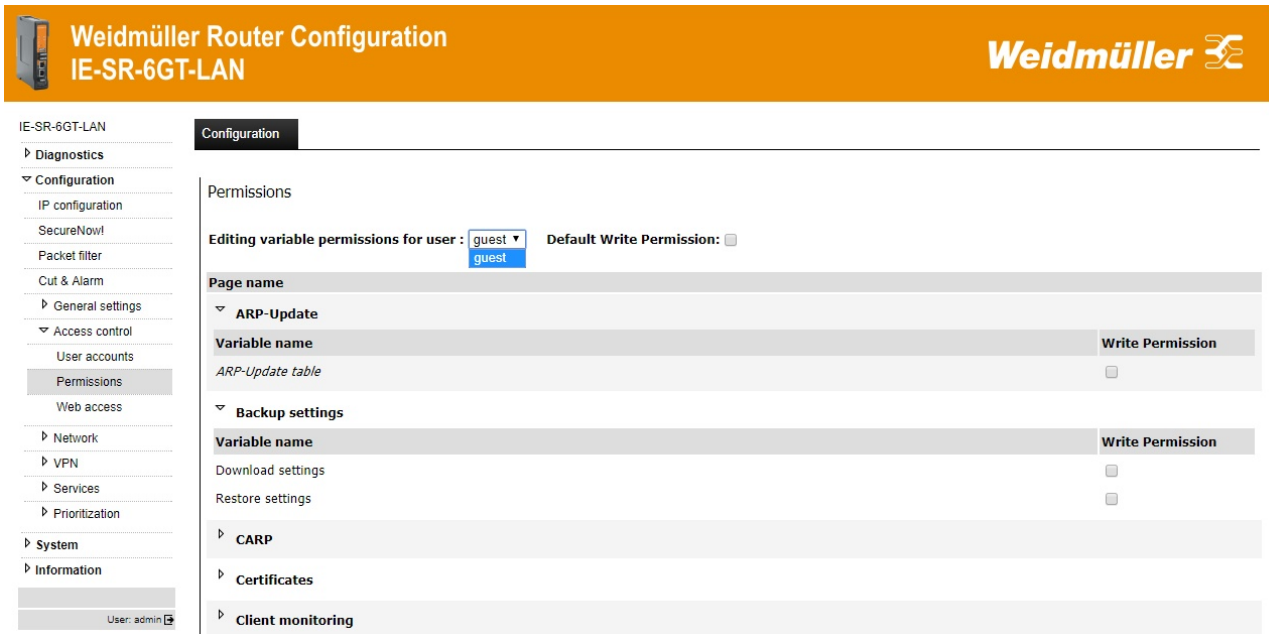
Add new user account

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	☐

Backup settings

Variable name	Write Permission
Download settings	☐
Restore settings	☐

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:	☒	☒	☒	☒
HTTPS:	☒	☒	☒	☒

Report access violations using syslog ☒

Apply settings Reset changes

Menu	Configuration → Access control → Web access
Function	Select the possible access modes of the web interface (via http and / or https) for the different interfaces. For cellular models additional checkboxes named „4G“ 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.

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	If the interface for accessing the Internet (e.g. WAN port) is configured statically then you must configure at least one accessible DNS server for resolving DNS names (e.g Google's name server with IP 8.8.8.8). If the Interface for Internet access is set to DHCP then typically the DNS server will be retrieved from DHCP server. In this case you do not need to enter the IP address of a DNS server. Generally at least one DNS server must be configured for resolving hostnames to IP addresses. A DNS server is mandatory if the Router is configured for using the u-link Remote Access Service. Note: See Tab „State“ to check the currently configured name server(s).
	Register host name at DHCP server	If enabled all DHCP requests by the device will register the specified hostname at the DHCP server. If the DHCP server is running dynamic DNS updates according to RFC2136 this will result in a valid DNS record on the DNS server with the specified Hostname
	Use all servers concurrently	If set active, incoming queries will be forwarded to all configured DNS servers. The fastest reply will be sent back to the requester. Otherwise, only one DHCP server will be used.
	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

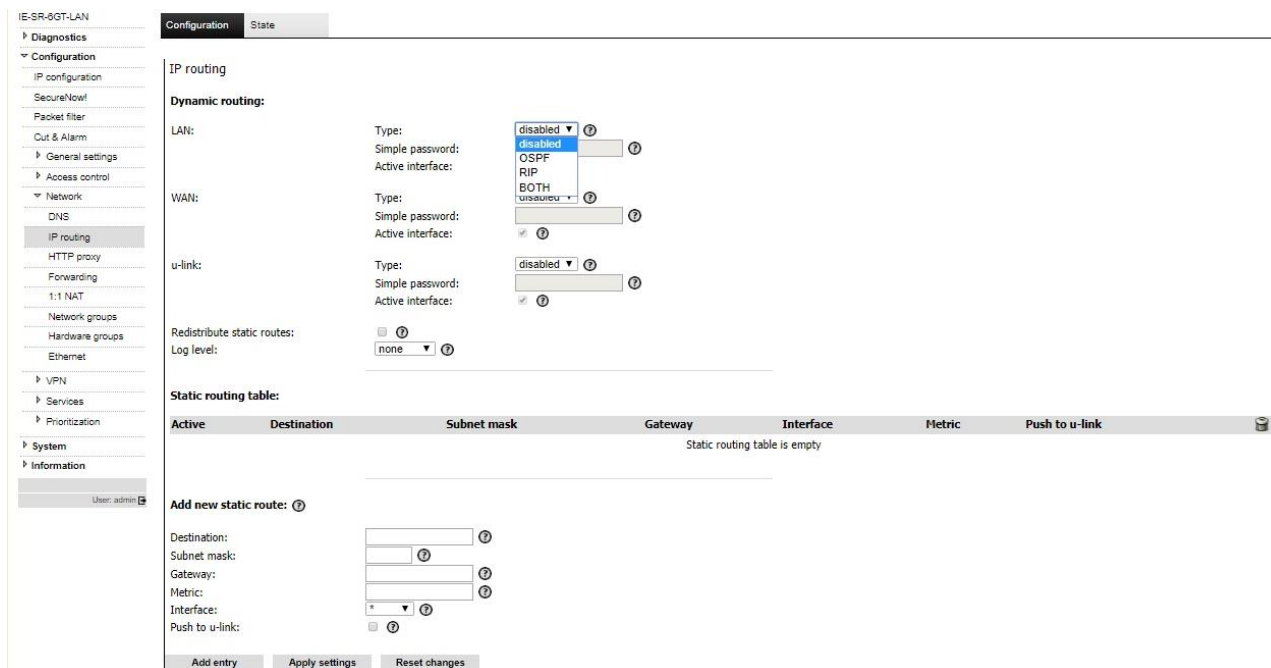
Domain suffix: fritz.box

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: ⓘ

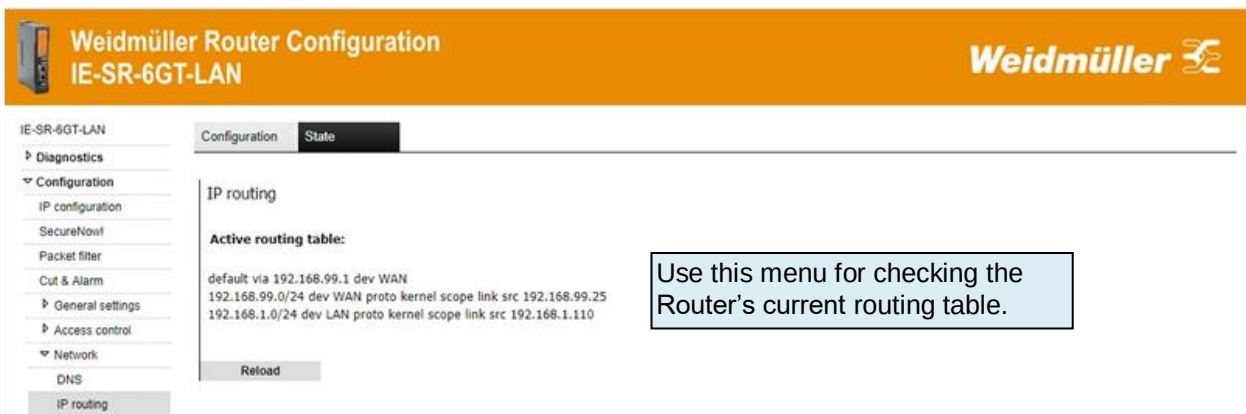
Destination: ⓘ
Subnet mask: ⓘ
Gateway: ⓘ
Metric: ⓘ
Interface: * ⓘ
Push to u-link: ☐ ⓘ

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. - 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	Displays all configured static routes Static routing forwards IP packets belonging to the specified network to the given gateway. The network is defined by an IP address and a subnet mask, which tells how many bits counted from the left are fixed. For example, IP 192.168.5.0 and subnet mask 24 means, that any IP of the format 192.168.5.xxx belongs to the network (3 bytes = 3 * 8 bit = 24 bits). Another example is 192.168.0.0 and subnet mask 16. Any IP of the format 192.168.xxx.xxx belongs to this network.
	Static Routing Destination	Network address of the destination network, i.e. 192.168.0.0
	Static Routing 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

Configuration | **State**

IP routing

Active routing table:

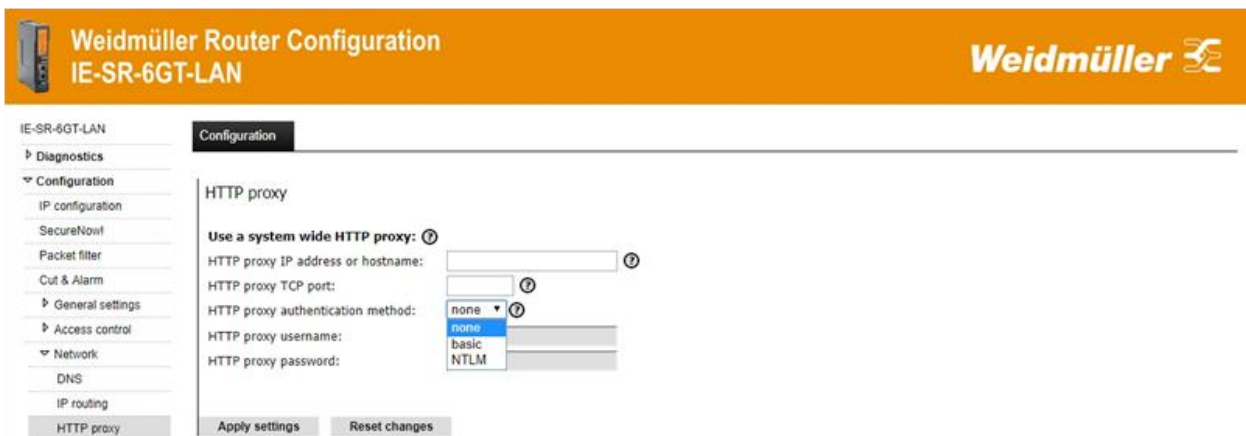
default via 192.168.99.1 dev WAN
 192.168.99.0/24 dev WAN proto kernel scope link src 192.168.99.25
 192.168.1.0/24 dev LAN proto kernel scope link src 192.168.1.110

Reload

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

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

Network → HTTP proxy



Weidmüller Router Configuration 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: none ?

HTTP proxy username: ?

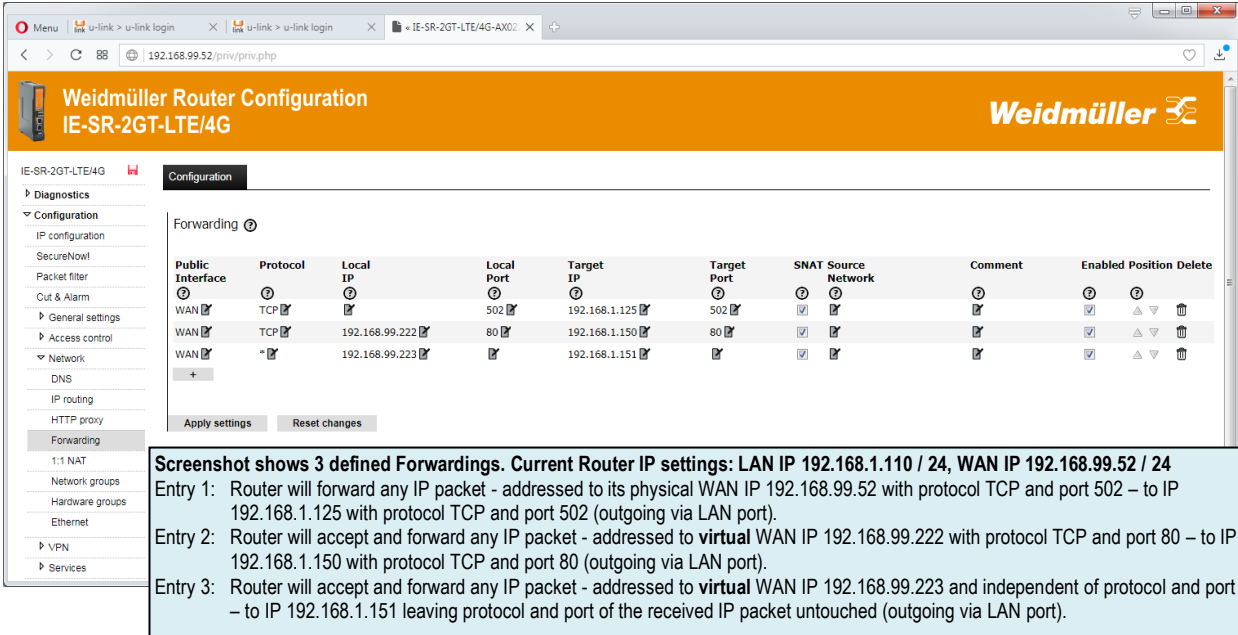
HTTP proxy password: ?

Apply settings Reset changes

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

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

Network → Forwarding



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).

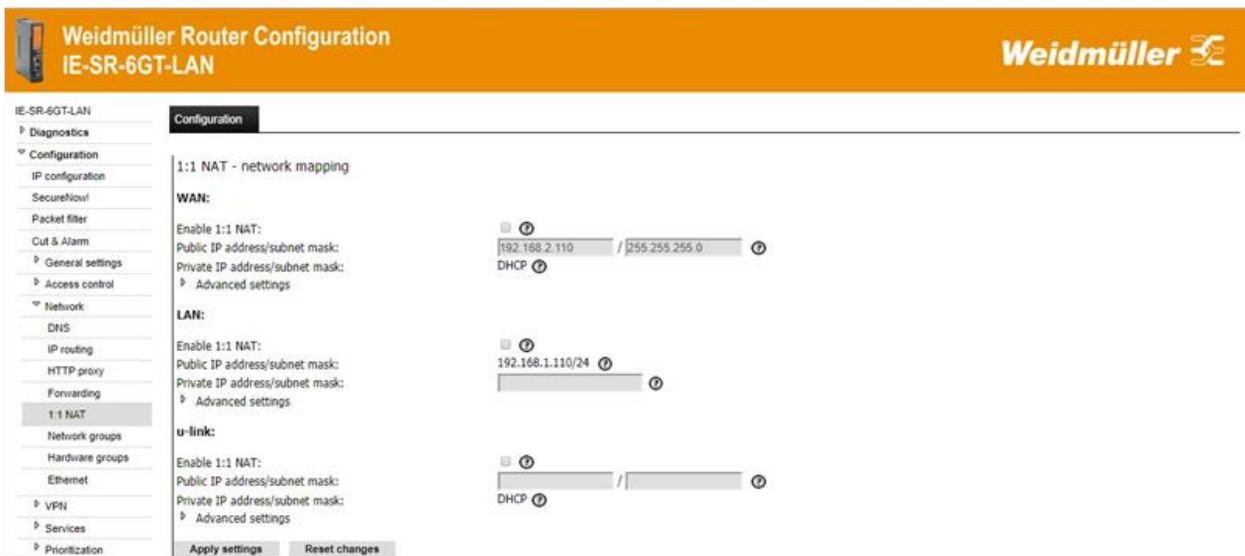
Entry 2: Router will accept and forward any IP packet - addressed to **virtual** WAN IP 192.168.99.222 with protocol TCP and port 80 – to IP 192.168.1.150 with protocol TCP and port 80 (outgoing via LAN port).

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	Configuring of forwardings based on IP address, protocol and port number. The forwarding can be used to forward IP packets incoming at selected “Public Interface” (e.g. WAN) and having as original target IP the Routers WAN IP to a defined Target IP e.g. behind LAN port. This can either be done on special TCP/UDP ports or on a whole IP address. The table supports IP aliases on the Public interface, source NAT of the request and conditional matching by filtering on the source address. Please take care of the position of each row, as the table is progressed from the top to the bottom for each packet until a match is found. If you run a restricting packet filter you must open the data paths there too. The packet filter will see the forwarding target as destination and always the original source independent of the SNAT checkbox. The feature „IP address forwarding“ (also called Virtual Mapping) can be used to forward an IP packet - addressed to “Local IP” – independent of protocol and port number – to a defined “Target IP”.	
	Public interface	Incoming interface on which the IP packet - which shall be forwarded - will arrive.
	Protocol	Select protocol TCP or UDP if you want to forward a special port. Use “*” if you want to forward all IP packets (ICMP, TCP, UDP) independent from protocol and port.

	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 then 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	With 1:1 NAT you can map a private subnet to the public subnet defined in the IP configuration. This allows you to resolve conflicts between identical networks. E.g. if all LAN ports in extended IP routing mode are connected to equal subnets, they can be accessed uniquely via the public subnet without the need for changing any configuration of the private subnets. 1:1 NAT can be configured for all active (physical and virtual) interfaces. Note: While the private subnets may be equal they must not conflict with the public IP subnets. For more detailed information about using 1:1 NAT please refer to application notes in appendix A.	
Enable 1:1 NAT	Enable 1:1 NAT for this interface.	Note: 1:1 NAT only can be activated if NAT (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:

?

Network address:

?

Apply settings

Reset changes

Menu	Configuration → Network → Network groups	
Function	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.	
	Group name	The group name for which a network should be added. It may contain letters and digits. If the given group does not exist, it will be created automatically. Hint: Click on an existing group name will fill the empty text field.
	Network address	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. Caution: Filter rules, that use a rule with a recently modified group, will not be updated until <Apply settings> is triggered (or <Save settings> respectively)

Network → Hardware Groups



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

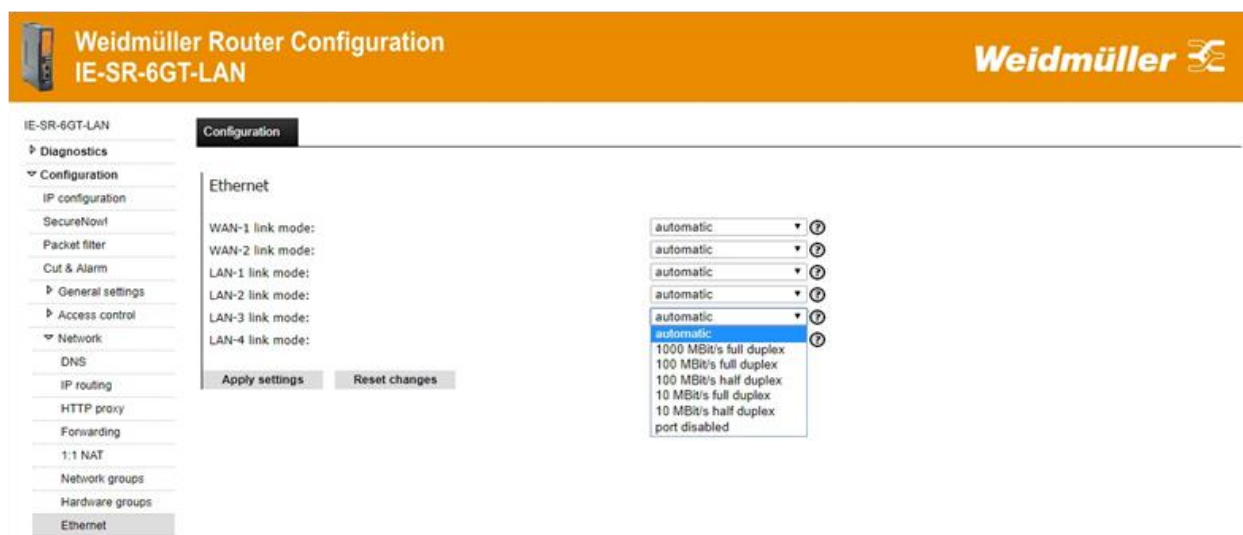
Reset changes

Version 2.04 / March 2020

Page 52 / 127

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

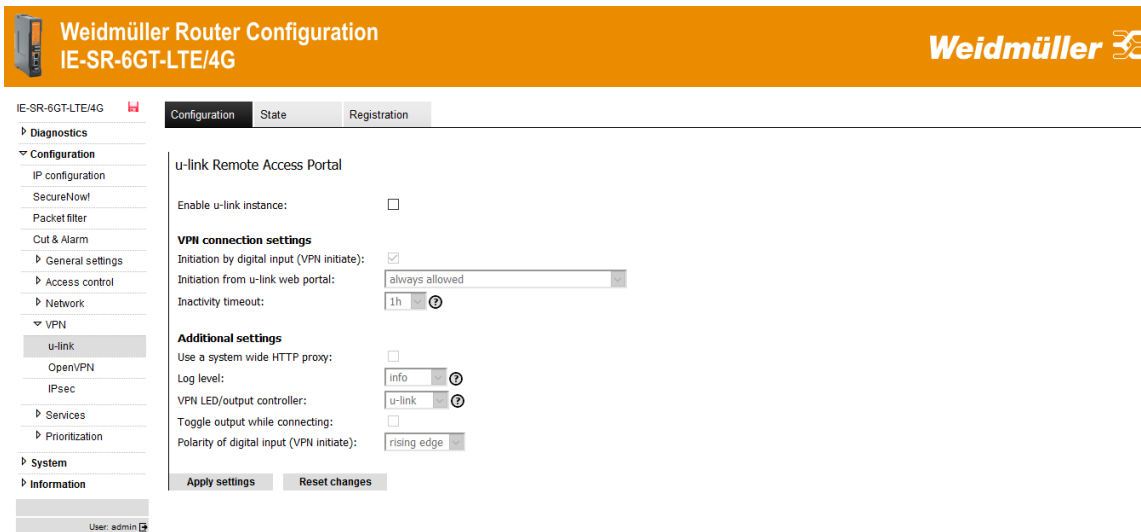
Network → Ethernet Interfaces



Menu	Configuration → Network → Ethernet
Function	Setting the transmission parameters of the LAN / WAN hardware interfaces. Note: Setting the Ethernet mode from automatic to something different than "automatic" will disable auto crossover feature of the Ethernet port (Auto-MDIX) and use MDI instead.

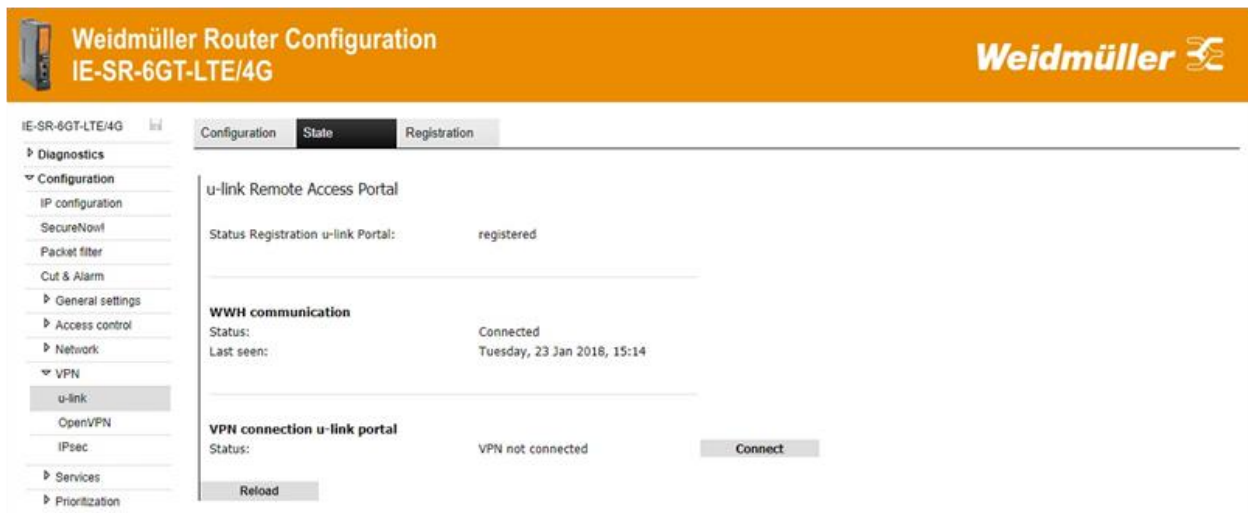
4.2.8 Configuration → VPN

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	<u>Never allowed:</u> u-link cannot be initiated remotely from the u-link portal <u>Always allowed:</u> u-link can be initiated remotely from the u-link portal <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.
	Use a system-wide HTTP proxy	Enable this checkbox if the HTTP/HTTPS based Internet access of the Router (for establishing an u-link VPN tunnel) is controlled by a proxy server which requires an authentication for passing. The system wide HTTP proxy must be configured under Configuration → Network → HTTP proxy.
	Log level	<u>None:</u> Will log no messages through the Event Log <u>Info:</u> Log only some information and critical errors <u>Debug:</u> Log state information too <u>Verbose:</u> Log all possible messages
	VPN LED/output controller	<u>Disabled:</u> The LED and digital output are not used by u-link. <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.
	Toggle output while connecting	Copies the behavior of the VPN LED to the digital output “VPN active”
	Polarity of digital input (VPN initiate)	Rising edge: VPN is triggered by rising edge of input voltage (from 0 V to 24 V) Falling edge: VPN is triggered by falling edge of input voltage (from 24 V to 0 V)

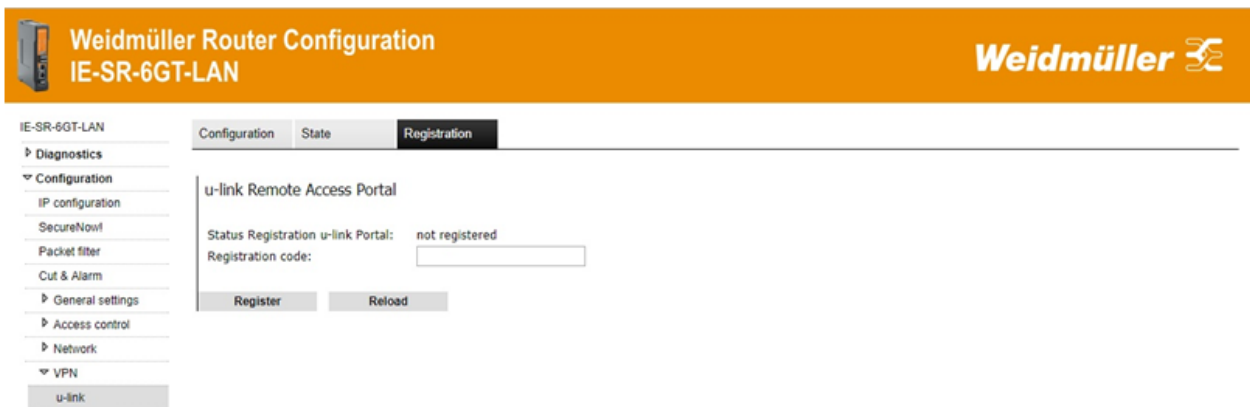
VPN → u-link (Tab State)



The screenshot shows the 'u-link Remote Access Portal' configuration page. The left sidebar lists various configuration options, with 'u-link' selected. The main content area displays the status of the u-link portal and WWH communication. The 'Status Registration u-link Portal' is 'registered'. The 'WWH communication' status is 'Connected', with the last seen time being 'Tuesday, 23 Jan 2018, 15:14'. The 'VPN connection u-link portal' status is 'VPN not connected', with a 'Connect' button available. A 'Reload' button is also present at the bottom left of the main content area.

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

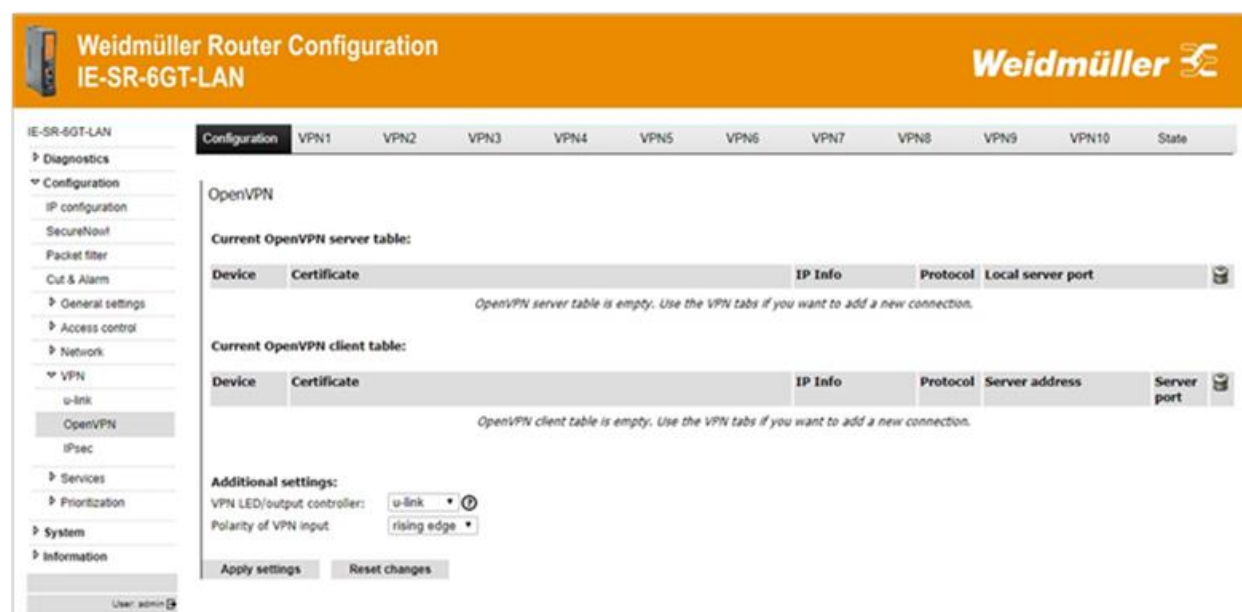
VPN→ u-link (Tab Registration)



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

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

VPN→ OpenVPN (Tab Configuration)



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

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

VPN→ OpenVPN (Tab VPN1)



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

Apply settings

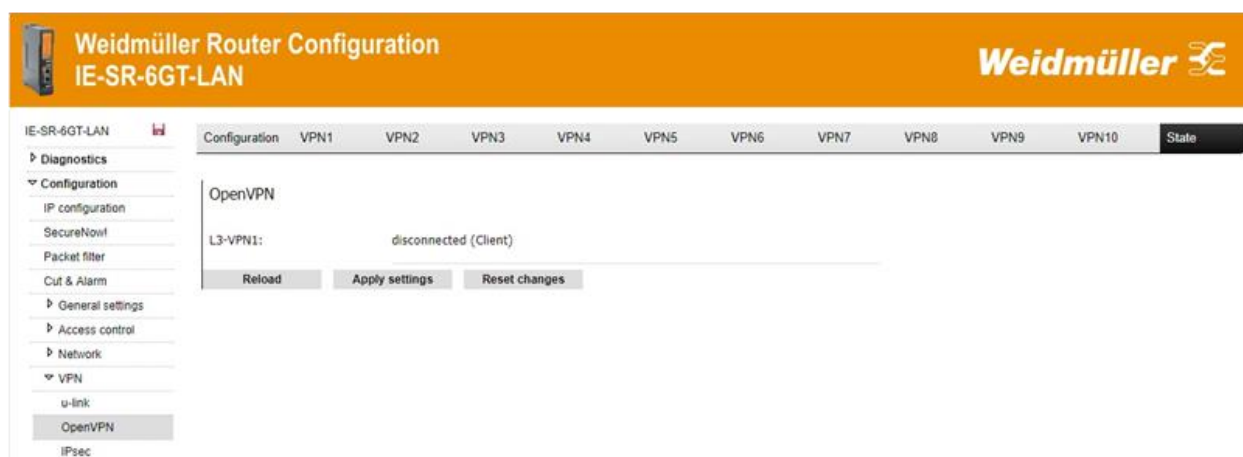
Reset changes

Configuration of OpenVPN connections on tabs VPN2 ...VPN10 are the same as for tab VPN1.

Menu	Configuration → VPN → OpenVPN → Tab „VPN1“	
Function	Screenshot of a configured OpenVPN-Client at tab VPN1	
	Enable VPN instance	Activates this OpenVPN connection
	Interface Mode	Select the connection mode which is either Server or Client Server: The device will run a TCP/UDP server which numerous clients can connect to Client: The device will establish a connection to an OpenVPN server
	Permanent connection	If enabled on a server instance the server will always be up. In enabled on a client instance, the client will try to connect if the connection gets lost. If not enabled the connection can be switched on using the VPN key, CUT or ALARM triggers, Modbus TCP or API.

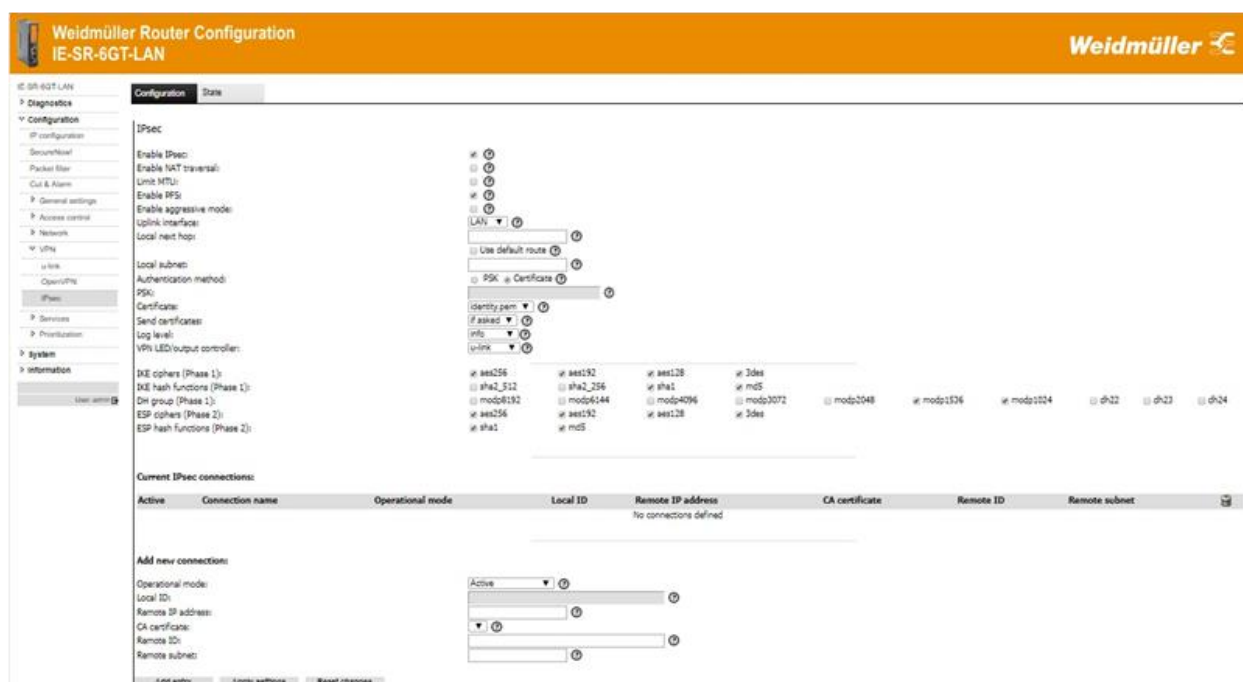
	Layer	The OpenVPN interface may operate on two different layers: Ethernet Layer (Layer 2), i.e. will be bridged with >LAN (interface)< IP Layer (Layer 3) with its own IP address which must be configured on the IP configuration page.
	OpenVPN device type	L3 interfaces can either be run as TUN or TAP devices. The 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	The IPsec menu allows to create and establish virtual private network connections based on the standard IPsec implementation. The Router can be configured both as IPsec client and IPsec server. IPsec allows the encryption of the complete communication flow between the Router and a remote site on IP level. IPsec provides encryption of subnets, which are located behind the respective VPN peers. IPsec connections can be used with both PSK encryption (pre-shared key using user name and password) as well as certificate based encryption.

Enable NAT traversal	NAT traversal is required when a router between the local and remote side does Network Address Translation (NAT) Note: IPsec pass through will break NAT traversal! If your router supports it, you must disable IPsec pass through!
Limit MTU	NAT traversal requires encapsulation of IP packets which possibly increases fragmentation leading to less network performance. If this happens it may help to slightly reduce the size of outgoing packets (MTU).
Enable PFS	With Perfect Forward Security (PFS) a session key (signed by the private key) is used to encrypt the data instead of the private key itself. This session key will be renewed after relatively short time. Thus, even if the private key (certificate) gets compromised previous communication cannot be decrypted by someone else since the temporary session keys cannot be restored. Therefore, PFS further increased security.
Enable aggressive mode	Enables IPsec aggressive mode
Uplink interface	The uplink interface on which the IPsec tunnel is supposed to be established.
Local next hop	To reach the remote site, it may be possible that IPsec needs to explicitly know the IP address or hostname of the next router. For example, this can be the router that connects you LAN with the internet.
Use default route	Use the default gateway (either set manually or by a DSL connection) as next hop.
Local Subnet	This is the local subnet which its traffic to the remote subnet is supposed to be encrypted when going out via the given interface. The subnet must be defined as IP/Network mask, e.g. 192.168.0.0/24. If no subnet is given, the IP address of the interface itself is used. Note: The local and remote subnet must not be equal! Note: Routed traffic is not generally encrypted! Only traffic between exactly the local and the remote network gets encrypted! For instance, if you use two Weidmüller Security Routers and leave both subnets empty the IPsec tunnel will be 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	The peer will identify (not authenticate) itself with this ID depending on the chosen authentication method. PSK: If no remote id is given the IP address of the remote site is checked. Entering the IP address is not the same as leaving the field empty! The remote ID must not contain blanks. Certificate: The complete certificate info of the peer must be specified. In case of another Weidmüller Security Router you can copy and paste the certificate info (C=... ST=...) from its certificates page. The order of info elements C, ST, L, O, OU, CN, E must be kept and all elements separated by a comma followed by a blank. Note: The remote ID must match exactly except when you are waiting for road warriors using certificates. Then also all fields must be present but "*" may be used as wild card (e.g. CN=*). For a road warrior setup with PSK no ids should be used. Note: The remote ID should be unique. If several connections share the same ID their tunnels will get periodically build up and torn down (traffic with interruptions is possible though).
	Remote subnet	This is the remote subnet to which the traffic coming from the local subnet is encrypted when going out via the given interface. The subnet must be defined as IP/Network mask, e.g. 192.168.0.0/24. If no subnet is given, the IP address of the interface itself is used. Note: The local and remote subnet must not be equal! Note: Routed traffic is not generally encrypted! Only traffic between exactly the local and the remote network gets encrypted! For instance, if you use two Weidmüller Security Routers and leave both subnets empty the IPsec tunnel will be established between two routers. Then only traffic originated from one router destined to the other router is encrypted. The traffic that is routed via both devices from networks behind them is not encrypted at all.

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

VPN → IPsec (Tab State)



Weidmüller Router Configuration
IE-SR-6GT-LAN

Weidmüller 

IE-SR-6GT-LAN

- ▶ Diagnostics
- ▼ Configuration
 - IP configuration
 - SecureNow!
 - Packet filter
 - Cut & Alarm
 - ▶ General settings
 - ▶ Access control
 - ▶ Network
 - ▼ VPN
 - u-link
 - OpenVPN
 - IPsec

Configuration

State

IPsec

Current IPsec tunnels:

Packets sent	Local subnet	Local endpoint	Remote endpoint	Remote subnet
No IPsec tunnels				

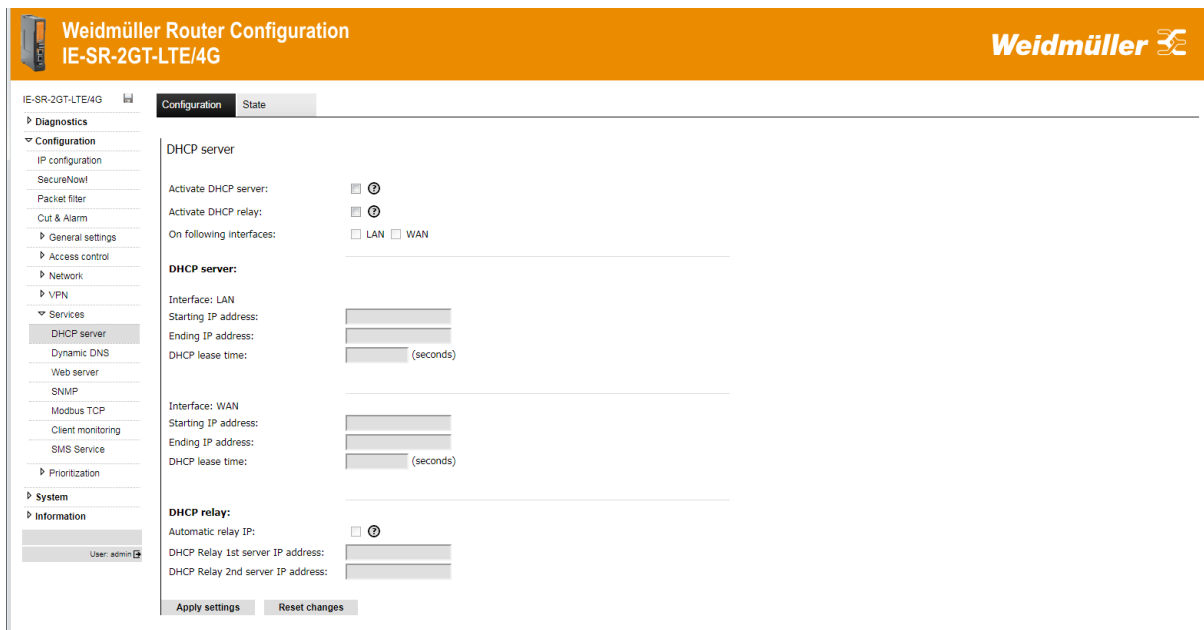
▶ Detailed debug state

Reload

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'.

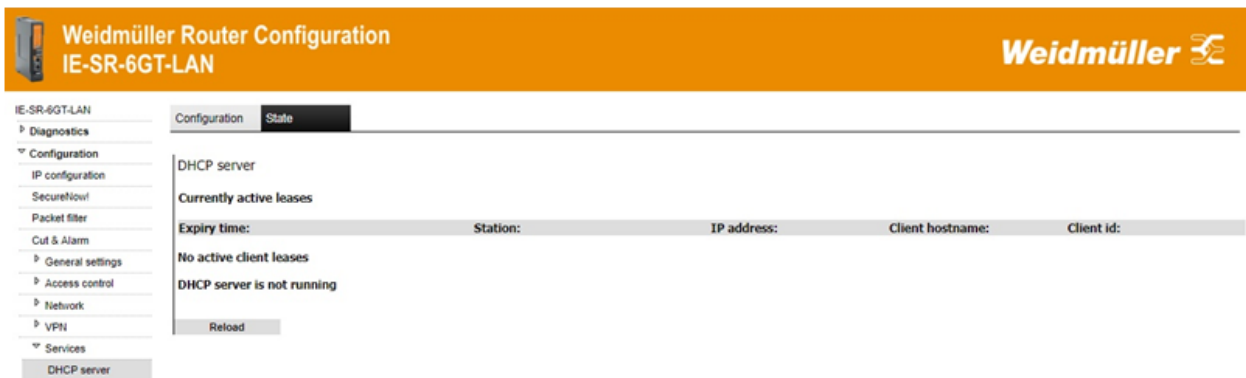
DHCP server configuration:

- Activate DHCP server: ☐ (with a question mark icon)
- Activate DHCP relay: ☐ (with a question mark icon)
- On following interfaces: ☐ LAN ☐ WAN
- DHCP server:**
 - Interface: LAN
 - Starting IP address: [text input]
 - Ending IP address: [text input]
 - DHCP lease time: [text input] (seconds)
- DHCP relay:**
 - Interface: WAN
 - Starting IP address: [text input]
 - Ending IP address: [text input]
 - DHCP lease time: [text input] (seconds)
- DHCP relay:**
 - Automatic relay IP: ☐ (with a question mark icon)
 - DHCP Relay 1st server IP address: [text input]
 - DHCP Relay 2nd server IP address: [text input]

Buttons at the bottom: 'Apply settings' and 'Reset changes'.

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.

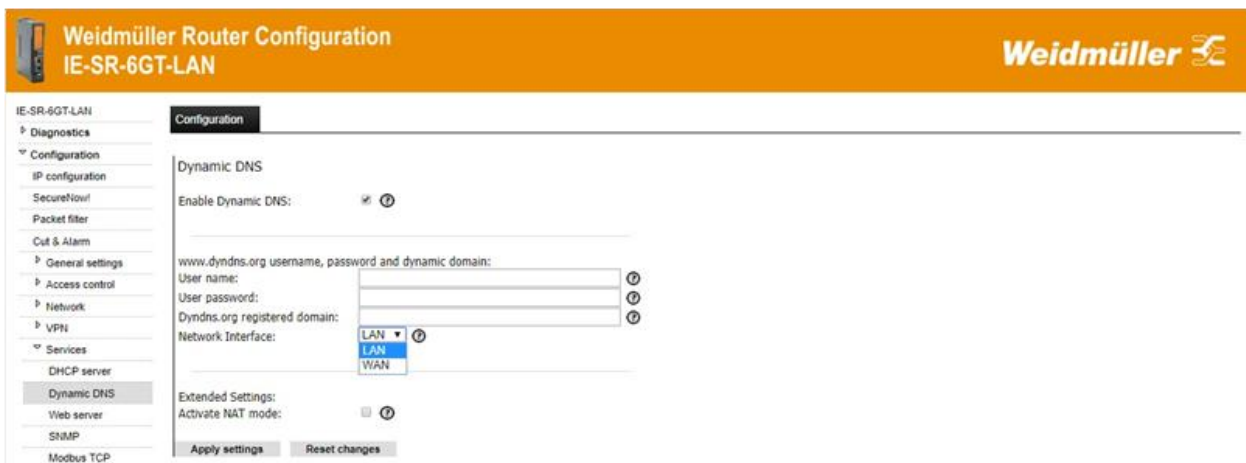
Services → DHCP Server (Tab State)



The screenshot shows the 'State' tab of the DHCP server configuration. The left sidebar lists navigation options: IE-SR-6GT-LAN, Diagnostics, Configuration (expanded), IP configuration, SecureNow!, Packet filter, Cut & Alarm, General settings, Access control, Network, VPN, and Services (expanded). Under Services, 'DHCP server' is selected. The main content area shows 'DHCP server' with 'Currently active leases' and a table with columns: Expiry time, Station, IP address, Client hostname, and Client id. Below the table, it states 'No active client leases' and 'DHCP server is not running'. A 'Reload' button is at the bottom.

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

Services → Dynamic DNS



The screenshot shows the 'Configuration' tab of the Dynamic DNS settings. The left sidebar is similar to the previous one, but 'Dynamic DNS' is selected under Services. The main content area has a 'Dynamic DNS' section with 'Enable Dynamic DNS' checked. Below this are fields for 'www.dyndns.org username, password and dynamic domain': 'User name', 'User password', and 'DynDNS.org registered domain'. A 'Network Interface' dropdown menu is set to 'LAN'. An 'Extended Settings' section has 'Activate NAT mode' unchecked. 'Apply settings' and 'Reset changes' buttons are at the bottom.

Menu	Configuration → Services → Dynamic DNS	
Function	This feature allows the Router - if connected to the Internet using dynamic IP address allocation - to be accessed by a „speaking“-name via the public Dynamic DNS service of provider „DynDNS.org“.	
	User name	Username registered on http://www.dyndns.org service.
	User password	Password registered on http://www.dyndns.org service.
	Dyndns.org registered domain	Domain registered on http://www.dyndns.org service, must be owned by the user given on the former field.
	Network interface	Choose the interface on which the internet connection will be established (interfaces may vary for cellular routers, extended routing mode or virtual interfaces).
	Activate NAT mode	Neither the local IP address of the given interface will get transmitted nor will the current DNS entry get checked against the local IP address. Instead an update will be sent every 5 minutes and the service will determine the IP address from the source address.

Services → Web server



The screenshot shows the 'Web server' configuration page in the Weidmüller Router Configuration interface. The left sidebar lists various configuration options, with 'Web server' selected under the 'Services' category. The main content area is titled 'Web server' and contains the 'HTTPS web server certificate' section. It includes a checkbox for 'Enable HTTPS server' (checked), a dropdown for 'Authentication certificate' (set to 'identity.pem'), and buttons for 'Apply settings' and 'Reset changes'.

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

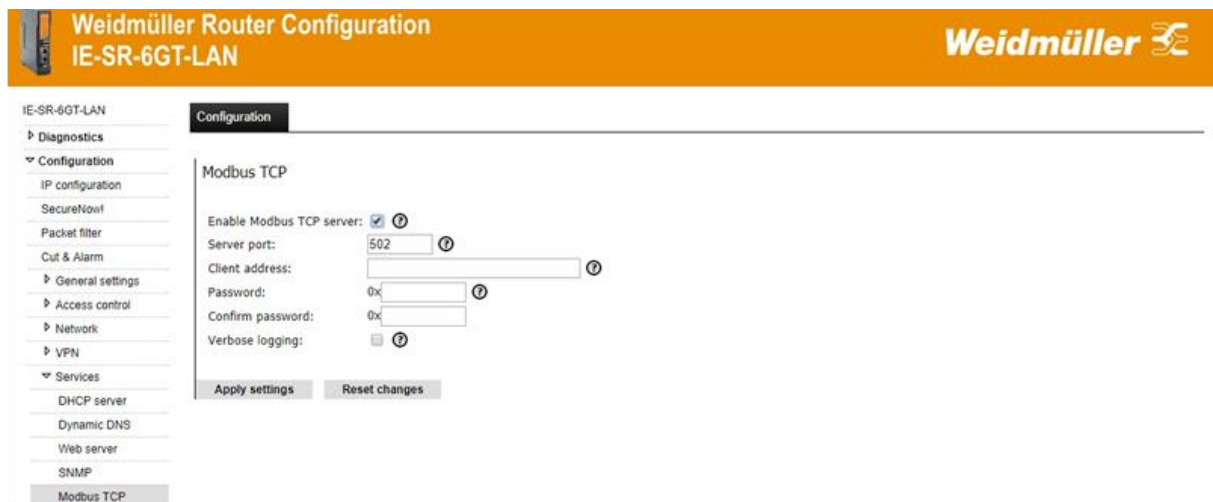


The screenshot shows the 'SNMP' configuration page in the Weidmüller Router Configuration interface. The left sidebar lists various configuration options, with 'SNMP' selected under the 'Services' category. The main content area is titled 'SNMP' and contains several sections for configuration. It includes checkboxes for 'Enable SNMP', 'SNMPv1/v2', and 'SNMPv3'. Below these are fields for 'SNMP read only access' and 'SNMP read/write access', each with sub-fields for 'Community Name', 'Community IP', and 'Community network mask'. There is also a section for 'SNMPv3 username and encryption' with fields for 'User name read only', 'Password', 'User name read/write', and 'Pre-shared Key for encryption'. At the bottom, there is a section for 'SNMP traps' with fields for 'Enable SNMP Trap Generation', 'SNMP Trap Community Name', and 'SNMP Trap Receiver IP'. Buttons for 'Apply settings' and 'Reset changes' are at the bottom.

Menu	Configuration → Services → SNMP	
Function	Activation / deactivation of the SNMP protocol (Simple Network Management Protocol). Versions v1/v2/v3 are supported. Router data can be requested using Standard MIB-II.	
	SNMPv1/v2	Use SNMPv1 or SNMPv2 protocol specifications. This protocol version is not encrypted and thus regarded as insecure
	SNMPv3	Use the SNMPv3 protocol. You must enter additional usernames and passwords in the fields below. SNMPv3 is regarded as secure.
	SNMP read or read/write access	You can decide whether the access with SNMP protocol should be "read only" or read and write. For pure diagnostics, the read-only option is recommended. You can also create two different accesses.
	Community name	The SNMP community name is used for authentication purposes like a password. Most devices use the strings public (read only) and private (read write) by default.

Community IP	Restricted access with the given community name to the following IP-Address. Use 0.0.0.0 for any source.
Community network mask	Network mask for the IP given above. Use 32 for a single host or 24 for a classic class C network.
User name	SNMPv3 only: Username for SNMPv3. More than 4 alphanumerical characters are required.
Password	SNMPv3 only: Password for SNMPv3. Authentication Protocol: MD5. More than 8 alphanumerical characters are required.
Pre-shared Key for encryption	SNMPv3 Pre-shared key for encryption. Privacy protocol AES
Enable SNMP Trap generation	Activate the SNMP trap generation subsystem.
SNMP Trap Community Name	SNMP trap community name for general trap identification
SNMP Trap Receiver IP	IP address of the server where the SNMP trap will be send to

Services → Modbus TCP



The screenshot shows the 'Modbus TCP' configuration page in the Weidmüller Router Configuration interface for the IE-SR-6GT-LAN model. The page is part of the 'Configuration' section, specifically under 'Services'. The configuration options are as follows:

- Enable Modbus TCP server:** A checkbox that is currently checked.
- Server port:** A text input field containing the value '502'.
- Client address:** A text input field that is currently empty.
- Password:** A text input field containing '0x'.
- Confirm password:** A text input field containing '0x'.
- Verbose logging:** A checkbox that is currently unchecked.

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

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

General information about implemented ModbusTCP functionality:

1. ModbusTCP server is running as a ModbusTCP slave.
2. Via the ModbusTCP protocol only following settings and status requests can be done:
 - Monitor, start and stop pre-defined VPN connections (IPsec, OpenVPN, u-link)
 - Acknowledge/Reset of CUT& ALARM
3. The server port can be selected freely. If no port is specified, the default port for ModbusTCP (502) waits for incoming requests.
4. The access can be restricted to a specific ModbusTCP Master by specifying either an IP address or as a host name that is resolved when the server is started. If nothing is specified, the connection can be established from any device (ModbusTCP Master).
5. To increase security, a 32-bit password can be specified. Before a Master can access status and control registers, it must write the password into the password registers. The higher-value 16 bits in register 0x01 and the lower-value 16 bits in register 0x02. If no password is specified, all registers can be accessed directly.
6. To keep the event log from overfilling, only access violations (if the IP address is restricted or if a password is requested) are normally reported. If checkbox "Verbose logging" is activated, additional information on connection establishment, requests and access times is also logged.

Important information:

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

Modbus/TCP implementation

Currently, only logical unit 0 can be addressed; this stands for the Router itself.

The following function codes can be processed by the Router:

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

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

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

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

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

Overview Modbus Register

Registers	Hex code	Data
General registers:	0x00	Version
	0x01	PASSWORD - higher-value 16 bits
	0x02	PASSWORD - lower-value 16 bits

Status registers:	0x10	CUT&ALARM
	0x11	Not used
	0x12	reserved
	0x13	IPsec
	0x14	OpenVPN1
	0x15	OpenVPN2
		...
	0x1D	OpenVPN10
	0x1E	u-link VPN
Status registers:	0x20	CUT&ALARM
	0x21	Not used
	0x22	reserved
	0x23	IPsec
	0x24	OpenVPN1
	0x25	OpenVPN2
		...
	0x2D	OpenVPN10
	0x2E	u-link VPN

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

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

General registers (Version and Password)

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

Registers CUT&ALARM

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

Registers IPsec

0x13 (Status)	Read-Only	Bits	Meaning	Explanation
		0	IPSec defined	At least one connection is defined
		1	Activated	IPsec generally is activated (Enabled)
		2	Connected	At least one tunnel is established
		3-7	Not used	
		8-15	Active tunnel	Number of currently established IPsec tunnels
0x23 (Set)	Read/Write	This register can be written either with values:		
		0x0000		Deactivate all defined IPsec connections
		0x0001		Activate all defined IPsec connections

Registers OpenVPN

OpenVPN-1

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

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

Register u-link

0x1E (Status)	Read-Only	Bits	Meaning	Explanation
		0	Not used	
		1	Activated	u-link instance is activated (Enabled)
		2	Connected	u-link VPN tunnel is established
		4-15	Not used	
0x2E (Set)	Read/Write	This register can be written either with values:		
		0x0000		Deactivate u-link VPN tunnel
		0x0001		Establish u-link VPN tunnel

Services → Client Monitoring



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
 - ▶ VPN
 - ▼ Services
 - DHCP server
 - Dynamic DNS
 - Web server
 - SNMP
 - Modbus TCP
 - Client monitoring**
 - COM port server

Configuration

Client monitoring

Current monitoring table:

IP address	Delay(ms)	Packet loss(%)	Action	State
Monitoring table is empty				

E-mail server:

E-mail address:

Add new entry:

IP address:	Delay:	Packet loss:	Action:
	ms	%	none ?

Add entry
Apply settings
Reset changes

Menu	Configuration → Services → Client Monitoring	
Function	Allows the monitoring (still alive?) of network devices via a cyclic query using the ICMP protocol (ping request). As an action if a monitored Ethernet device is no longer available an „Alarm“ or „Cut“ event can be triggered. Additionally, the connection to a mail server and a target mail address can be configured to send the information about a lost connection of a monitored device by mail.	
	Current monitoring table	Table showing all monitored IP addresses
	E-mail server	The server which the router can use to send e-mails in case of monitored events (must run as mail forwarder).
	E-mail address	The e-mail address to which the router sends the e-mails in case of monitored events.
	Add new entry	Adding a new device which will be monitored. <u>IP address:</u> The IP address of the monitored device. <u>Delay:</u> The Router sends every 50 seconds a block of 5 ping requests to the defined IP address. If the average response time (based on 5 ping requests) is longer than the configured Delay-time in milliseconds then this trigger condition will match. <u>Packet loss:</u> If the lost share [%] (no response) of 5 ping requests is greater than the configured value then this trigger condition will match. <u>Action:</u> None (Generates only an entry in the Event log), Alarm or Cut (Internet events, event Alarm will also set digital output 'Alarm')

Services → SMS Service



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

IE-SR-2GT-LTE/4G

Configuration

Diagnostics
 Configuration
 IP configuration
 SecureNow!
 Packet filter
 Cut & Alarm
 General settings
 Access control
 Network
 VPN
 Services
 DHCP server
 Dynamic DNS
 Web server
 SNMP
 Modbus TCP
 Client monitoring
SMS Service
 Prioritization
 System
 Information

SMS Service

Enable SMS service: ☒ ?

Password SMS Control: ?

Mobile Number 1: ?

Mobile Number 2:

Mobile Number 3:

Allowed SMS Control functions

Enable SMS Control: ☒ ?

Reboot: ☒ ?

Establish/Cancel mobile network connection: ☒ ?

Establish/Cancel VPN connection: ☒ ?

Set digital output Alarm on/off: ☒ ?

Enable SMS Traps: ☒ ?

Send SMS after power up/reboot: ☒ ?

Send SMS if connected to mobile network: ☒ ?

Send SMS after disconnection from mobile network: ☒ ?

Send SMS after change of VPN connection (On-/Offline): ☒ ?

Send this message when digital input (Cut) changes to "On": ☒ Digital input /CUT/ changed ?

Send this message when digital input (Cut) changes to "Off": ☒ Digital input /CUT/ changed ?

Send this message when digital output (Alarm) changes to "On": ☒ Digital output -Alarm- change ?

Send this message when digital output (Alarm) changes to "Off": ☒ Digital output /Alarm/ change ?

Apply settings
Reset changes

Menu	Configuration → Services → SMS Service	
Functions	Router sends information via SMS messages (output). Router can be controlled via SMS messages (input). Menu available for IE-SR-2GT-LTE/4G and IE-SR-6GT-LTE/4G only.	
	Enable SMS service	Enables or disables generally the use of text messages for control functions (SMS input) and sending information (SMS output).
	Password SMS Control	If a password is entered then each incoming SMS control message must be secured by this password. Otherwise received text message will be dropped. Format of a password-secured SMS control message: #<password>?<command> Examples: #Detmold?reboot or #Detmold?OutputAlarm=on Note: The password is case sensitive, the command is NOT case sensitive.
	Mobile number 1 - 3	Only defined mobile numbers may send SMS control messages to the router and can receive information messages (SMS traps) from the router. For using SMS services at least one mobile number has to be configured. (Use international format +xxxxxxxxxxxxxx).
	Enable SMS Control	Allows or denies generally the use of text messages for control functions (SMS input).

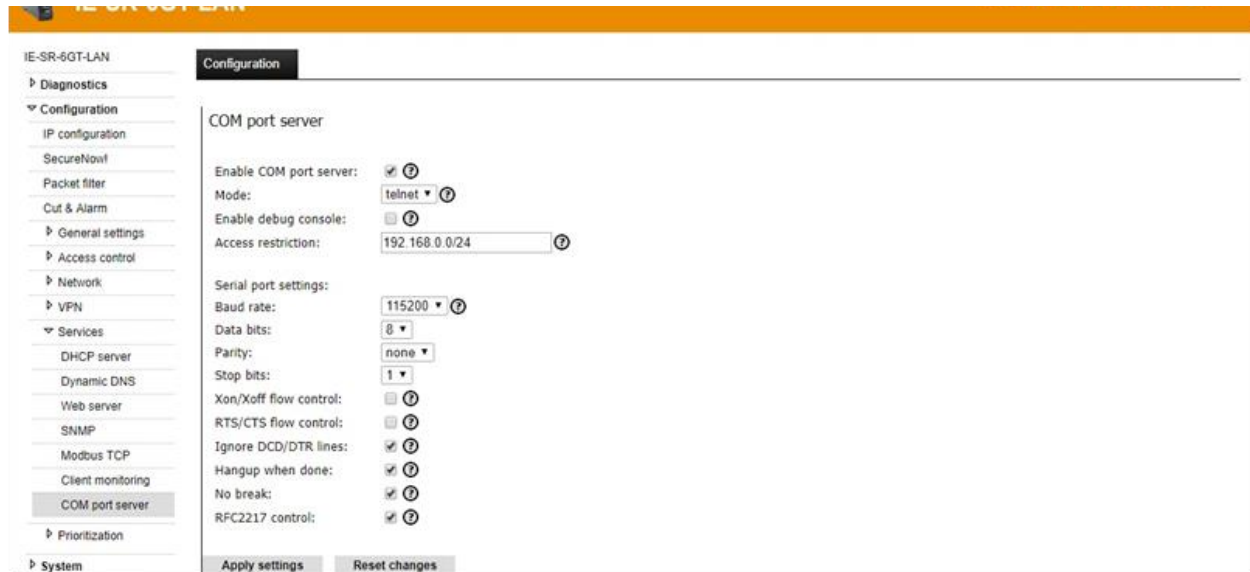
Version 2.04 / March 2020

Page 71 / 127

Reboot	Allows/denies a device reboot via SMS command. Commands: <i>#password?reboot</i> or <i>?reboot</i> if no password is set. Note: For feedback about a successful reboot please activate SMS trap "Send SMS after power up / reboot".
Establish/Cancel mobile network connection	Allows/denies establishing or cancel the Internet connection of the mobile interface via SMS command. Commands: <i>#password?MobileConnection=on/off</i> or <i>?MobileConnection=on/off</i> if no password is set. Note: For feedback about the required action please activate the related SMS traps (mobile network connection/disconnection).
Establish/Cancel VPN connection	Allows/denies establishing or cancel a predefined VPN connection (OpenVPN1 - 10, IPsecVPN or u-linkVPN) via SMS command. Commands: <i>#password?OpenVPN1=on/off</i> or <i>?OpenVPN1=on/off</i> or <i>#password?u-linkVPN=on/off</i> or <i>?IPsecVPN=on/off</i> if no password is set). Note: For feedback about the required action please activate the related SMS trap "Send SMS after change of VPN connection (On-/Offline)".
Set digital output 'Alarm# on/off	Allows/denies setting the digital output (Alarm) on or off via SMS command Command: <i>#password?OutputAlarm=on/off</i> or <i>?OutputAlarm=on/off</i> if no password is set. Note: For feedback about the required action please activate the SMS traps related to the digital output (Alarm).
Enable SMS Traps	Enables/disables the sending of SMS traps. Note: SMS traps only will be sent to the defined mobile numbers 1 - 3.
Trap: Send SMS after power up/reboot.	If enabled the message <i><system name>: Reboot/Power Up at <system time></i> will be sent to the defined mobile numbers 1-3 after reboot or power-up.
Trap: Send SMS if connected to mobile network.	If enabled the message <i><System-Name>: Connected to <provider>; <network mode>; <signal strength>; <IP></i> will be sent to the defined mobile numbers 1-3 after connection to the mobile internet.
Trap: Send SMS after disconnection from mobile network.	If enabled the message <i><system name>: Disconnected from mobile network at <system time></i> will be sent to the defined mobile numbers 1-3 after disconnection from the mobile internet.
Trap: Send SMS after change of VPN connection (On-/Offline).	If enabled the message <i><system name>: OpenVPN1...10 / IpsecVPN / u-linkVPN established/disconnected</i> will be sent to the defined mobile numbers 1-3 after change of one of the defined VPN connections.
Trap: Send this message when digital input (Cut) changes to "On".	If enabled the message <i><system name>: <Entered text></i> will be sent to the defined mobile numbers 1-3 after changing of digital input (Cut) to ON.
Trap: Send this message when digital input (Cut) changes to "Off".	If enabled the message <i><system name>: <Entered text></i> will be sent to the defined mobile numbers 1-3 after changing of digital input (Cut) to OFF.

	Trap: Send this message when digital output (Alarm) changes to "On".	If enabled the message <system name>: <Entered text> will be sent to the defined mobile numbers 1-3 after changing of digital output (Alarm) to ON.
	Trap: Send this message when digital output (Alarm) changes to "OFF".	If enabled the message <system name>: <Entered text> will be sent to the fined mobile numbers 1-3 after changing of digital output (Alarm) to OFF.

Services → COM port server



The screenshot shows the 'Configuration' page for the 'COM port server'. The left sidebar lists various configuration categories, with 'Services' expanded and 'COM port server' selected. The main content area displays the following settings:

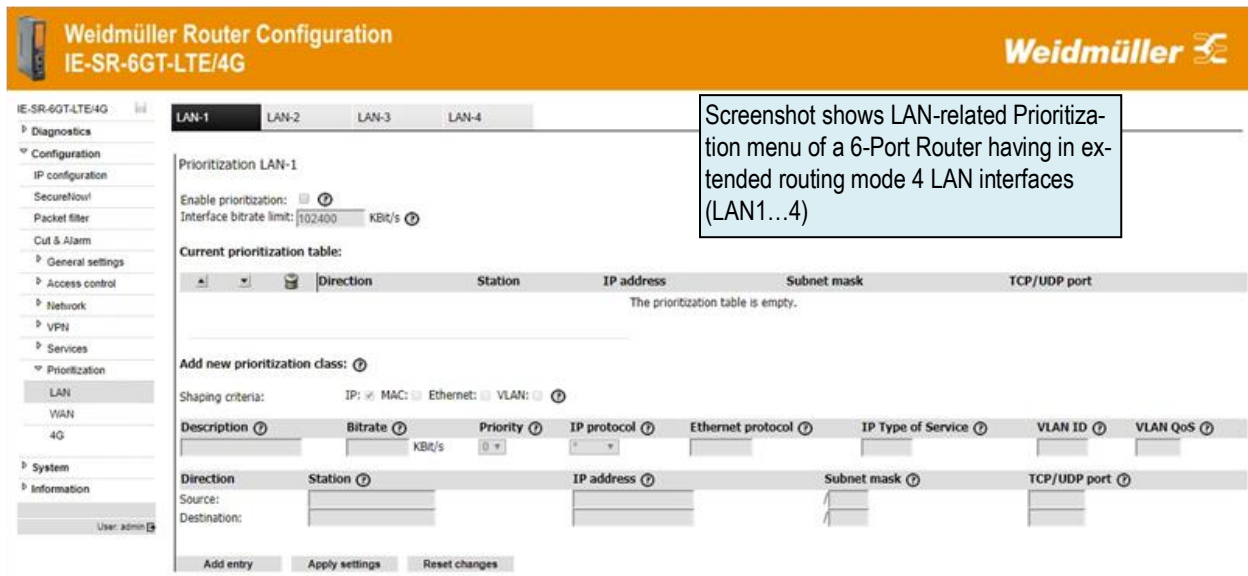
- Enable COM port server:** ☒ (with a help icon)
- Mode:** telnet (with a help icon)
- Enable debug console:** ☐ (with a help icon)
- Access restriction:** 192.168.0.0/24 (with a help icon)
- Serial port settings:**
 - Baud rate:** 115200 (with a help icon)
 - Data bits:** 8
 - Parity:** none
 - Stop bits:** 1
 - Xon/Xoff flow control:** ☐ (with a help icon)
 - RTS/CTS flow control:** ☐ (with a help icon)
 - Ignore DCD/DTR lines:** ☒ (with a help icon)
 - Hangup when done:** ☒ (with a help icon)
 - No break:** ☒ (with a help icon)
 - RFC2217 control:** ☒ (with a help icon)

At the bottom of the configuration area are two buttons: 'Apply settings' and 'Reset changes'.

Menu	Configuration → Services → COM port server	
Function	Enable the serial port COM server. The router will open TCP port 3001 for incoming connections which will be redirected to the RS232 interface.	
	Mode:	Telnet: use for serial console terminals, you can directly use telnet to TCP port 3001. Raw: use the raw mode for virtual serial port clients.
	Enabling debug console:	Enable a control and diagnose console on telnet TCP port 20000. The access restriction will apply here too.
	Access Restriction:	Enter IP address/mask i.e. 192.168.0.0/24. Connections from this source are allowed, all others get blocked.
	Baud rate:	Select the baud rate of the interface.
	Data bits:	Choose whether there are 7 or 8 data bits.
	Parity:	Non, even or odd
	Stop bits:	1 or 2 stop bits
	Xon/Xoff flow control	Enable/disable
	RTS/CTS flow control	Enable/disable
	Ignore DCD/DTR lines:	Enable/disable
	Hang-up when done:	Lower the local DCD/DTR lines if the remote connection gets disconnected.
	No break:	Disables the automatic clearing of the break setting.
	RFC2217 control	Allow remote RFC2217 control of the serial parameters.

4.2.10 Configuration → Prioritization

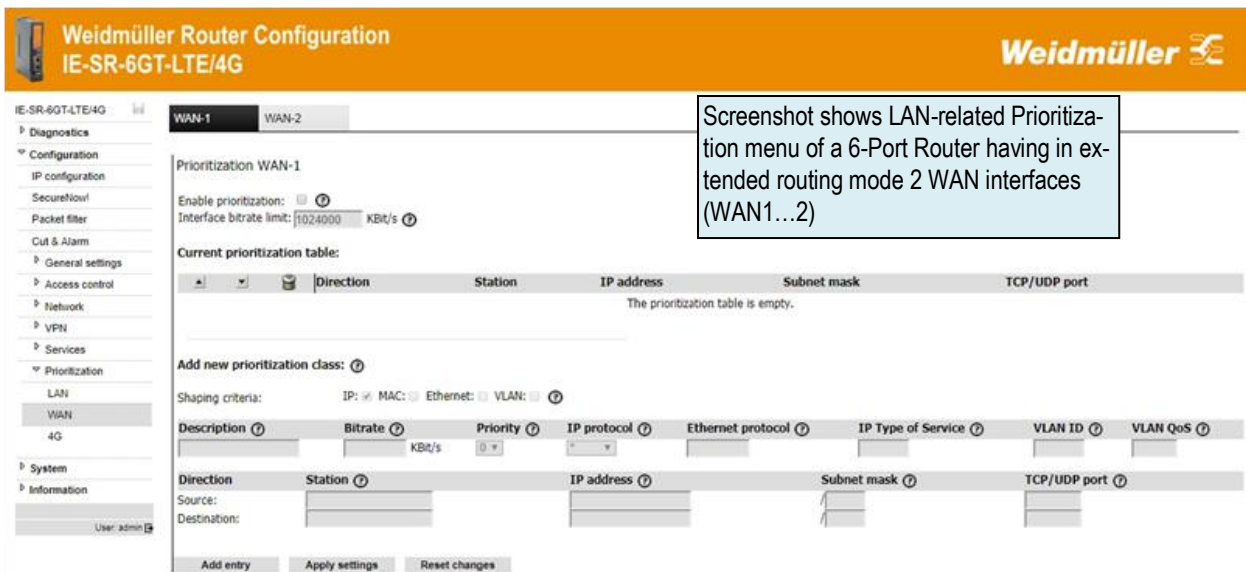
Prioritization → LAN



Menu	Configuration → Prioritization → LAN	
Function	With this feature, outgoing traffic on the LAN interfaces can be classified and prioritized. The prioritization ("traffic shaping") can be configured on both Layer 2 (based on MAC addresses) and at Layer 3 (IP addresses and protocols). On extended routing mode, all LAN interfaces can be configured separately by selecting the appropriate tab.	
	Interface bitrate limit	Total bandwidth of interface that must be specified if prioritization is enabled. If a new prioritization class is added and no bitrate limit is yet defined, a default value will be used. Hint: If the sum of all defined classes below exceeds this value, no prioritization will be done, only shaping. Every bitrate will be the allowed maximum for the corresponding class and the priority value will be used.
	Current prioritization table	Table that displays all configured rules.
	Add a new prioritization class	Outgoing packets that match the given criteria (e.g. the protocol) will be sorted into the class and sent according to the given bitrate and priority. Traffic is sorted into the first matching class of the prioritization table. Traffic that does not match any class is handled with priority 7.
	Shaping criteria	Select which kind of criteria should be checked to classify traffic. Note: Not all combinations are possible. If no set of criteria is selected any traffic will match this class. This can be used to overwrite the default priority 7 (lowest) for traffic that does not match any other prioritization class.
	Description	Short alphanumerical (no blanks) description (20 characters max.) for this class. May be left empty

	Bitrate	Guaranteed bandwidth available to this class, independent of priority. If greater than the interface bitrate limit, it is reduced to the interface limit internally. Note: In addition to the minimum rate defined here, a class may lend bandwidth from other classes. If you want this value to be the maximum bitrate for a class. Make sure that the sum of all classes bitrates is one plus the bandwidth of the interface as defined above.
	Priority	A value between 0 and 7 that indicates how important this class is compared to others. 0 is highest and 7 is lowest priority. Will only be used if the sum of all bitrates does not exceed the interface bitrate limit.
	IP protocol	Use * for any IP protocol, select TCP, UDP or ICMP
	Ethernet protocol	Ether type of packets as hexadecimal value (e.g. 0x88cc). If may range from 0x0600 to 0Xffff 8SEE. http://iana.org/assignments/Ethernet-numbers). If the VLAN header is checked, enter the encapsulated ether type, e.g. 0.0800 for IPv4
	IP Type of Service (ToS)	The IP Type of Service is a hexadecimal value (e.g. 0x80) that specifies the kind of traffic (e.g. voice data). Leave empty or use * for any ToS.
	VLAN ID	The VLAN ID is a decimal value that identifies a virtual LAN. It may range from 1 to 4094. Note VLAN ID and priority cannot be checked at the same time. If you want to classify traffic by VLAN priority (QoS) the ID must be set to 0 (or left empty).
	VLAN Quality of Service (QoS)	The VLAN priority (QoS) ranges between 0 and 7. The higher the value the more important a packet is. Note: VLAN ID and priority cannot be checked at the same time. If you want to classify traffic by VLAN ID, this field must be left empty.
	Station	MAC address of source and destination (e.g. 00:15:7E:FE:23:1A). Leave empty or use * for any address.
	IP address	IP address of source and destination (e.g. 192.168.1.110). Leave empty or use * for any address.
	Subnet mask	Subnet mask as number of fixed bits of IP address counted from the left (e.g. equals subnet mask 255.255.255.0). Leave empty if given IP address is either arbitrary (*) or supposed to match exactly. Otherwise the value must be between 8 and 32.
	TCP/UDP port	TCP/UDP port between 1 and 65535 or a port range (e.g. 1024:10000.). Leave empty or use * for any port.

Prioritization → LAN



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

Configuration

Prioritization WAN-1

Enable prioritization: ☐
Interface bitrate limit: 1024000 KBit/s

Current prioritization table:

Direction	Station	IP address	Subnet mask	TCP/UDP port
The prioritization table is empty.				

Add new prioritization class:

Shaping criteria: IP: ☒ MAC: ☐ Ethernet: ☐ VLAN: ☐

Description	Bitrate	Priority	IP protocol	Ethernet protocol	IP Type of Service	VLAN ID	VLAN QoS
	KBit/s	0	*				

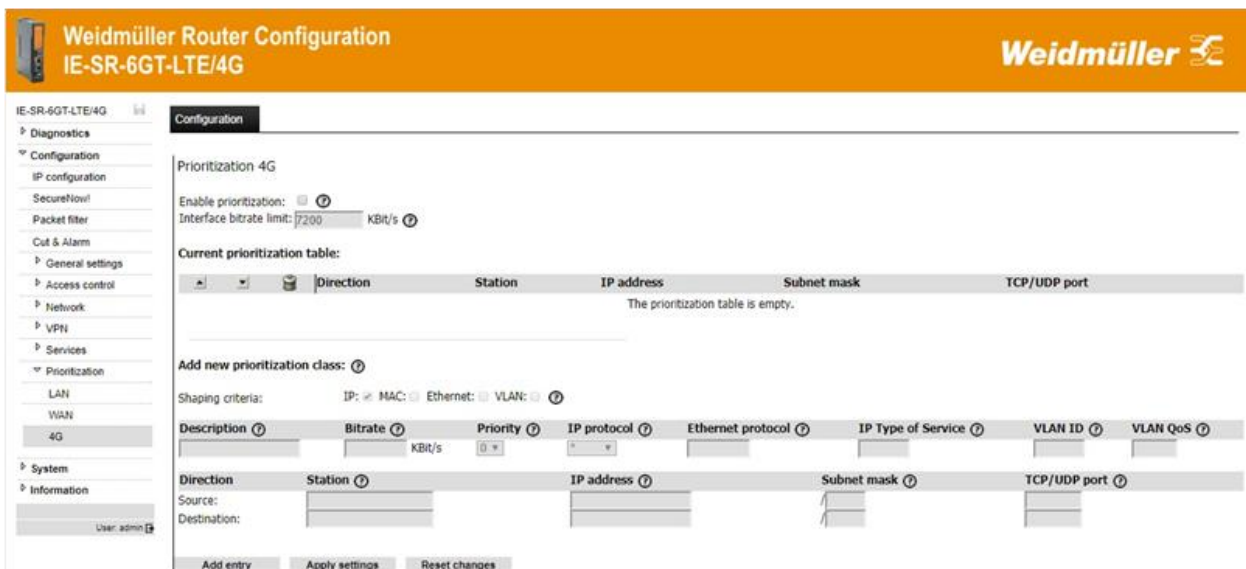
Direction **Station** **IP address** **Subnet mask** **TCP/UDP port**

Source:
Destination:

Add entry **Apply settings** **Reset changes**

Menu	Configuration → Prioritization → WAN
Function	With this feature, outgoing traffic on the WAN interface can be classified and prioritized. The prioritization ("traffic shaping") can be configured on both Layer 2 (based on MAC addresses) and at Layer 3 (IP addresses and protocols). On extended routing mode, all WAN interfaces can be configured separately by selecting the appropriate tab. Uses the same attributes as for Prioritization → LAN.

Prioritization → 4G



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

Configuration

Prioritization 4G

Enable prioritization: ☐
Interface bitrate limit: 7200 KBit/s

Current prioritization table:

Direction	Station	IP address	Subnet mask	TCP/UDP port
The prioritization table is empty.				

Add new prioritization class:

Shaping criteria: IP: ☒ MAC: ☐ Ethernet: ☐ VLAN: ☐

Description	Bitrate	Priority	IP protocol	Ethernet protocol	IP Type of Service	VLAN ID	VLAN QoS
	KBit/s	0	*				

Direction **Station** **IP address** **Subnet mask** **TCP/UDP port**

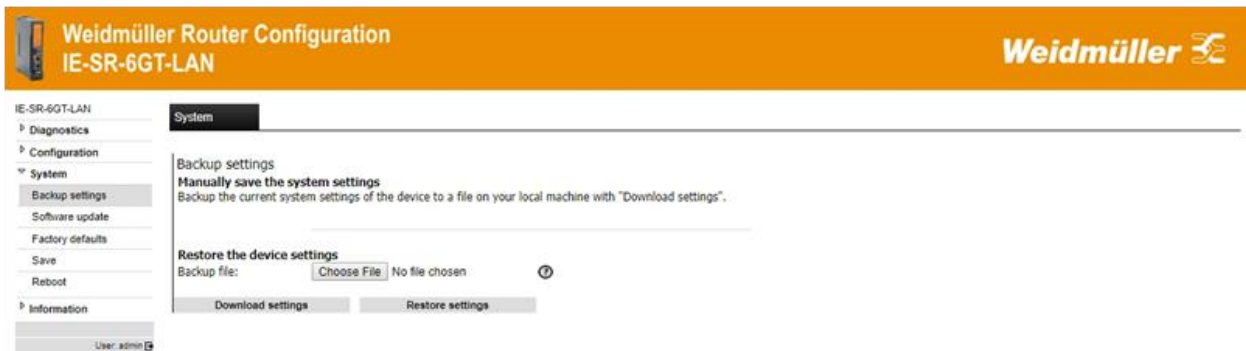
Source:
Destination:

Add entry **Apply settings** **Reset changes**

Menu	Configuration → Prioritization → 4G
Function	With this feature, outgoing traffic on the 4G interface can be classified and prioritized. The prioritization ("traffic shaping") can be configured on both Layer 2 (based on MAC addresses) and at Layer 3 (IP addresses and protocols). Only for cellular routers. Uses the same attributes as for Prioritization → LAN.

4.3 Section System

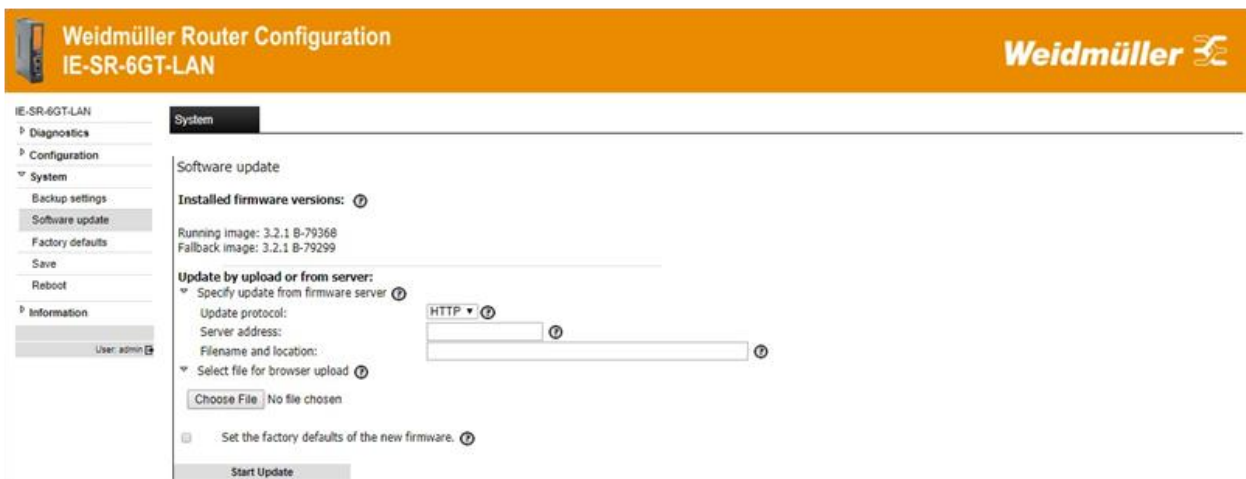
4.3.1 System → Backup settings



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

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

4.3.2 System → Software update



Menu	System → Software update
Function	With this menu item a firmware update can be carried out. The Weidmüller Firmware for Security Routers can be used for all router models. It can be downloaded e.g. from the Weidmüller online catalog in section “Downloads” of the relevant product. With this action the Running image will become the Fallback image and the Fallback image will be deleted. The easiest way to update the Router with a new firmware is to use the function „Update by browser upload“.

	Specify update from firmware server	Update the device with a firmware from a remote HTTP/FTP/TFTP server. 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. 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. Filename and location: Filename of the firmware file including the path on the remote server i.e. updates/firmware-1.0.0.bin Note: There must be no leading / on HTTP
	Select file for browser update	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.
	Set the factory defaults of the new firmware	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.

4.3.3 System → Factory defaults



Menu	System → Factory default										
Function	With this menu item the Router can be set to factory default settings. Please note that doing a reset to factory values the IP addresses will be changed and the connection between the Router and the configuration PC can be lost. <u>Basic factory settings:</u> <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		
		
	This icon (disk symbol) starts flashing if the configuration has been changed and activated but not saved. Clicking on the icon the web interface jumps into this menu item (regardless the window which currently is displayed)	

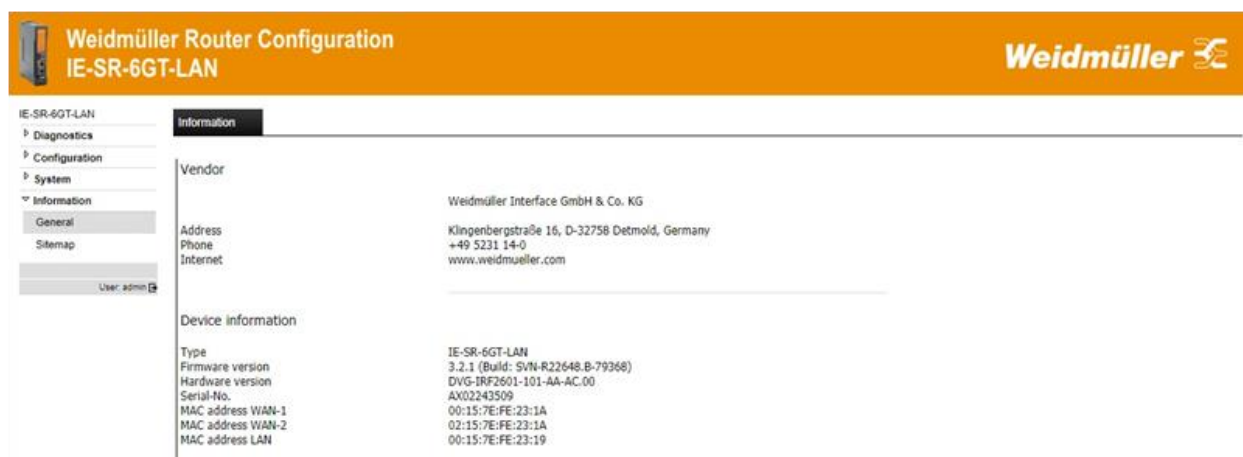
4.3.5 System → Reboot



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

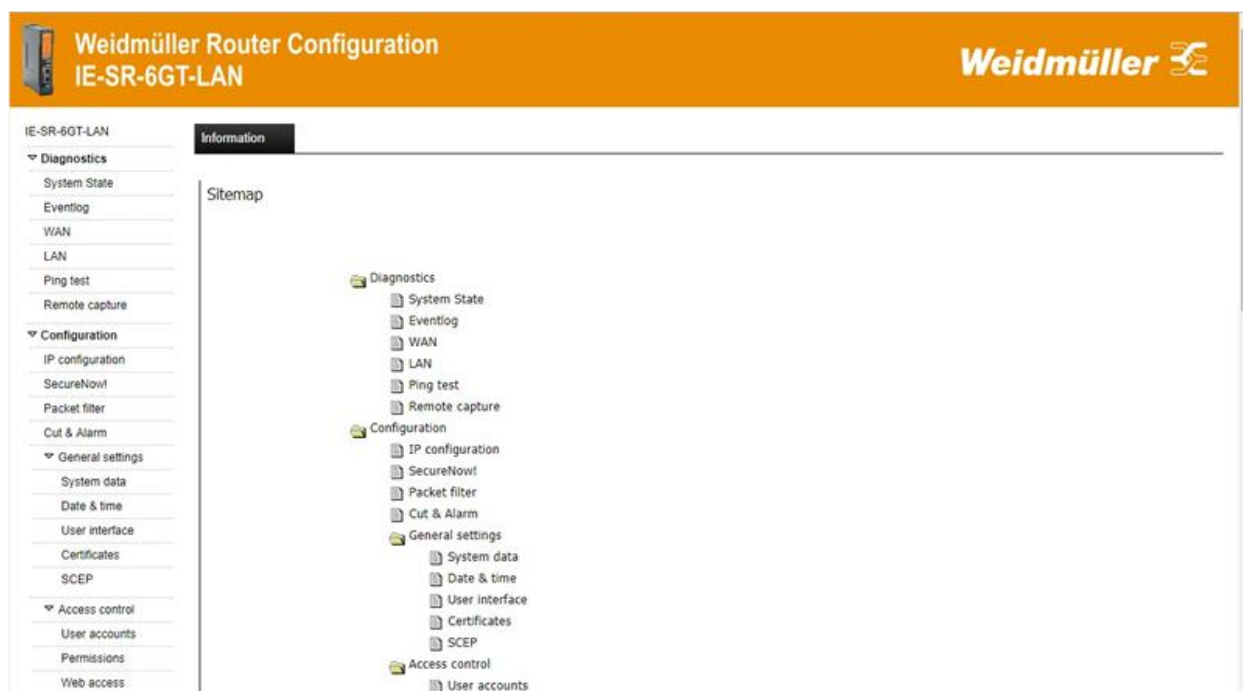
4.4 Section Information

4.4.1 Information → General



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

4.4.2 Information → Sitemap



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

5. Appendix A (Configuration examples)

A1 – Restore configuration from USB stick

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

How to do:

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

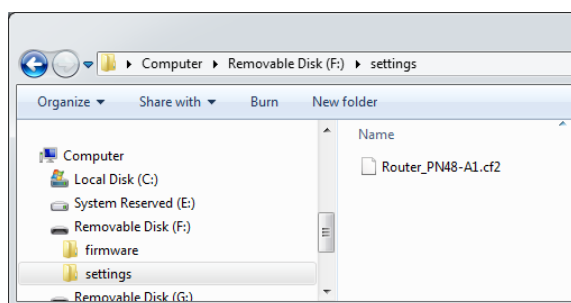
How to check the result of the import procedure via USB stick:

Method 1: Open Web interface and check the configuration.

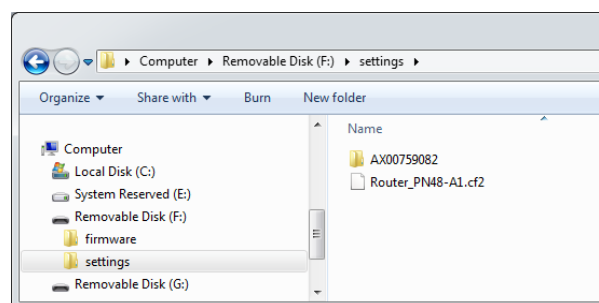
Method 2: Plug the USB stick into a PC and check directory **settings** which now should have a new sub directory with a name same as the device serial number (e.g. **AX1367406**). This directory contains a log file named **settings.log** created by the Router at configuration upload.

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

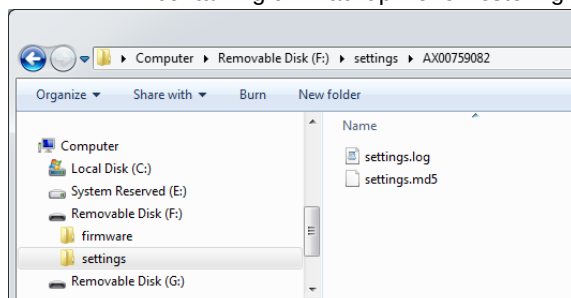
Note: If you will use the same USB stick - containing a general template configuration file - for an initial setup of several Routers, then each Router will create during the restoring process its own sub directory **AX....** (based on the unique serial number) below directory **settings** containing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



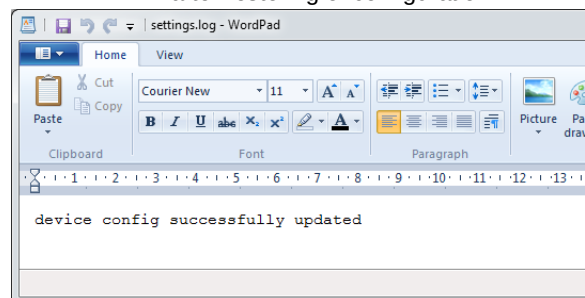
Screenshot 1: Directory "settings" of USB stick containing cf2-Backup file for restoring



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



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

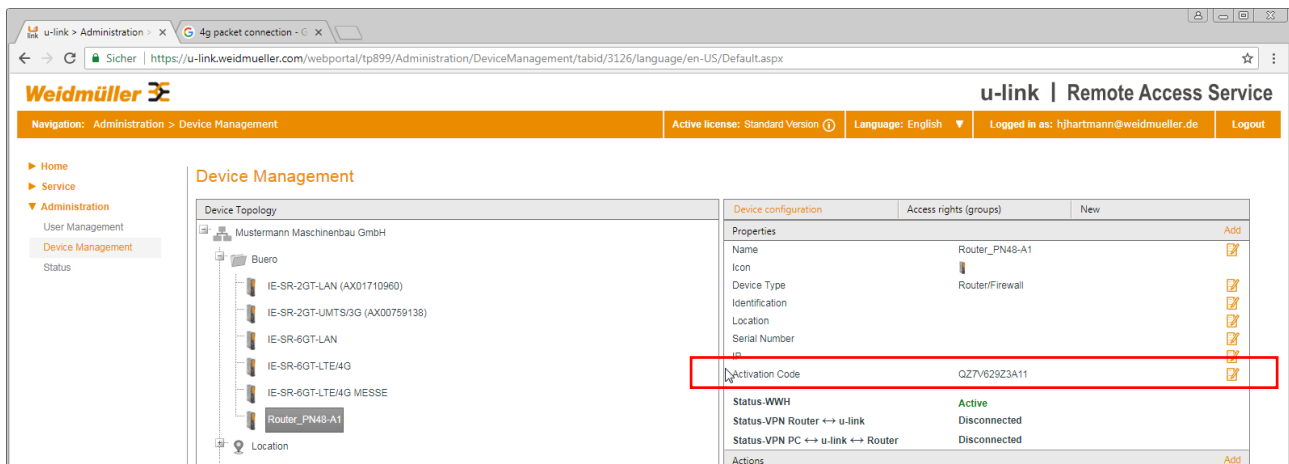


Screenshot 4: Content of status file "settings.log"

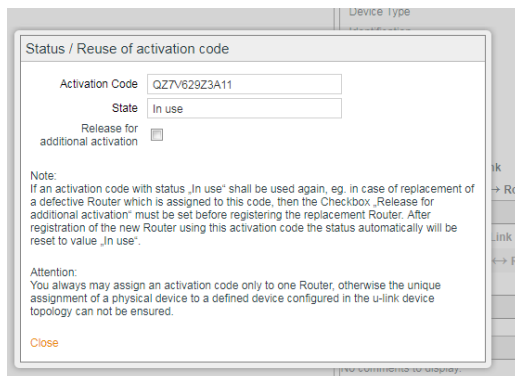
Important note if you will use this method for replacement of an already registered u-link Router!

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

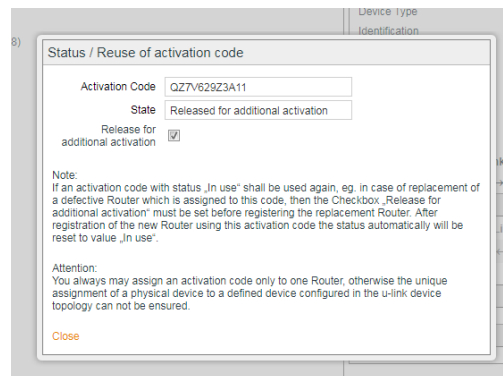
- Step 1: Login (as administrator or user) into the u-link web portal.
- Step 2: Open menu Administration → Device Management.
- Step 3: Expand container "Device Topology" and select the Router object representing the physical Router which shall be replaced.
- Step 4: Click "Edit" icon in the row of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



Device Management of u-link Web portal



Current status of activation code (In use)



New status "Released for additional activation"

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

Application requirements:

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

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

In this example the IP address ranges are set to

192.168.10.0 / 255.255.255.0 for Network 1 and

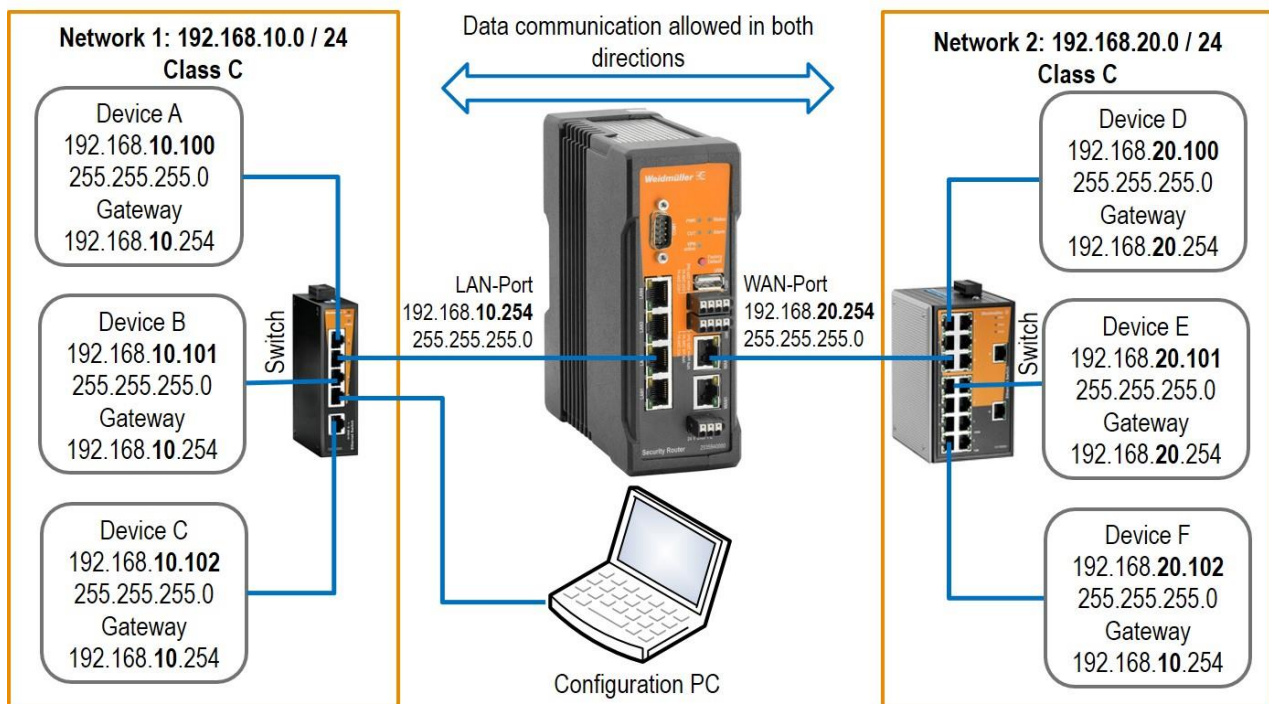
192.168.20.0 / 255.255.255.0 for Network 2

The Router interfaces will be set to

192.168.10.254 / 255.255.255.0 for LAN interface and

192.168.20.254 / 255.255.255.0 for WAN interface

Network diagram of below described application scenario



How to configure the Router

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

1. Connect the configuration PC to Router LAN Port.

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

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

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

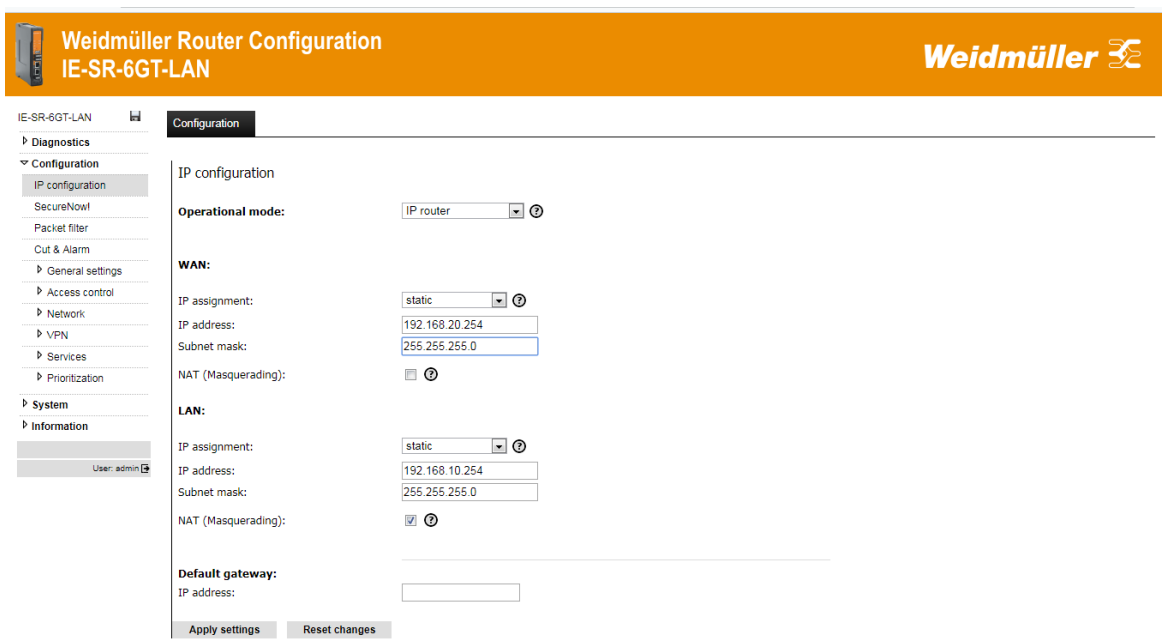
3. Start a web browser and login into the web Interface of Router (<http://192.168.1.110>)

User: admin
 Password: Detmold

4. Set the basic IP configuration

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

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



Weidmüller Router Configuration
IE-SR-6GT-LAN

Configuration

IE-SR-6GT-LAN

Configuration

IP configuration

Operational mode: IP router

WAN:

IP assignment: static

IP address: 192.168.20.254

Subnet mask: 255.255.255.0

NAT (Masquerading): ☐

LAN:

IP assignment: static

IP address: 192.168.10.254

Subnet mask: 255.255.255.0

NAT (Masquerading): ☒

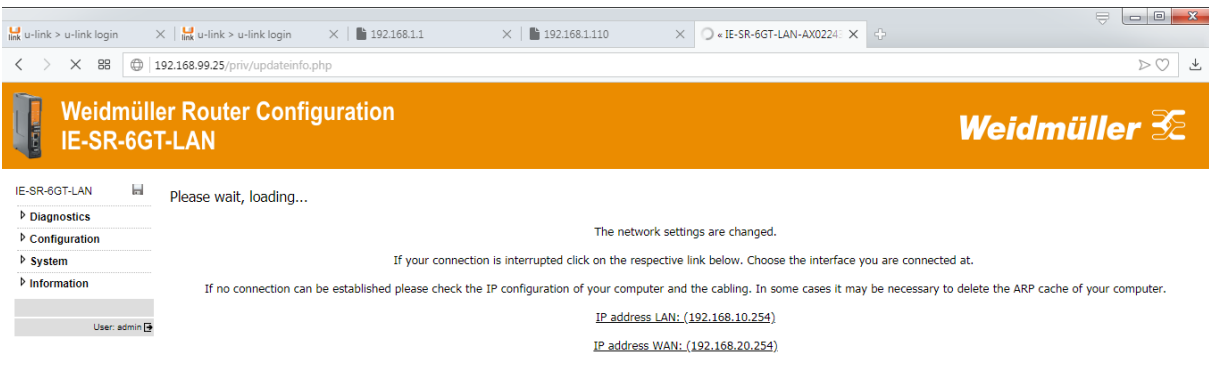
Default gateway:

IP address:

Apply settings Reset changes

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

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



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

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

IP address: 192.168.10.99

Subnet mask: 255.255.255.0

Standard-Gateway: 192.168.10.254

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

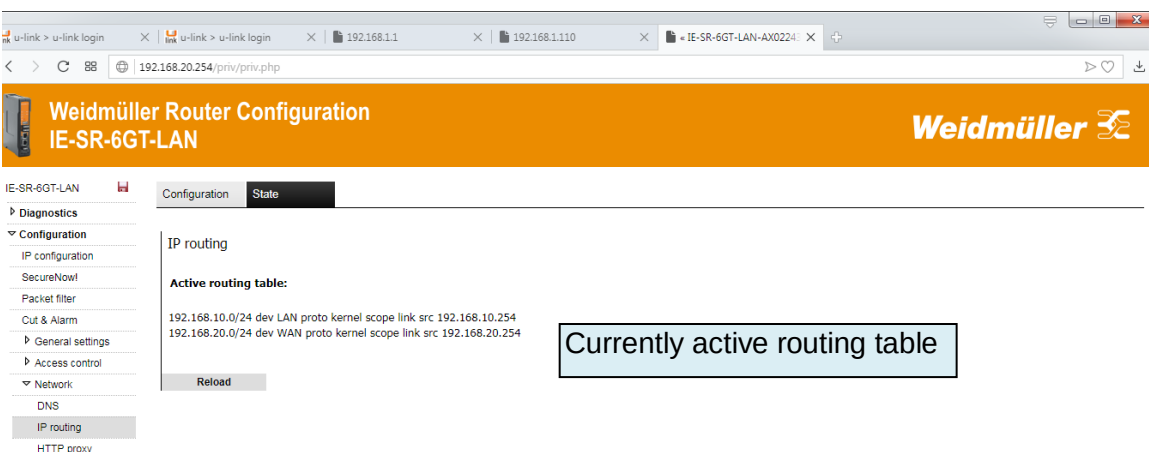
Use IP address 192.168.10.254 (http://192.10.1.254) on LAN port

User: admin

Password: Detmold

6. Check the currently active “routes”

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



7. Saving the new configuration

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

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

- Select menu **System → Backup settings**

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

Now the configuration of the Router is finished!

Testing the accessibility between Ethernet Devices of both networks

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

- ping 192.168.20.100
- ping 192.168.20.101
- ping 192.168.20.102

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

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

- ping 192.168.10.100
- ping 192.168.10.101
- ping 192.168.10.102

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



Note

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

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

Application requirements:

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

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

Solution:

1. Activating “NAT masquerading” at **WAN** port of the Router which is connected to network 2. As result the sender IP addresses of any outgoing traffic at WAN port – initiated by devices of network 1 connect to LAN port – will be translated to the IP address of the Router’s WAN port. From the perspective of the receivers the sender is always the Router WAN port. The IP addresses of devices connected to the LAN port will be hidden and are not visible.
2. To get access to the devices C and D of the hidden network 1 the Router’s “IP address forwarding” feature can be used, which assigns devices C and D an additional and unused IP address from the range of network 2. Effectively the Router will have 3 IP addresses at WAN port (Physical WAN IP address and 2 virtual IP addresses). This feature acts as a special kind of “port forwarding” using only IP addresses and omitting the ports.



Note

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

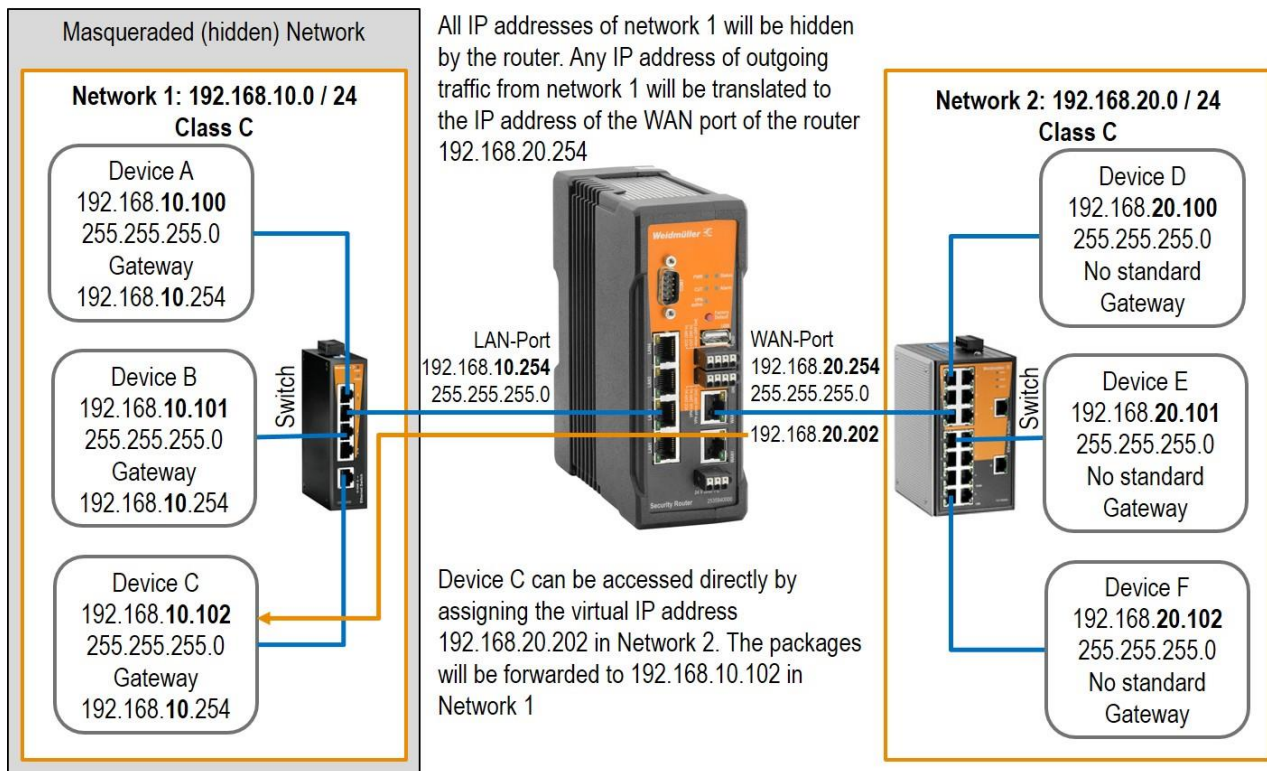
In this example the IP address ranges are set to

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

The Router interfaces will be set to

192.168.**10**.254 / 255.255.255.0 for LAN interface and
192.168.**20**.254 / 255.255.255.0 for WAN interface

Network diagram of below described application scenario



How to configure the Router

Starting situation

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

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

Note: Use autonegotiation on the Ethernet Interface of the PC

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

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

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

User: admin
 Password: Detmold

4. Set the basic IP configuration and activate NAT masquerading

- Select menu **Configuration** → **IP configuration**
- Configure the menu entries as below described

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

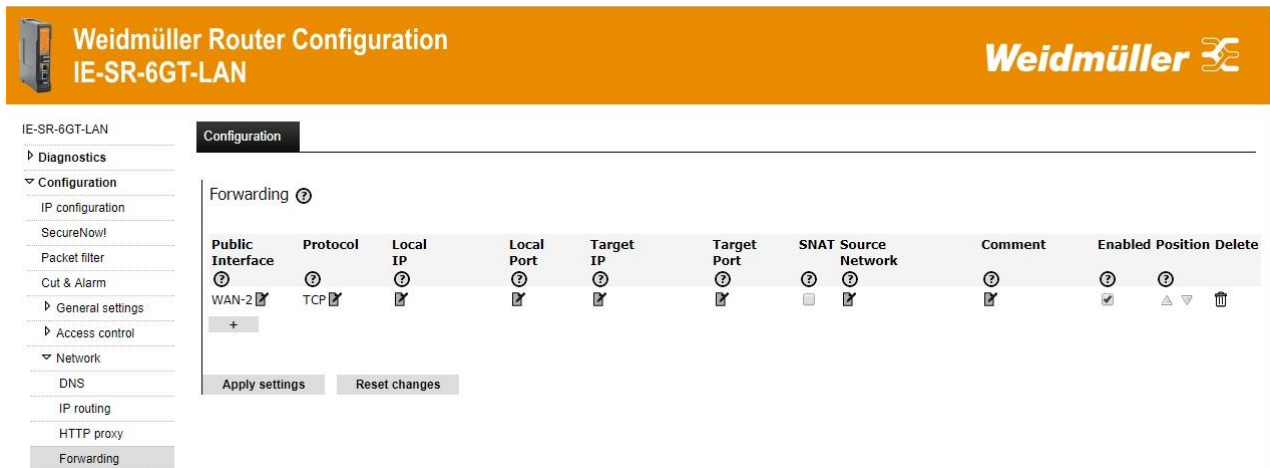


Figure 3: Empty IP forwarding table

- ▶ 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 4
 - Ensure that each input will be completed by clicking the icon .
- ▶ Now click button “Apply settings” to activate the “IP address forwarding table”

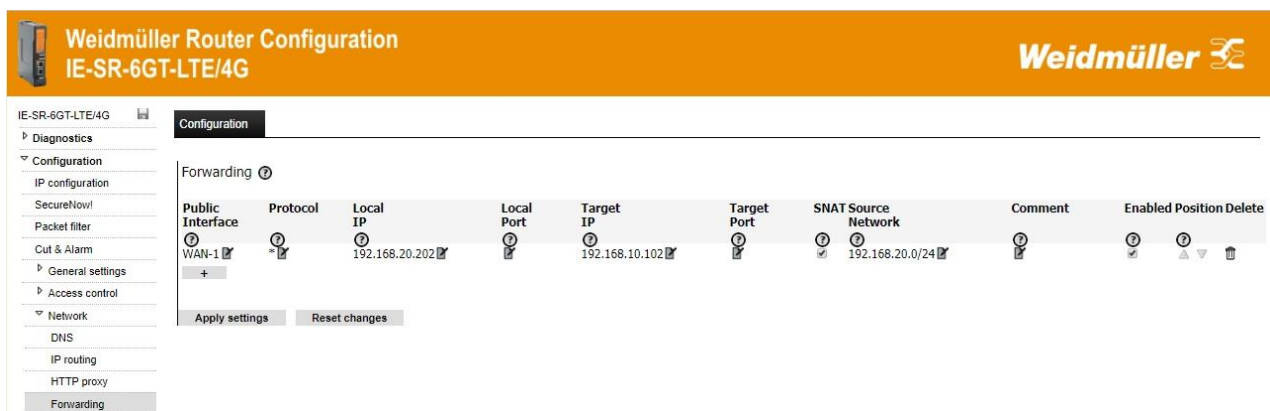


Figure 4: IP forwarding

Now the configuration of the Router is finished!

Testing the NAT masquerading feature

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

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

Results showing in the Wireshark window:

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

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

Testing the configured IP address forwarding

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

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

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

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



Note

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

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

Application requirements:

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

This application can be done with all router models.

Solution:

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

In this example the IP address ranges are set to

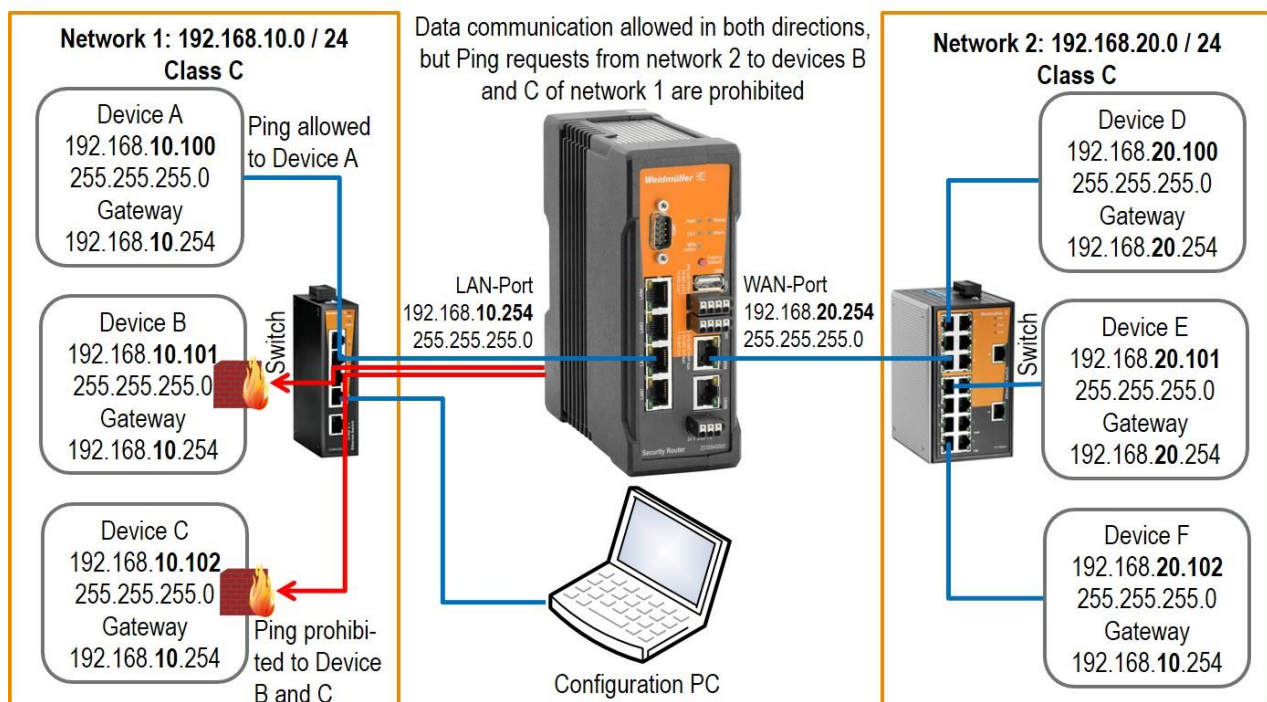
192.168.10.0 / 255.255.255.0 for Network 1 and

192.168.20.0 / 255.255.255.0 for Network 2

The Router interfaces will be set to

192.168.10.254 / 255.255.255.0 for LAN interface and

192.168.20.254 / 255.255.255.0 for WAN interface



Network diagram of below described application scenario

How to configure the Router

Starting situation

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

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

Note: Use autonegotiation on the Ethernet Interface of the PC

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

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

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

User: admin
 Password: Detmold

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

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

Operational mode:	IP Router
IP address parameters WAN Port:	Static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) NOT SET
IP address parameters LAN Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) NOT SET
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”

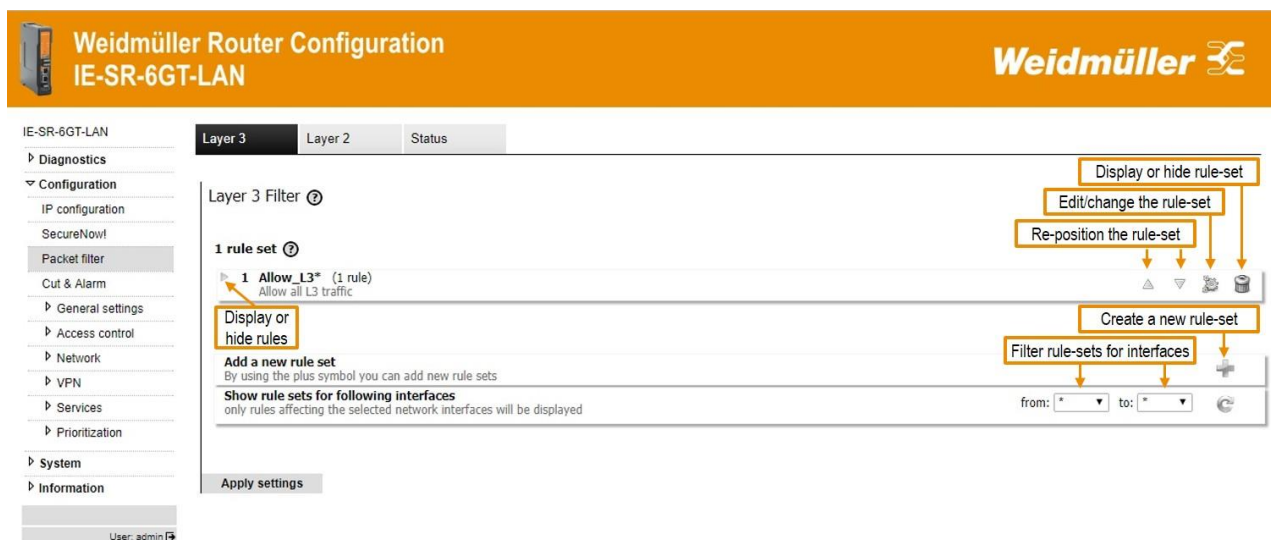


Figure 5: Packet filter

- 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)

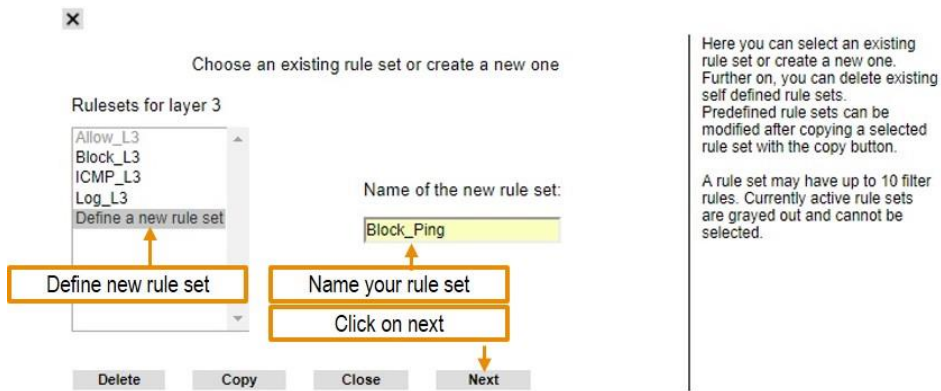


Figure 6: Create a new rule-set

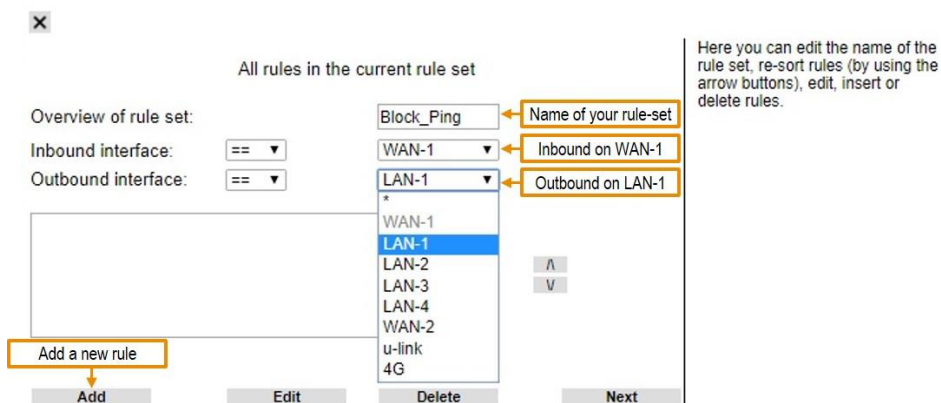


Figure 7: Define additional parameters of the new rule-set

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.

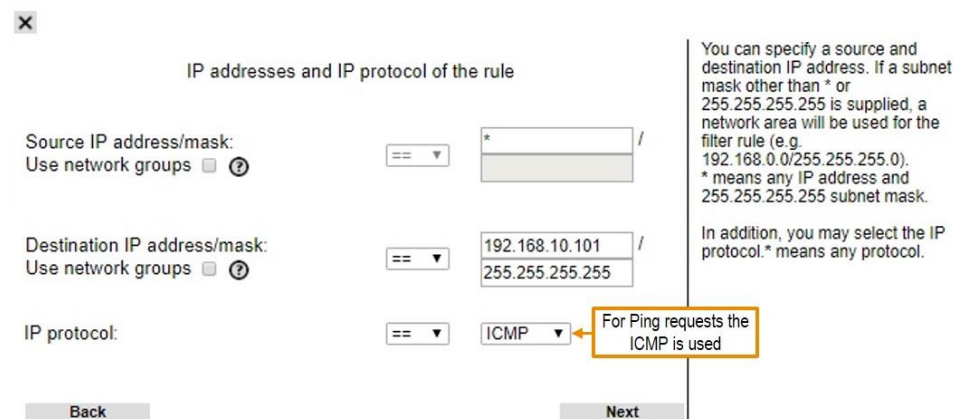


Figure 8: Define the first rule

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 9: Define additional parameters of the first rule

Check input/output signals for the rule

	Check signal	Signal high
CUT:	☐	☐
VPN KEY:	☐	☐
VPN UP:	☐	☐

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 10: 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 11: 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 12: 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 13: 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 14: Time limitations on filter rule-sets

Set time and date limitations for the rule-set.

Version 2.04 / March 2020

Page 97 / 127

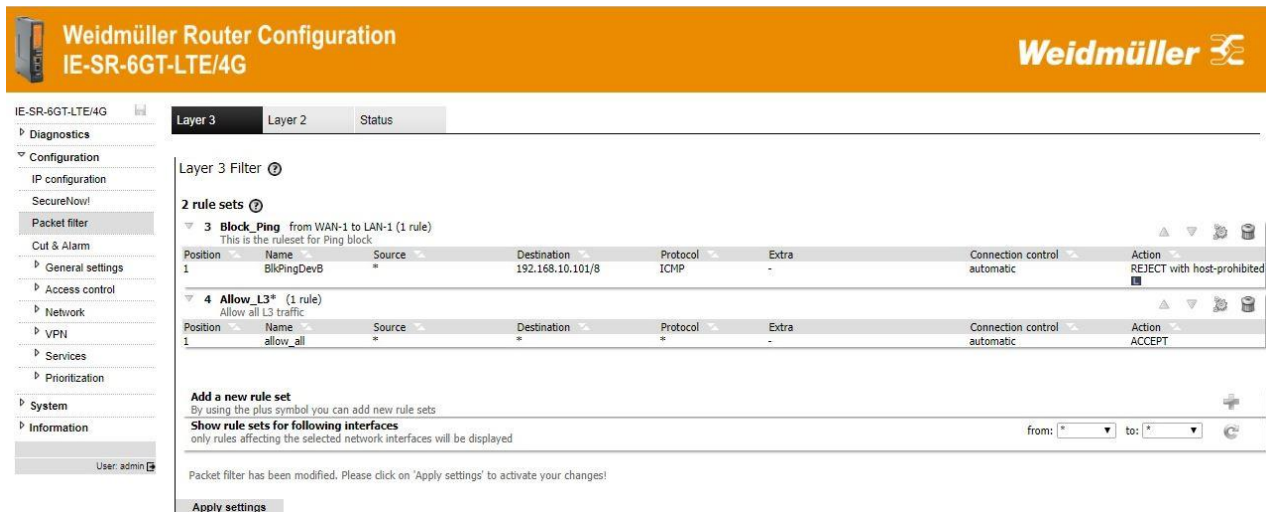


Figure 15: Overview of Packet filter rules

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

Now the firewall configuration (packet filter) is finished!

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

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

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

Results:

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

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

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

Task: The communication between Modbus Master devices and Modbus slave devices inside of the same switched network shall be controlled and secured by Firewall rules.

The Router shall act as a Layer-2 firewall (controlling MAC-based Ethernet frames) and being transparent for the devices inside of the switched network.

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

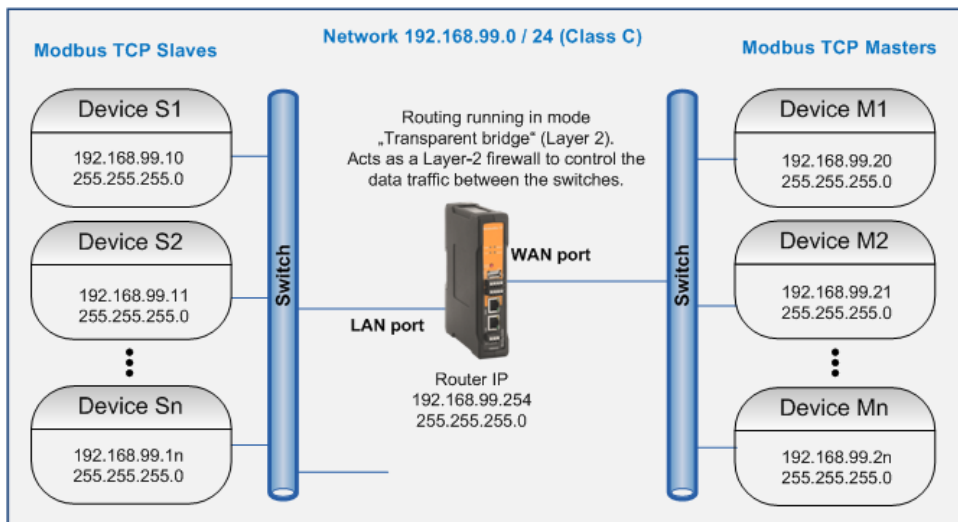


Figure 16: Example network topology

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

A5-1 Configuration of initial parameters

► Goto menu Configuration → IP configuration

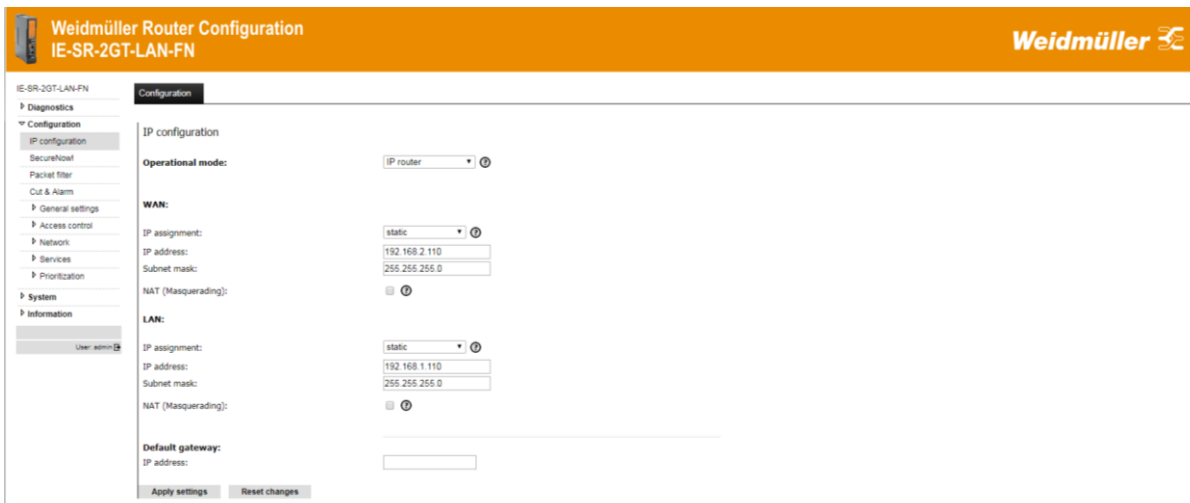


Figure 18: IP configuration factory defaults

- 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”

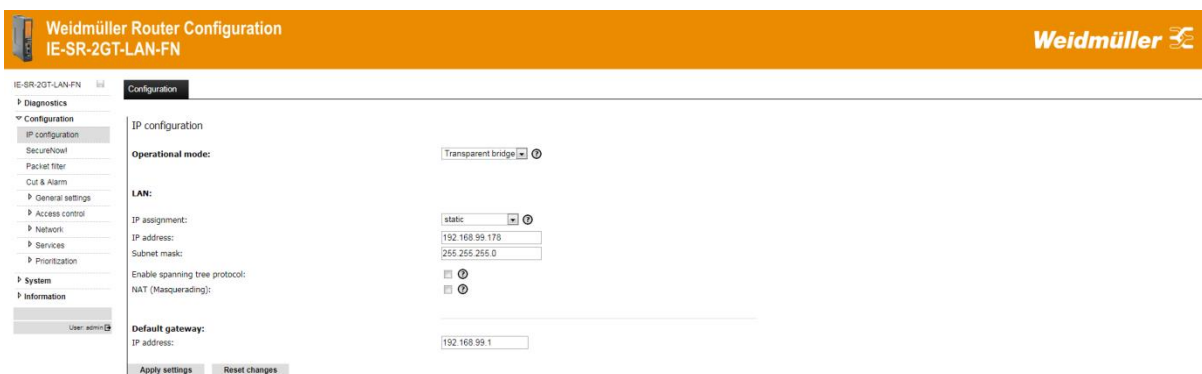
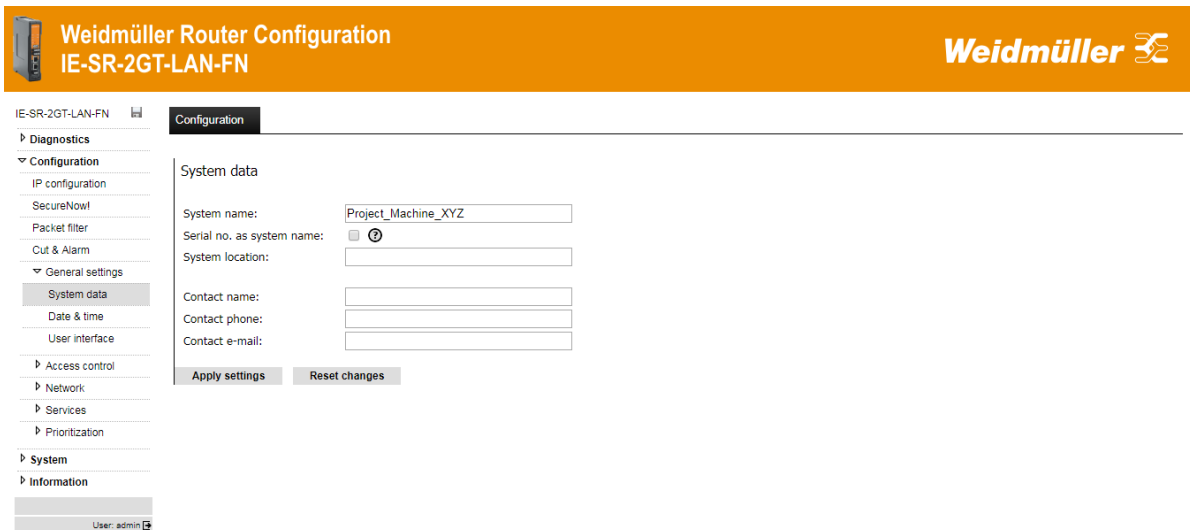


Figure 19: New IP configuration running as “Transparent bridge” (Layer 2)

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 20: 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 21: 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 22: 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 23: Tab “State” – showing NTP server statistics

A5-2 Configuration of the packet filter (Firewall)

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

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

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

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

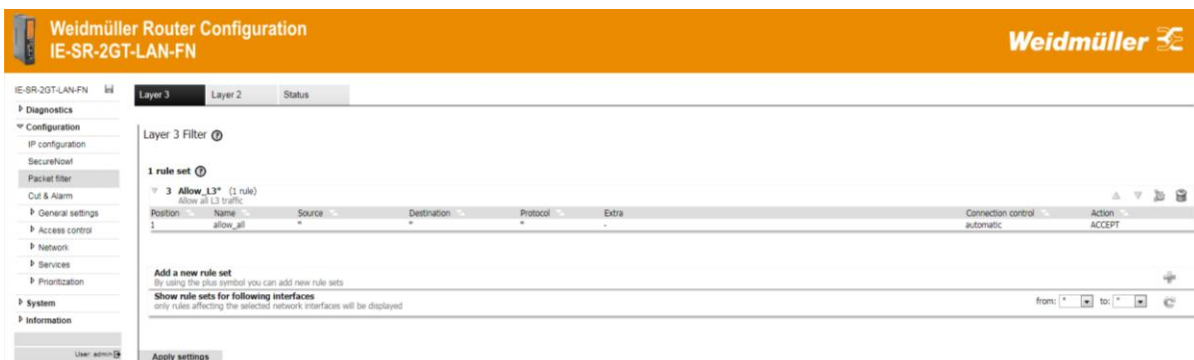


Figure 24: Factory default settings of Layer-3 Packet filter (firewall), valid for operation mode “IP Router”

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).

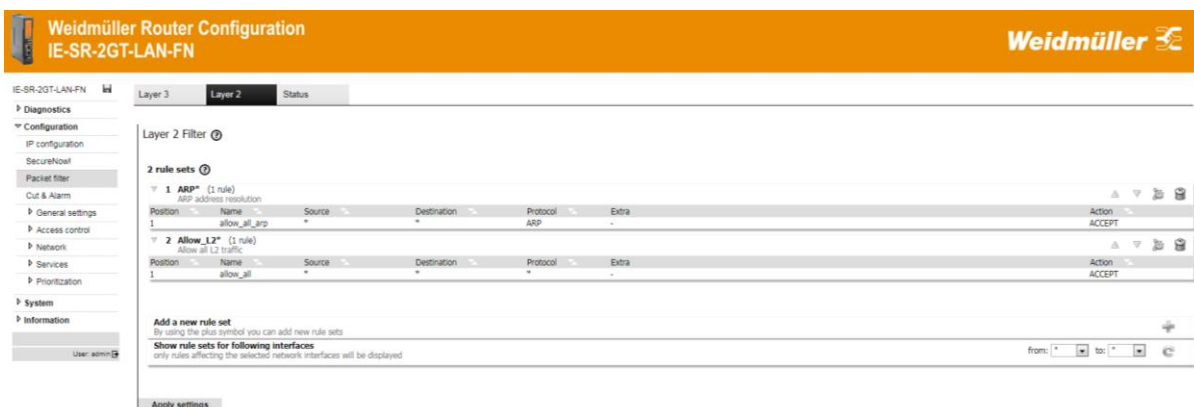


Figure 25: Factory default settings of Layer-2 Packet filter (firewall), valid for operation mode “Transparent bridge”

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.

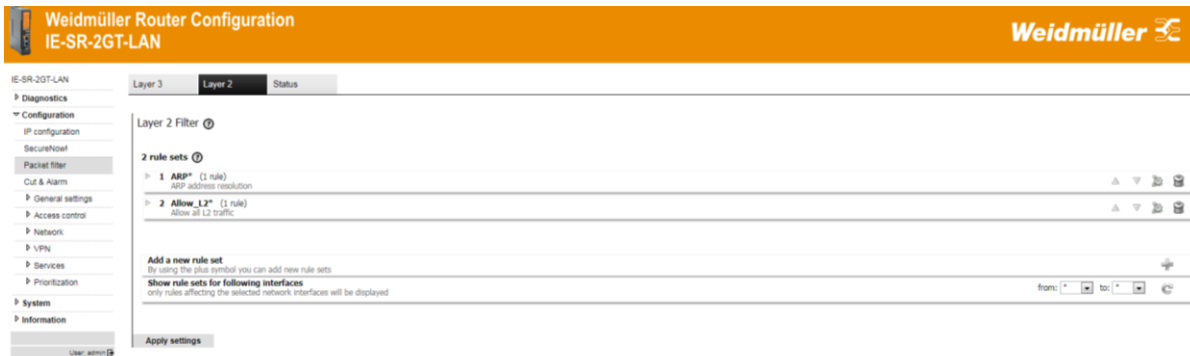
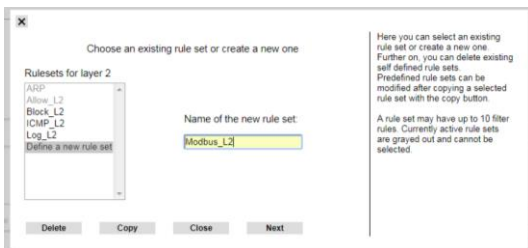
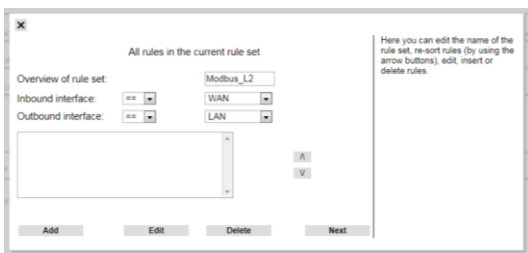


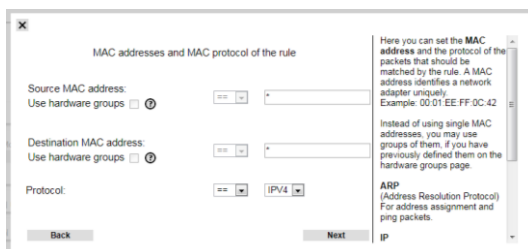
Figure 26: Factory default settings of Layer-2 Packet filter (firewall)



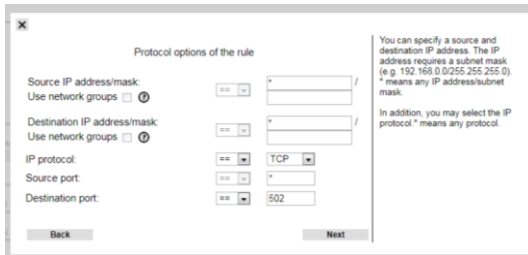
- Add a name for new rule-set (here Modbus_L2).
- Click ‘Next’.



- 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: *

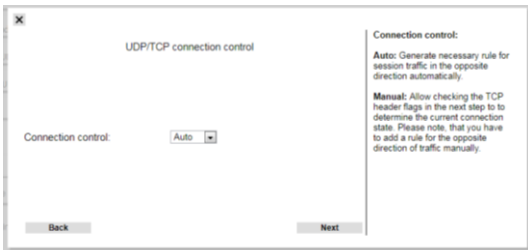
Destination port: 502

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

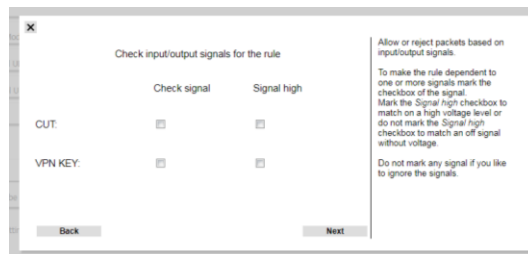
Connection control:

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

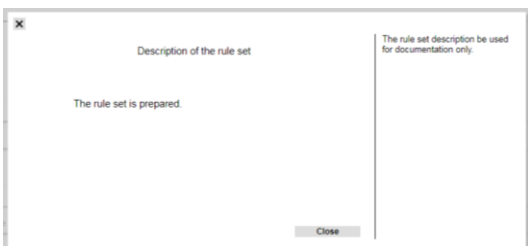
The rule set description is used for documentation only.

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 is used for documentation only.

The rule set is prepared.

Close

► Click Close



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

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

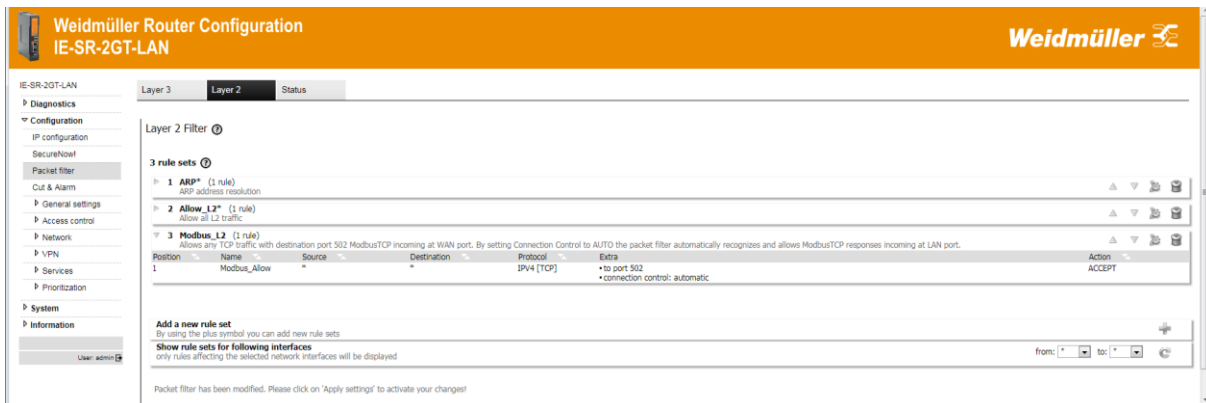
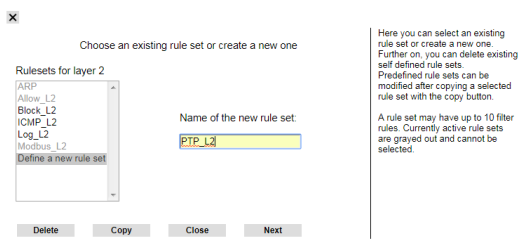


Figure 11: Layer-2 filter list containing new rule-set “Modbus_L2”

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

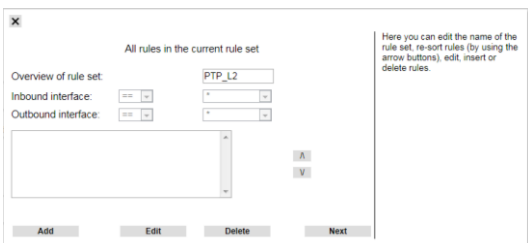
2.2 Configuration of a rule-set containing 2 rules which allow any PTP communication based on protocol UDP, ports 319 and 320, either initially incoming at WAN port or LAN port.

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

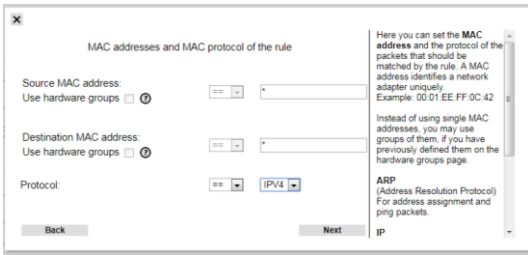


► Add a name for the new rule-set (here PTP_L2).

► Click Next.



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



MAC addresses and MAC protocol of the rule

Source MAC address:
Use hardware groups ☐ *

Destination MAC address:
Use hardware groups ☐ *

Protocol:
 IPv4

Back Next

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

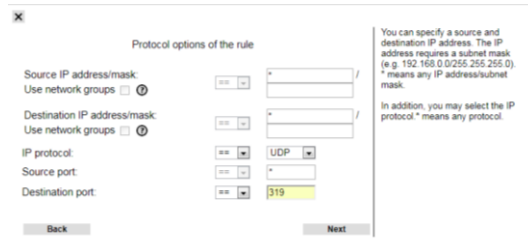
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

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

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

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

► Click Next.



Protocol options of the rule

Source IP address/mask:
Use network groups ☐ *

Destination IP address/mask:
Use network groups ☐ *

IP protocol:
 UDP

Source port:
 *

Destination port:
 319

Back Next

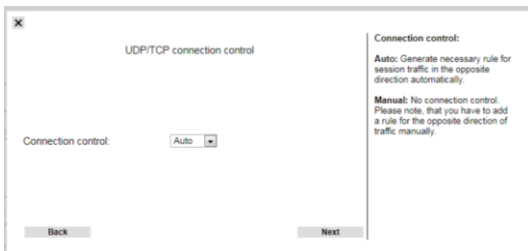
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.

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

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

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

► Click 'Next'.



UDP/TCP connection control

Connection control:
Auto

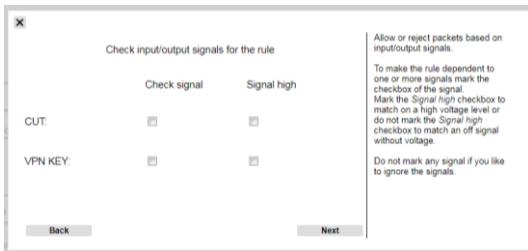
Back Next

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

► Select auto for Connection control.

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

► Click 'Next'.



Check input/output signals for the rule

	Check signal	Signal high
CUT:	☐	☐
VPN KEY:	☐	☐

Back Next

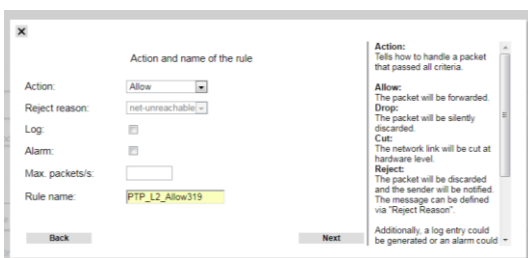
Allow or reject packets based on input/output signals.

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

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

► No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action:
Allow

Reject reason:
net-unreachable

Log:
☐

Alarm:
☐

Max. packets/s:

Rule name:
PTP_L2_Allow319

Back Next

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

Allow:
The packet will be forwarded.

Drop:
The packet will be silently discarded.

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

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

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

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

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

► Click 'Next'.



All rules in the current rule set

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

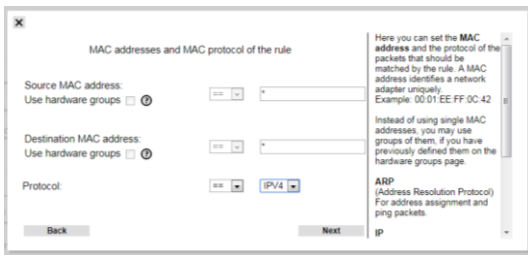
PTP_L2_Allow319

Add Edit Delete Next

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

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

► Click 'Add' to add a new rule.



MAC addresses and MAC protocol of the rule

Source MAC address:
Use hardware groups ☐

Destination MAC address:
Use hardware groups ☐

Protocol: **IPv4**

Back Next

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

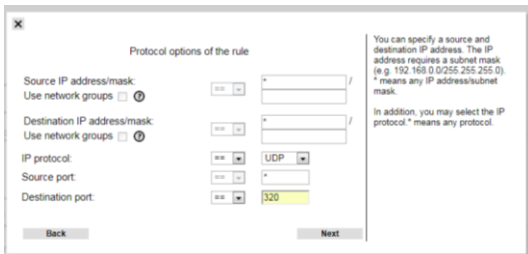
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

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

► Enter wild character * for source and destination MAC addresses

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

► Click 'Next'.



Protocol options of the rule

Source IP address/mask:
Use network groups ☐

Destination IP address/mask:
Use network groups ☐

IP protocol: **UDP**

Source port: *

Destination port: **320**

Back Next

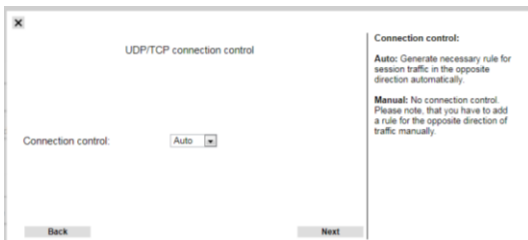
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.

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

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

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

► Click 'Next'.



UDP/TCP connection control

Connection control: **Auto**

Back Next

Connection control:

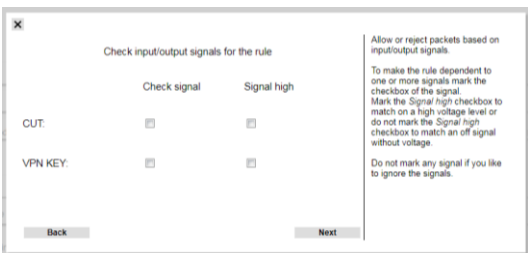
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

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

► Select auto for Connection control.

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

► Click 'Next'.



Check input/output signals for the rule

Check signal Signal high

CUT: ☐ ☐

VPN KEY: ☐ ☐

Back Next

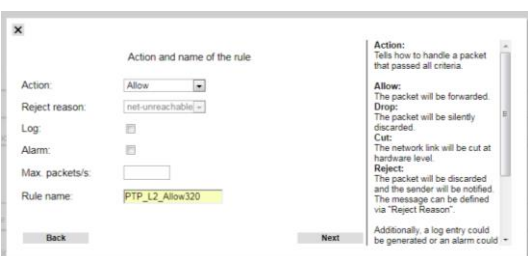
Allow or reject packets based on input/output signals.

To make the rule dependent to one or more signals mark the checkbox of the signal. Mark the Signal high checkbox to match on a high voltage level or do not mark the Signal high checkbox to match 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.

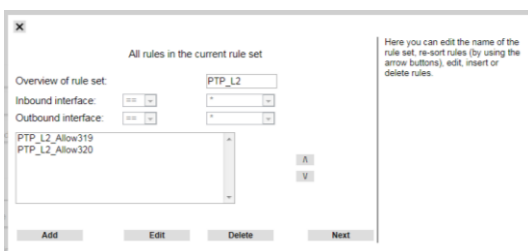
Reject: The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

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

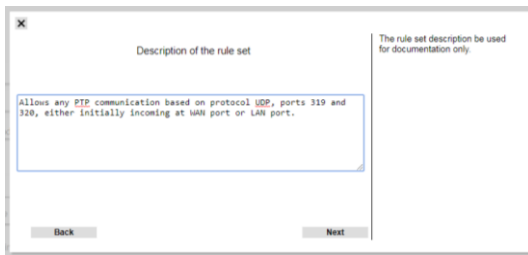
PTP_L2_Allow320

Add Edit Delete Next

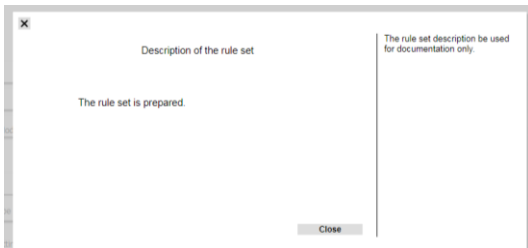
Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

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'.

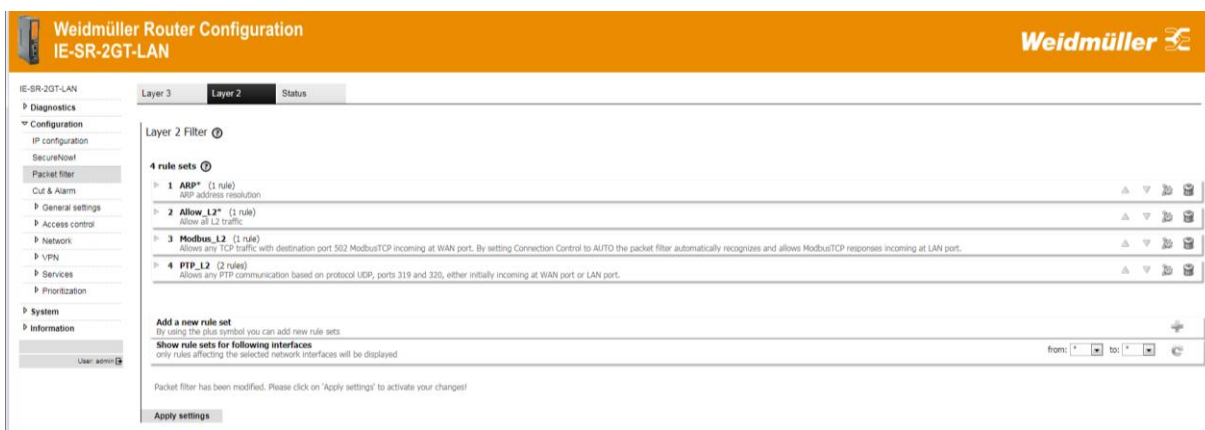
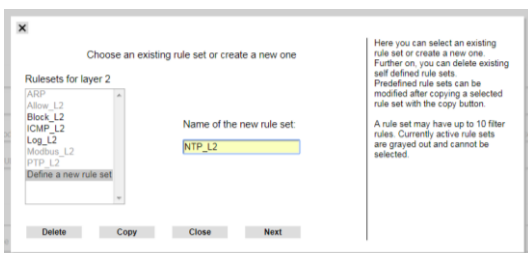


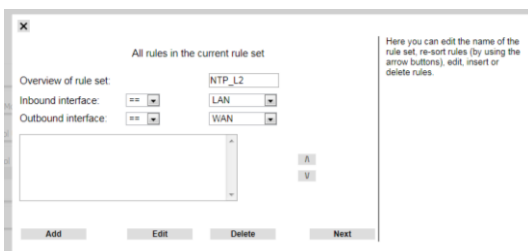
Figure 12: Layer-2 filter list containing new rule-set “PTP_L2”

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).

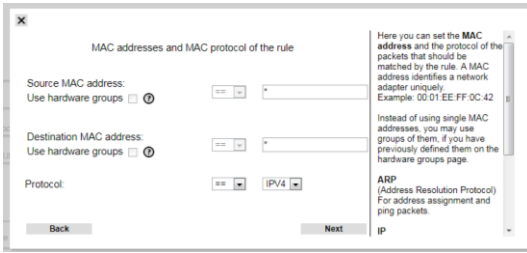
- Click '+' icon to add a new rule-set.



- 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'.



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

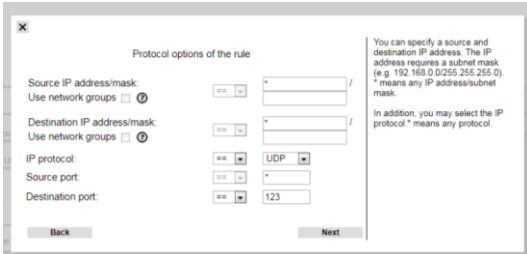
Instead of using single MAC addresses, you may use groups of them, if you have previously defined them on the hardware groups page.

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: == 123

Back Next

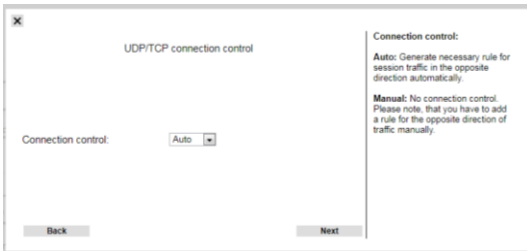
You can specify a source and destination IP address. The IP address requires a subnet mask (e.g. 192.168.0.0/255.255.255.0). * means any IP address/subnet mask.

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

► 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'.



UDP/TCP connection control

Connection control: Auto

Back Next

Connection control:

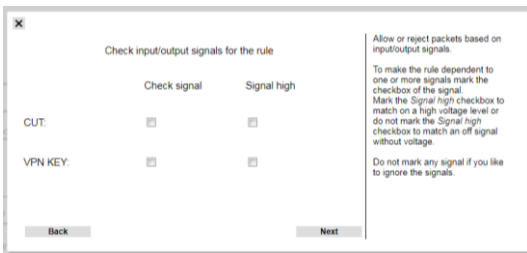
Auto: Generate necessary rule for session traffic in the opposite direction automatically.

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 an stateful inspection firewall and recognizes/allows automatically answers based on an initiated request).

► Click 'Next'.



Check input/output signals for the rule

Check signal Signal high

CUT: ☐ ☐

VPN KEY: ☐ ☐

Back Next

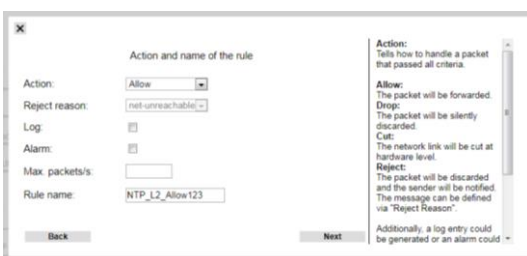
Allow or reject packets based on input/output signals.

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

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

No signal check and setting.

► Click 'Next'.



Action and name of the rule

Action: Allow

Reject reason: not-acceptable

Log: ☐

Alarm: ☐

Max. packets/s:

Rule name: NTP_L2_Allow123

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:

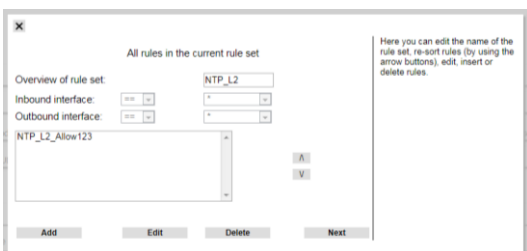
The packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".

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

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

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

► Click 'Next'.



All rules in the current rule set

Overview of rule set: NTP_L2

Inbound interface: *

Outbound interface: *

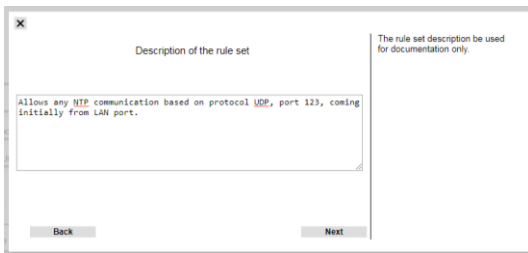
NTP_L2_Allow123

Add Edit Delete Next

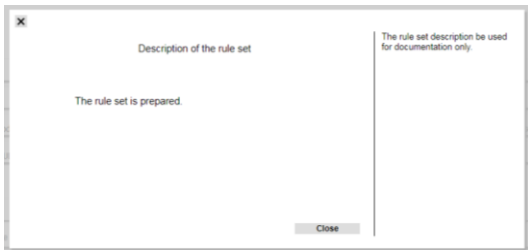
Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

Now the necessary rule is configured.

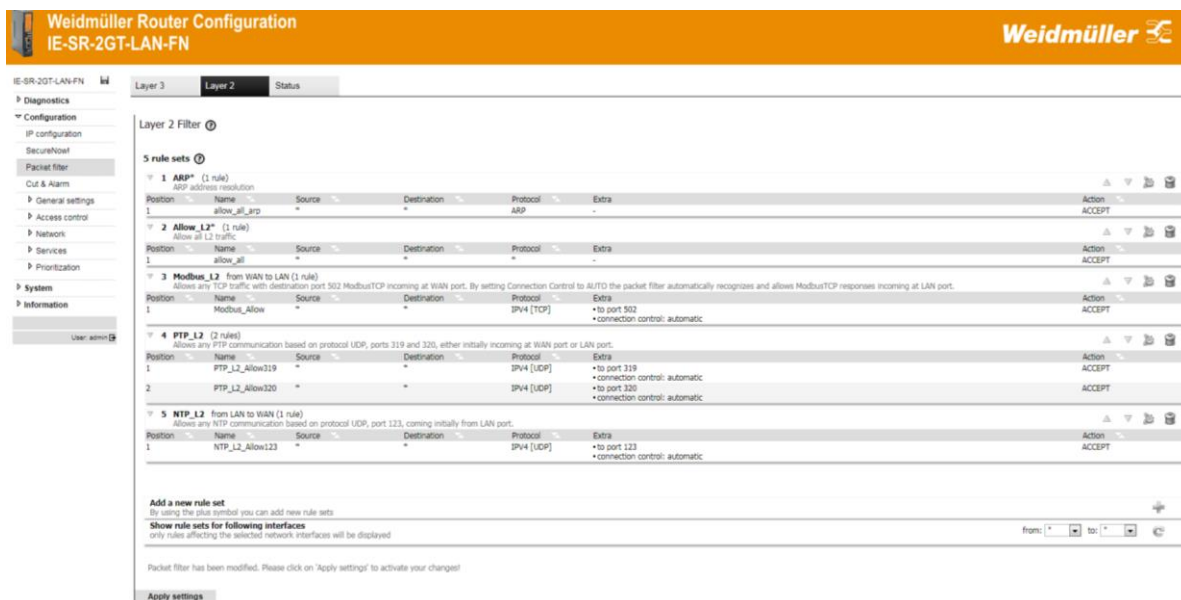
► Click 'Next' to finish the configuration of this rule-set.



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



- Click 'Close'.



Layer 2 Filter

5 rule sets

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

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

Show rule sets for following interfaces
only rules affecting the selected network interfaces will be displayed

from: [] to: []

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

Apply settings

Figure 27: 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.

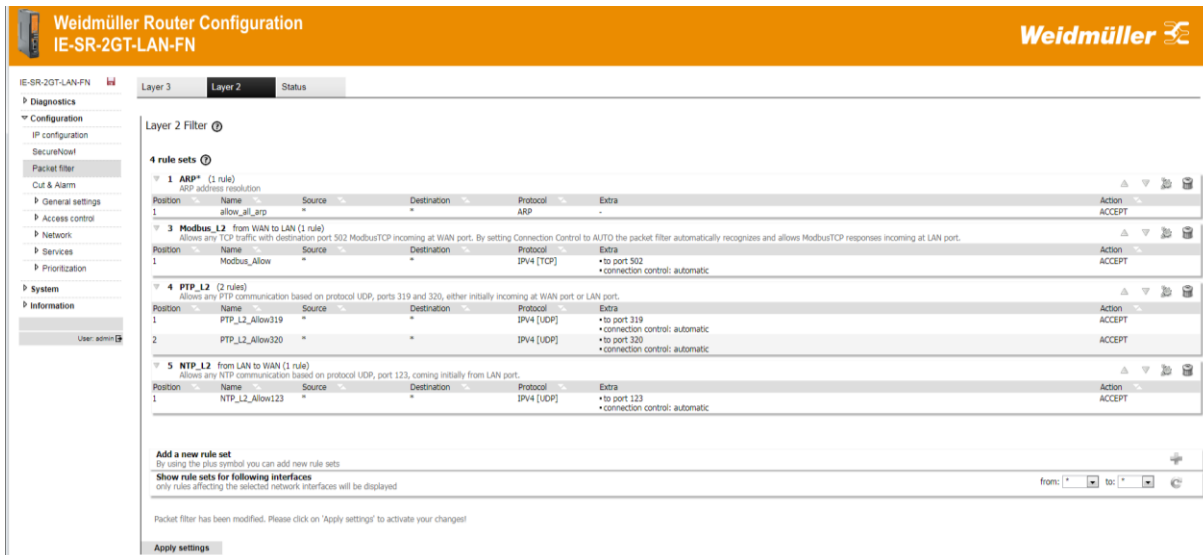
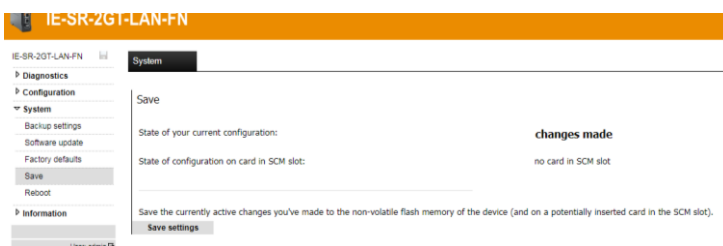


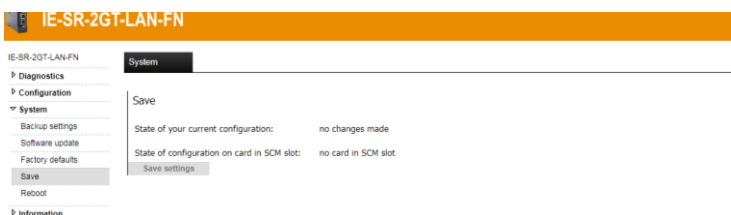
Figure 28: Final list of Layer-2 filter

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

A5-3 Save the configuration

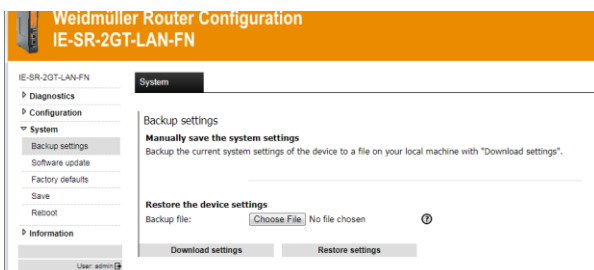


- Goto menu System → Save.
- Click ‘Save settings’.

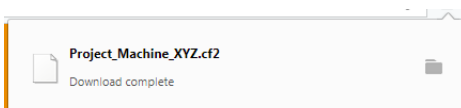


Now the settings are saved in the flush memory.

A5-4 Create a backup file of the configuration



- Goto menu System → Backup Settings.
- Click button ‘Download Settings’.



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

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

Application scenario:

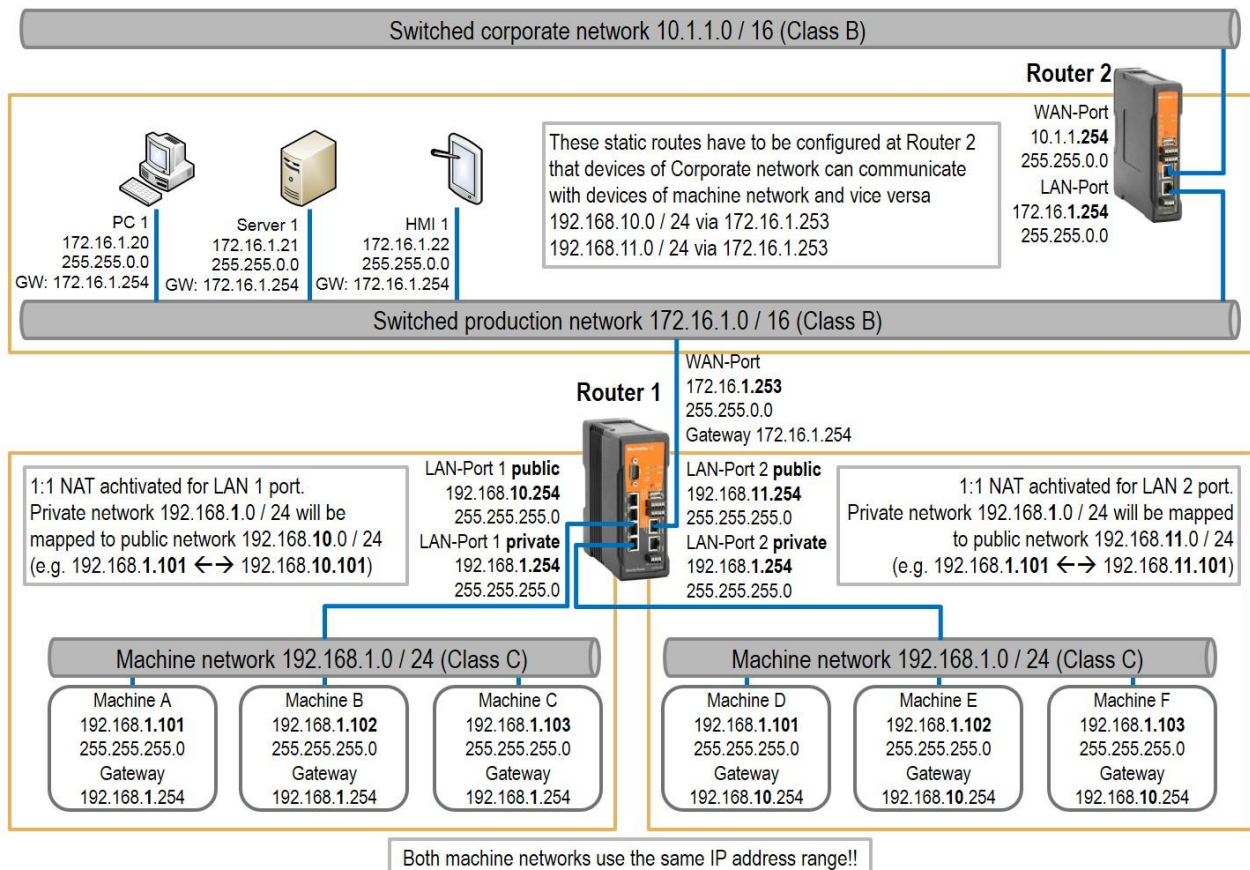
There are 2 machine networks and one upper-level production network. Both machine networks are connected to the production network by a 6-port Security Router in extended routing mode. The production network itself is connected to the corporate network via its own Router. Both machine networks have the same IP address range 192.168.1.0 of type class C: The production network uses the IP address range 172.16.1.0 of type class B.

This application can only be done using a 6-Port router model. Otherwise there is a dedicated router necessary for every machine network.

Task and solution:

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

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



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

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

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

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

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

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

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

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

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

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

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

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

Examples of IP address mapping (private/public) using 1:1 NAT at LAN port			
IP address and subnet of a device connected to LAN port (used as private IP address)	Configured private IP address and subnet on Router's LAN port	Configured public IP address and subnet on Router's LAN port	Resulting public IP address and subnet of a device connected to LAN port (1:1 NAT)
	Subnets of private and public network must be the same		This IP address is known by devices of other subnets
192.168.1. 101 / 255.255.255.0	192.168. 1.254 / 255.255.255.0	192.168. 10.254 / 255.255.255.0	192.168.10. 101 / 255.255.255.0
192.168.1. 102 / 255.255.255.0			192.168.10. 102 / 255.255.255.0
192.168.1. 103 / 255.255.255.0			192.168.10. 103 / 255.255.255.0
10.8. 1.10 / 255.255.0.0	10.8.1.254 / 255.255. 0.0	172.16.1.254 / 255.255. 0.0	172.16. 1.10 / 255.255.0.0
10.8. 2.10 / 255.255.0.0			172.16. 2.10 / 255.255.0.0
In a class C network with subnet mask 255.255.255.0 only the last segment of an IP address is translated			
In a class B network with subnet mask 255.255.0.0 the last two segments of an IP address are translated			

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

General note:

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

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

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

→ The alternative method using dynamic routing is described in chapter A7 - Using dynamic IP routing alternatively to manually configured static routes.

Starting situation

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

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

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

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

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

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

User: admin
 Password: Detmold

4. Set the basic IP configuration

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

Configuration Router 1:

Operational mode:	IP Router (extended)
IP address parameters WAN 1 Port:	Static
	172.16.1.253
	255.255.0.0 (Class B)
	NAT (masquerading) NOT SET
IP address parameters LAN 1 Port:	Static
	192.168.10.254
	255.255.255.0 (Class C)
	NAT (masquerading) NOT SET
IP address parameters LAN 2 Port:	Static
	192.168.11.254
	255.255.255.0 (Class C)
	NAT (masquerading) NOT SET
WAN 2 Port	Enable WAN switch, you can then use the second port to connect
LAN 3-4 Ports	Leave them as they are, we do not need them in this application
Default gateway	172.16.1.254

Configuration Router 2:

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

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

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

5. Change the IP address of configuration PC

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

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

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

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

Only for Router 1: Use IP address 172.16.1.253 (<http://172.16.1.252>) on WAN port

Only for Router 2: Use IP address 172.16.1.254 (<http://172.16.1.254>) on LAN port

User: admin
Password: Detmold

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

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

- Select menu Configuration → Network → 1:1 NAT

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

- Activate parameter “Enable 1:1 NAT” → Click on checkbox
- Private IP address/subnet mask: 192.168.1.254/24

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

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

Note:

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

The 1:1 NAT (address translation) is working in that way that every address of the private Class C network will be changed to the corresponding public address.

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

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

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

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

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

7. Configuring static routes for Router 2

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

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

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

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

- Click button “Add entry” to add the new static route to the routing table.
- Click button “Add entry” to add the new static route to the routing table.
- Then click button “Apply settings” to activate the new settings.

8. Monitoring the new activated “routes” at Router 3

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

9. Saving the new configuration

- ▶ Select menu System → Save
- ▶ Click on button “Save settings” to save the current configuration to the non-volatile flash memory of the Router. If a SIM memory card is installed the configuration additionally will be stored on the SIM memory card. Additionally, the configuration can be stored on the file system of the PC.
- ▶ Select menu **System → Backup settings**
- ▶ Click on button “Download settings” to write the configuration file to the PC hard disk (Backup file has the default extension *.cf2”)

Now Router configuration is finished!

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

Note: You can use a PC for simulating an Ethernet device (machine) of networks 1. Use a second PC to be a member of the production network.

Ensure that the PC simulating machine A of network 1 is configured using following parameters:

→ IP: 192.168.1.101, net mask: 255.255.255.0, Standard Gateway: 192.168.1.254

Ensure that the PC of production network is configured using following parameters:

→ IP: 172.16.1.20, net mask: 255.255.255.0, Standard Gateway: 172.16.1.252 (pointing to WAN port of your Router)

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

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

- 1.2 Try to send a ping request from PC of production network (172.16.1.20) to machine **A** (192.168.1.101) by using the public IP address 192.168.10.101.

Result: Machine A should reply the “ping request” with reply IP address 192.168.10.101 (due to configured 1:1 NAT).

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

Note: You can use PC's for simulating the Ethernet devices (machines) of networks 1 and 2.

Ensure that the Ethernet devices of both machine networks are configured using following parameters:

IP: 192.168.1.100, net mask: 255.255.255.0, Standard Gateway: 192.168.1.254

- 2.1 Try to send a ping request from machine **A** (192.168.1.101) to machine **D** (same IP 192.168.1.101) by using the public IP address 192.168.11.101.

Result: Machine **D** should reply the “ping request” with reply IP address 192.168.11.101 (due to configured 1:1 NAT).

- 2.2 Try to send a ping request from machine **D** (192.168.1.101) to machine **A** (same IP 192.168.1.101) by using the public IP address 192.168.10.100.

Result: Machine A should reply the “ping request” with reply IP address 192.168.20.100 (due to configured 1:1 NAT).



Note

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

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

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

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

Configuring dynamic IP routing

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

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

Configure below described entries in the section **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)

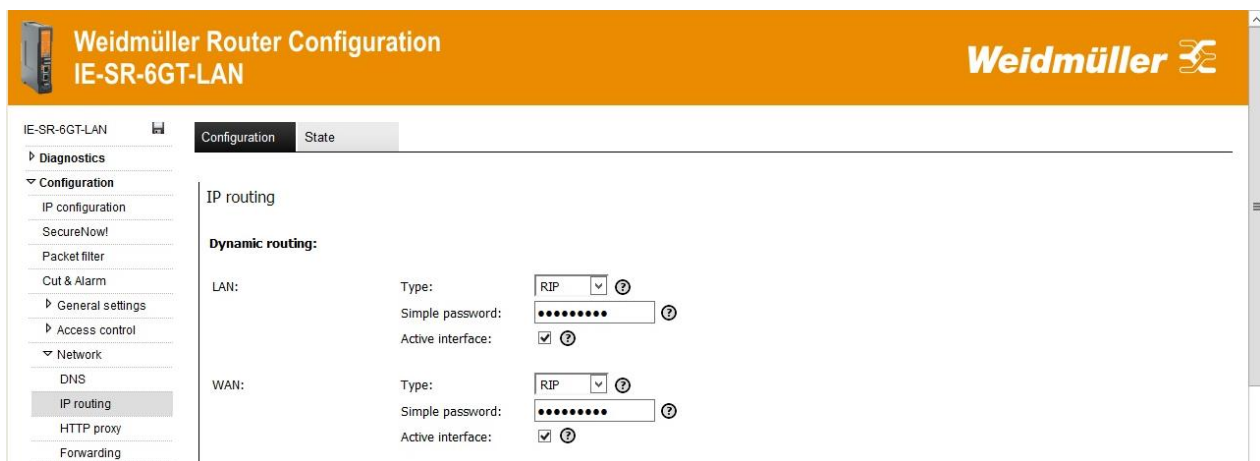


Figure 29: Configuration of dynamic routing using RIP

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

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

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

Now Router configuration is finished!

Testing the accessibility between Ethernet Devices of network 1 and 2

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

Send “ping 192.168.11.101”

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

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

Send “ping 192.168.10.101”

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

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

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

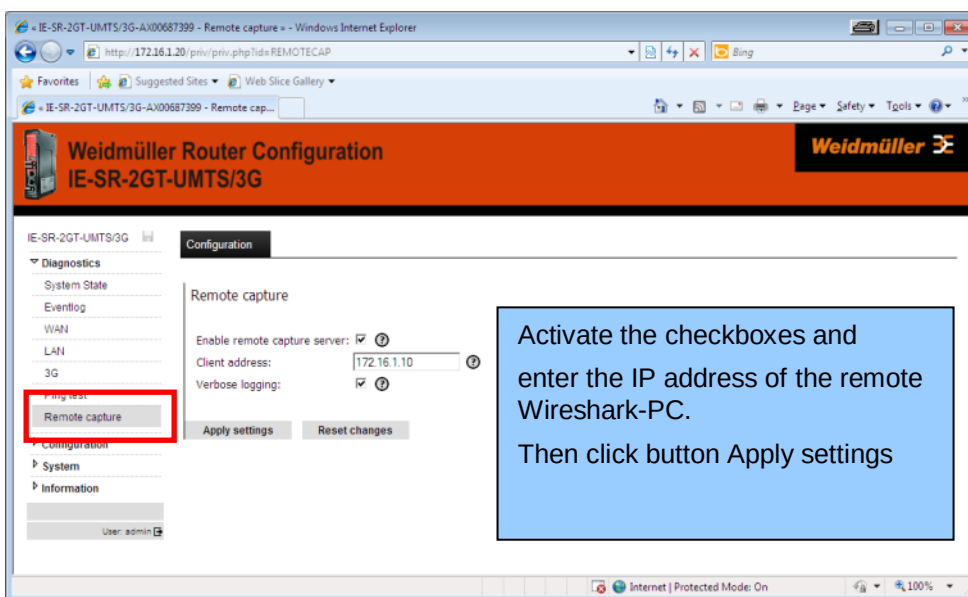
A8 - How to use feature “Remote Capture” with Wireshark to analyse Router’s LAN/WAN traffic

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.

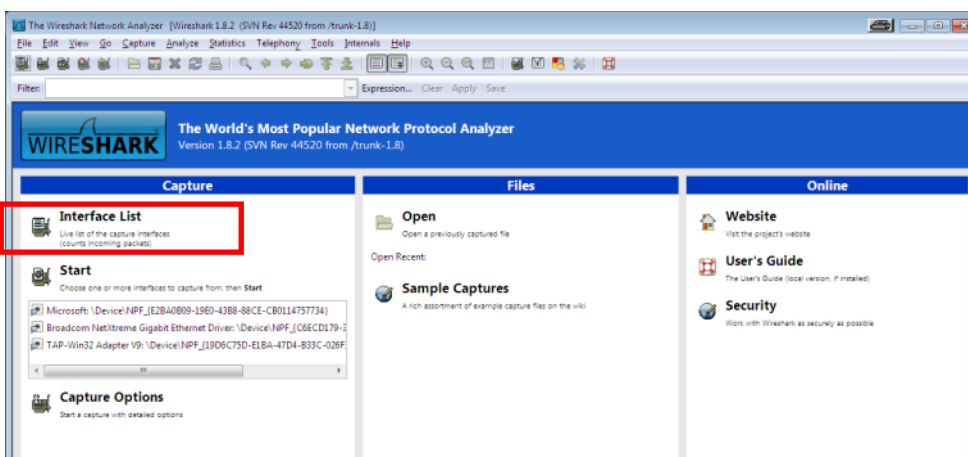
Step-by-step guidance

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

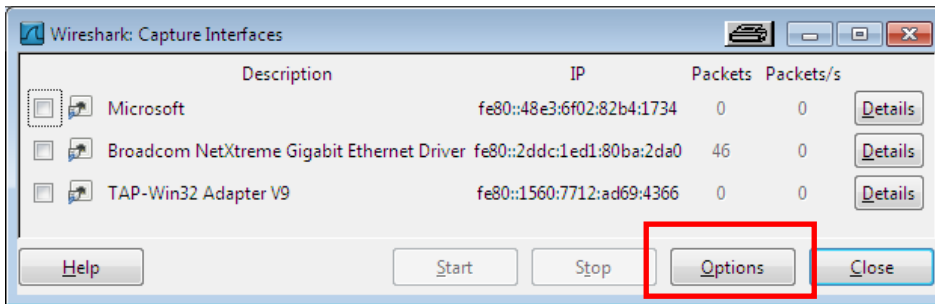
Note: Only one Wireshark-Client-PC (here 172.16.1.10) can be used at the same time record the traffic by Wireshark. Please deactivate this feature if you no longer need to analyse the traffic because it has an impact on the performance of the Router.



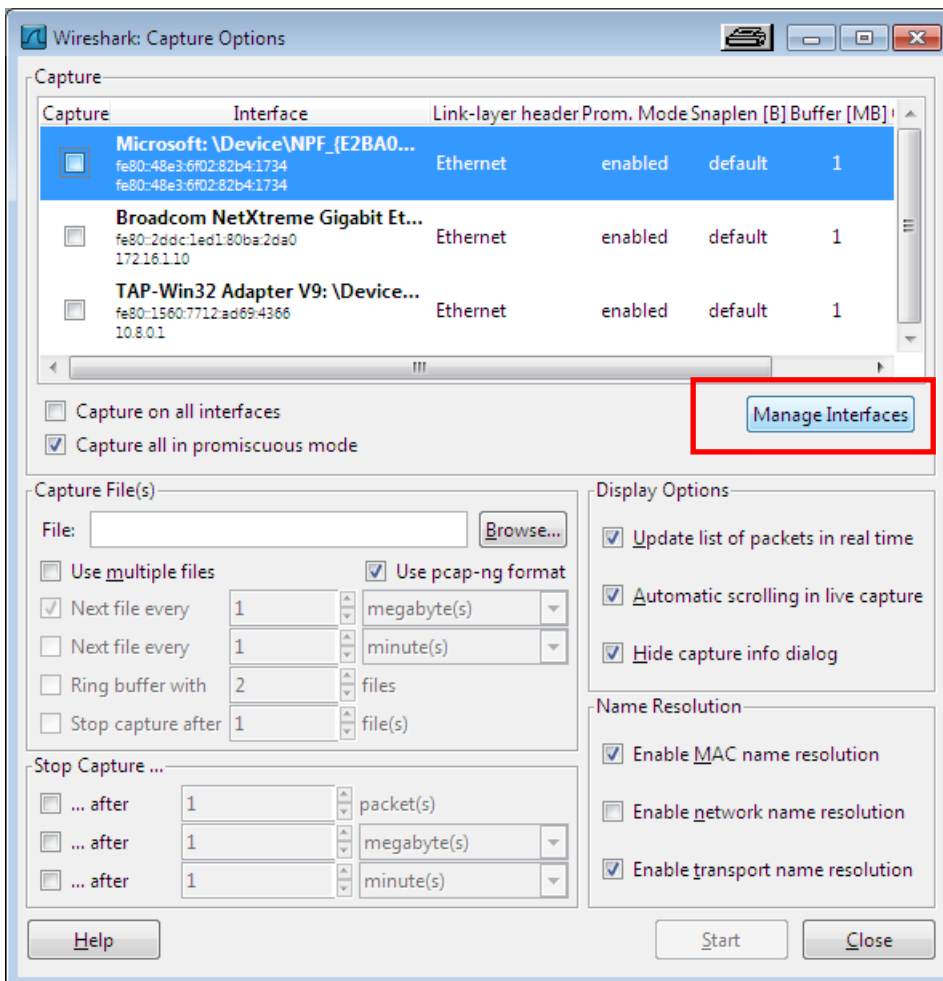
2. Start Wireshark at your PC
3. Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”



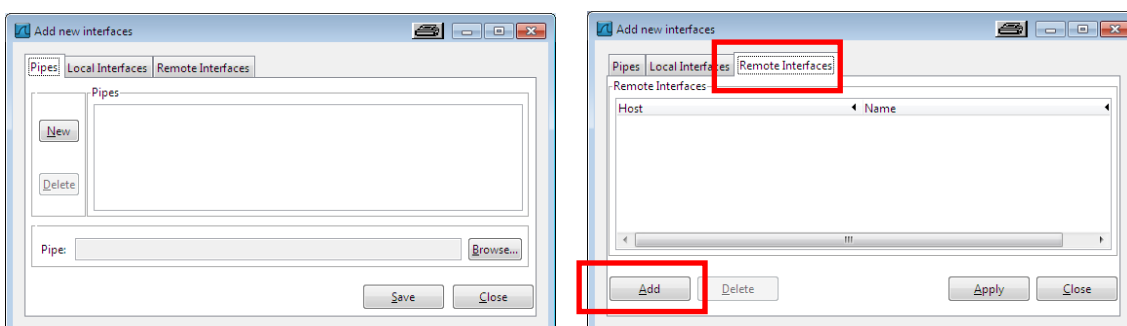
The local Ethernet Interfaces of the computer will be displayed.



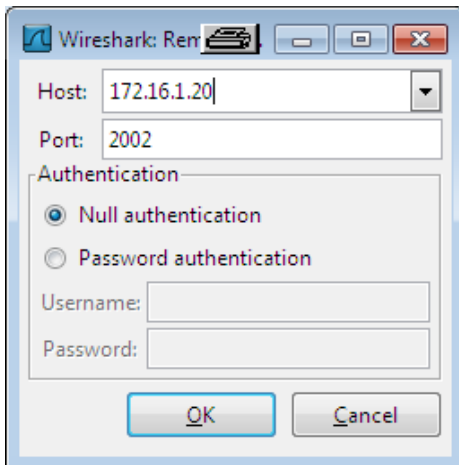
4. Click button “Options”



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



6. Click button “Add”

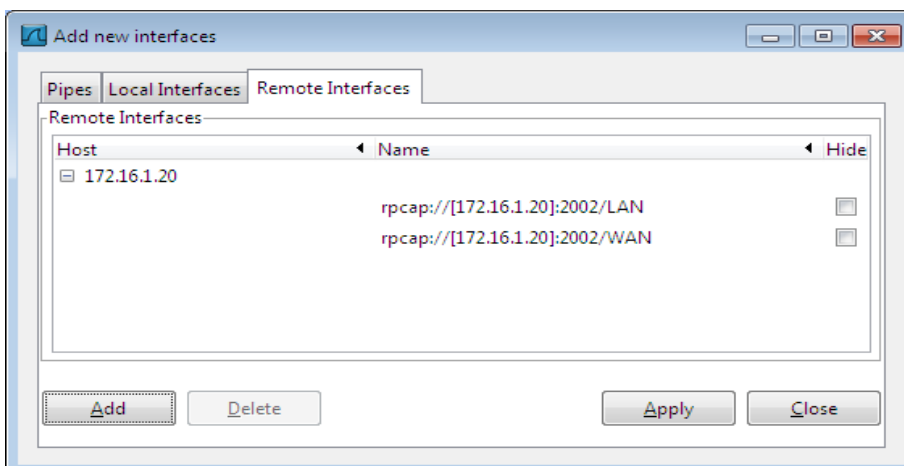


7. Enter the IP address of the Router to field "Host"

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.

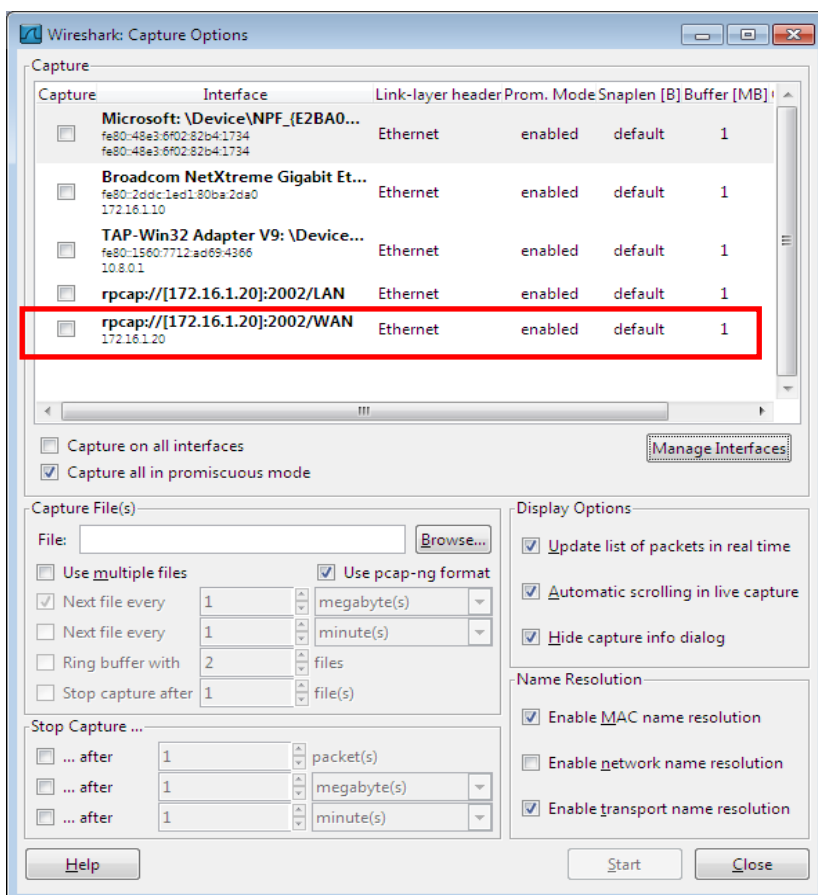
8. Enter into field "Port" the value 2002 (will be filled automatically if you enter an IP address)
9. Click button OK

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



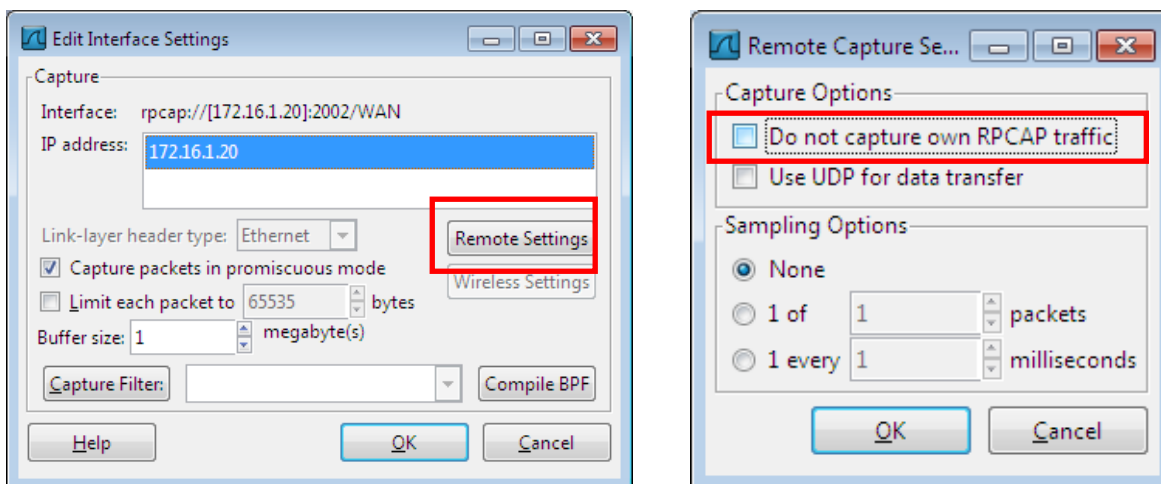
10. Click button Close

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**

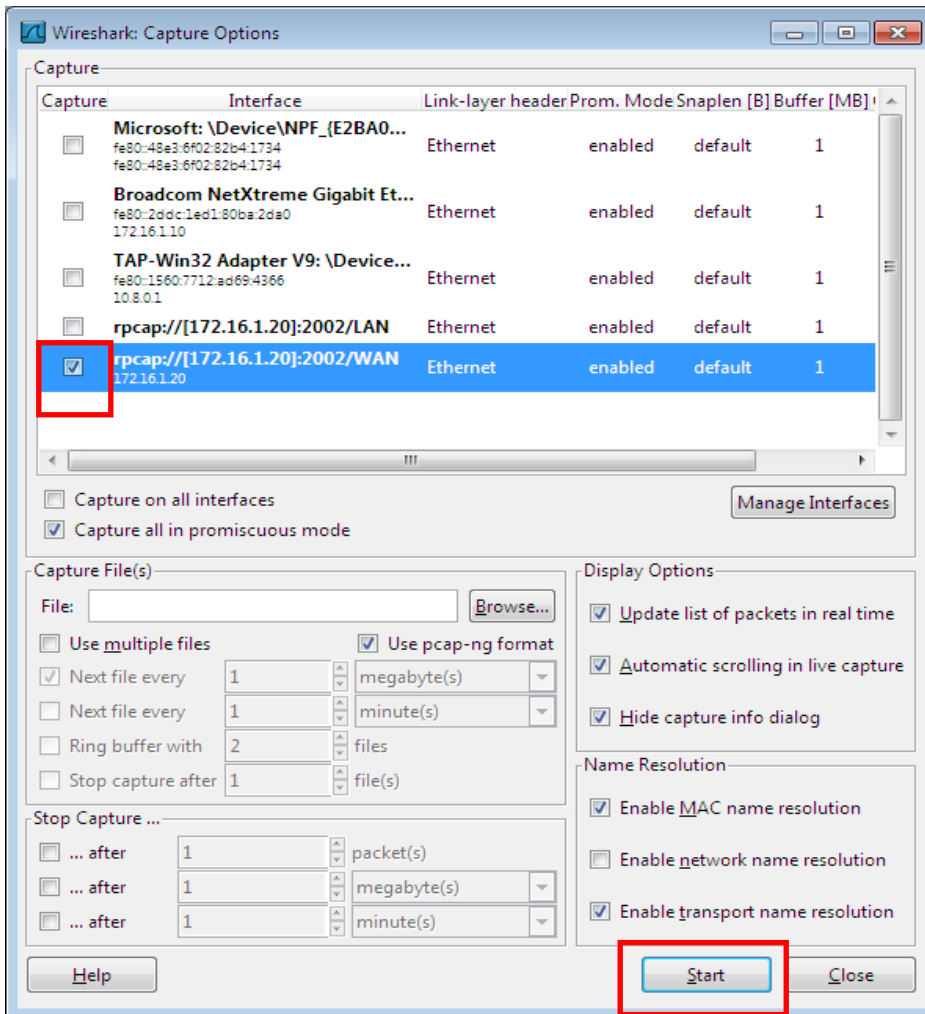


12. Click button “Remote Settings”

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

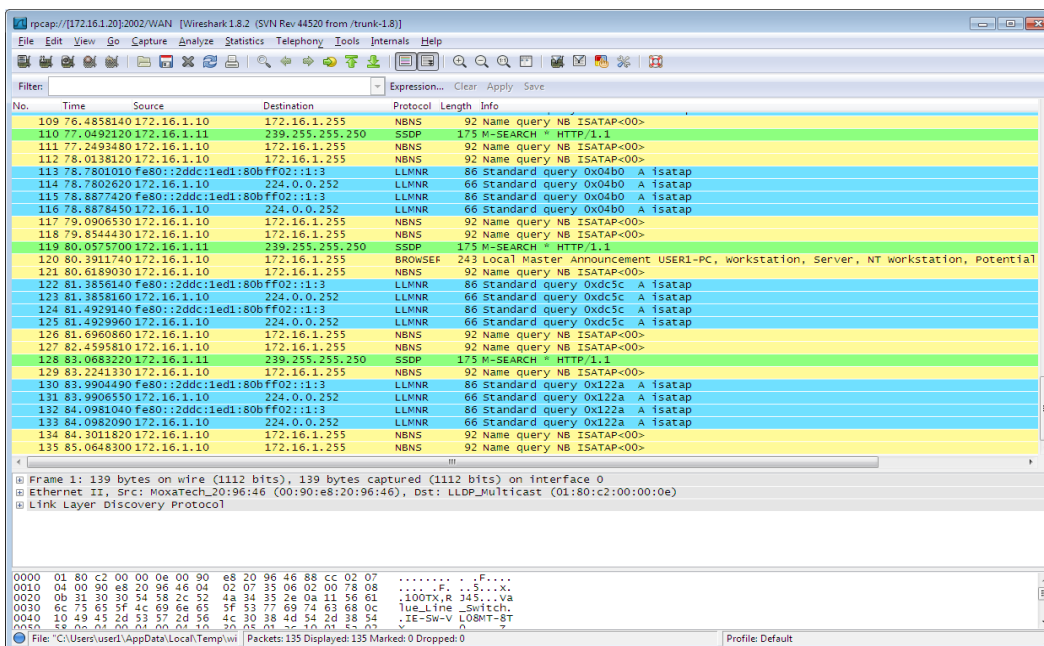
14. Click button “OK”

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**

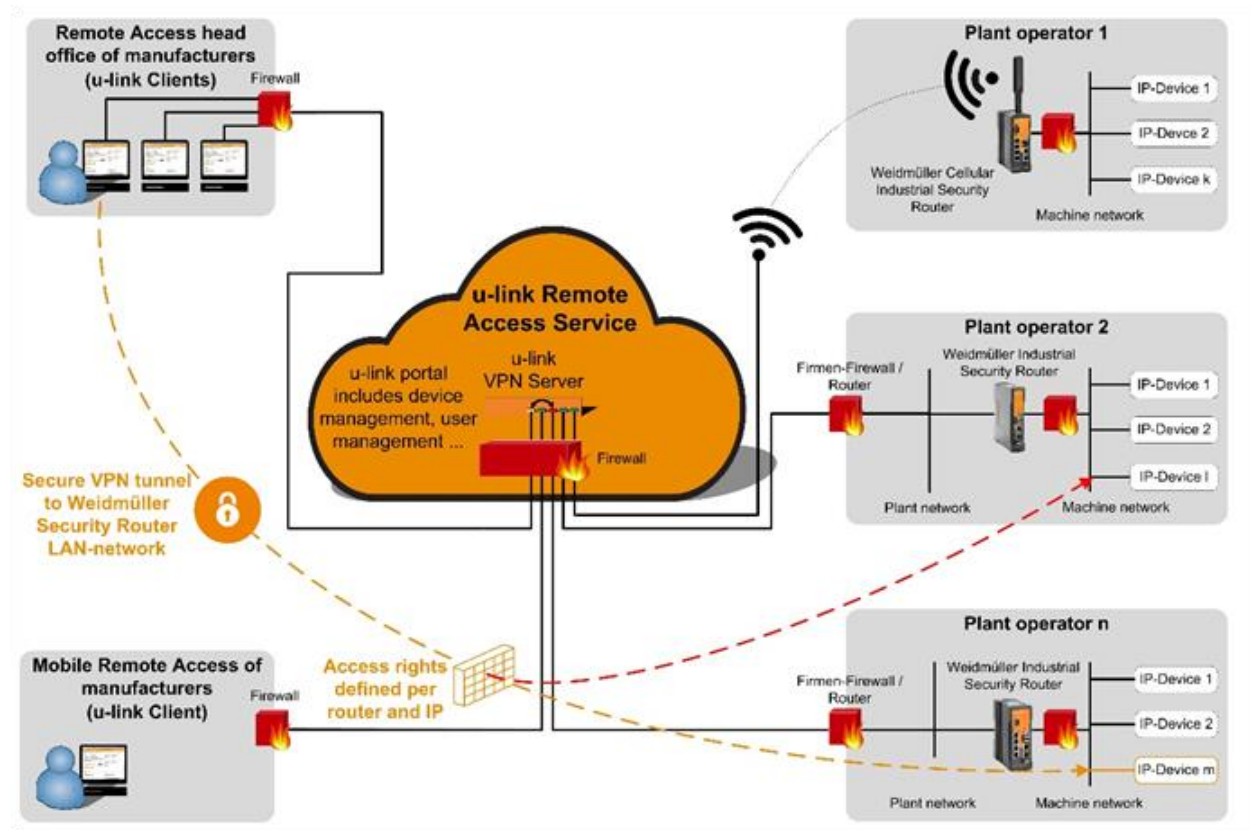
17. Click button “Start” to record the traffic at Routers WAN port



A9 - 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

For more details about u-link please download documents

- u-link Introduction and Overview and
- u-link Technical User Guide

from web page "Maintenance and cloud service" (using below link).

<http://www.weidmueller.com/int/products/electronics-and-automation/maintenance-and-cloud-service>