Industrial Security Router / Firewall

IE-SR-2GT-LAN

IE-SR-2GT-UMTS/3G

Manual

Version 1.2.4

September 2013

Important notes:

This document continously will be updated and completed step-by-step.

This version refers to Router firmware version 2.3.1 and above.

You may download a new version from the Weidmüller web site using the following path:

1. Open http://www.weidmueller.com/IE
2. Select section „Industrial Ethernet“ → „Documents”
3. Select category „Manuals“
4. Download “ Manual_IE-SR-2GT-LAN-3G-UMTS_EN_Vx_yy.pdf

Industrial Security Router / Firewall

IE-SR-2GT-LAN
IE-SR-2GT-UMTS/3G

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

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 16
32758 Detmold
Germany

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

Table of Contents

1. Introduction

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. The Router also allows an industrial IP network to access the Internet via an external DSL modem (via PPPoE). The Router is responsible for routing IP packets between an industrial network and an external network (such as the Internet). Internet access is automatically activated when needed. 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.

2. Package Checklist

Models IE-SR-2GT-LAN and IE-SR-2GT-UMTS/3G

1 x Industrial Security Router (IE-SR-2GT-LAN or IE-SR-2GT-UMTS/3G)

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, Color red)

1 x Hardware Installation Guide

Additional for model IE-SR-2GT-UMTS/3G (with an additional 3G modem)

1 x antenna for mobile connection

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

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 behaviour of neighbouring networked facilities and their connected devices. Personal injury and property damage can occur as a result 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 as a result 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 synchronise 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 synchronise 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.

.

4. Mounting the device

Caution

- This device is designed only for a 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

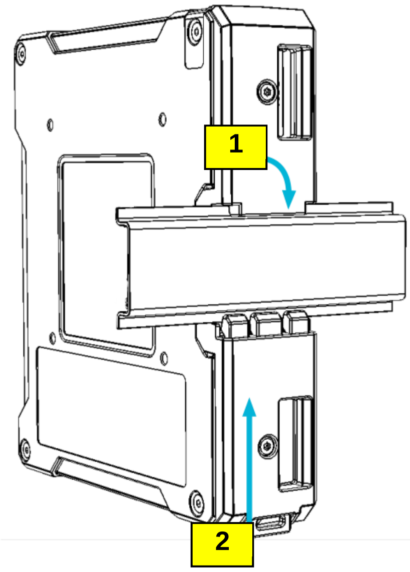
- A minimum of 2 inch (5 cm) gap should be kept between the Router and neighbouring devices <u>from the top and bottom</u>. This will ensure that the Router is sufficiently ventilated and prevent induction from developing.

- The top-hat rail should be located 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 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 (2).

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



5. Technical data

Operation mode	
IP-Router	• Static or dynamic routing according to RIPv2 or OSPF protocol
Transparent Bridge	• 2-Port-Switch with additional Layer-2 filter
Network Services	• DHCP Server / DHCP Relay • DNS-Relay • NTP-Client • DynDNS (DHCP-Client nach RFC 2136)
Firewall	• IPv4 Stateful inspection Firewall • NAT-Masquerading, 1:1 NAT, Portforwarding • Layer-2/3-Filter (VLAN ID, VLAN QoS Tag, MAC adddress based, Ethertype Frame) • "Auto-Learning"-function to create new packet filter rules (Analysis of the network traffic) • Layer 2/3 packet priorizitation (Ethernet Frame, IP Header, VLAN Tag)

VPN	
OpenVPN	• Configurable as OpenVPN server or client (Layer 2 and Layer 3) • Authentication with X.509 Certificates • Tunnel support via HTTP-Proxy • A maximum of 10 different server configurations • Unlimited number of client connections in server mode

IPsec	• Can be configured as an IPsec server or client • Authentication with PSK (user ID, password) or X.509 certificates • Hardware encryption for faster data flow rate • A maximum of 64 simultaneous connections (subnet with subnet or as IPsec server) • Encryption algorithms DES-56, 3DES-168, AES 128, AES 192, AES-256

Management	• Configuration with web interface (HHTP/HTTPS) • Web interface selectable in english or german language • 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	The Modbus/TCP interface enables the control of the Router by a PLC. Following functions are imaged in the registers: • Cut & Alarm, status request & acknowledgment • IPsec, on/off switchable generally • OpenVPN, separate status request and activation / deactivation of the 10 possible OpenVPN connections
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 error

Interfaces	
RJ45-Ports	• 2 * 10/100/1000BaseT(X)
USB-Port	• option for future expansion
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)
LED display	• Signaling the status for power, device status, Cut, Alarm, active VPN connection and an active 3G connection
Digital Outputs	• "Alarm" -> Indicates a configurable network status or error (24V out)

	• "VPN-active" -> Indicates an active VPN connection (24 V out)
Digital Inputs	• "Cut" -> Disconnects physically (link down) the WAN port (24 V In) • "VPN-initiate" -> Enables a pre-configured VPN connection (24 V In)
Reset-Button	• Restore to the factory settings

Power	
Input Voltage	• 1* 24 VDC (7 bis 36 Volt)
Current consumption	• max. 600mA @ 24 VDC

Technical data (housing)	
Housing	• Metal, protection IP20
Dimensions (width, height, depth)	• 35 * 159 * 134 mm (without antenna) • 35 * 255 * 134 mm (with 3G antenna)
Mounting	• TS35 (DIN rail)

Environmental conditions	
Operating Temperature	• -20°C to +70°C
Storage Temperature	• -20°C to + 85°C
Ambient Humidity	• 6 to 90% noncondensing

DSL and 3G/HSDPA	
DSL	• DSL Internet access by connecting an external DSL modem via LAN or WAN port • Free configuration of the PPPoE login
DynDNS	• Support for automatic registration
UMTS/3G (Only model IE-SR-2GT-UMTS/3G)	• Built-in quad-band 3G / HSPA modem 21.1 Mbps peak downlink • 5.8 Mbps peak uplink • **GSM, GPRS, EDGE:** 850 MHz, 900 MHz, 1800 MHz, 1900 MHz • **UMTS, WCDMA, HSDPA, HSUPA:** 850 MHz, 900 MHz, 1900 MHz, 2100 MHz • FCC, CE, FCC, IC, NCC, PTCRB, Bell, AT&T

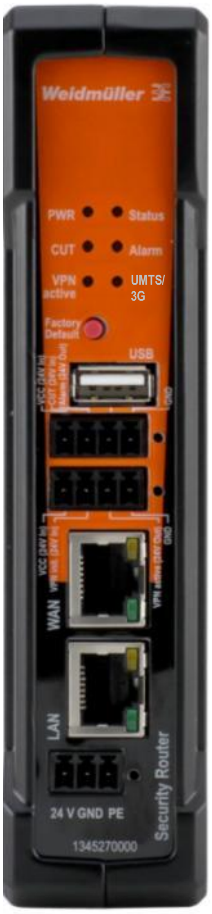
Approvals	
Security	• cULus (UL508)
EMC	• FCC Part 15 Class A, EN 55022 Class A EN61000-4-2 (ESD) EN61000-4-3 (RS), EN61000-4-4 (EFT) EN61000-4-5 (Surge) EN61000-4-6 (CS)

Shock	• DIN EN 60068-2-29
Vibration	• DIN EN 60068-2-6

Warranty	
Period of time	• 3 years

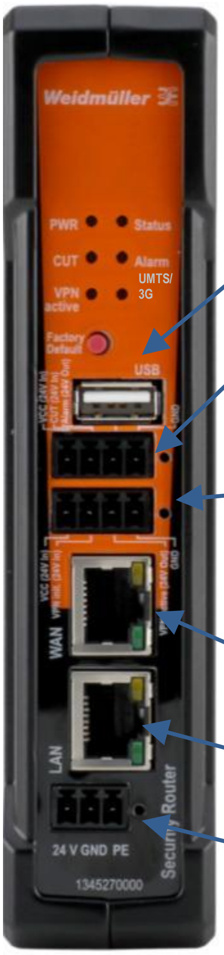
Order data	Model name / Order number
LAN/WAN Router	• IE-SR-2GT-LAN / 1345270000
LAN / WAN Router with integrated modem UMTS/3G	• IE-SR-2GT-UMTS/3G / 1345250000

6. Hardware related functional descriptions



Description of LED status indicators

LED	**Signal**	**Meaning**
PWR	off	The device is not powered
	Flashing green	Device is turned on, the boot process is running
	green	Device is turned on and ready to run
Status	off	The device is not powered
	red	Error after boot process or recovering an image
Cut	off	CUT Input is not powered
	red	A Cut event is triggered. LED lights up and the WAN port is disabled
Alarm	off	No Alarm
	red	An Alarm event is triggered
VPN active	off	No activated VPN tunnel.
	green	Active VPN tunnel (triggered by external VPN key)
Only model	**IE-SR-2GT-UMTS/3G**	
3G (UMTS)	off	No active GSM / 3G / UMTS connection
	Flashing yellow	Searching wireless network
	yellow	Connected to a network provider but no active data connection (Offline)
	Flashing green	Connected to a network provider. Router activates the connection on data flow (Standby)



Description of device interfaces at top and front side

Only model IE-SR-2GT-UMTS/3G: Connector for UMTS/3G antenna at top side
Connector type: **SMA female**

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

Note: Corresponding socket connector is included

4-pin connector („VPN initiate“ and „VPN active“)

- ► 24 VDC **input** for initiating a VPN tunnel (Predefined OpenVPN tunnel)
- ► 24 VDC **output** for signaling an active VPN tunnel

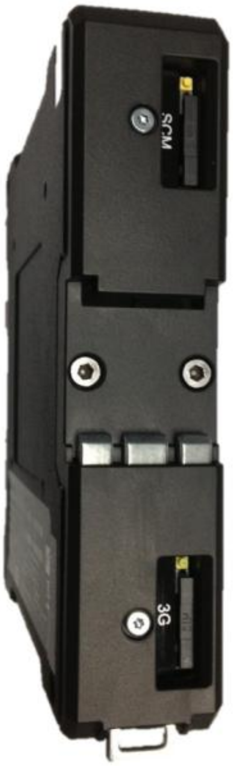
Note: Corresponding socket connector is included

RJ45-Connector WAN (10/100/1000BaseTX)

RJ45-Connector LAN (10/100/1000BaseTX)

3-pin connector for 24V DC power supply

Note: Corresponding socket connector is included



Description of device interfaces at rear side

SCM slot / socket
SIM memory card reader for external backup and restore of the Router configuration

3G slot / socket
Slot for mobile SIM card (only 3G/UMTS model)

Connector for UMTS / 3G antenna of type **SMA female**

Any external antenna can be used which is compliant to following parameters:

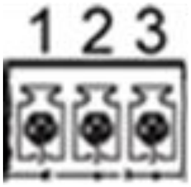
Diversity Support: 900/1900/2100 MHz

Antenna Connector:50 Ohm compatible

Pin assignment of power supply connector

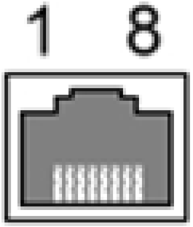
Note: Allowed input voltage range from 7 to 36 VDC (24 VDC typical)

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



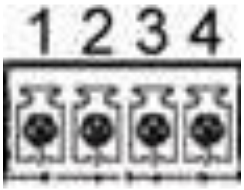
Pin assignment of RJ45 Ethernet ports (LAN and WAN)

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-



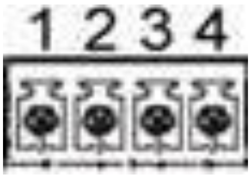
Pin assignment of 4-pin connector for „VPN initiate“ and „VPN active“

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“

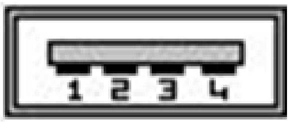
Pin number	SIGNAL NAME
1	24V DC (VCC)
2	Cut (Disabling WAN-Port, 24 V In)
3	Signalize Alarm (24 V Out)
4	GND



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.

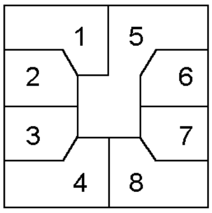
Pin number	SIGNAL NAME
1	VDC
2	D -
3	D+
4	GND

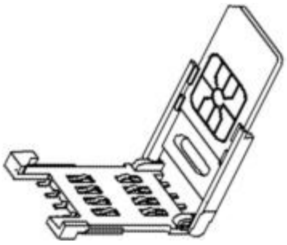


Pin assignment of Smartcard Reader (ISO 7816 Standard)

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





7. Initial start-up / Getting Started

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 Internet browser (Microsoft Internet Explorer or Mozilla Firefox) can be used.

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

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

The default IP addresses and net masks of the Router are:

LAN port :	192.168.1.110	/	255.255.255.0
WAN port :	192.168.2.110	/	255.255.255.0

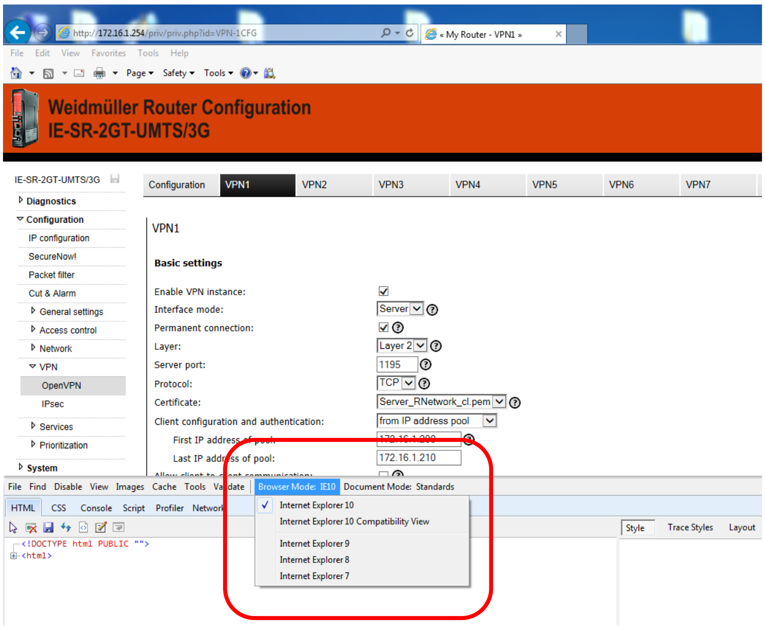
Starting the Web interface

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 your a using is allowed to 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 are able to 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.



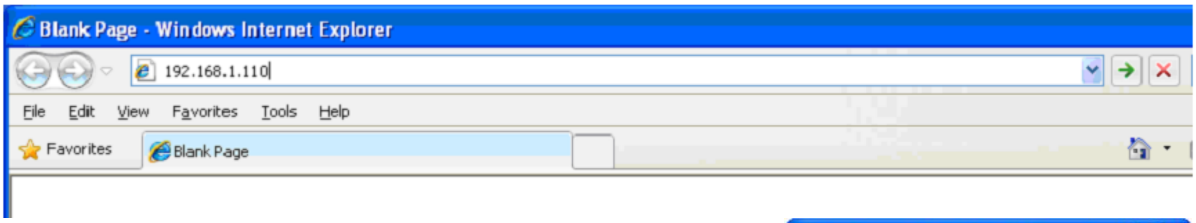
VPN1

Basic settings

Enable VPN instance: ☑
Interface mode: Server
Permanent connection: ☑
Layer: Layer 2
Server port: 1195
Protocol: TCP
Certificate: Server_RNetwork_cl.pem
Client configuration and authentication: from IP address pool
First IP address of pool: 172.16.1.200
Last IP address of pool: 172.16.1.210
Allow client to client communication: □

```
<!DOCTYPE html PUBLIC "">
<html>
```

Start your Web browser and enter the IP address of the connected Router port into the browser's address line.



Blank Page - Windows Internet Explorer

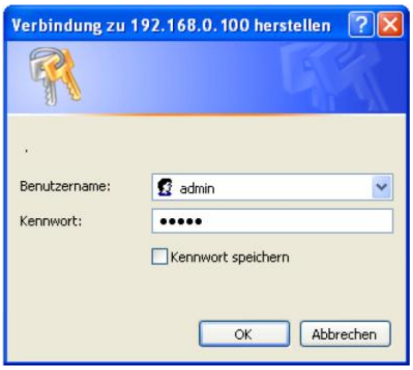
192.168.1.110

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

Confirm your input by pressing the OK button.



Verbindung zu 192.168.0.100 herstellen

Benutzername: admin

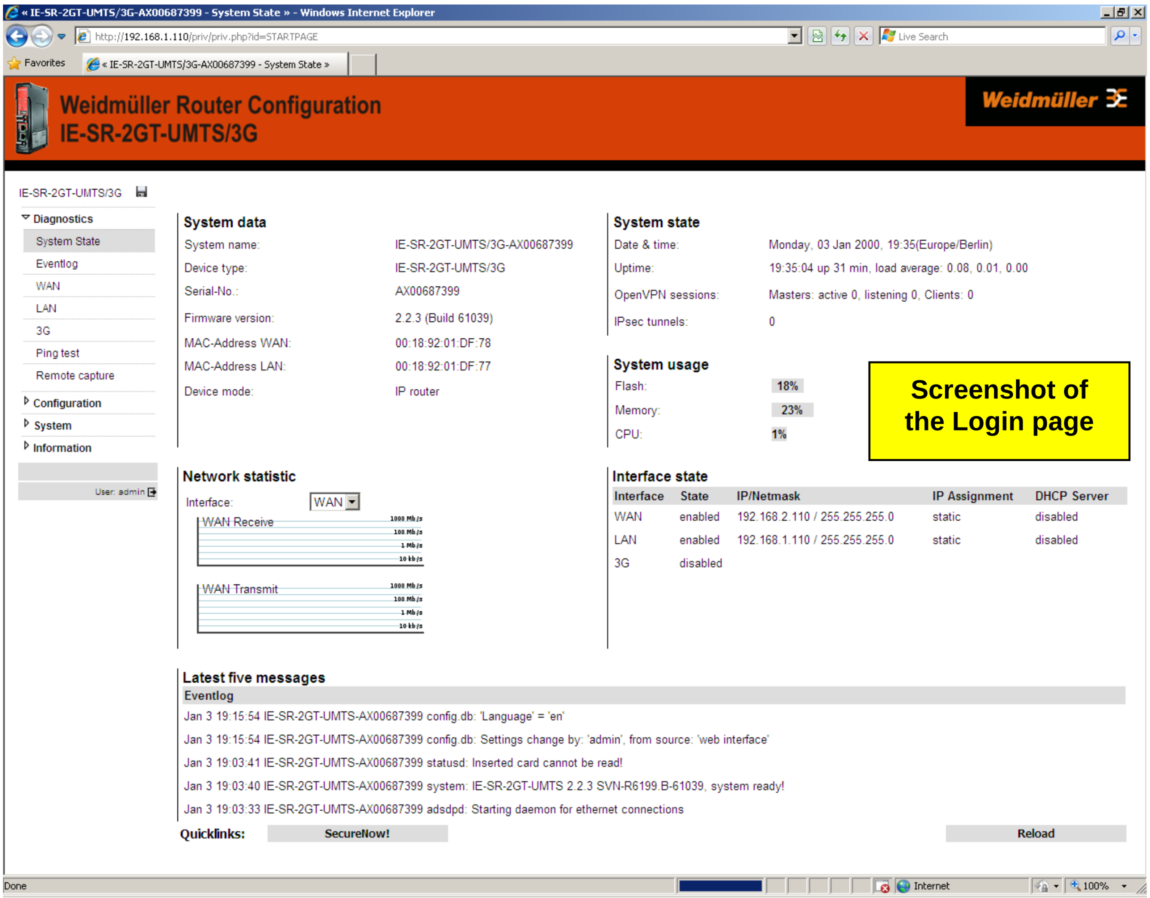
Kennwort: •••••

☐ Kennwort speichern

!	**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

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

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



« IE-SR-2GT-UMTS/3G-AX00687399 - System State » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=STARTPAGE

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

System data

System name:	IE-SR-2GT-UMTS/3G-AX00687399
Device type:	IE-SR-2GT-UMTS/3G
Serial-No.:	AX00687399
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:18:92:01:DF:78
MAC-Address LAN:	00:18:92:01:DF:77
Device mode:	IP router

System state

Date & time:	Monday, 03 Jan 2000, 19:35(Europe/Berlin)
Uptime:	19:35:04 up 31 min, load average: 0.08, 0.01, 0.00
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	23%
CPU:	1%

Screenshot of the Login page

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled
3G	disabled			

Latest five messages

Eventlog

```
Jan 3 19:15:54 IE-SR-2GT-UMTS-AX00687399 config.db: 'Language' = 'en'
Jan 3 19:15:54 IE-SR-2GT-UMTS-AX00687399 config.db: Settings change by: 'admin', from source: 'web interface'
Jan 3 19:03:41 IE-SR-2GT-UMTS-AX00687399 statusd: Inserted card cannot be read!
Jan 3 19:03:40 IE-SR-2GT-UMTS-AX00687399 system: IE-SR-2GT-UMTS 2.2.3 SVN-R6199 B-61039, system ready!
Jan 3 19:03:33 IE-SR-2GT-UMTS-AX00687399 adsdpd: Starting daemon for ethernet connections
```

8. 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 (around 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.

Default factory settings of the Router:

Language:	Englisch user interface
Operation mode :	IP Router
IP address LAN port:	192.168.1.110 (static value)
Subnet mask:	255.255.255.0
NAT (Masquerading) on LAN port:	Not activated
IP address WAN port:	192.168.2.110 (static value)
Subnet mask:	255.255.255.0
NAT (Masquerading) on WAN port:	Not activated
Default gateway:	No entry
DNS:	DNS relay not activated
Firewall (Packet filter):	By default, data traffic in both directions between LAN and WAN is allowed on both level 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 (OSPF, RIP) disabled

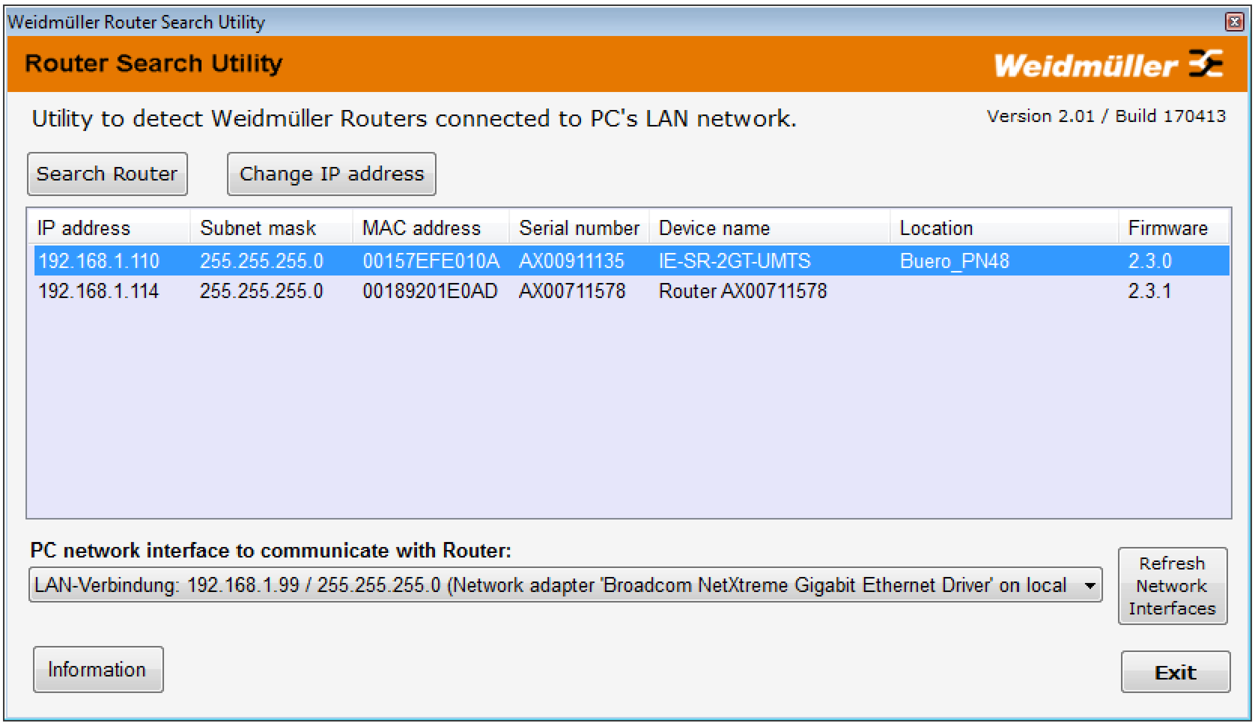
SNMP / DHCP / DNS	Disabled
VPN:	Disabled
Data prioritization	Disabled

Only model IE-SR-2GT-UMTS/3G	
3G Modem	Disabled

9. Using the Weidmüller Router-Search-Utility

The software tool Weidmüller Router- Search-Utility can be used to find Weidmüller Routers and detect theirs 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 parameters like Device name, MAC address and IP address with Subnet mask
- → Change the IP address of a detected Router
- → Open the web interface of a detected Router



Utility to detect Weidmüller Routers connected to PC's LAN network.

Version 2.01 / Build 170413

IP address	Subnet mask	MAC address	Serial number	Device name	Location	Firmware
192.168.1.110	255.255.255.0	00157EFE010A	AX00911135	IE-SR-2GT-UMTS	Buero_PN48	2.3.0
192.168.1.114	255.255.255.0	00189201E0AD	AX00711578	Router AX00711578		2.3.1

PC network interface to communicate with Router:

LAN-Verbindung: 192.168.1.99 / 255.255.255.0 (Network adapter 'Broadcom NetXtreme Gigabit Ethernet Driver' on local

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. Select category "Industrial Security Router (IE-SR-2GT-LAN, …3G/UMTS)"
5. Download " Weidmueller_Router_Search_Utility.zip"

Alternatively you can download this software from this web page:

1. Open www.weidmueller.com
2. Select Downloads
3. Select Software
4. Select Industrial Ethernet
5. Download from section *Industrial Security Router (Firmware and Software for IE-SR-2GT-LAN/3G/UMTS)*

10. Basic description of the 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/3G)
- Feature for testing the data communication between the Router and other Ethernet devices (Ping test)

Section Configuration

- Setting of operation mode (eg „IP Router“) 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
- User administration (assignment of rights)
- IP-Routing (static, dynamic) and IP address management (Masquerading, 1:1 NAT, Portforwarding)
- Configuration of VPN connections (OpenVPN, IPsec)
- Configuration of general network services (e.g. DHCP, DBS, SNMP)
- Prioritization of network traffic (Layer-2 and Layer-3 level)

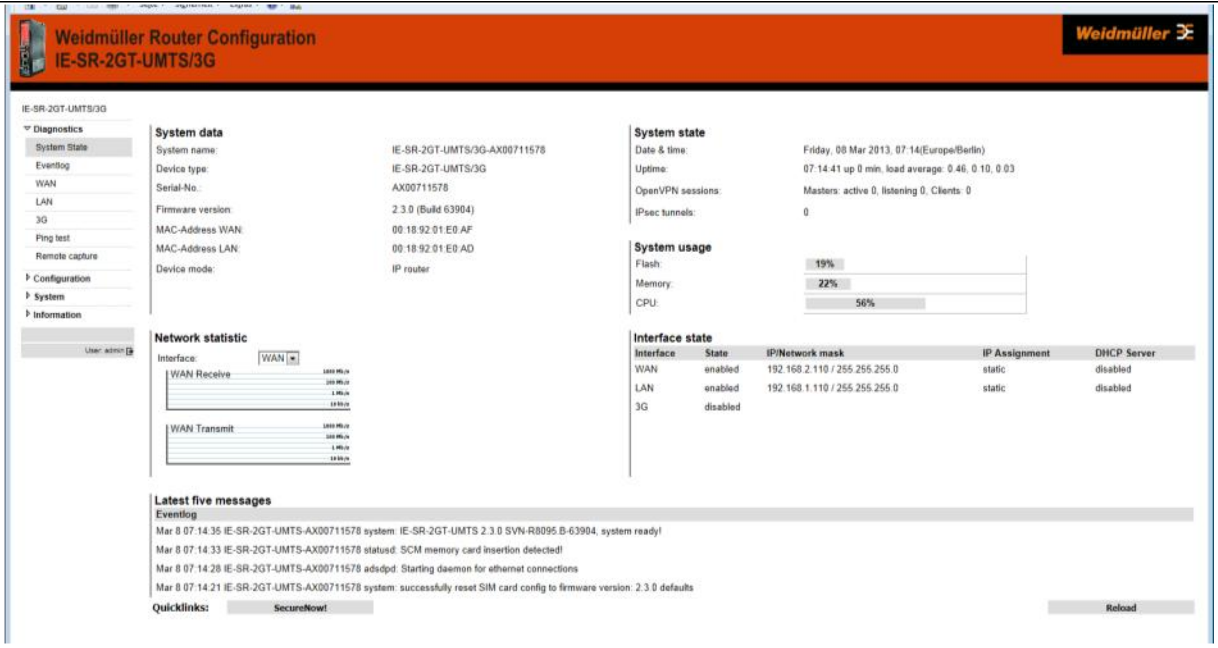
Section System

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

Section Informations

- Display of technical data and hardware information (eg serial number and MAC address)

11. Explanation of the menu items of web interface in chronological order



System data

System name:	IE-SR-2GT-UMTS/3G-AX00711578
Device type:	IE-SR-2GT-UMTS/3G
Serial-No.:	AX00711578
Firmware version:	2.3.0 (Build 63904)
MAC-Address WAN:	00:18:92:01:E0:AF
MAC-Address LAN:	00:18:92:01:E0:AD
Device mode:	IP router

System state

Date & time:	Friday, 08 Mar 2013, 07:14(Europe/Berlin)
Uptime:	07:14:41 up 0 min, load average: 0.46, 0.10, 0.03
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	19%
Memory:	22%
CPU:	56%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled
3G	disabled			

Latest five messages

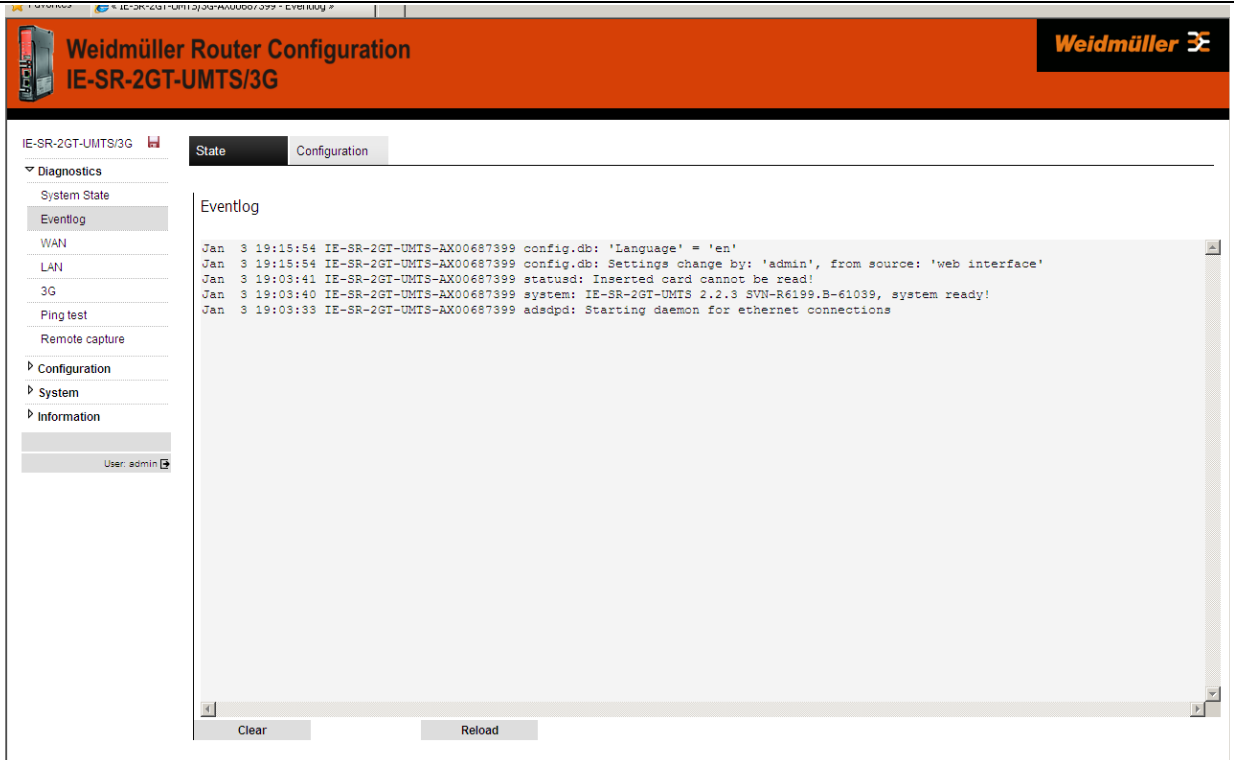
Eventlog

```
Mar 8 07:14:36 IE-SR-2GT-UMTS-AX00711578 system: IE-SR-2GT-UMTS 2.3.0 SVN-R8095.B-63904, system ready!
Mar 8 07:14:33 IE-SR-2GT-UMTS-AX00711578 statusd: SCM memory card insertion detected!
Mar 8 07:14:28 IE-SR-2GT-UMTS-AX00711578 adsdpd: Starting daemon for ethernet connections
Mar 8 07:14:21 IE-SR-2GT-UMTS-AX00711578 system: successfully reset SIM card config to firmware version: 2.3.0 defaults
```

Quicklinks:

Figure 1: Diagnostics → Systemstatus

Startup screen of the web interface after login. Displays current configuration and status data.

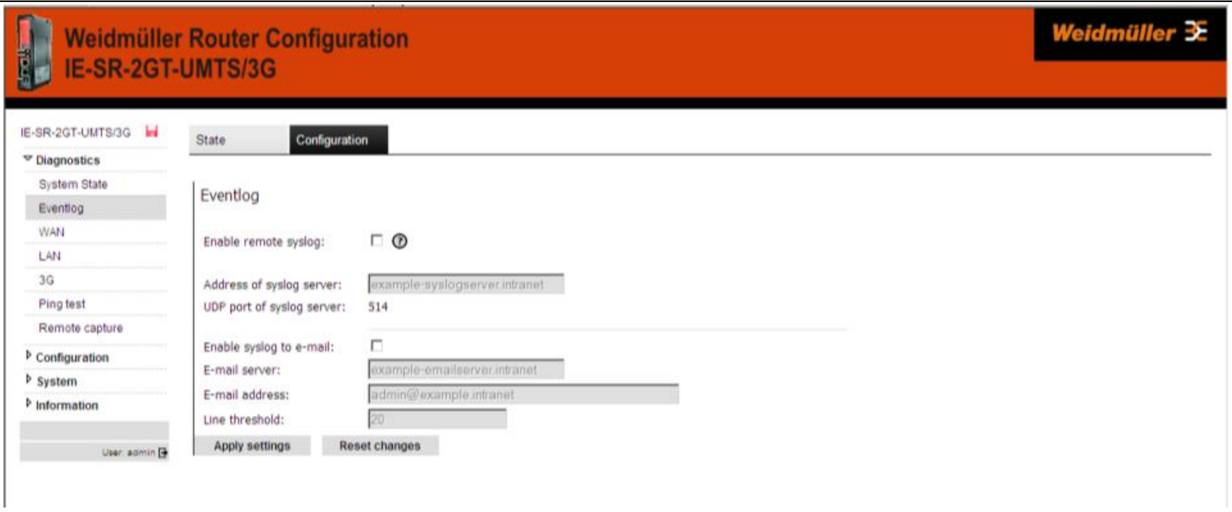


Eventlog

```
Jan  3 19:15:54 IE-SR-2GT-UMTS-AX00687399 config.db: 'Language' = 'en'
Jan  3 19:15:54 IE-SR-2GT-UMTS-AX00687399 config.db: Settings change by: 'admin', from source: 'web interface'
Jan  3 19:03:41 IE-SR-2GT-UMTS-AX00687399 statusd: Inserted card cannot be read!
Jan  3 19:03:40 IE-SR-2GT-UMTS-AX00687399 system: IE-SR-2GT-UMTS 2.2.3 SVN-R6199.B-61039, system ready!
Jan  3 19:03:33 IE-SR-2GT-UMTS-AX00687399 adsdpd: Starting daemon for ethernet connections
```

Figure 2: Diagnostics → Eventlog →Tab State

Display events and error messages that have occurred.



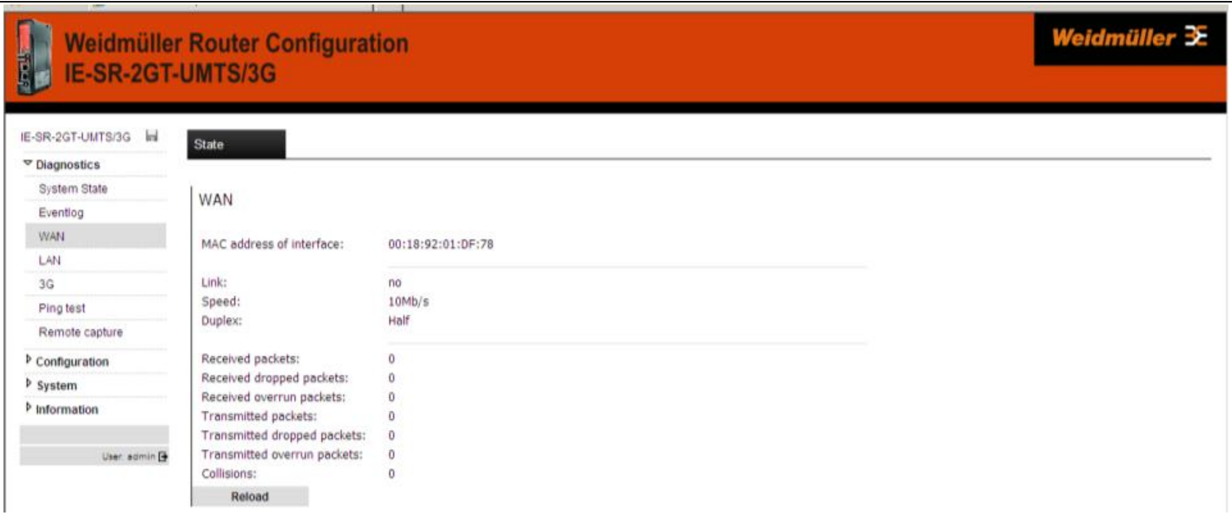
Eventlog

Enable remote syslog: □

Address of syslog server: example-syslogserver.intranet
UDP port of syslog server: 514

Enable syslog to e-mail: □
E-mail server: example-emailserver.intranet
E-mail address: admin@example.intranet
Line threshold: 20

Figure 3: Diagnostics → Eventlog →Tab Configuration
Event and error messages can be sent to a syslog server (PC on the network) and also sent as emails.



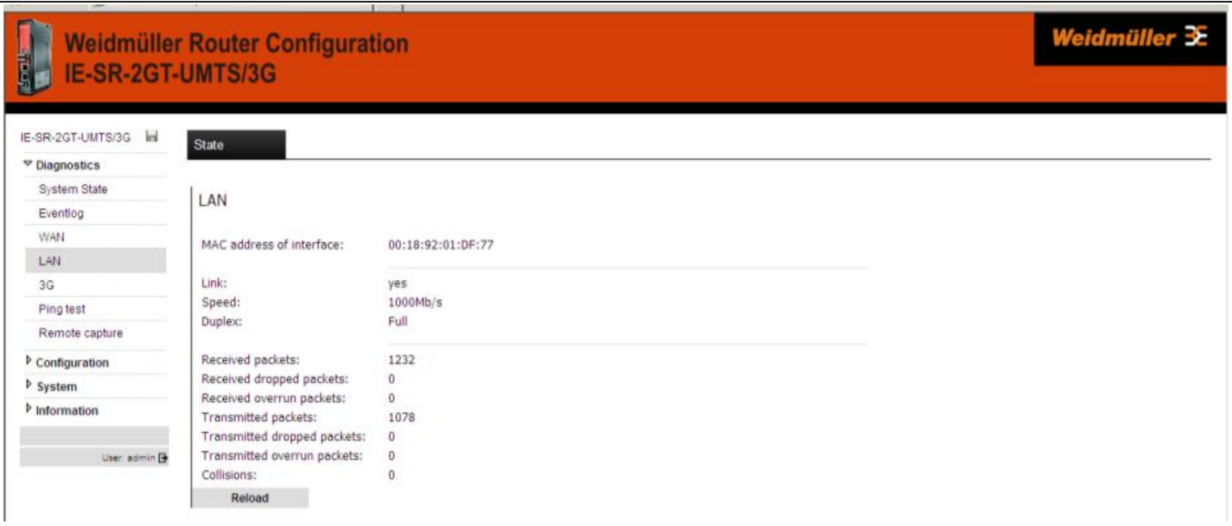
WAN

MAC address of interface: 00:18:92:01:DF:78

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

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

Figure 4: Diagnostics → WAN
Display of the current status of the WAN port.



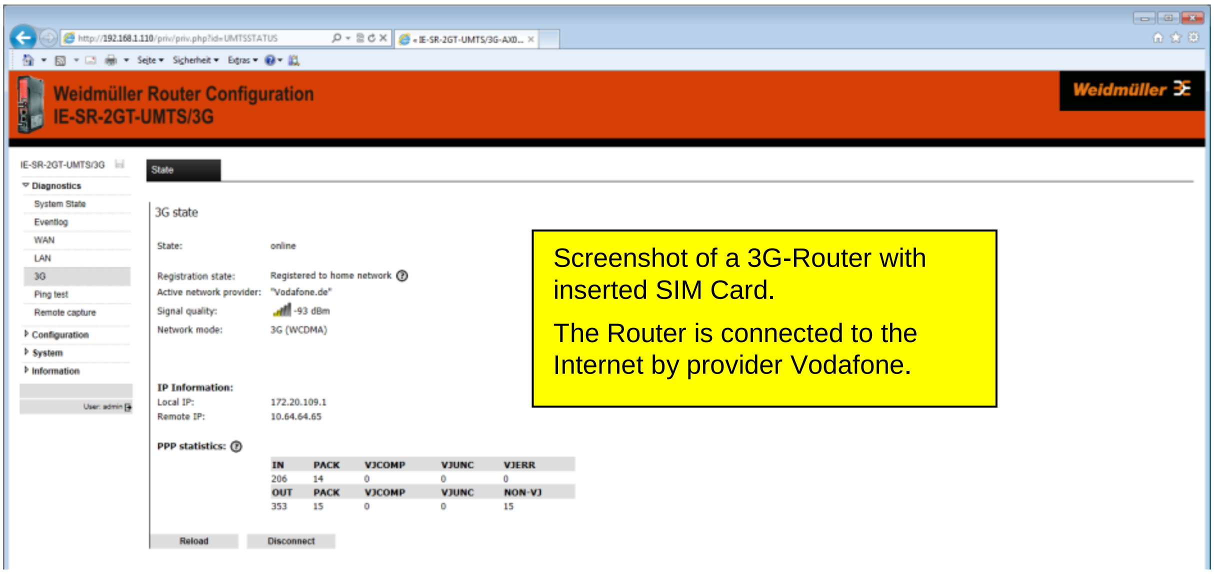
LAN

MAC address of interface: 00:18:92:01:DF:77

Link: yes
Speed: 1000Mb/s
Duplex: Full

Received packets: 1232
Received dropped packets: 0
Received overrun packets: 0
Transmitted packets: 1078
Transmitted dropped packets: 0
Transmitted overrun packets: 0
Collisions: 0

Figure 5: Diagnostics → LAN
Display of the current status of the LAN port.



3G state

State: online

Registration state: Registered to home network
Active network provider: "Vodafone.de"
Signal quality: -93 dBm
Network mode: 3G (WCDMA)

IP Information:
Local IP: 172.20.109.1
Remote IP: 10.64.64.65

PPP statistics:

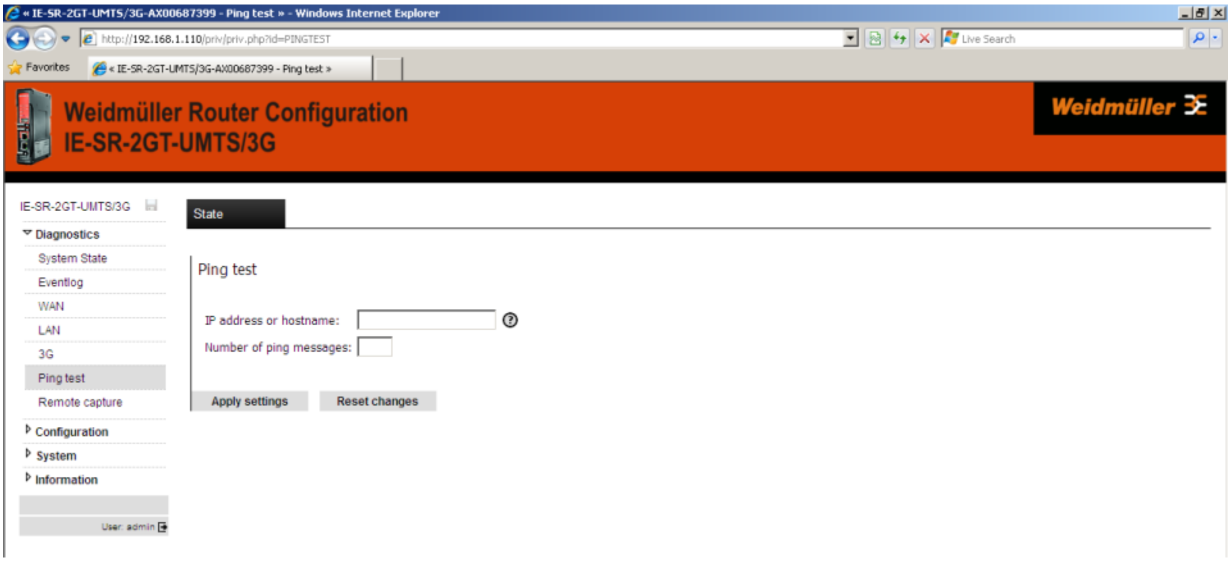
IN	PACK	VJCOMP	VJUNC	VJERR
206	14	0	0	0
OUT	**PACK**	**VJCOMP**	**VJUNC**	**NON-VJ**
353	15	0	0	15

Screenshot of a 3G-Router with inserted SIM Card.

The Router is connected to the Internet by provider Vodafone.

Figure 6: Diagnostics → 3G

Displays the current status of the 3G mobile connection.

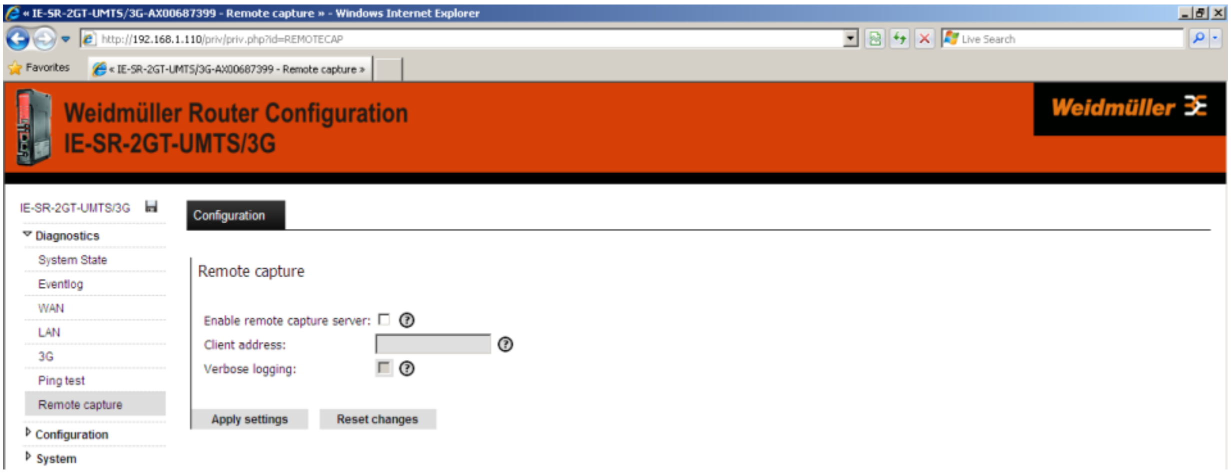


Ping test

IP address or hostname:
Number of ping messages:

Figure 7: Diagnostics → Ping-Test

Allows sending of ICMP packets (ping) to test network connections between the Router and other Ethernet devices.


« IE-SR-2GT-UMTS/3G-AX00687399 - Remote capture » - Windows Internet Explorer
http://192.168.1.110/priv/priv.php?id=REMOTECAP
Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G
IE-SR-2GT-UMTS/3G
Diagnostics
System State
Eventlog
WAN
LAN
3G
Ping test
Remote capture
Configuration
System
Configuration
Apply settings
Reset changes

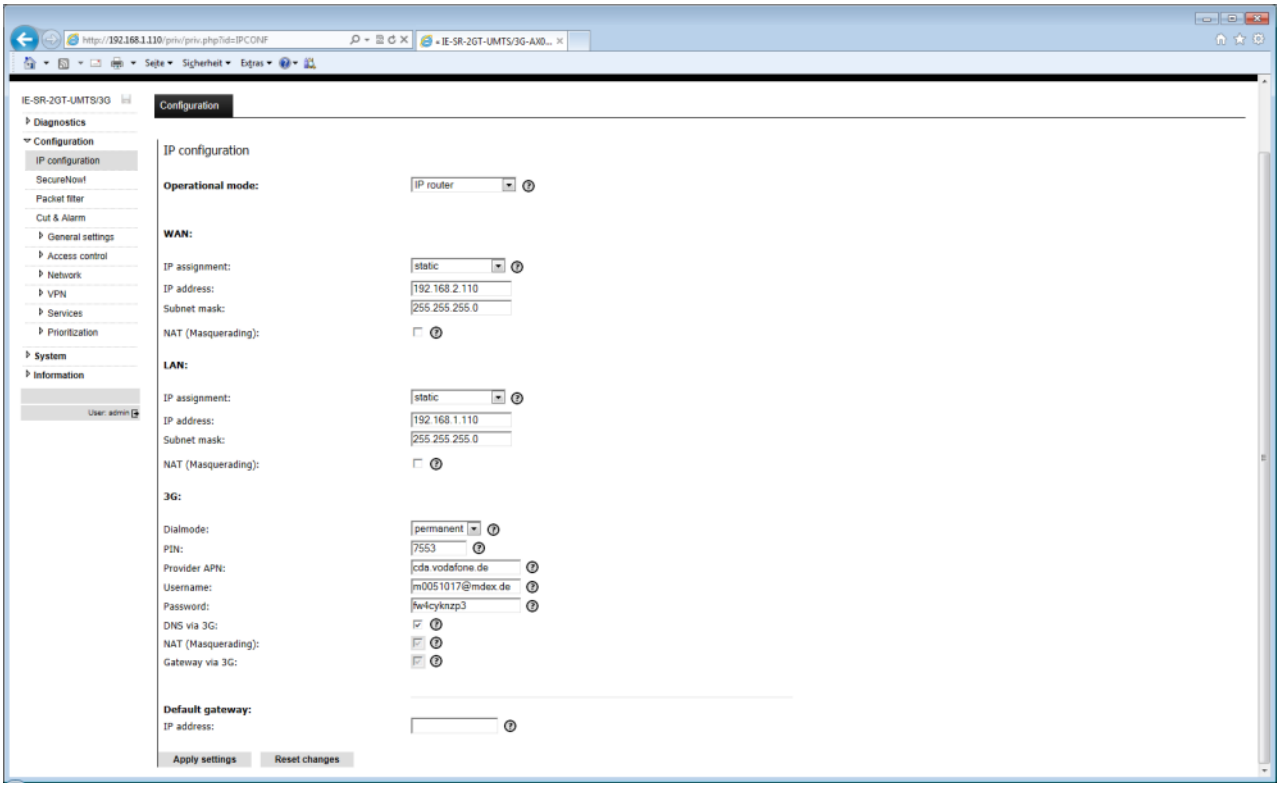
Remote capture

Enable remote capture server: □
Client address:
Verbose logging: □

Figure 8: Diagnostics → Remote-Capture

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 which must have installed the tool "Wireshark".

How to use please refer to application note in Appendix C3.



IP configuration

Operational mode: IP router

WAN:

IP assignment: static
IP address: 192.168.2.110
Subnet mask: 255.255.255.0
NAT (Masquerading): □

LAN:

IP assignment: static
IP address: 192.168.1.110
Subnet mask: 255.255.255.0
NAT (Masquerading): □

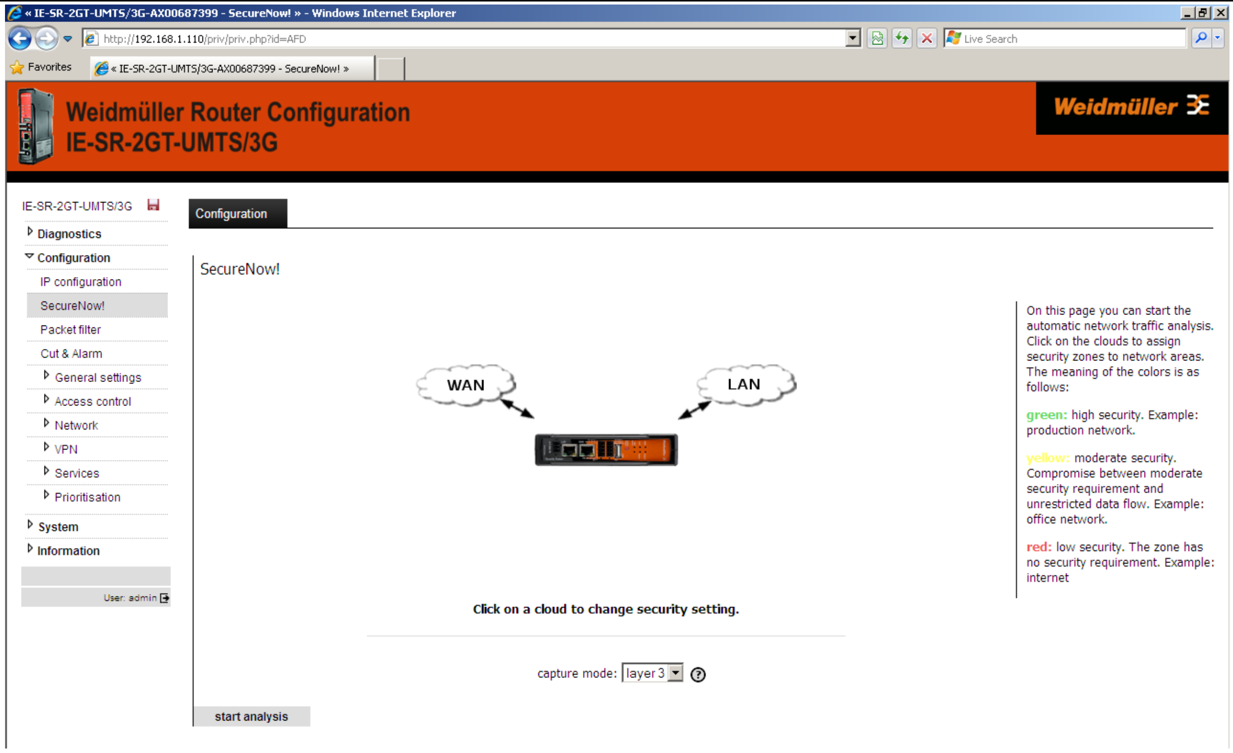
3G:

Dialmode: permanent
PIN: 7553
Provider APN: cda.vodafone.de
Username: m0051017@mdex.de
Password: fw4cyknzp3
DNS via 3G: ☑
NAT (Masquerading): ☑
Gateway via 3G: ☑

Default gateway:
IP address:

Figure 9: Configuration → IP Configuration

This is the basic configuration window of the Router for assignment of IP addresses on the LAN and WAN port. Each of the two interfaces can be configured with static or dynamic (DHCP) IP addresses. For models of type IE-SR-3GT-UMTS/3G (as shown above) additionally a section „3G“ will be displayed to configure the 3G connection.



SecureNow!

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.

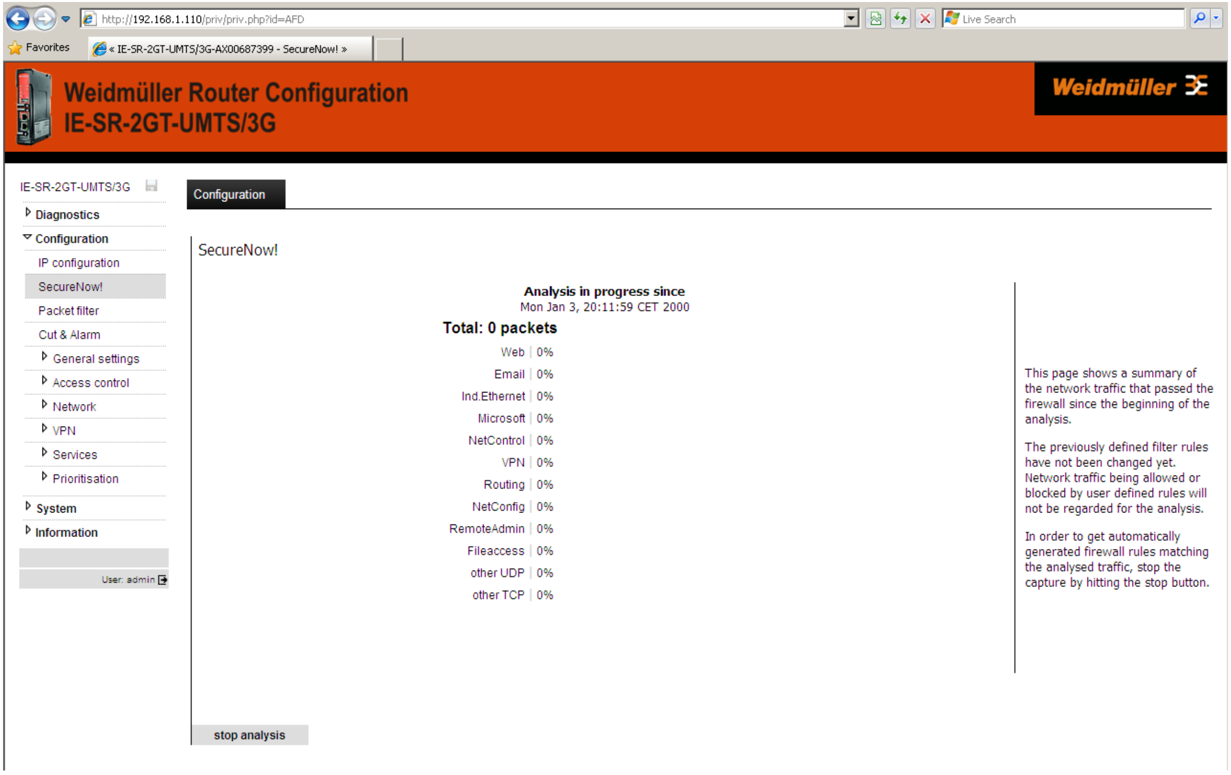
red: low security. The zone has no security requirement. Example: internet

Click on a cloud to change security setting.

capture mode: layer 3

Figure 10: Configuration → SecureNow

This is an auxiliary function for "independent learning" firewall rules based on temporary recording of data traffic. By pressing the button "Start Analysis" button the Router begins to analyze the network traffic (ports LAN, WAN and possibly UMTS/3G). As a result, 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.



SecureNow!

Analysis in progress since
Mon Jan 3, 20:11:59 CET 2000

Total: 0 packets

Web	0%
Email	0%
Ind.Ethernet	0%
Microsoft	0%
NetControl	0%
VPN	0%
Routing	0%
NetConfig	0%
RemoteAdmin	0%
Fileaccess	0%
other UDP	0%
other TCP	0%

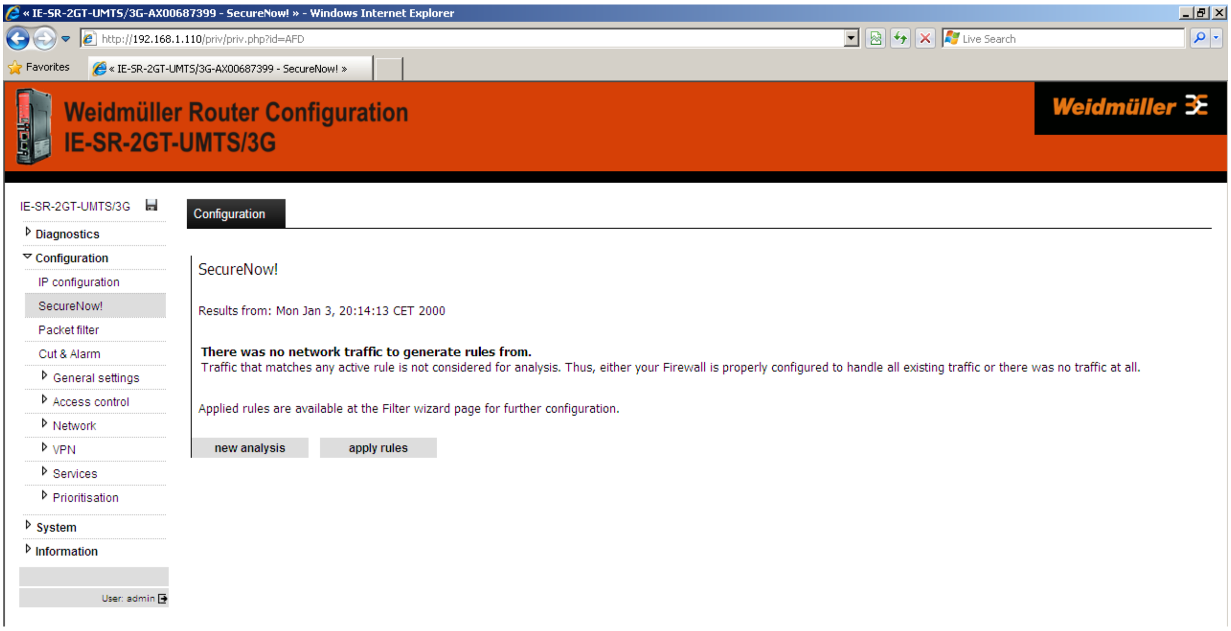
This page shows a summary of the network traffic that passed the firewall since the beginning of the analysis.

The previously defined filter rules have not been changed yet. Network traffic being allowed or blocked by user defined rules will not be regarded for the analysis.

In order to get automatically generated firewall rules matching the analysed traffic, stop the capture by hitting the stop button.

Figure 11: Configuration → SecureNow → „running analysis“

Window screen after starting the network analysis displaying the current network traffic.



SecureNow!

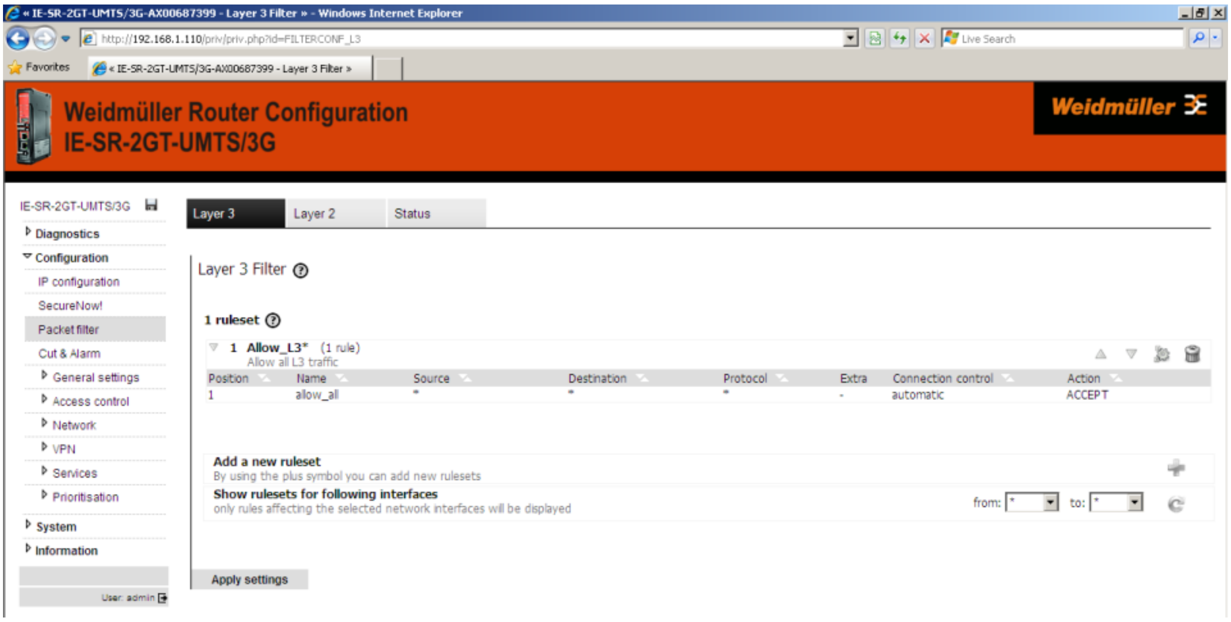
Results from: Mon Jan 3, 20:14:13 CET 2000

There was no network traffic to generate rules from.
Traffic that matches any active rule is not considered for analysis. Thus, either your Firewall is properly configured to handle all existing traffic or there was no traffic at all.

Applied rules are available at the Filter wizard page for further configuration.

Figure 12: Configuration → SecureNow → „Analysis stopped“

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. Then previous filter rules would be valid again.



Layer 3 Filter

1 ruleset

1 **Allow_L3*** (1 rule)
Allow all L3 traffic

Position	Name	Source	Destination	Protocol	Extra	Connection control	Action
1	allow_all	*	*	*	-	automatic	ACCEPT

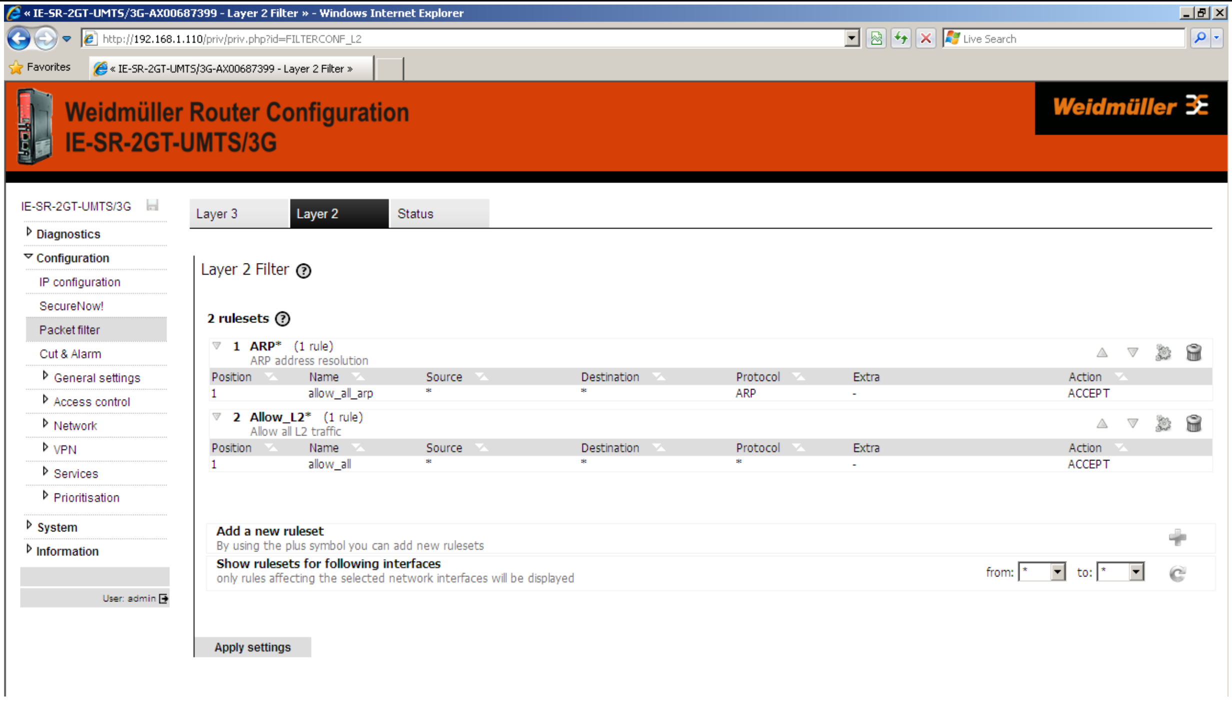
Add a new ruleset
By using the plus symbol you can add new rulesets

Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed   from: * to: *

Figure 13: Configuration → Packet filter → Tab „Layer 3“

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.

Fore more detailed information about using the packet filter please refer to Appendix A3.



Layer 2 Filter

2 rulesets

1 ARP* (1 rule)
ARP address resolution

Position	Name	Source	Destination	Protocol	Extra	Action
1	allow_all_arp	*	*	ARP	-	ACCEPT

2 Allow_L2* (1 rule)
Allow all L2 traffic

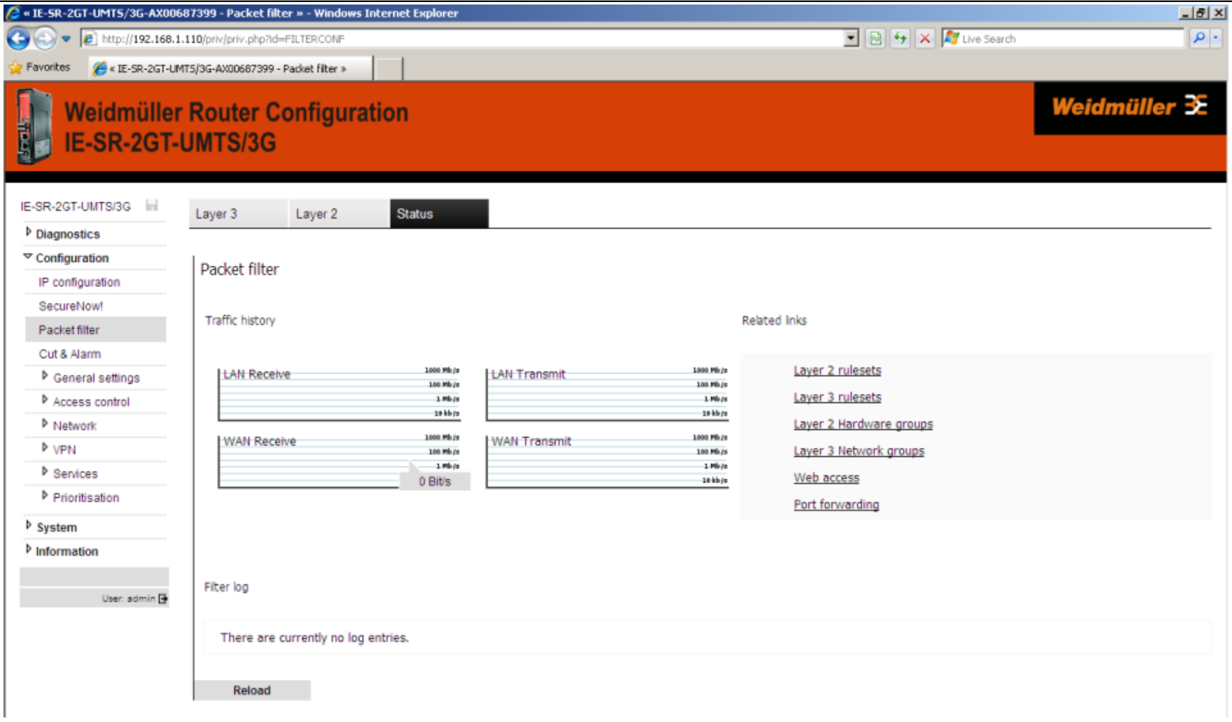
Position	Name	Source	Destination	Protocol	Extra	Action
1	allow_all	*	*	*	-	ACCEPT

Add a new ruleset
By using the plus symbol you can add new rulesets

Show rulesets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *

Figure 14: Configuration → Packet filter → Tab „Layer 2“

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

Traffic history

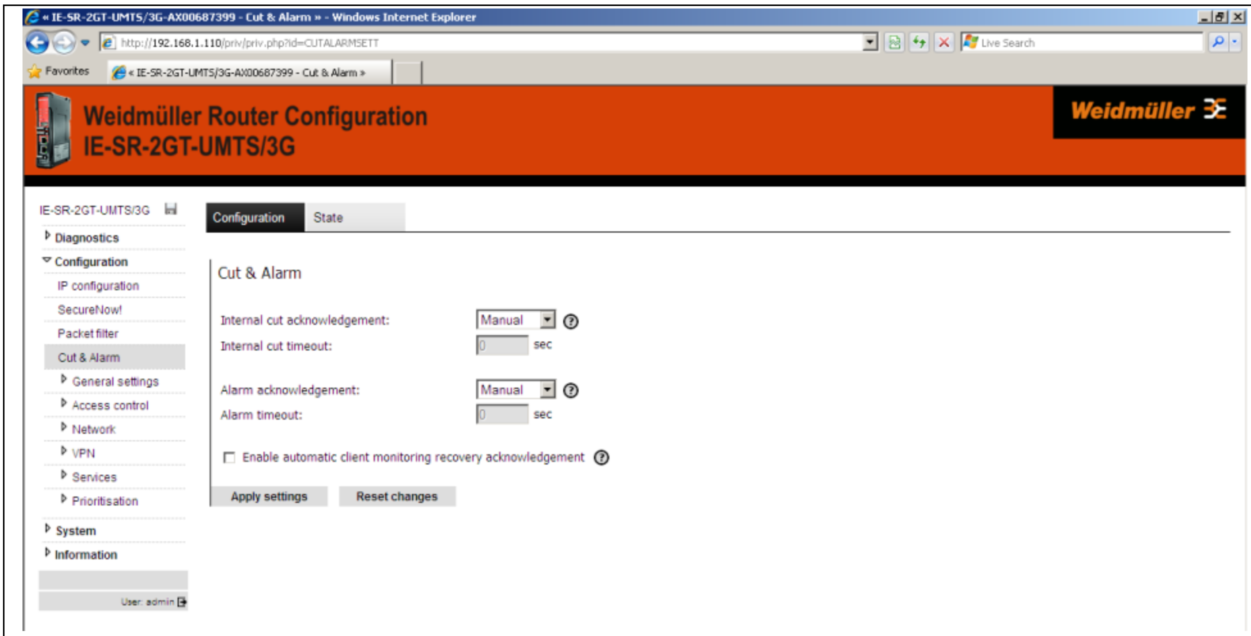
Related links

Filter log

There are currently no log entries.

Figure 15: Configuration → Packet filter → Tab „Status“

Overview of transmit and receive activities of the Ethernet interfaces. In addition, firewall-related information is displayed under the heading "Filter Log".



Cut & Alarm

Internal cut acknowledgement: Manual

Internal cut timeout: 0 sec

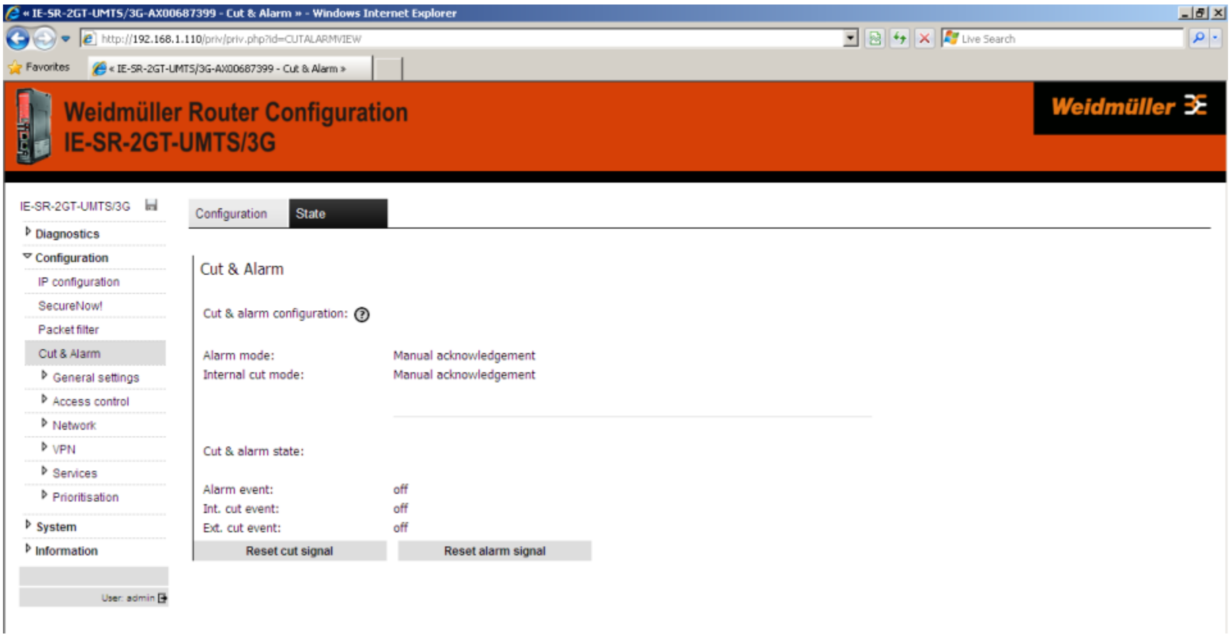
Alarm acknowledgement: Manual

Alarm timeout: 0 sec

□ Enable automatic client monitoring recovery acknowledgement

Figure 16: Configuration → Cut & Alarm → Tab „Configuration“

In this menu it can be configured how the events "Cut" and "Alarm" - after they have occurred – will be reset (either manually by clicking on a button on the tab “State” or automatically after an elapsed time).
For more information please refer to Appendix C2 (Method 2).



Cut & Alarm

Cut & alarm configuration:

Alarm mode: Manual acknowledgement

Internal cut mode: Manual acknowledgement

Cut & alarm state:

Alarm event: off

Int. cut event: off

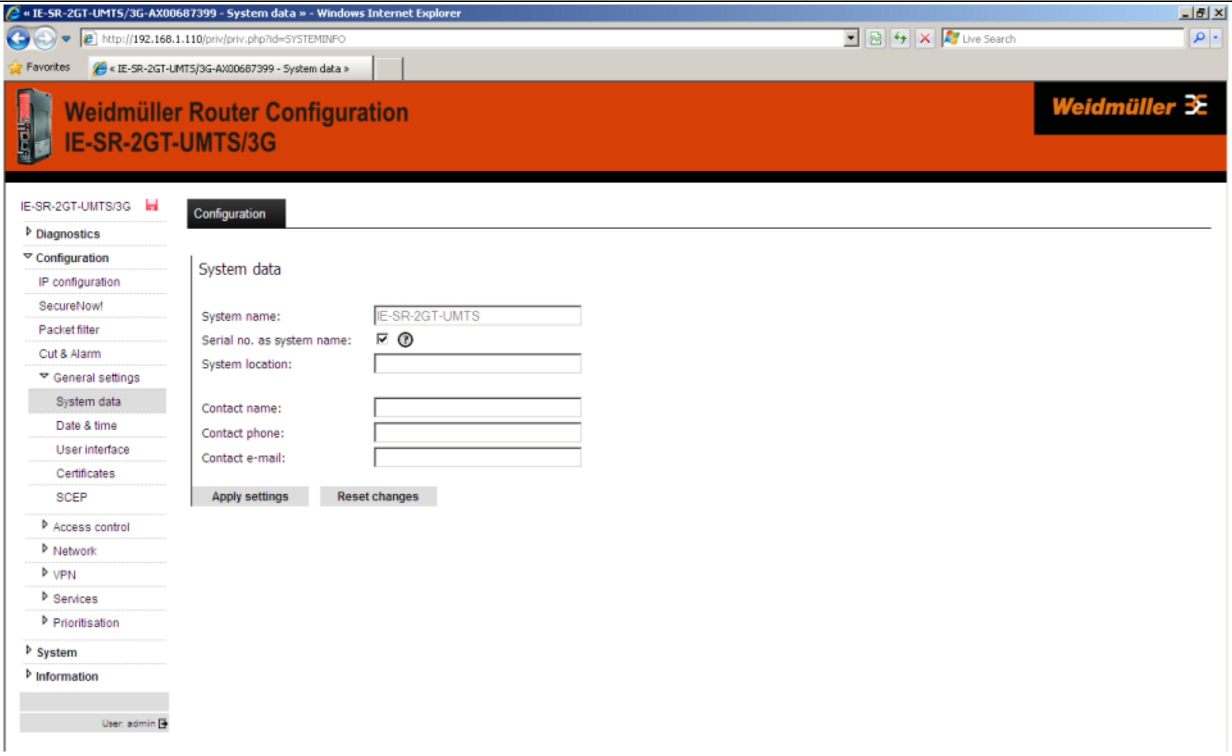
Ext. cut event: off

Figure 17: Configuration → Cut & Alarm → Tab „State“

Displays the current status of the events

"Internal Cut" → triggered eg by a special firewall rule
"External Cut" → Input of 24 VDC at 4-pin connector (at front side of the Router)
"Alarm" → → triggered eg by a special firewall rule or by the function „Client monitoring“

By clicking on the buttons „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 at the 4-pin connector will be removed.

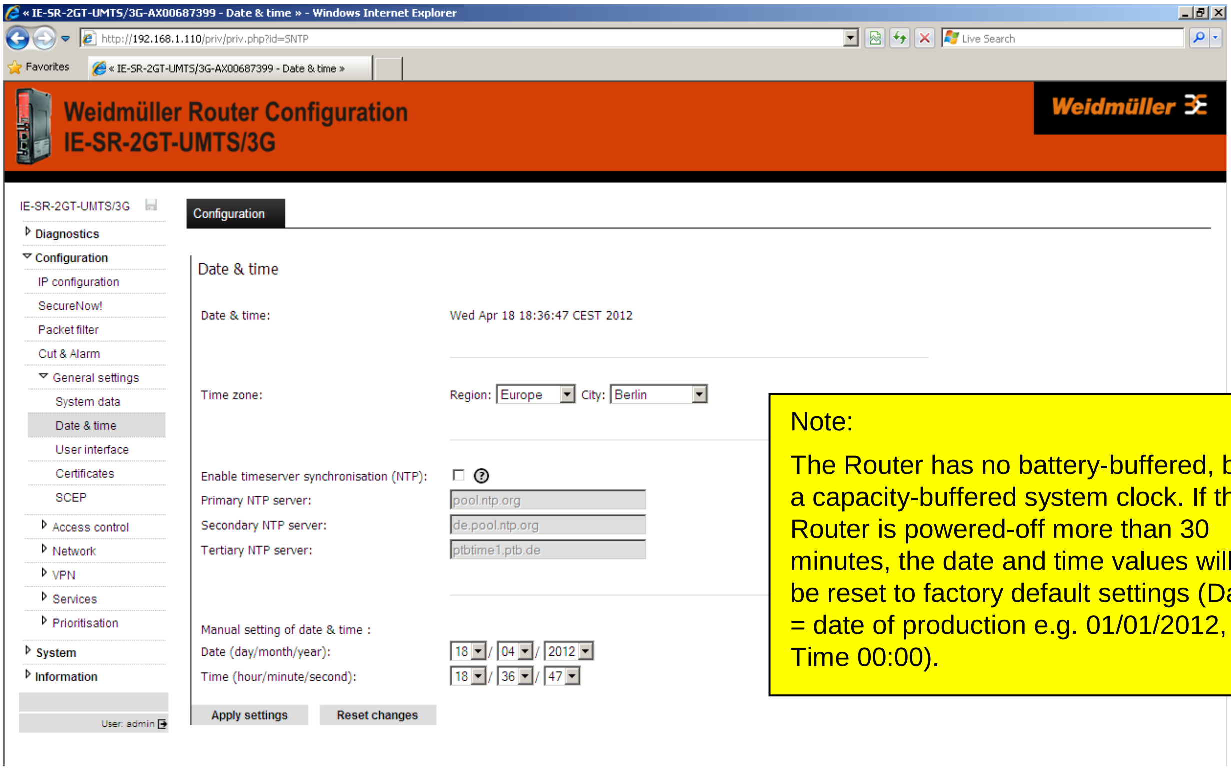


System data

System name: IE-SR-2GT-UMTS
Serial no. as system name: ☑
System location:
Contact name:
Contact phone:
Contact e-mail:

Figure 18: Configuration → General settings → System data → Tab „Configuration“

Configuring application-related data of the Router (free text).



Date & time

Date & time: Wed Apr 18 18:36:47 CEST 2012

Time zone: Region: Europe City: Berlin

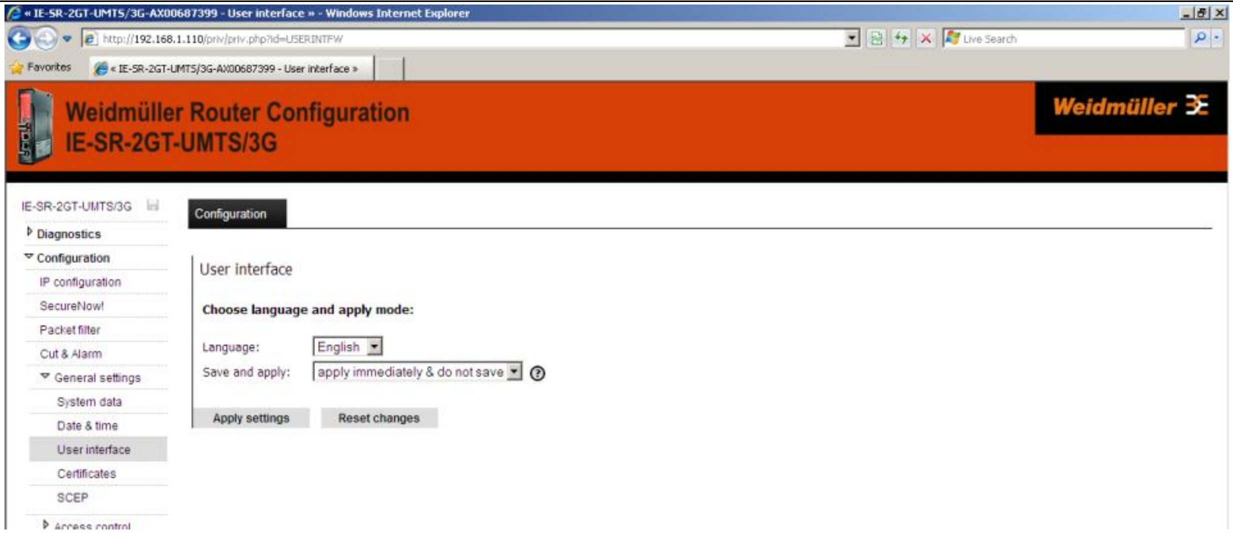
Enable timeserver synchronisation (NTP): □
Primary NTP server: pool.ntp.org
Secondary NTP server: de.pool.ntp.org
Tertiary NTP server: ptbtime1.ptb.de

Manual setting of date & time :
Date (day/month/year): 18 / 04 / 2012
Time (hour/minute/second): 18 / 36 / 47

> Note:
>
> The Router has no battery-buffered, but a capacity-buffered system clock. If the Router is powered-off more than 30 minutes, the date and time values will be reset to factory default settings (Date = date of production e.g. 01/01/2012, Time 00:00).

Figure 19: Configuration → General settings → Date & time → Tab „Configuration“

Setting of date, time and time zone. Alternatively, the date/time setting can be configured via using the "Network Time Protocol" and accessing an external NTP server.



« IE-SR-2GT-UMTS/3G-AX00687399 - User interface » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=USERINTFW

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

User interface

Choose language and apply mode:

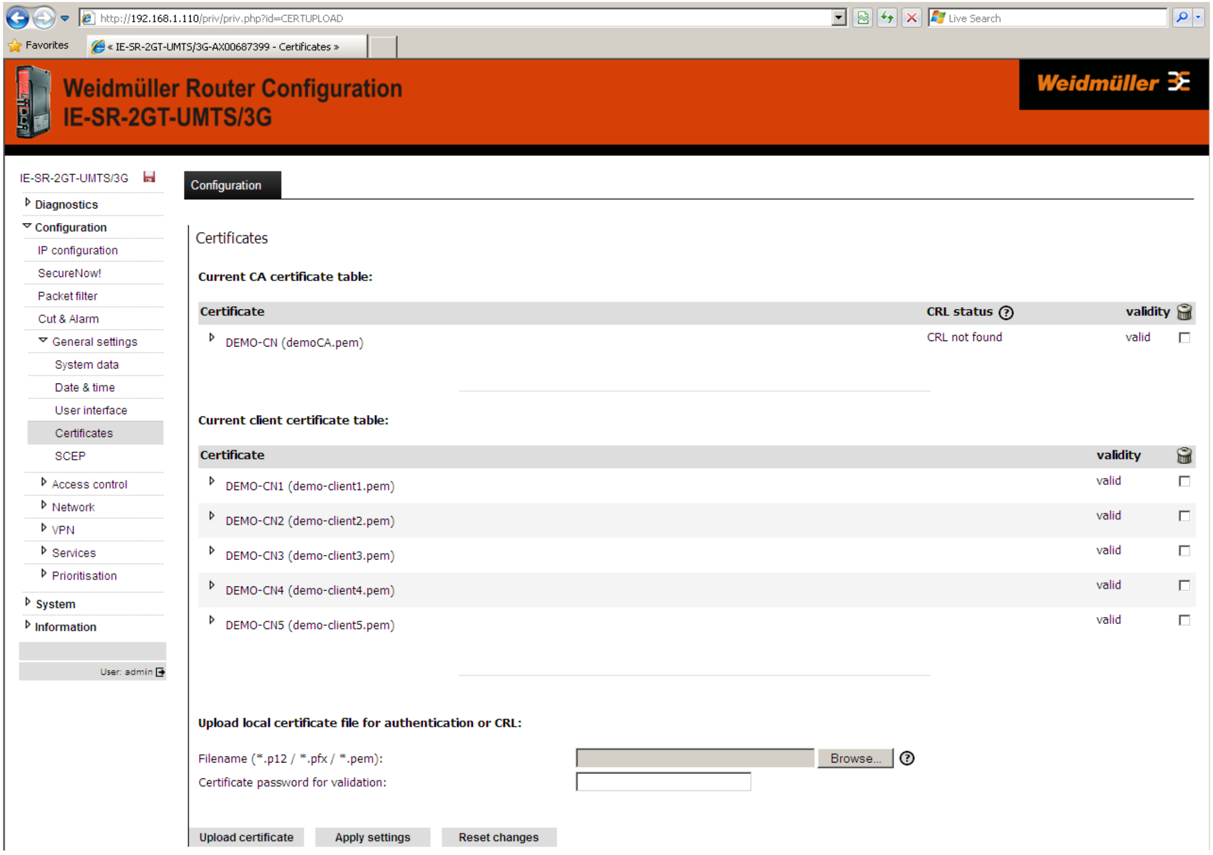
Language: English

Save and apply: apply immediately & do not save

Figure 20: Configuration → General settings → User interface → Tab „Configuration“

Language → Setting the language (German or English) of the Web interface.

Save and apply → Setting the behaviour of the button "Activate" respectively „Save“ in the configuration windows. If you chose the entry „Apply immediately and do not save“ then configuration changes will be immediately activated but not saved. If you chose the entry „Save only and do not apply“ then the button named „Apply“ in the configuration windows will be changed to a button named „Saved“. In this case all done changes will be only saved and not activated. Saved changes come into effect after a restart.



http://192.168.1.110/priv/priv.php?id=CERTUPLOAD

« IE-SR-2GT-UMTS/3G-AX00687399 - Certificates »

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Certificates

Current CA certificate table:

Certificate	CRL status	validity	
DEMO-CN (demoCA.pem)	CRL not found	valid	□

Current client certificate table:

Certificate	validity	
DEMO-CN1 (demo-client1.pem)	valid	□
DEMO-CN2 (demo-client2.pem)	valid	□
DEMO-CN3 (demo-client3.pem)	valid	□
DEMO-CN4 (demo-client4.pem)	valid	□
DEMO-CN5 (demo-client5.pem)	valid	□

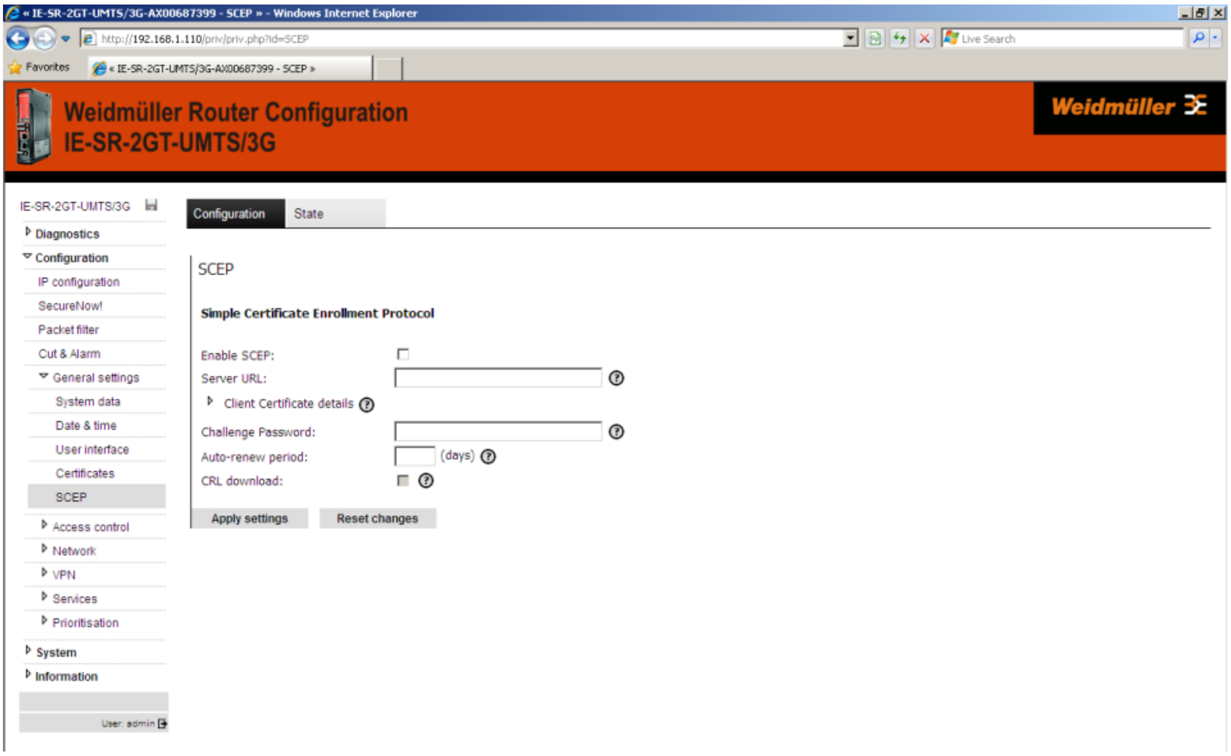
Upload local certificate file for authentication or CRL:

Filename (*.p12 / *.pfx / *.pem):

Certificate password for validation:

Figure 21: Configuration → General settings → Certificates → Tab „Configuration“

Adding or deleting of certificates for VPN applications (used for both IPsec and OpenVPN).
How to use certificates (CA Root, Server, Client) please refer to Appendix B1 (Link to document TechNote_Router_RemoteAccess_via_MeetingPoint_V1_??.pdf).



« IE-SR-2GT-UMTS/3G-AX00687399 - SCEP » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=SCEP

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

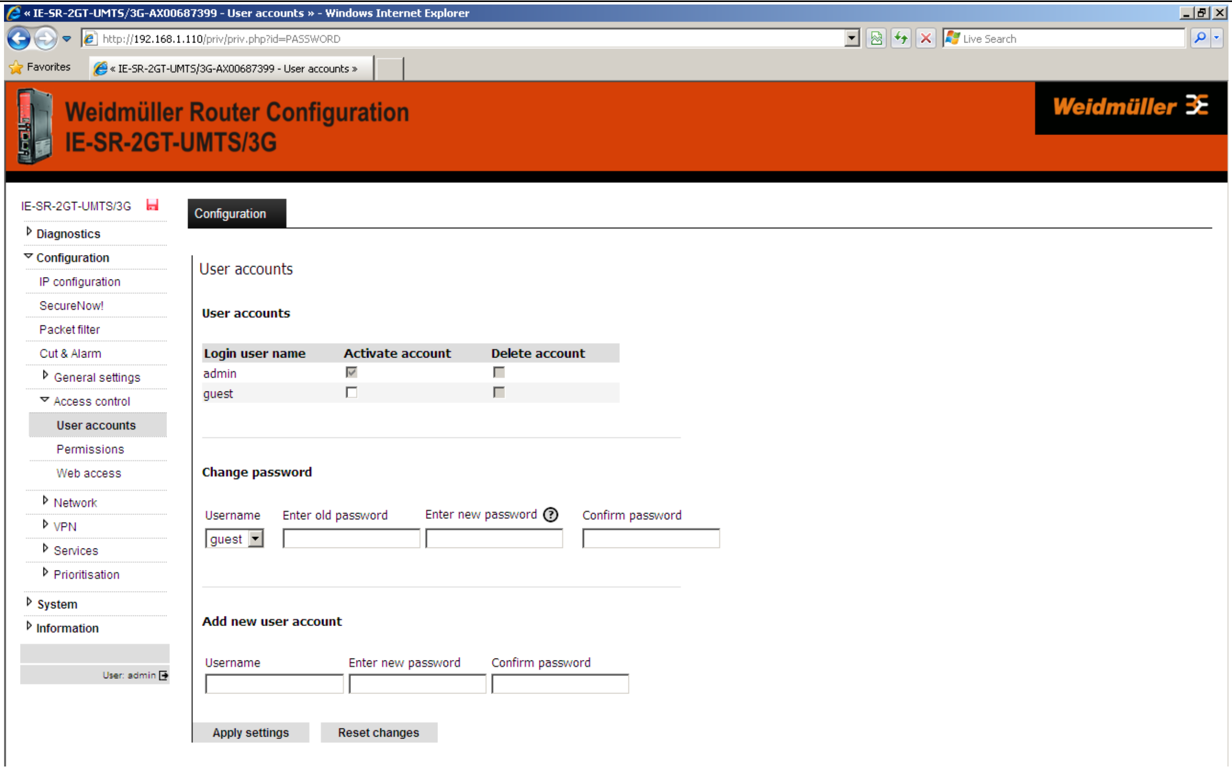
SCEP

Simple Certificate Enrollment Protocol

Enable SCEP: □
Server URL:
Client Certificate details
Challenge Password:
Auto-renew period: (days)
CRL download: □

Figure 22: Configuration → General settings → SCEP → Tab „Configuration“

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.



« IE-SR-2GT-UMTS/3G-AX00687399 - User accounts » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=PASSWORD

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

User accounts

User accounts

Login user name	Activate account	Delete account
admin	☑	□
guest	□	□

Change password

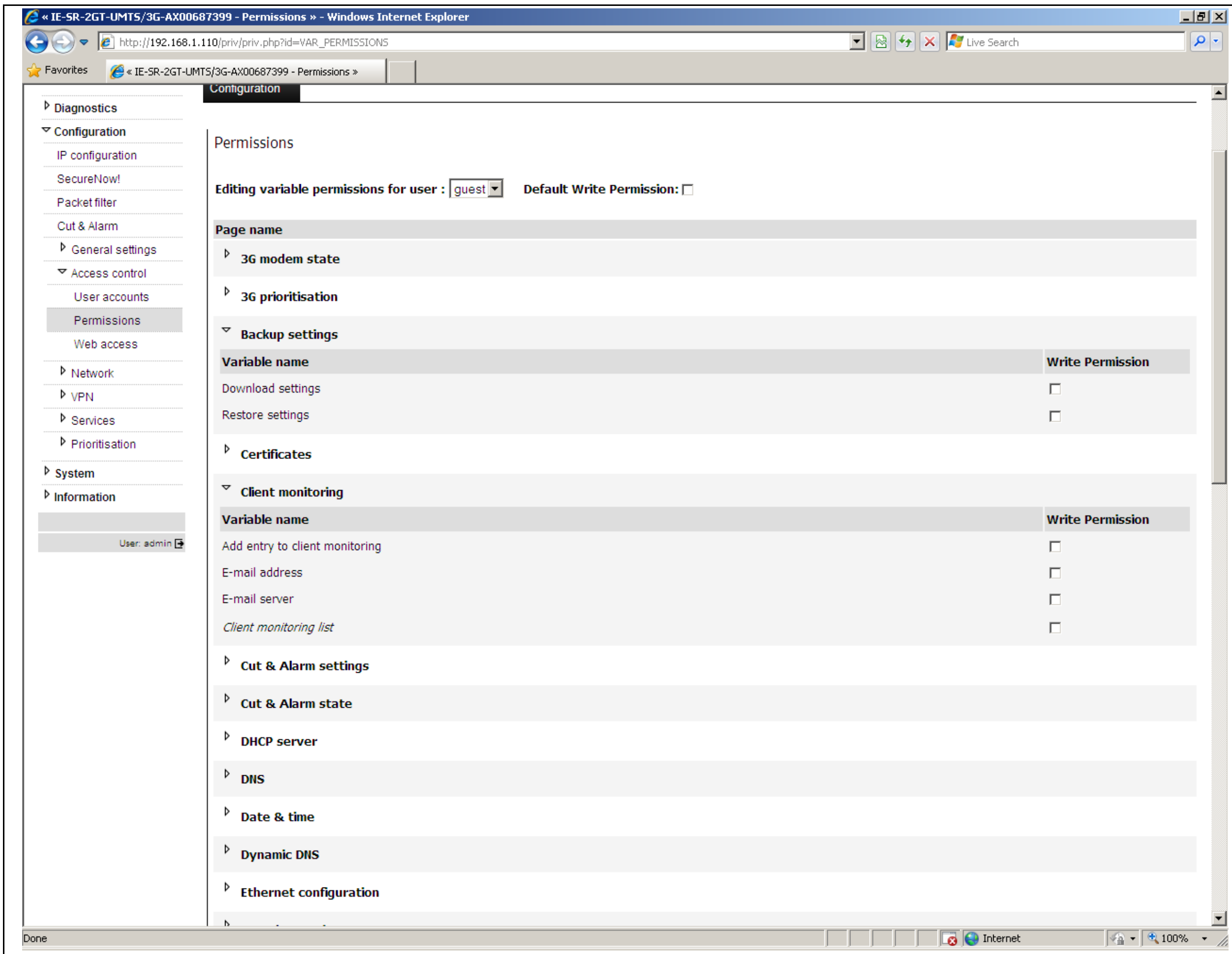
Username: guest
Enter old password
Enter new password
Confirm password

Add new user account

Username
Enter new password
Confirm password

Figure 23: Configuration → Access control → User accounts → Tab „Configuration“

Create and delete other user accounts



« IE-SR-2GT-UMTS/3G-AX00687399 - Permissions » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=VAR_PERMISSIONS

Permissions

Editing variable permissions for user : guest   Default Write Permission: □

Page name

- 3G modem state
- 3G prioritisation
- Backup settings

Variable name	Write Permission
Download settings	□
Restore settings	□

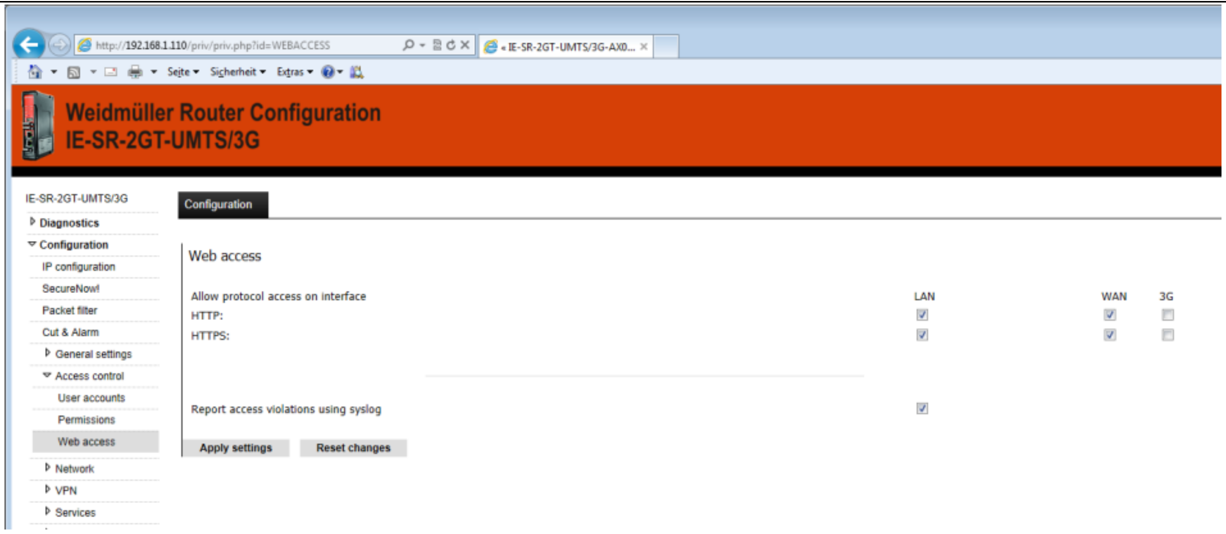
- Certificates
- Client monitoring

Variable name	Write Permission
Add entry to client monitoring	□
E-mail address	□
E-mail server	□
Client monitoring list	□

- Cut & Alarm settings
- Cut & Alarm state
- DHCP server
- DNS
- Date & time
- Dynamic DNS
- Ethernet configuration

Figure 24: Configuration → Access control → Permissions → Tab „Configuration“

Detailed assignmnet of individual rights for the created user accounts.
Note: The Administrator account always has full access. It cannot be deleted.



http://192.168.1.110/priv/priv.php?id=WEBACCESS

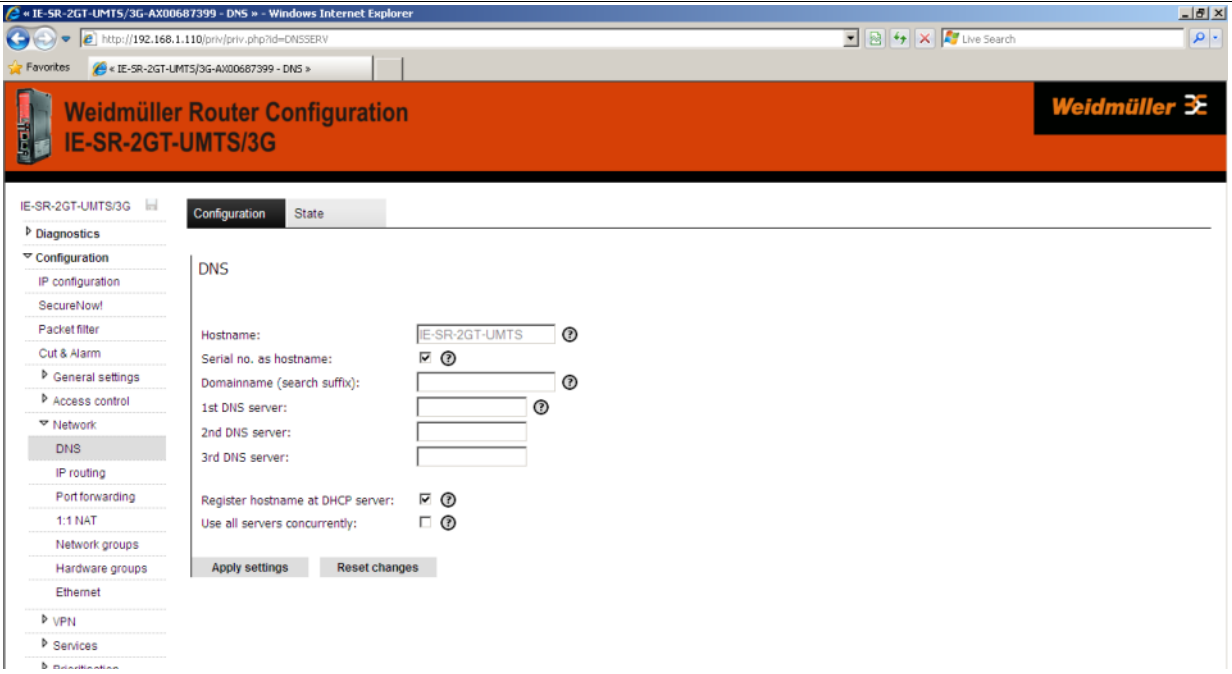
Web access

Allow protocol access on interface	LAN	WAN	3G
HTTP:	☑	☑	□
HTTPS:	☑	☑	□

Report access violations using syslog ☑

Figure 25: Configuration → Access control → Web access → Tab „Configuration“

Select the possible access modes of the web interface (via http and / or https). For models of type IE-SR-3GT-UMTS/3G additionally section „3G“ (as shown above) will be displayed to allow access to the Webinterface via 3G connection.



« IE-SR-2GT-UMTS/3G-AX00687399 - DNS » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=DNSSERV

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

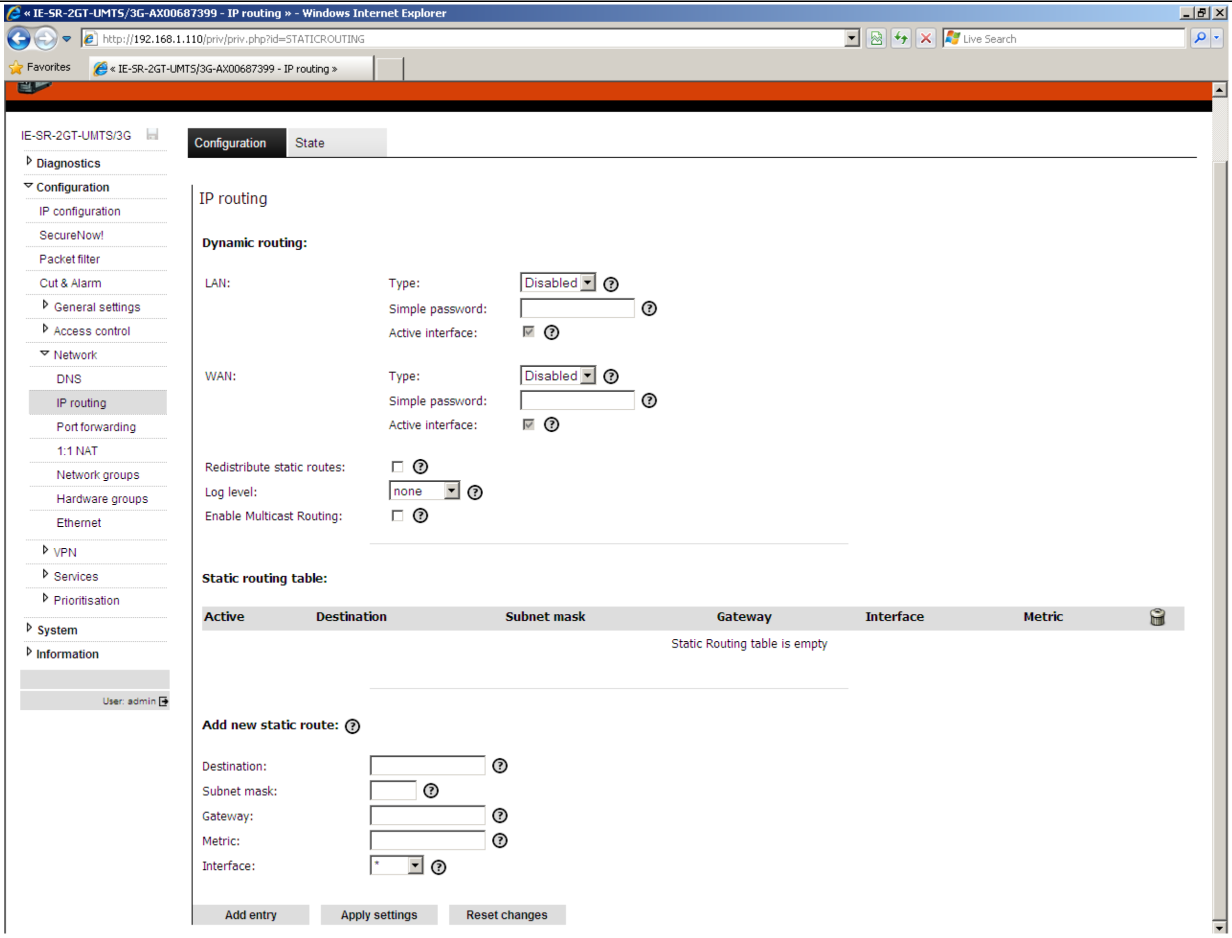
DNS

Hostname: IE-SR-2GT-UMTS
Serial no. as hostname: ☑
Domainname (search suffix):
1st DNS server:
2nd DNS server:
3rd DNS server:

Register hostname at DHCP server: ☑
Use all servers concurrently: □

Figure 26: Configuration → Network → DNS → Tab „Configuration“

Registration of up to 3 DNS servers for name resolution. The Router acts as a DNS relay server.



« IE-SR-2GT-UMTS/3G-AX00687399 - IP routing » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=STATICROUTING

IP routing

Dynamic routing:

LAN: Type: Disabled
Simple password:
Active interface: ☑

WAN: Type: Disabled
Simple password:
Active interface: ☑

Redistribute static routes: □
Log level: none
Enable Multicast Routing: □

Static routing table:

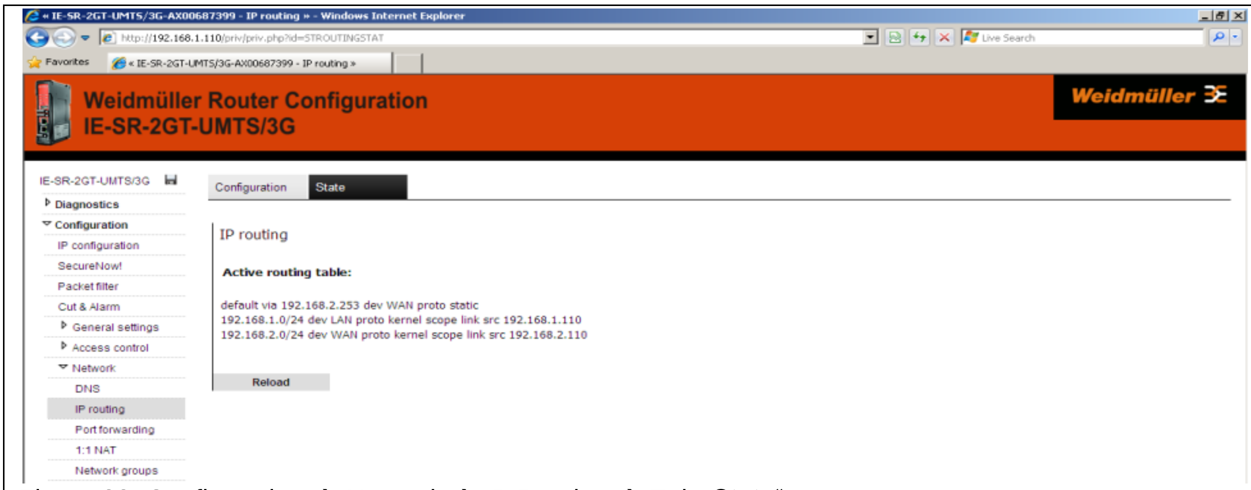
Active	Destination	Subnet mask	Gateway	Interface	Metric

Static Routing table is empty

Add new static route:

Destination:
Subnet mask:
Gateway:
Metric:
Interface: *

Figure 27: Configuration → Network → IP Routing → Tab „Configuration“
Registration of static IP routes and activating/deactivating of dynamic routing. For dynamic routing both can be selected the RIP and the OSPF protocol. Up to 10 static IP routes can be configured.



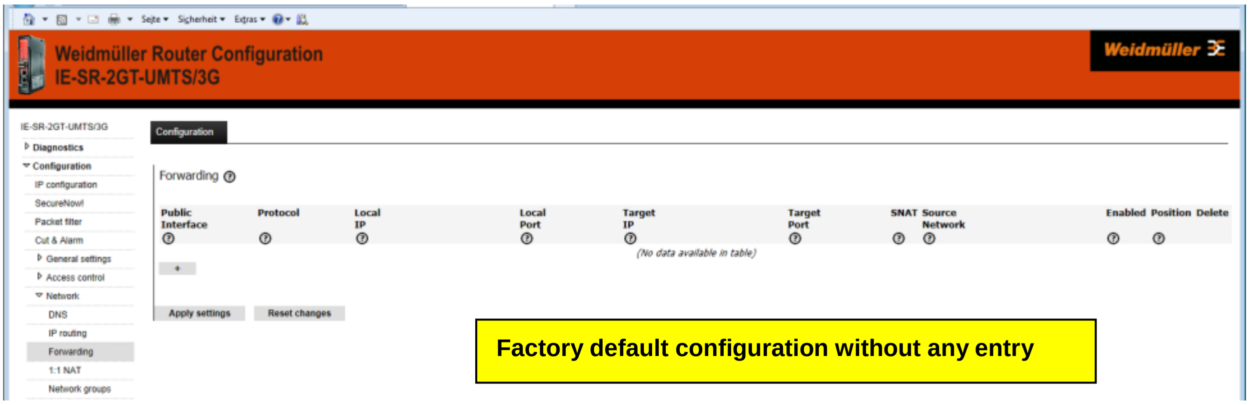
IP routing

Active routing table:

```
default via 192.168.2.253 dev WAN proto static
192.168.1.0/24 dev LAN proto kernel scope link src 192.168.1.110
192.168.2.0/24 dev WAN proto kernel scope link src 192.168.2.110
```

Figure 28: Configuration → Network → IP Routing → Tab „State“

Display of currently valid routing table.



Forwarding

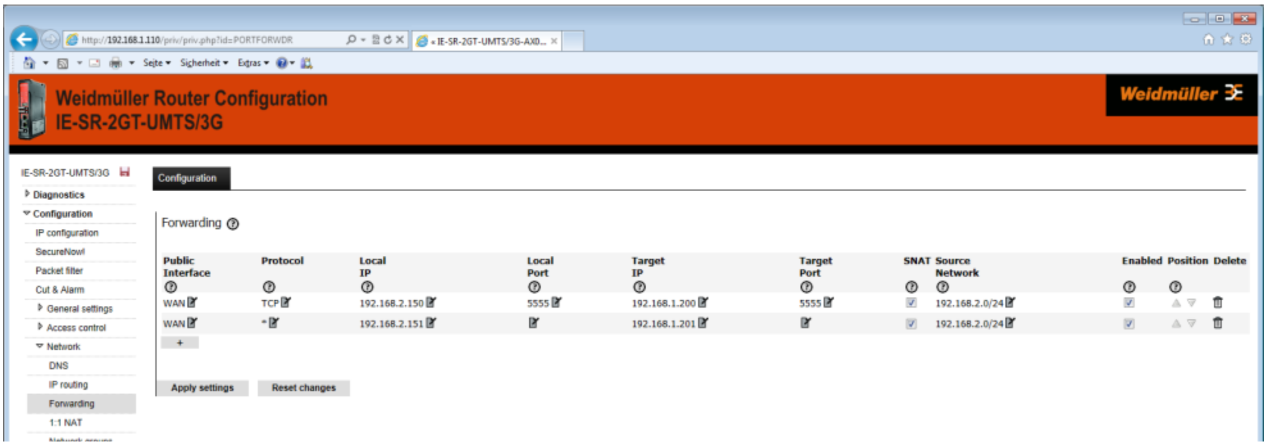
Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT	Source Network	Enabled	Position	Delete
				(No data available in table)						

Factory default configuration without any entry

Figure 29: Configuration → Network → Forwarding → Tab „Configuration“

Configuring standard port forwardings (IP address with port) and pure IP address forwardings. Additonally for each forwarding the feature SNAT (Source network address translation) can be activated to hide the original source.

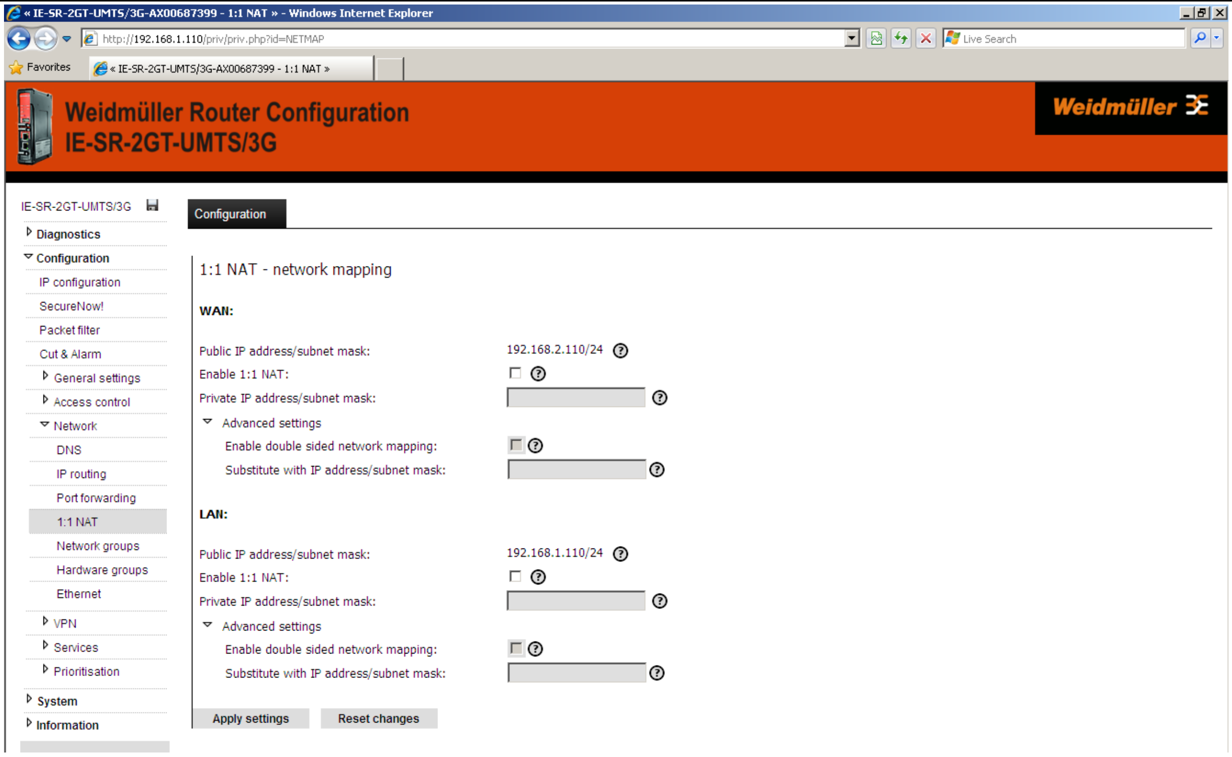
„IP address forwarding“ can be configured using an IP address and a wildcard port number (*) instead of a fixed port number. With this features it is possible to get access to an Ethernet device behind a masqueraded interface only by IP address. From the behavior this fea-ture is similar to a virtual mapping giving an Ethernet device a second public IP address.



Forwarding

Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT	Source Network	Enabled	Position	Delete
WAN	TCP	192.168.2.150	5555	192.168.1.200	5555	☑	192.168.2.0/24	☑	△ ▽	🗑
WAN	*	192.168.2.151		192.168.1.201		☑	192.168.2.0/24	☑	△ ▽	🗑

Figure 30: Configuration → Network → Forwarding → Tab „Configuration“ (2 Forwardings configured)



1:1 NAT - network mapping

WAN:

Public IP address/subnet mask: 192.168.2.110/24

Enable 1:1 NAT: □

Private IP address/subnet mask:

Advanced settings

Enable double sided network mapping: □

Substitute with IP address/subnet mask:

LAN:

Public IP address/subnet mask: 192.168.1.110/24

Enable 1:1 NAT: □

Private IP address/subnet mask:

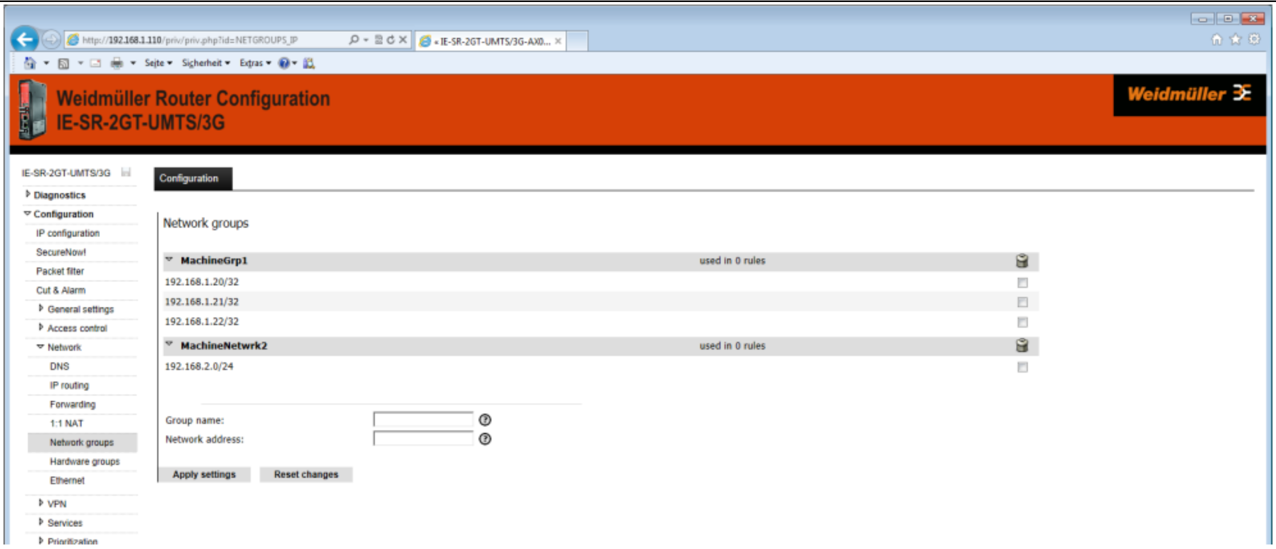
Advanced settings

Enable double sided network mapping: □

Substitute with IP address/subnet mask:

Figure 31: Configuration → Network → 1:1 NAT → Tab „Configuration“

Configuration of the mapping (assignment) of IP address ranges between LAN and WAN port, and vice-versa.
For more detailed information please refer to Appendix A2.



Network groups

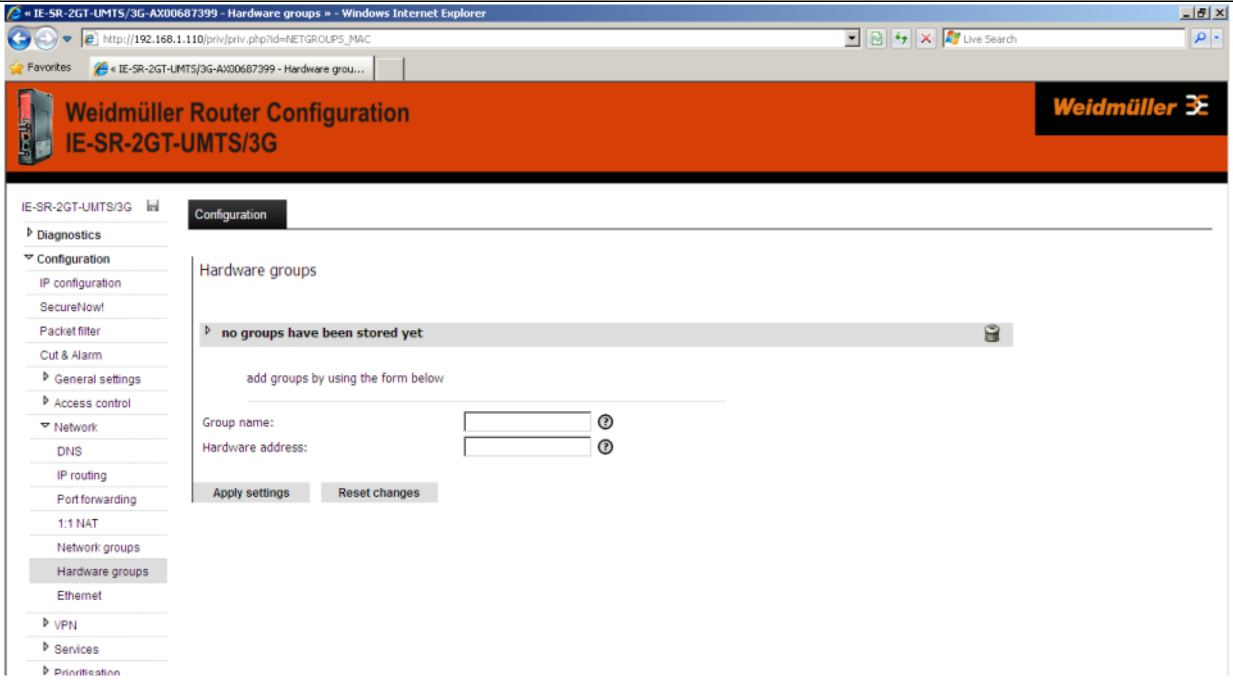
MachineGrp1	used in 0 rules	
192.168.1.20/32		□
192.168.1.21/32		□
192.168.1.22/32		□
MachineNetwrk2	used in 0 rules	
192.168.2.0/24		□

Group name:

Network address:

Figure 32: Configuration → Network → Network groups → Tab „Configuration“

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 (eg 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).



Hardware groups

no groups have been stored yet

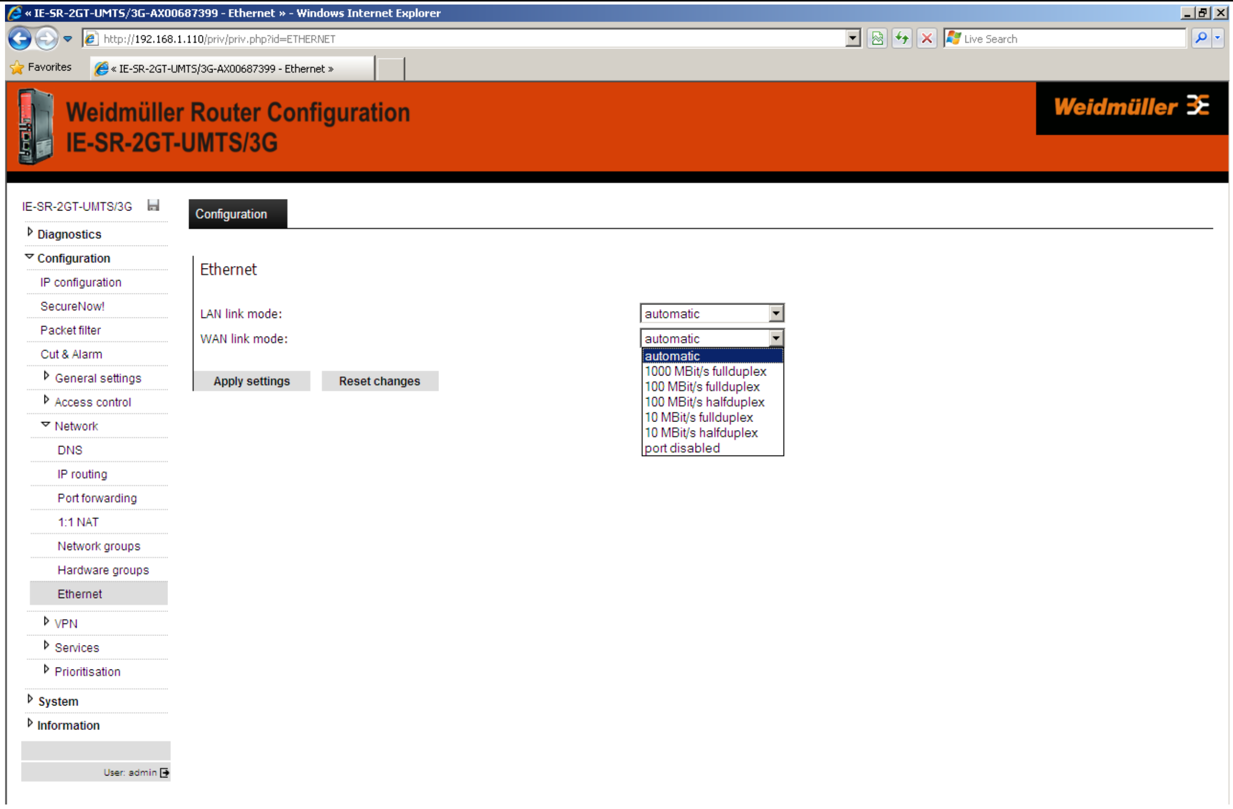
add groups by using the form below

Group name:

Hardware address:

Figure 33: Configuration → Network → Hardware groups → Tab „Configuration“

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 → Packet filters → Layer 2).



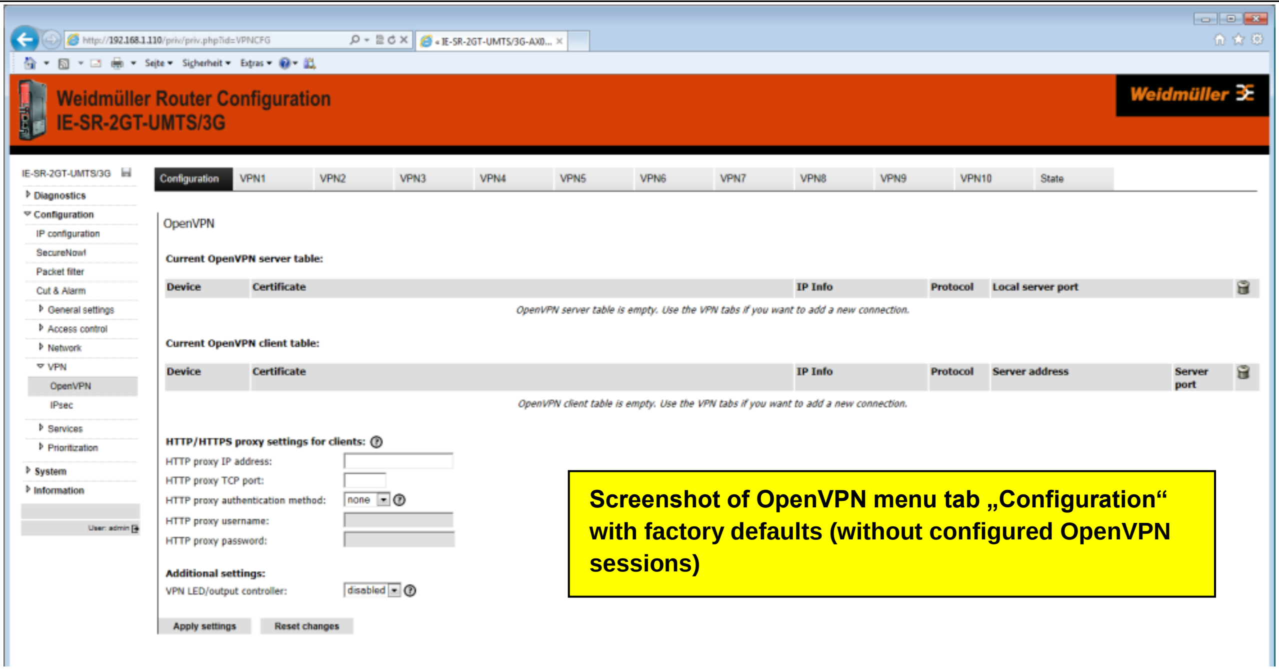
Ethernet

LAN link mode: automatic

WAN link mode: automatic

Figure 34: Configuration → Network → Ethernet → Tab „Configuration“

Setting the transmission parameters of the LAN / WAN hardware interfaces.



OpenVPN

Current OpenVPN server table:

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

Current OpenVPN client table:

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

HTTP/HTTPS proxy settings for clients:

HTTP proxy IP address:
HTTP proxy TCP port:
HTTP proxy authentication method: none
HTTP proxy username:
HTTP proxy password:

Additional settings:

VPN LED/output controller: disabled

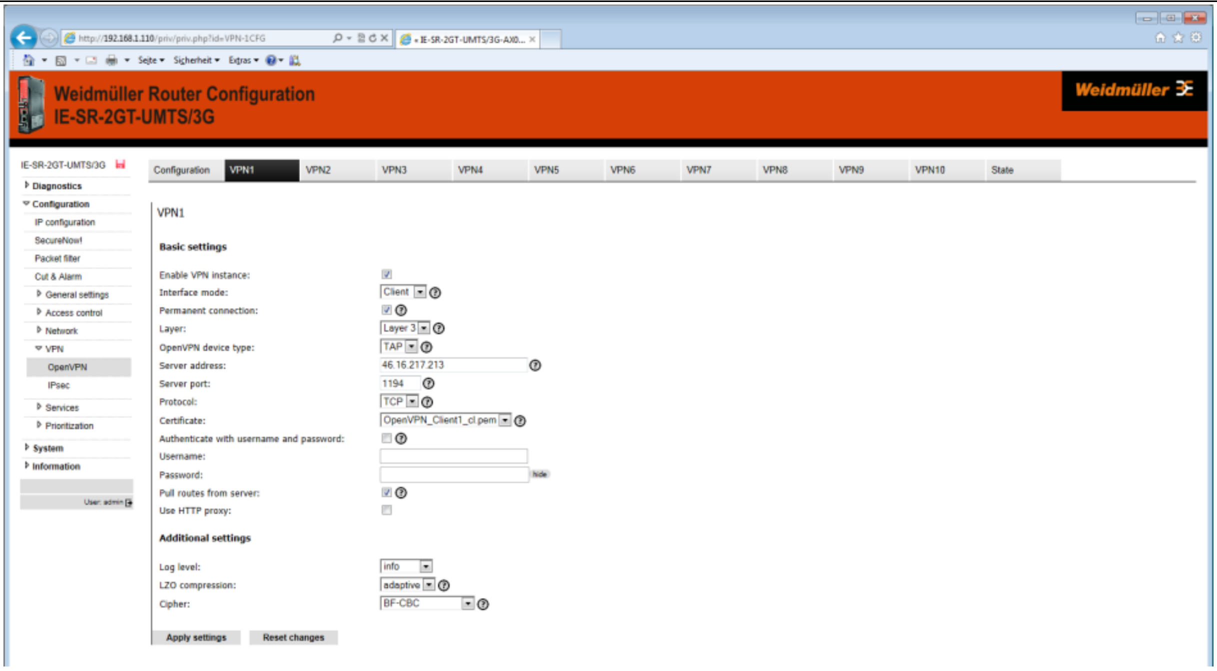
Screenshot of OpenVPN menu tab „Configuration“ with factory defaults (without configured OpenVPN sessions)

Figure 35: Configuration → VPN → OpenVPN → Tab „Configuration“

The OpenVPN menu allows to create and establish virtual private network connections based on the OpenVPN 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).



VPN1

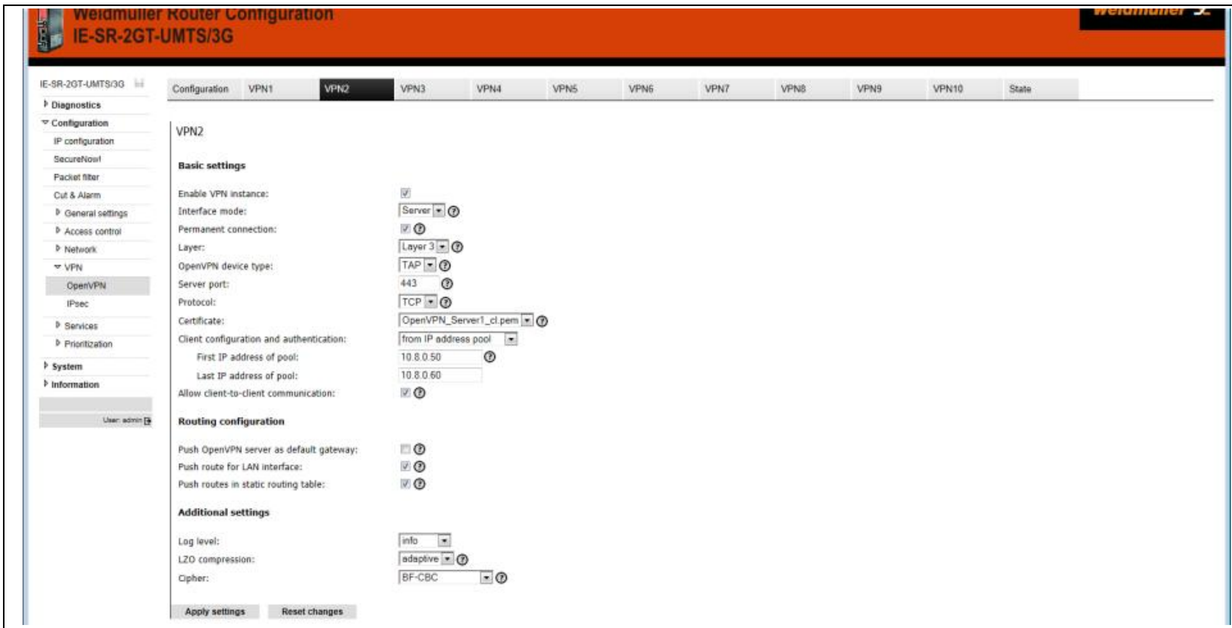
Basic settings

Enable VPN instance: ☑
Interface mode: Client
Permanent connection: ☑
Layer: Layer 3
OpenVPN device type: TAP
Server address: 46.16.217.213
Server port: 1194
Protocol: TCP
Certificate: OpenVPN_Client1_cl.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

Figure 36: Configuration → VPN → OpenVPN → Tab „VPN1“
Screenshot of a configured OpenVPN-Client at tab VPN1



VPN2

Basic settings

Enable VPN instance: ☑
Interface mode: Server
Permanent connection: ☑
Layer: Layer 3
OpenVPN device type: TAP
Server port: 443
Protocol: TCP
Certificate: OpenVPN_Server1_cl.pem
Client configuration and authentication: from IP address pool
First IP address of pool: 10.8.0.50
Last IP address of pool: 10.8.0.60
Allow client-to-client communication: ☑

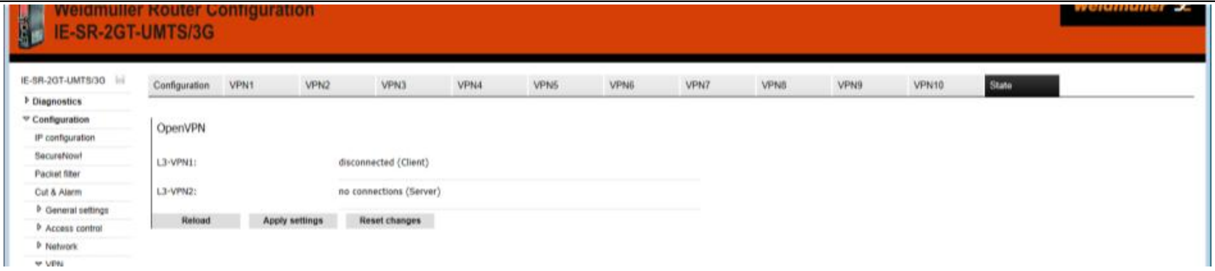
Routing configuration

Push OpenVPN server as default gateway: ☐
Push route for LAN interface: ☑
Push routes in static routing table: ☑

Additional settings

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

Figure 37: Configuration → VPN → OpenVPN → Tab „VPN2“
Screenshot of a configured OpenVPN-Server at tab VPN2.

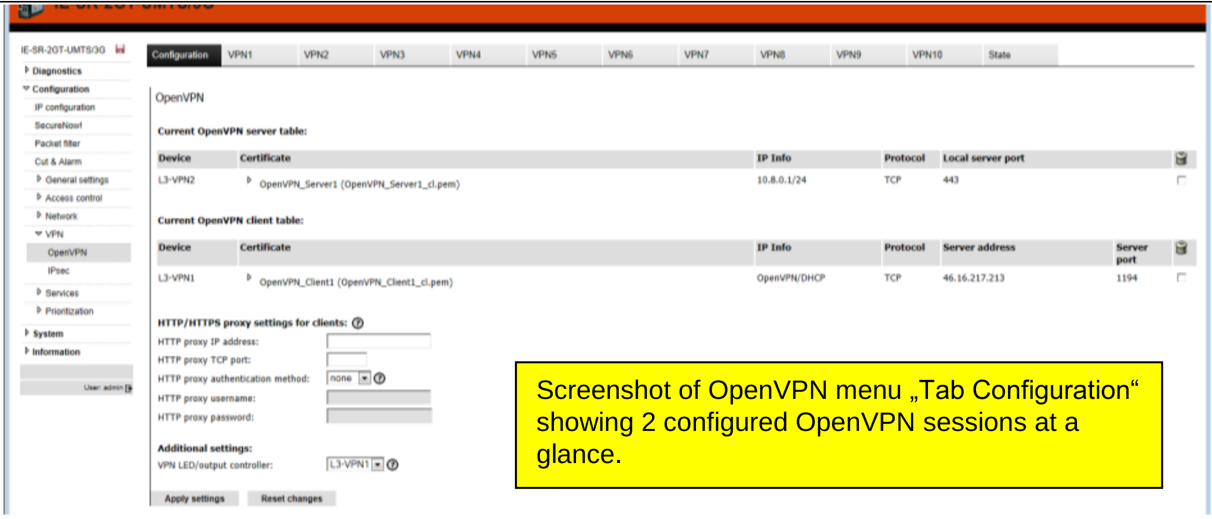


OpenVPN

L3-VPN1: disconnected (Client)
L3-VPN2: no connections (Server)

Figure 38: Configuration → VPN → OpenVPN→ Tab “State”

This screenshot is displaying the status of a configured OpenVPN-Client session (L3, VPN1, currently disconnected) and an OpenVPN-Server session (L3, VPN2, currently no connected remote clients).



OpenVPN

Current OpenVPN server table:

Device	Certificate	IP Info	Protocol	Local server port	
L3-VPN2	OpenVPN_Server1 (OpenVPN_Server1_cl.pem)	10.8.0.1/24	TCP	443	☐

Current OpenVPN client table:

Device	Certificate	IP Info	Protocol	Server address	Server port	
L3-VPN1	OpenVPN_Client1 (OpenVPN_Client1_cl.pem)	OpenVPN/DHCP	TCP	46.16.217.213	1194	☐

HTTP/HTTPS proxy settings for clients:
HTTP proxy IP address:
HTTP proxy TCP port:
HTTP proxy authentication method: none
HTTP proxy username:
HTTP proxy password:

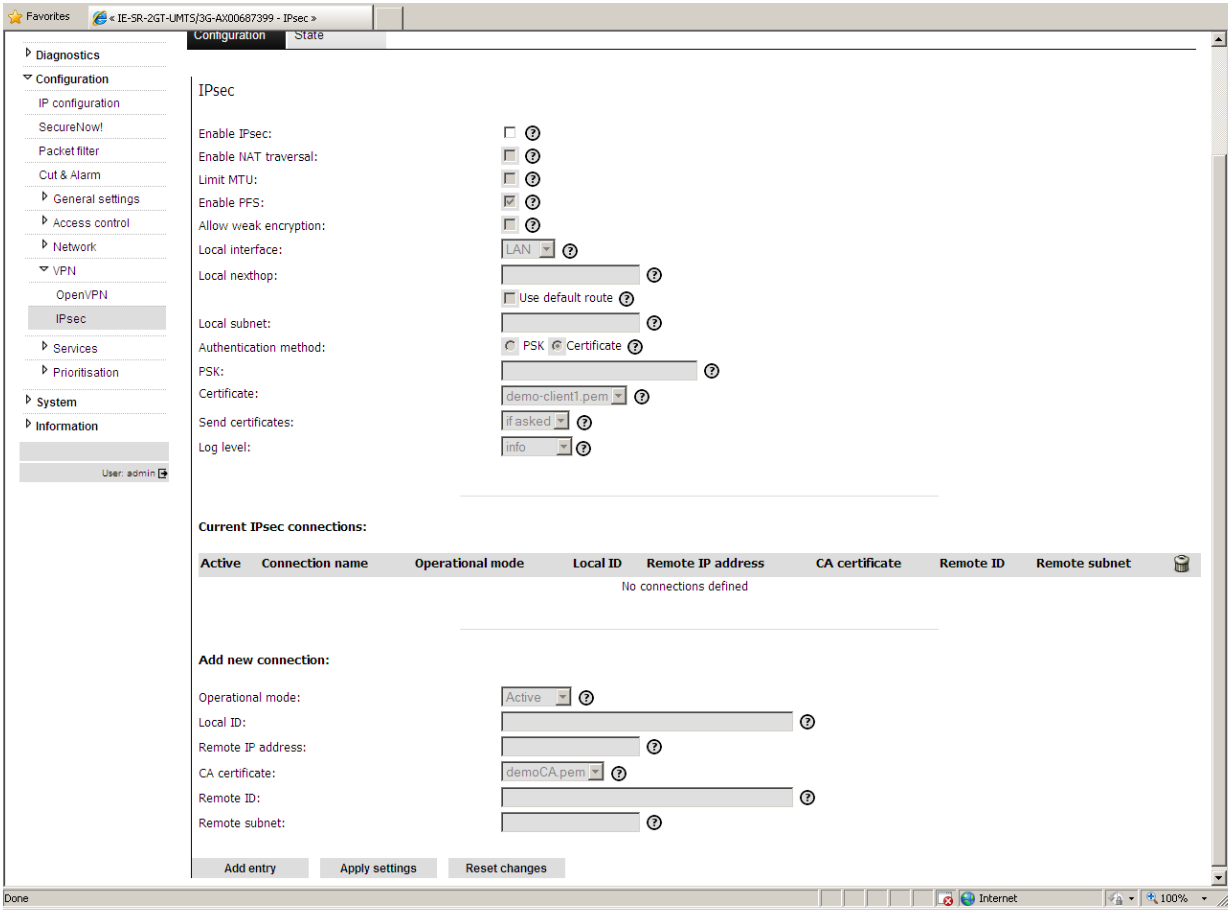
Additional settings:
VPN LED/output controller: L3-VPN1

Screenshot of OpenVPN menu „Tab Configuration“ showing 2 configured OpenVPN sessions at a glance.

Figure 39: Configuration → VPN → OpenVPN→ Tab “Configuration”

After configuration of OpenVPN sessions the configured connected will be displayed at a glance in this menu.

How to configure OpenVPN connections please refer to Appendix B (Link to technical documents about OpenVPN based remote access scenarios).



IPsec

Enable IPsec: □
Enable NAT traversal: □
Limit MTU: □
Enable PFS: ☑
Allow weak encryption: □
Local interface: LAN
Local nexthop:
□ Use default route
Local subnet:
Authentication method: ○ PSK ● Certificate
PSK:
Certificate: demo-client1.pem
Send certificates: if asked
Log level: info

Current IPsec connections:

Active	Connection name	Operational mode	Local ID	Remote IP address	CA certificate	Remote ID	Remote subnet
No connections defined							

Add new connection:

Operational mode: Active
Local ID:
Remote IP address:
CA certificate: demoCA.pem
Remote ID:
Remote subnet:

Add entry | Apply settings | Reset changes

Figure 40: Configuration → VPN → IPsec → Tab „Configuration“

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.

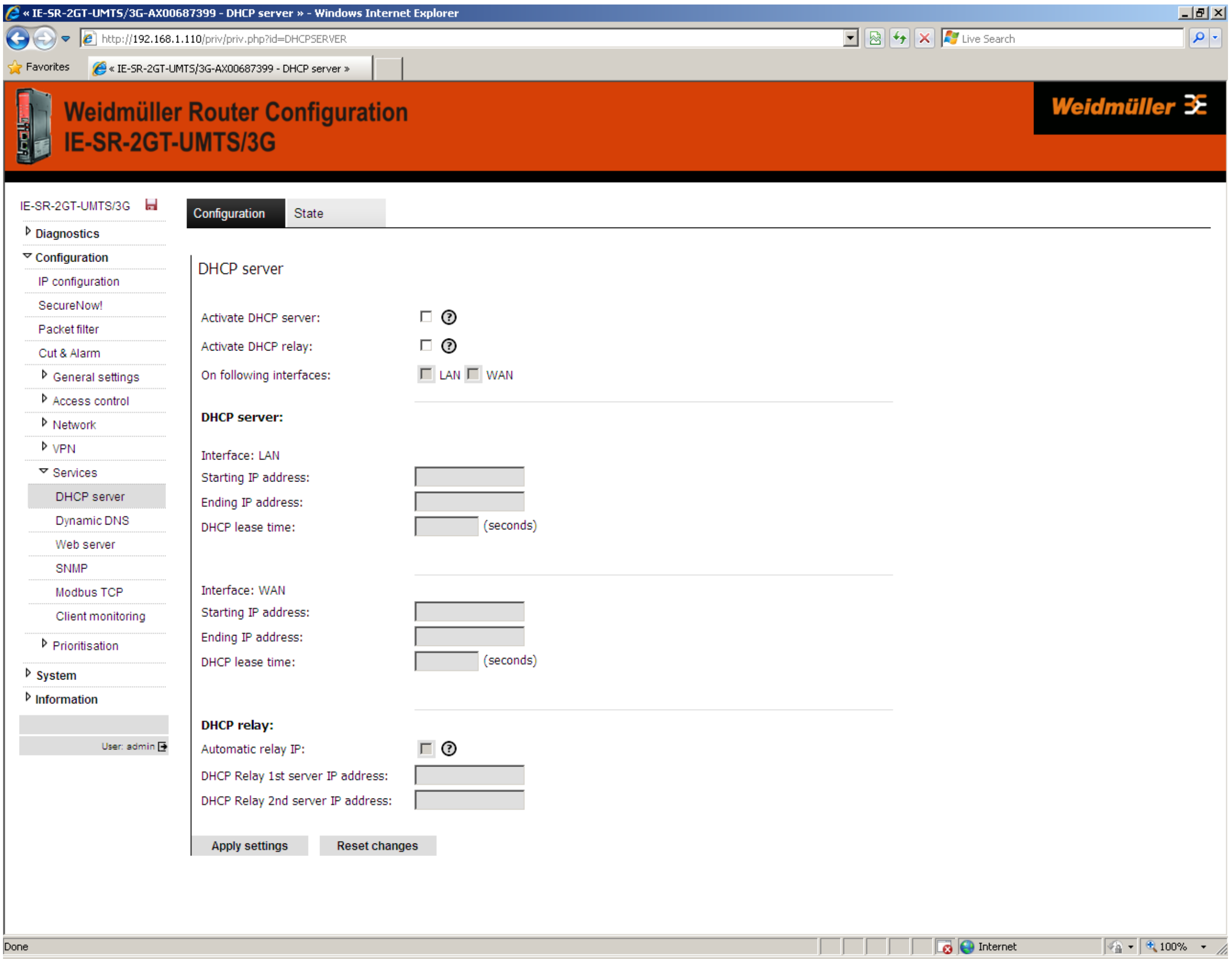
IPsec allows the encryption of the complete communication flow between the Router and a remote site on IP level. IPsec provides encryption of subnets, which are located behind the respective VPN peers.

IPsec connections can be used with both PSK encryption (pre-shared key using user name and password) as well as certificate based encryption.
Implemented IPsec features:

Key exchange:	IKE (Internet Key Exchange) basedon ISAKMP (Internet Security Association and Key Management Protocol)
IKE-Phases:	Main-Mode (Phase 1) and Quick-Mode (Phase 2)
Authentication:	X.509-certificates or Pre-shared-key
DH groups:	DH group 1 MODP 768, DH group 2 MODP 1024, DH group 5 MODP 1536
Data integrity:	MD5 (128bit), SHA1 (160bit)
Encoding:	DES (64bit), 3DES (192bit), AES (128bit), AES (192bit), AES (256bit)

Integrated hardware-based encoding
Ipsec mode: ESP tunnel
Maximum number of Ipsec connections: 64
NAT-Traversal: Yes
Dead-Peer-Detection: Yes

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!



DHCP server

Activate DHCP server: □

Activate DHCP relay: □

On following interfaces: □ LAN □ WAN

DHCP server:

Interface: LAN

Starting IP address:

Ending IP address:

DHCP lease time: (seconds)

Interface: WAN

Starting IP address:

Ending IP address:

DHCP lease time: (seconds)

DHCP relay:

Automatic relay IP: □

DHCP Relay 1st server IP address:

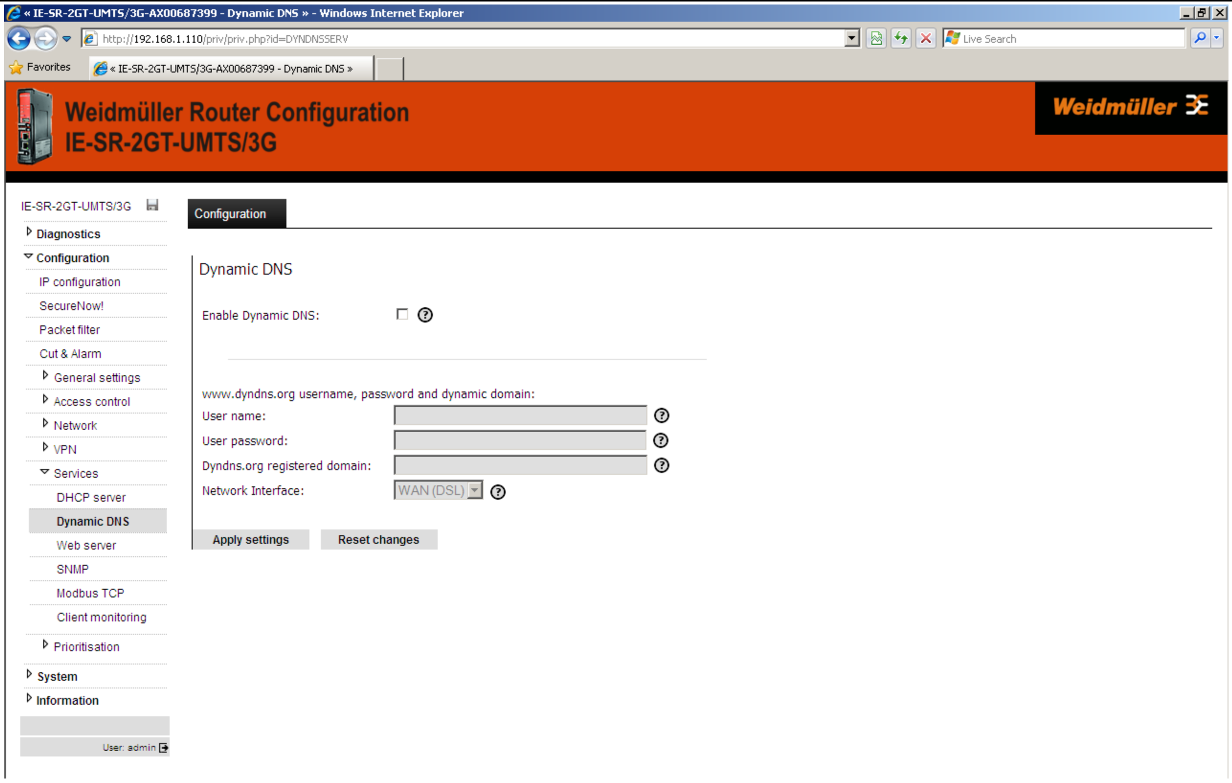
DHCP Relay 2nd server IP address:

Figure 41: Configuration → Services → DHCP Server → Tab „Configuration“

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 (factory settings) the DHCP server is switched off.

Note:
The range of the IP addresses – which will be allocated to connecting DHCP clients - must be in the same range as the IP address of the Router interface (LAN or WAN).

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.



Dynamic DNS

Enable Dynamic DNS: □

www.dyndns.org username, password and dynamic domain:

User name:

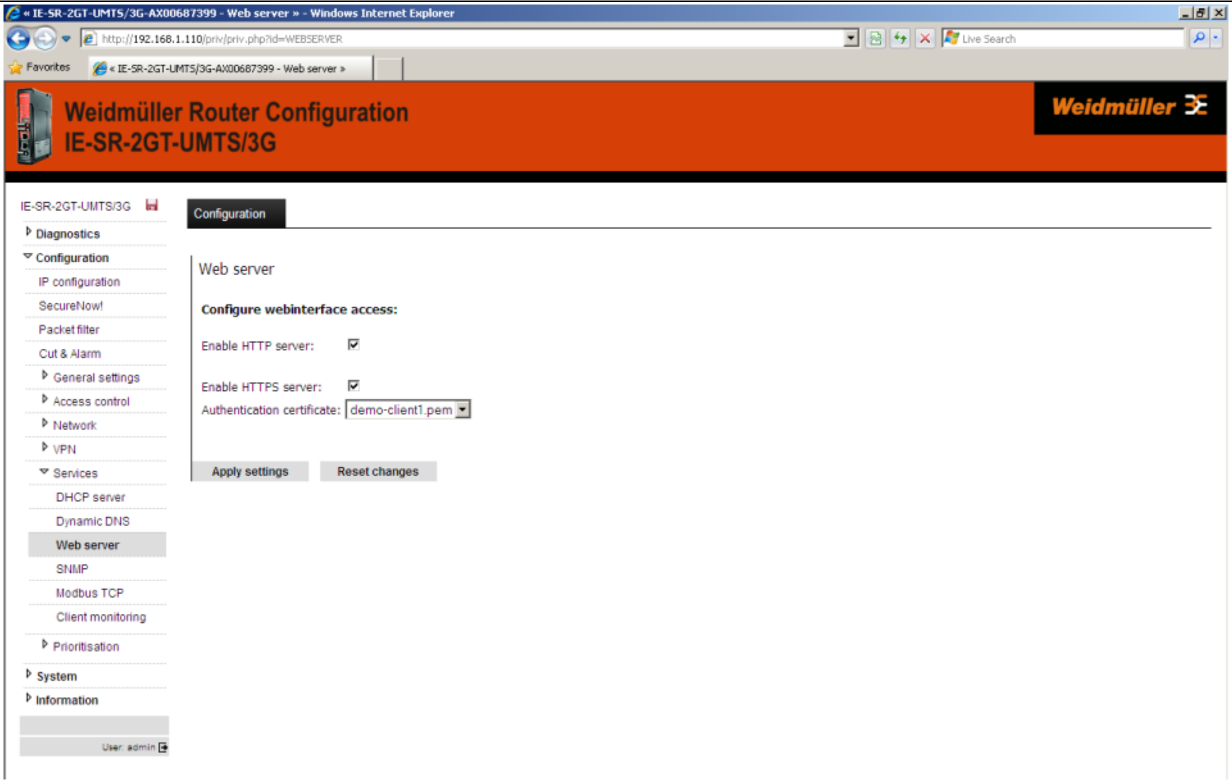
User password:

Dyndns.org registered domain:

Network Interface: WAN (DSL)

Figure 42: Configuration → Services → Dynamic DNS → Tab „Configuration“

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“.



Web server

Configure webinterface access:

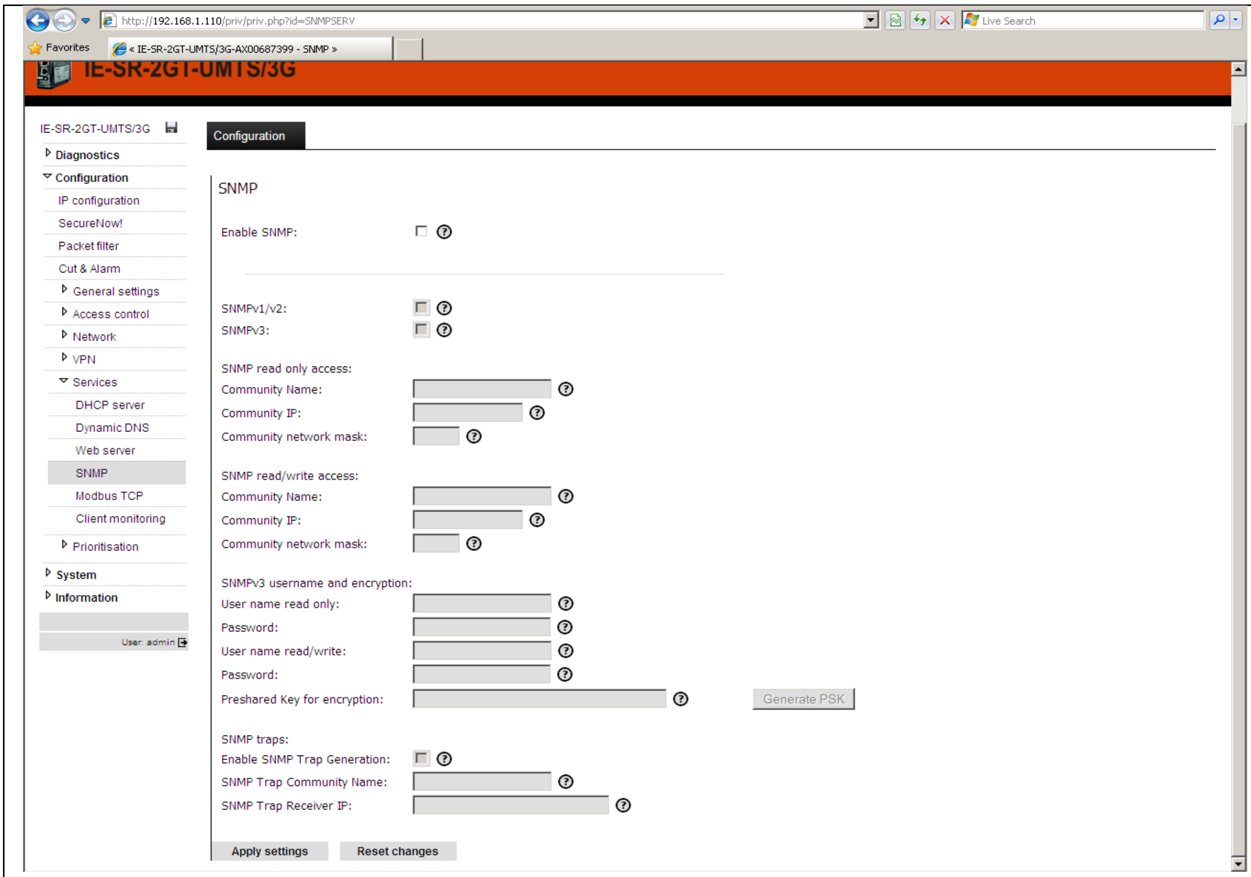
Enable HTTP server: ☑

Enable HTTPS server: ☑

Authentication certificate: demo-client1.pem

Figure 43: Configuration → Services → Web server → Tab „Configuration“

Via this menu item the access protocol to the Web interface (http or https) can be configured.



IE-SR-2GT-UMTS/3G

Configuration

SNMP

Enable SNMP: □

SNMPv1/v2: □

SNMPv3: □

SNMP read only access:

Community Name:

Community IP:

Community network mask:

SNMP read/write access:

Community Name:

Community IP:

Community network mask:

SNMPv3 username and encryption:

User name read only:

Password:

User name read/write:

Password:

Preshared Key for encryption:

SNMP traps:

Enable SNMP Trap Generation: □

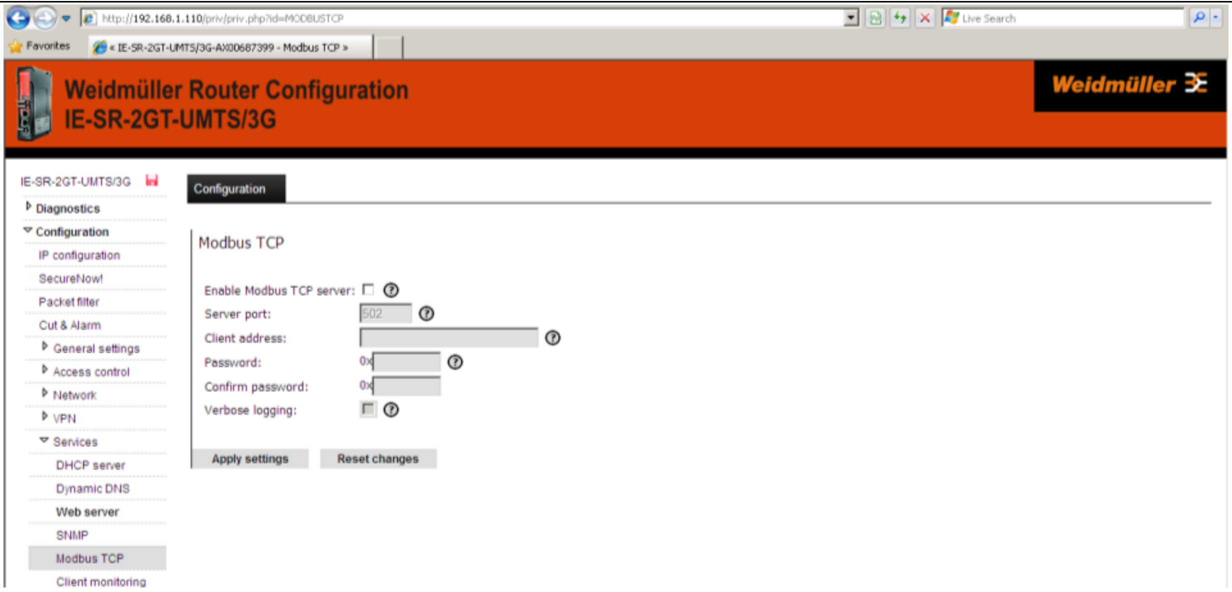
SNMP Trap Community Name:

SNMP Trap Receiver IP:

Figure 44: Configuration → Services → SNMP → Tab „Configuration“

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.

Note: Currently no SNMP-traps are implemented.



Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Configuration

Modbus TCP

Enable Modbus TCP server: □

Server port: 502

Client address:

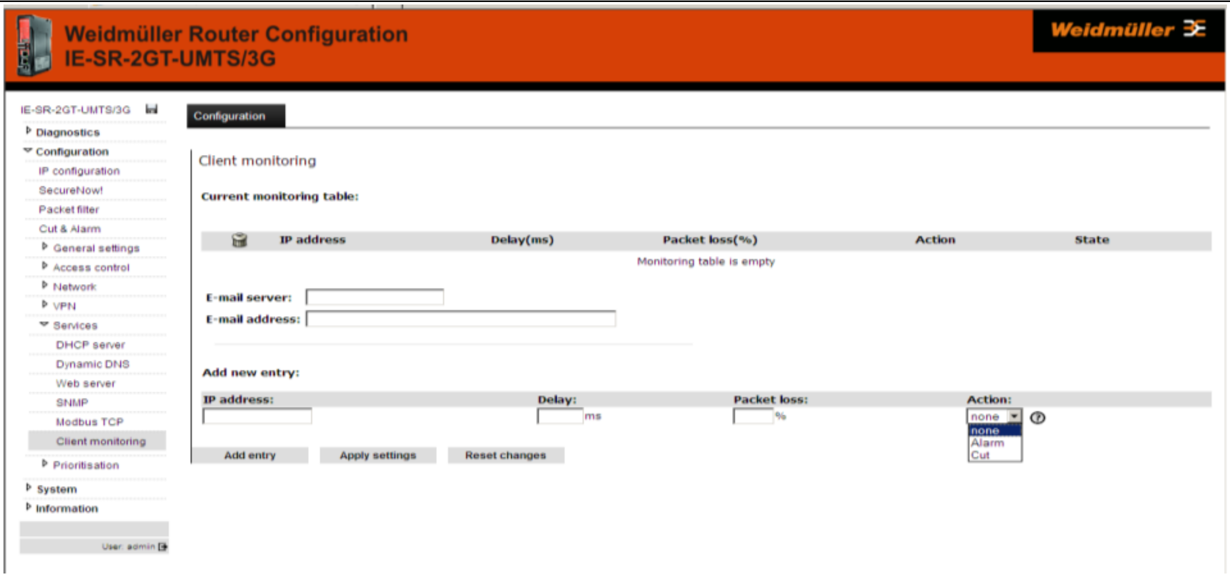
Password: 0x

Confirm password: 0x

Verbose logging: □

Figure 45: Configuration → Services → Modbus TCP → Tab „Configuration“

Activation / deactivation of the integrated ModbusTCP-Server. Allows external Ethernet controllers that understand the ModbusTCP protocol to query Router states and control information. Using the ModbusTCP protocol e.g. VPN connections (IPsec and OpenVPN) can be activated and deactivated. Additionally events like „Cut“ or „Alarm“ can be monitored and reset (acknowledged).



Client monitoring

Current monitoring table:

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

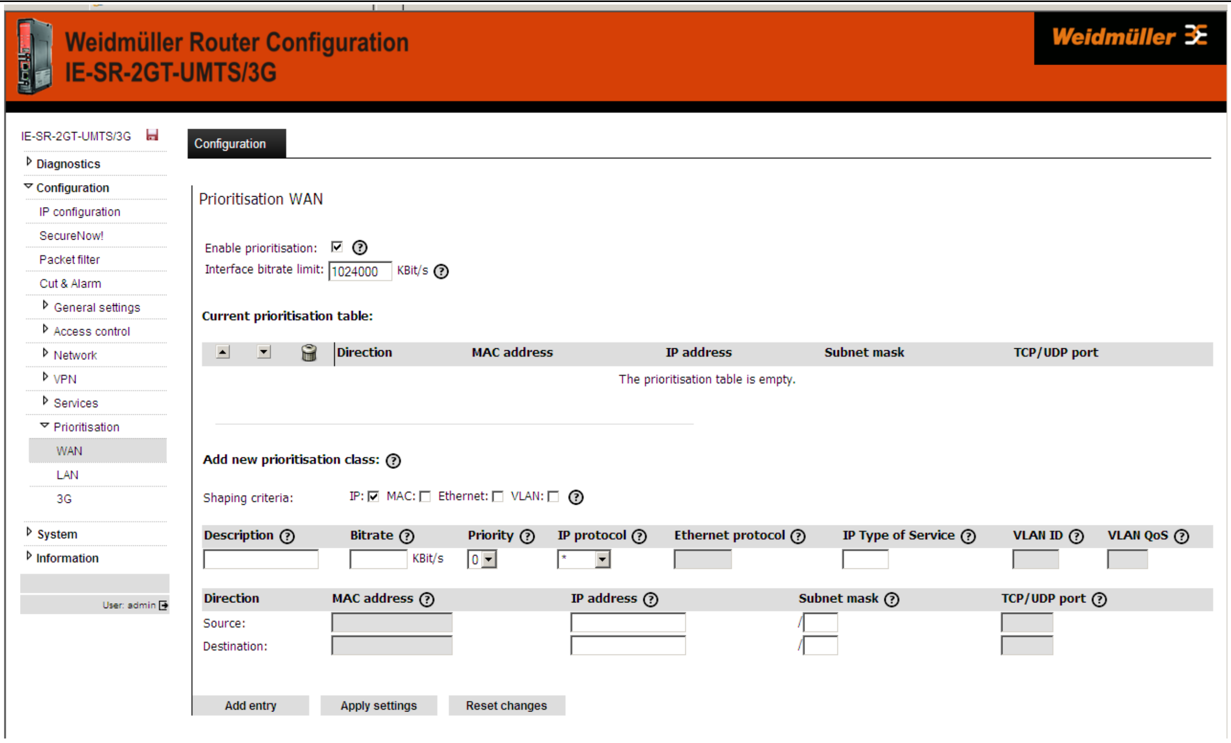
E-mail server:
E-mail address:

Add new entry:

IP address:	Delay:	Packet loss:	Action:
	ms	%	none none Alarm Cut

Figure 46: Configuration → Services → Client Monitoring → Tab „Configuration“

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 a „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.
Fore more detailed information please refer to Appendix C2 (Method 3).



Prioritisation WAN

Enable prioritisation: ☑ ?
Interface bitrate limit: 1024000 KBit/s ?

Current prioritisation table:

▲	▼		Direction	MAC address	IP address	Subnet mask	TCP/UDP port
The prioritisation table is empty.							

Add new prioritisation class: ?

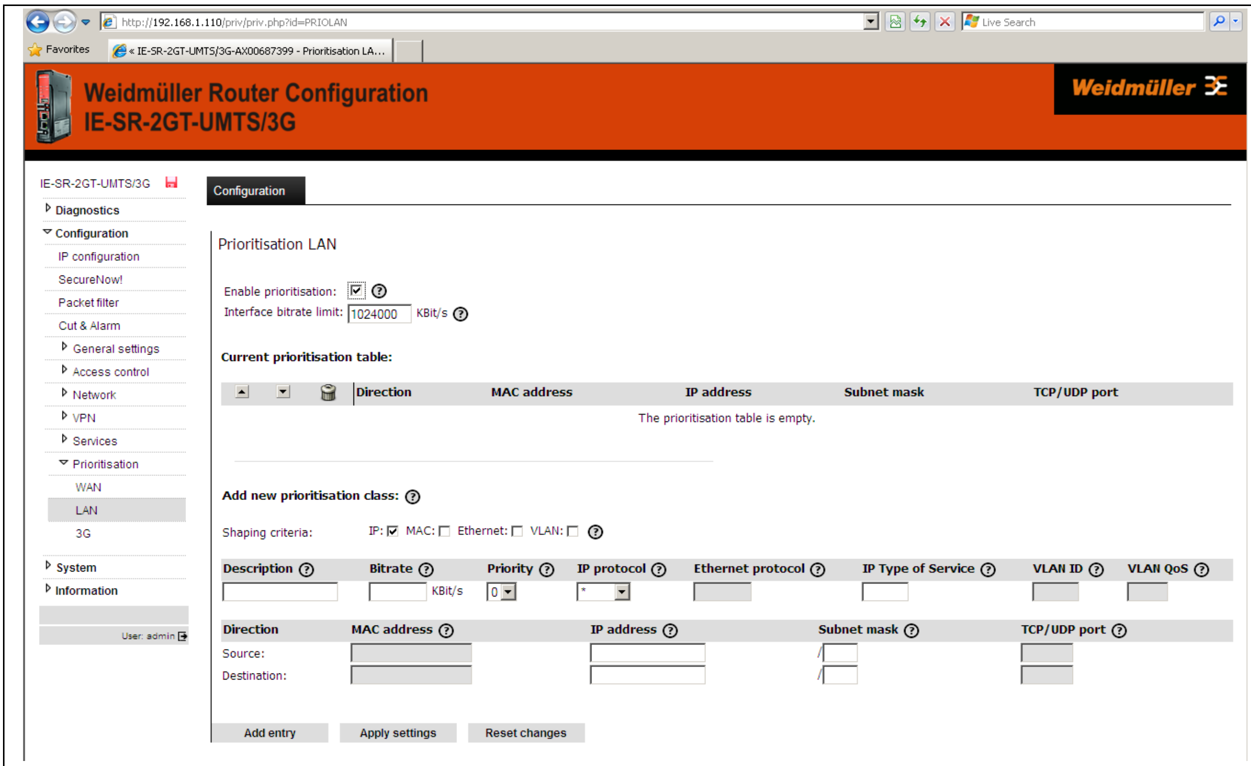
Shaping criteria: IP: ☑ MAC: □ Ethernet: □ VLAN: □ ?

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

Direction	MAC address ?	IP address ?	Subnet mask ?	TCP/UDP port ?
Source:			/	
Destination:			/	

Figure 47: Configuration → Prioritization → WAN → Tab „Configuration“

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).



Prioritisation LAN

Enable prioritisation: ☑

Interface bitrate limit: 1024000 KBit/s

Current prioritisation table:

			Direction	MAC address	IP address	Subnet mask	TCP/UDP port

The prioritisation table is empty.

Add new prioritisation class:

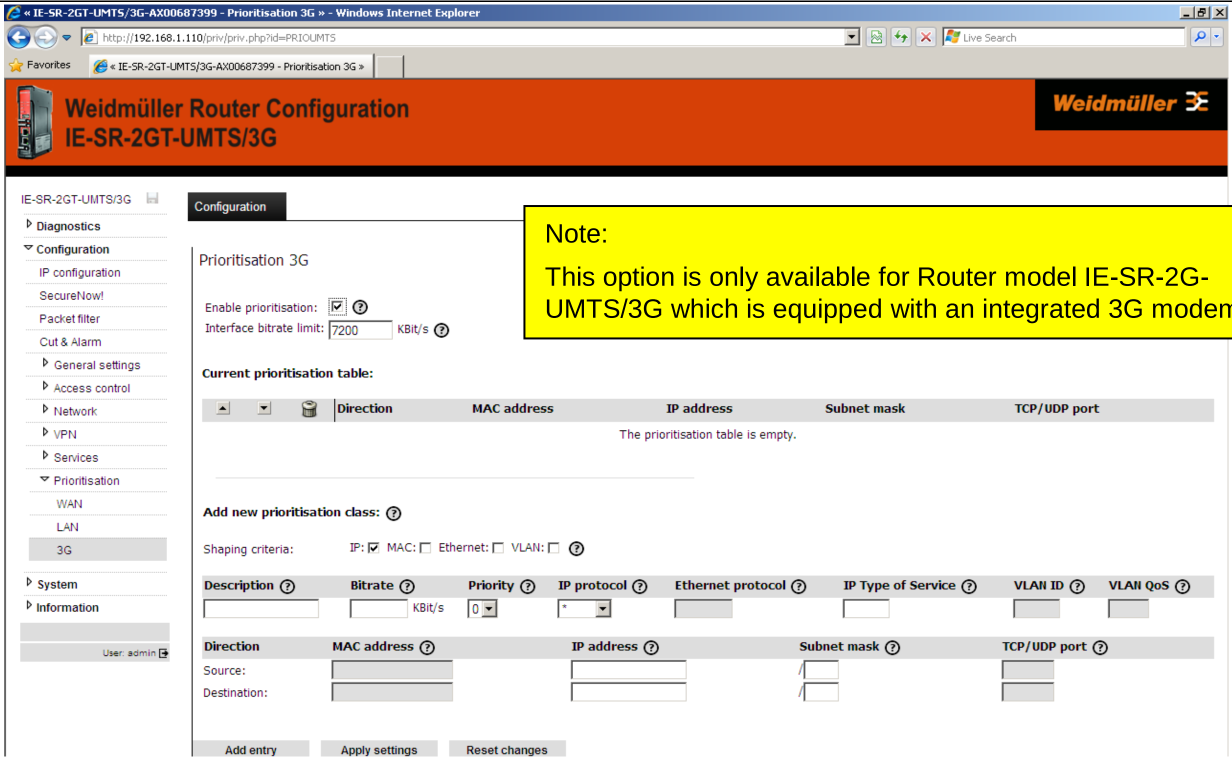
Shaping criteria: IP: ☑ MAC: □ Ethernet: □ VLAN: □

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

Direction	MAC address	IP address	Subnet mask	TCP/UDP port
Source:			/	
Destination:			/	

Figure 48: Configuration → Prioritization → LAN → Tab „Configuration“

With this feature **outgoing** traffic on the **LAN** 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).



Note:

This option is only available for Router model IE-SR-2G-UMTS/3G which is equipped with an integrated 3G modem.

Prioritisation 3G

Enable prioritisation: ☑

Interface bitrate limit: 7200 KBit/s

Current prioritisation table:

			Direction	MAC address	IP address	Subnet mask	TCP/UDP port

The prioritisation table is empty.

Add new prioritisation class:

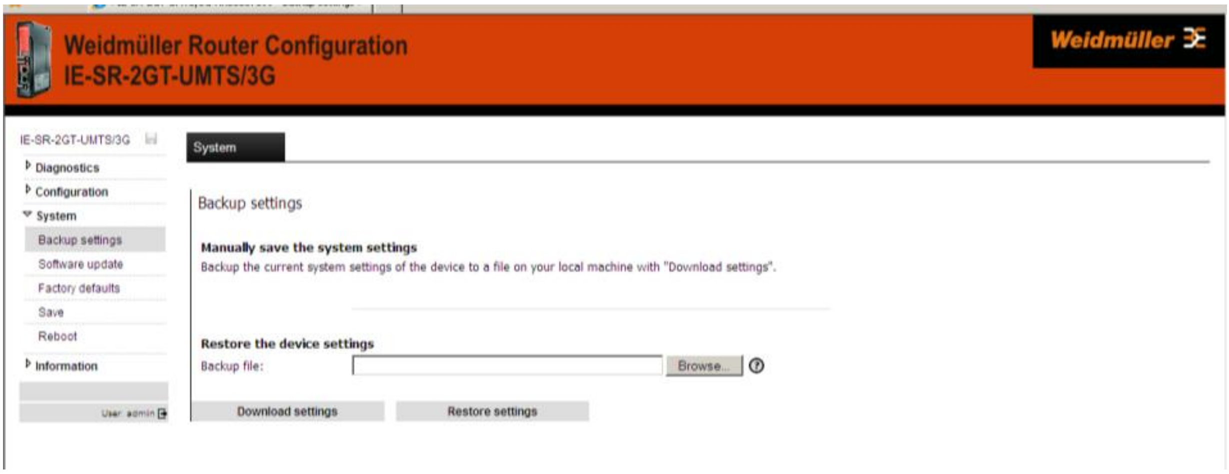
Shaping criteria: IP: ☑ MAC: □ Ethernet: □ VLAN: □

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

Direction	MAC address	IP address	Subnet mask	TCP/UDP port
Source:			/	
Destination:			/	

Figure 49: Configuration → Prioritization → 3G → Tab „Configuration“

With this feature **outgoing** traffic on the **3G wireless 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).



Backup settings

Manually save the system settings

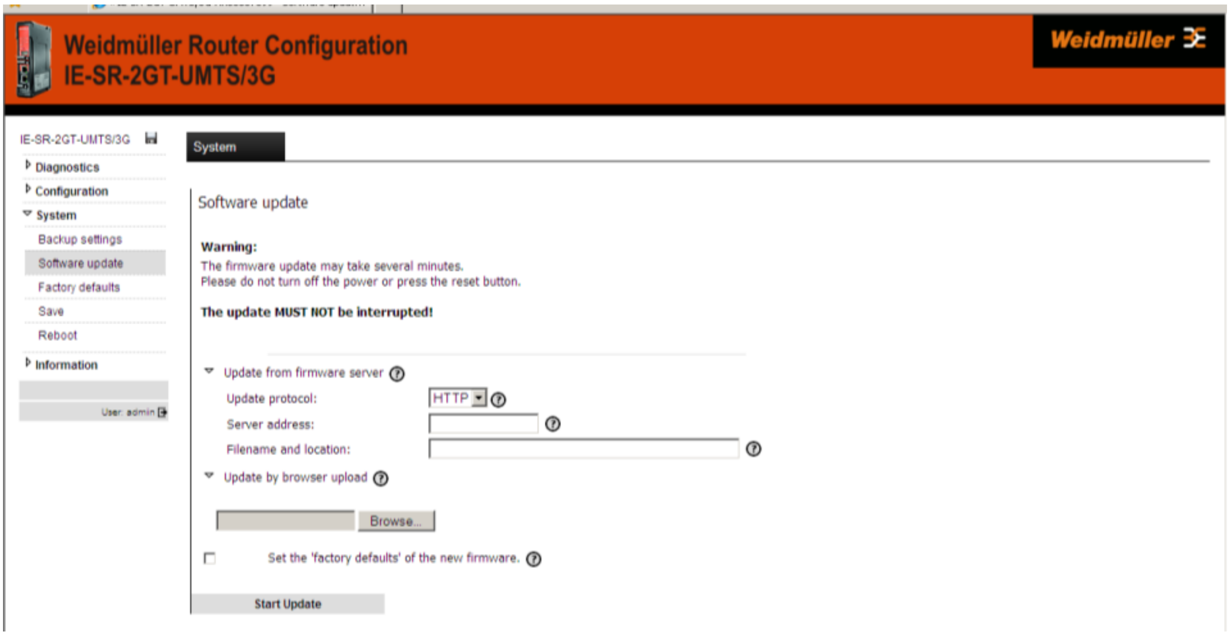
Backup the current system settings of the device to a file on your local machine with "Download settings".

Restore the device settings

Backup file:

Figure 50: System → Backup settings → Tab „System“

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.



Software update

Warning:
The firmware update may take several minutes.
Please do not turn off the power or press the reset button.

The update MUST NOT be interrupted!

Update from firmware server

Update protocol: HTTP

Server address:

Filename and location:

Update by browser upload

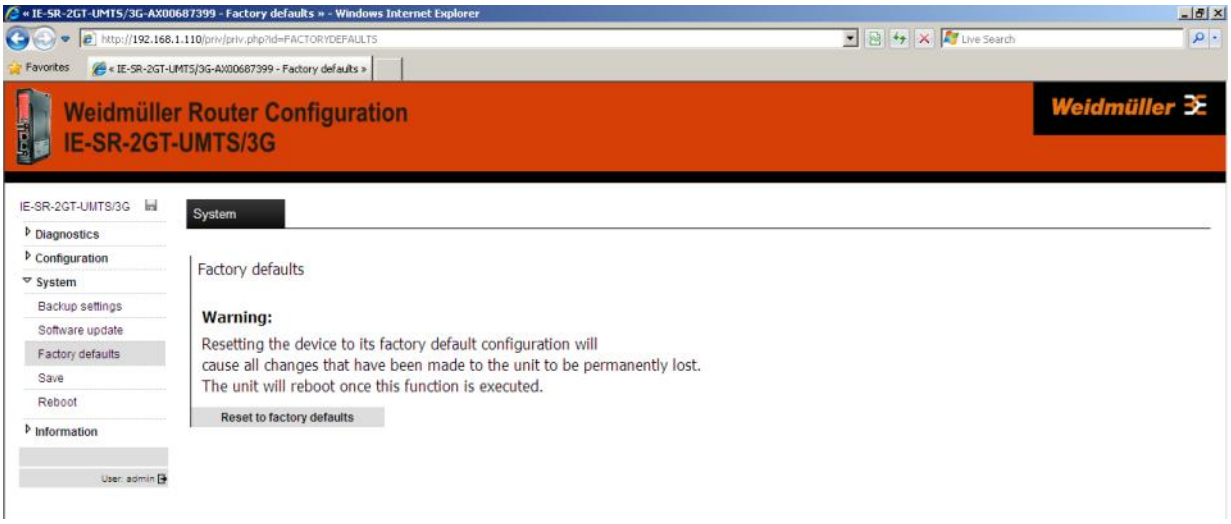
□ Set the 'factory defaults' of the new firmware.

Figure 51: System → Software update → Tab „System“

With this menu item a firmware update can be carried out.

The firmware update can be done via a FTP, TFTP or HTTP server or by a browser upload getting the firmware file directly from the connected configuration PC.
The easiest way to update the Router with a new firmware is to use the function „Update by browser upload“.

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.



« IE-SR-2GT-UMTS/3G-AX00687399 - Factory defaults » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=FACTORYDEFAULTS

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Factory defaults

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

Reset to factory defaults

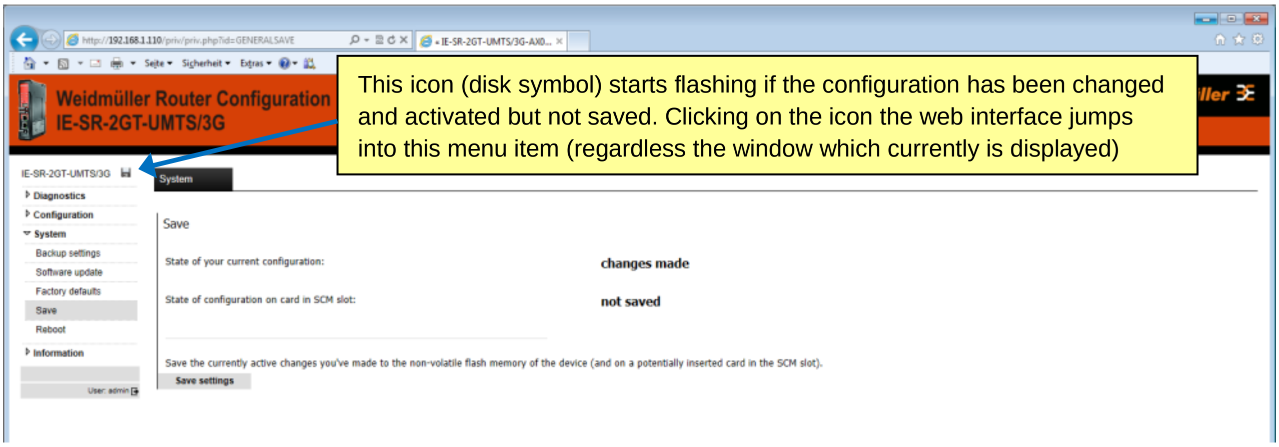
Figure 52: System → Factory defaults → Tab „System“

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>

IP address LAN port :	192.168.1.110
IP address WAN port :	192.168.2.110
User name :	admin
Password :	Detmold



http://192.168.1.110/priv/priv.php?id=GENERALSAVE

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

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)

Save

State of your current configuration: **changes made**

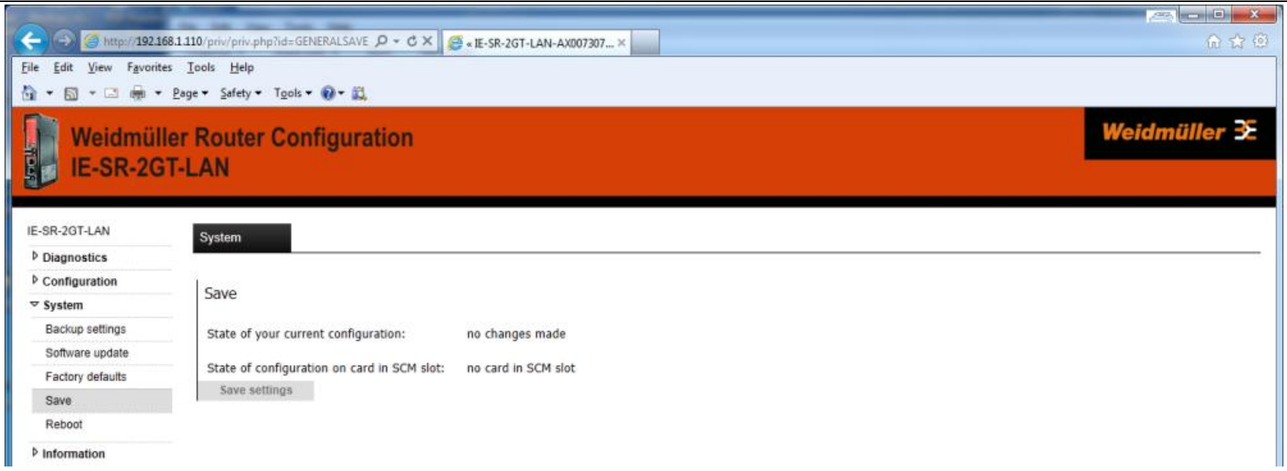
State of configuration on card in SCM slot: **not saved**

Save the currently active changes you've made to the non-volatile flash memory of the device (and on a potentially inserted card in the SCM slot).

Save settings

Figure 53: System → Save → Tab „System“ (Screenshot of Router **with** inserted SIM memory card)

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.



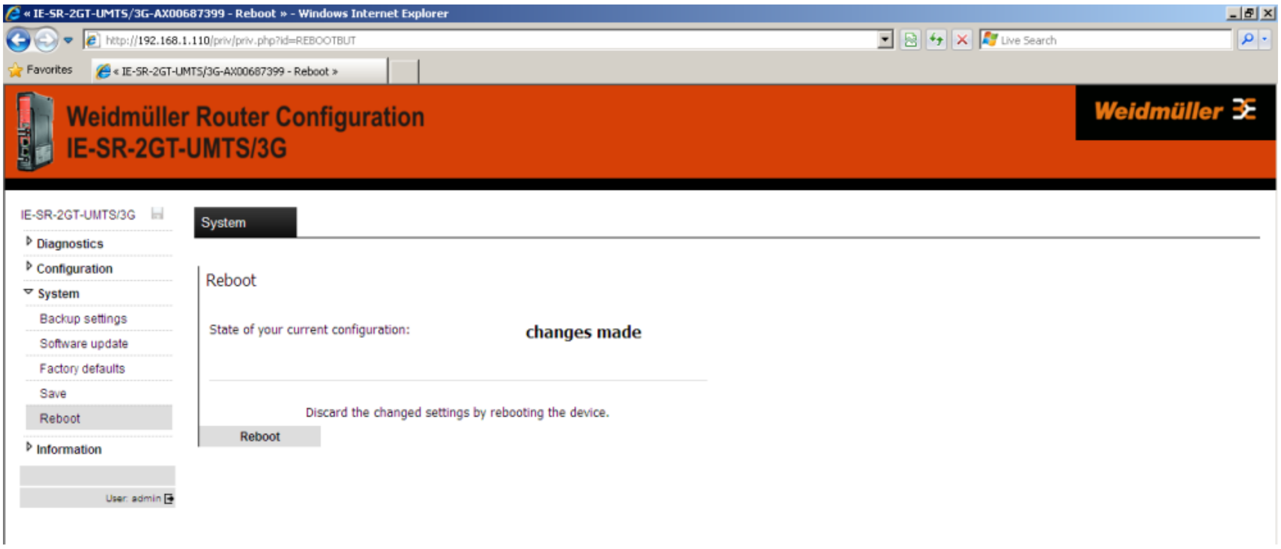
Save

State of your current configuration: no changes made

State of configuration on card in SCM slot: no card in SCM slot

Save settings

Figure 54: System → Save → Tab „System“ (Screenshot of Router **without** SIM memory card)


« IE-SR-2GT-UMTS/3G-AX00687399 - Reboot » - Windows Internet Explorer
http://192.168.1.110/priv/priv.php?id=REBOOTBUT
Live Search
Favorites
« IE-SR-2GT-UMTS/3G-AX00687399 - Reboot »
Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G
Weidmüller
IE-SR-2GT-UMTS/3G
Diagnostics
Configuration
System
Backup settings
Software update
Factory defaults
Save
Reboot
Information
User: admin
System

Reboot

State of your current configuration: **changes made**

Discard the changed settings by rebooting the device.

Reboot

Figure 55: System → Reboot → Tab „System“

Forcing a reboot of the Router.

The status message indicates whether the current configuration is saved or not.

A. Application scenarios (Uses cases) for Routing, NAT and Firewalling

A1 - Configuring the Router to connect 2 networks with different IP address ranges

This Technical Note applies to the Weidmüller Industrial Router IE-SR-2GT-LAN and IE-SR-2GT-UMTS/3G

Application requirements:

There are 2 industrial Ethernet networks which shall be connected by the Router. Each network has its own IP address range. Every Ethernet node in both networks shall have the possibility to communicate with each other.
No special firewall filter rules shall be configured.

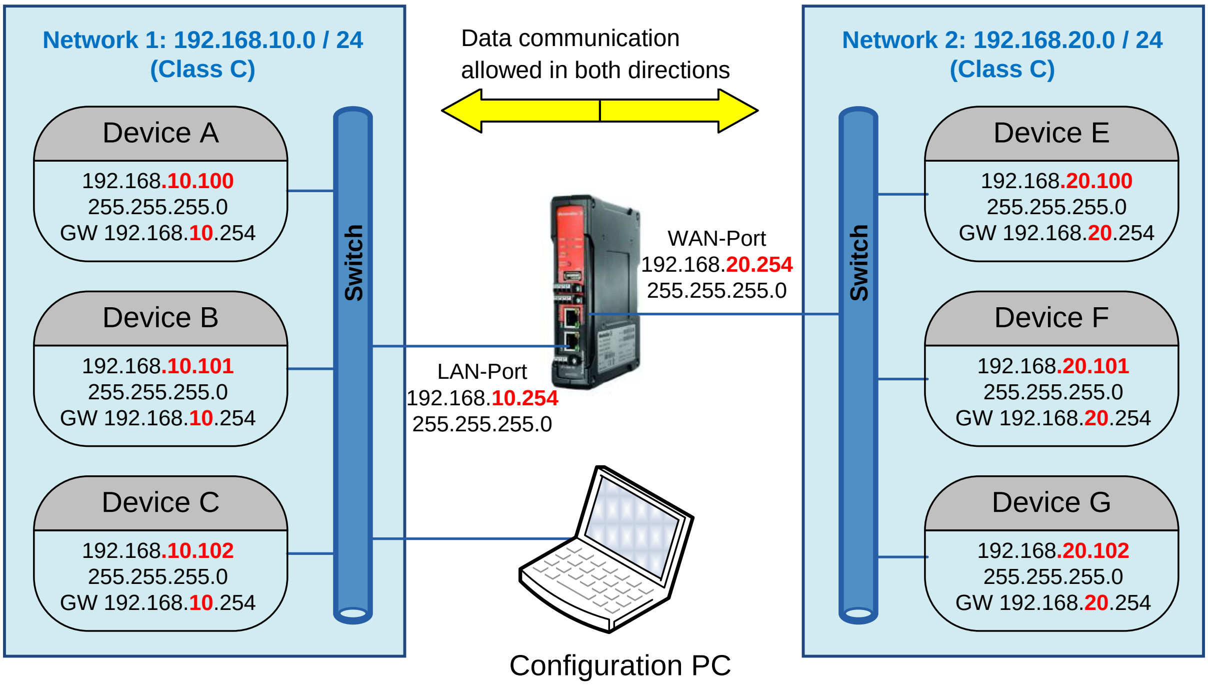
In this example the IP address ranges are set to

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

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).

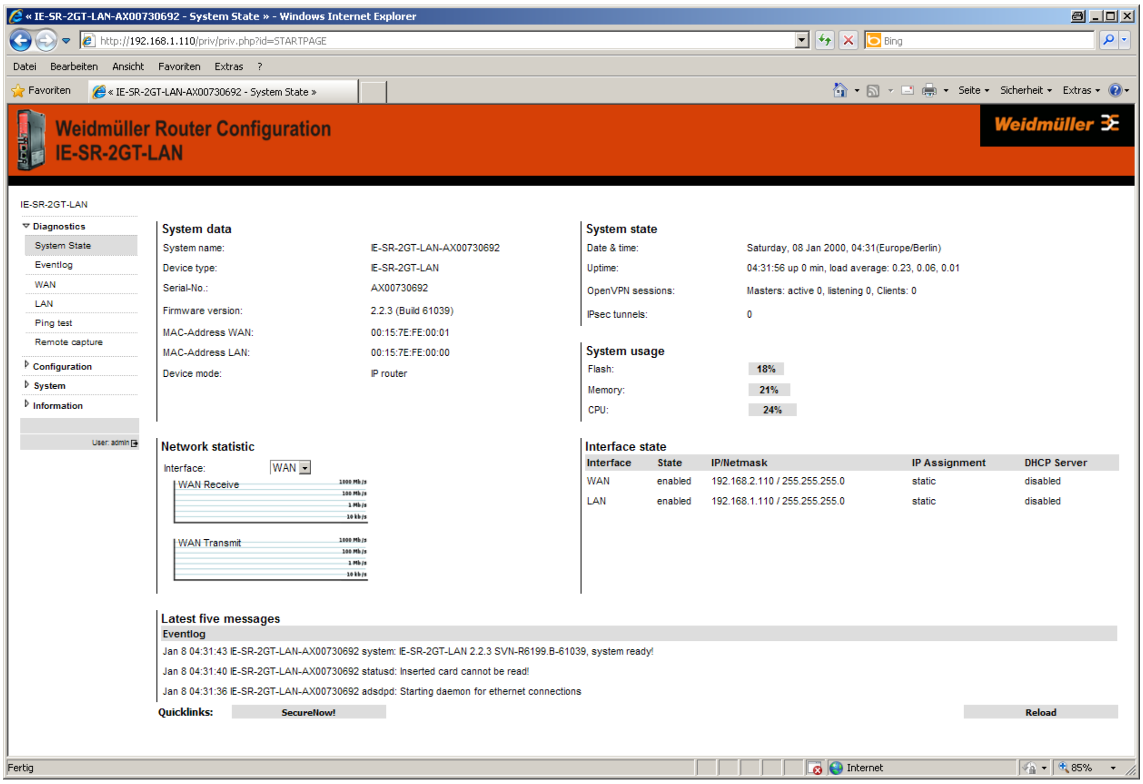
Note: Use autonegotiation on the Ethernet Interface of the PC

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
	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



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:31(Europe/Berlin)
Uptime:	04:31:56 up 0 min, load average: 0.23, 0.06, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	21%
CPU:	24%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled

Latest five messages

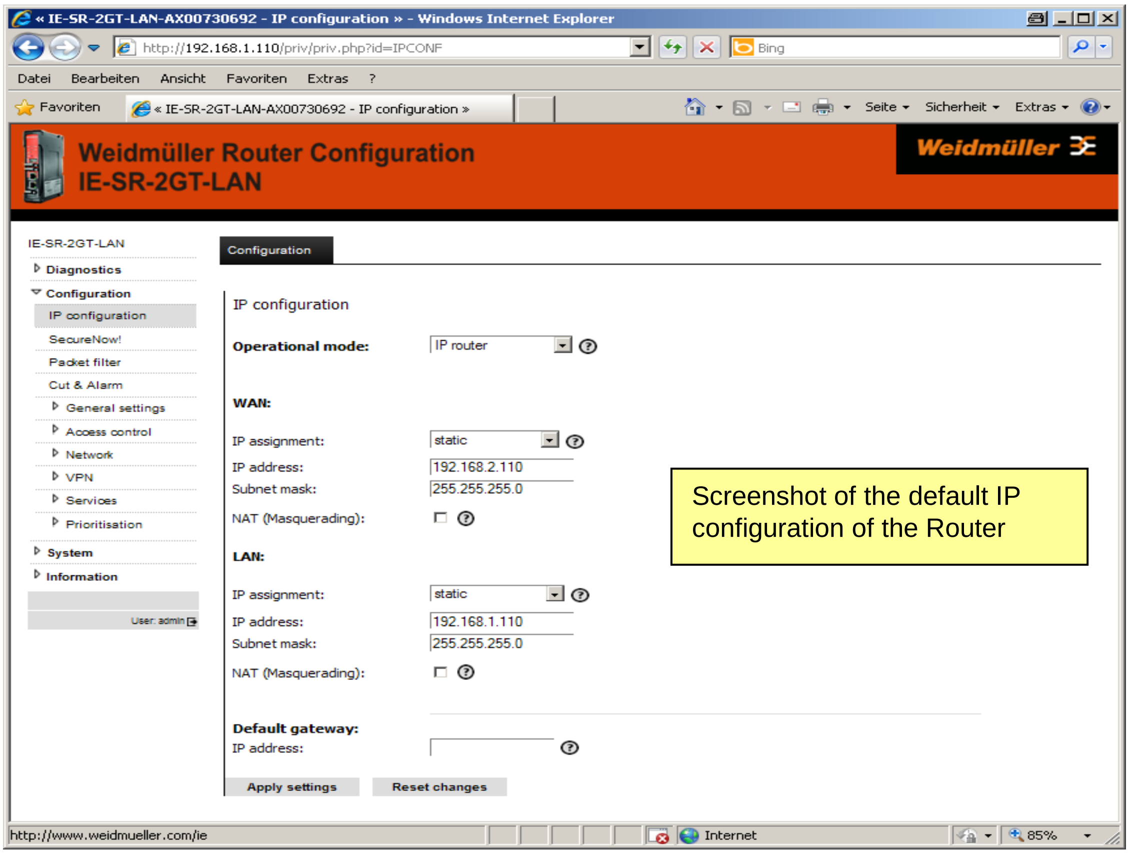
Eventlog

```
Jan 8 04:31:43 IE-SR-2GT-LAN-AX00730692 system: IE-SR-2GT-LAN 2.2.3 SVN-R6199.B-61039, system ready!
Jan 8 04:31:40 IE-SR-2GT-LAN-AX00730692 statusd: Inserted card cannot be read!
Jan 8 04:31:36 IE-SR-2GT-LAN-AX00730692 adsdpd: Starting daemon for ethernet connections
```

Figure A1-1: Login page of the Router (equivalent with menu Diagnostics → System State)

4. Set the basic IP configuration

► Select menu **Configuration → IP configuration**



IP configuration

Operational mode: IP router

WAN:

IP assignment: static
IP address: 192.168.2.110
Subnet mask: 255.255.255.0
NAT (Masquerading): □

LAN:

IP assignment: static
IP address: 192.168.1.110
Subnet mask: 255.255.255.0
NAT (Masquerading): □

Default gateway:
IP address:

Screenshot of the default IP configuration of the Router

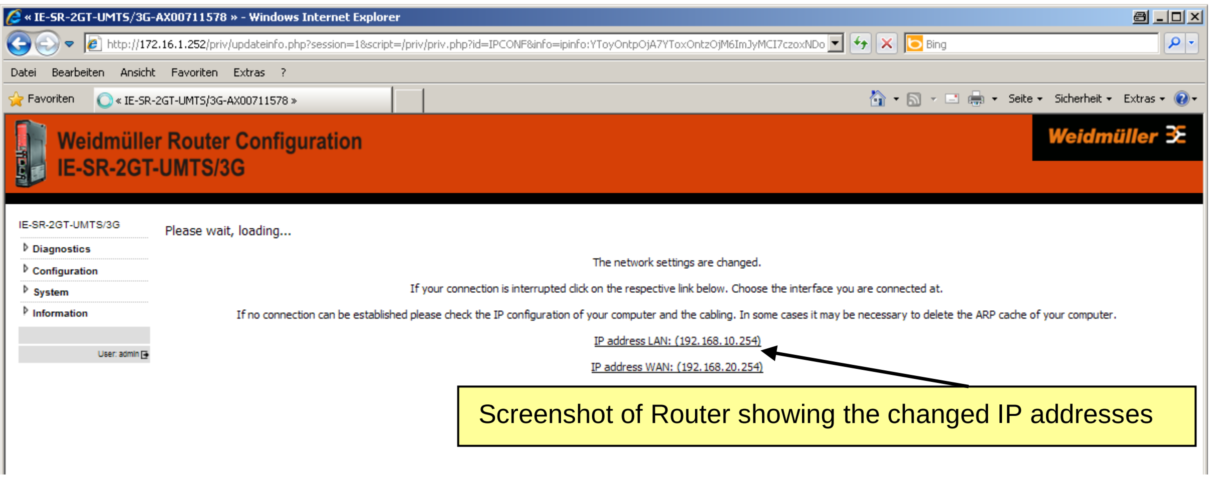
Figure A1-2: Default values of menu **IP configuration**

► 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 (leave checkbox empty)
IP address parameters **LAN** Port:	static
	192.168.**10**.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
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 now have lost the Router connection due to changing the IP address range of your connected LAN port.


« IE-SR-2GT-UMTS/3G-AX00711578 » - Windows Internet Explorer
http://172.16.1.252/priv/updateinfo.php?session=1&script=/priv/priv.php?id=IPCONF&info=ipinfo:YToyOntpOjA7YToxOntzOjM6ImJyMCI7czoxNDo
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G
IE-SR-2GT-UMTS/3G
Diagnostics
Configuration
System
Information
User: admin

Please wait, loading...

The network settings are changed.

If your connection is interrupted click on the respective link below. Choose the interface you are connected at.

If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.

IP address LAN: (192.168.10.254)

IP address WAN: (192.168.20.254)

Screenshot of Router showing the changed IP addresses

Figure A1-3: Display of activated new IP addresses of LAN and WAN port

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

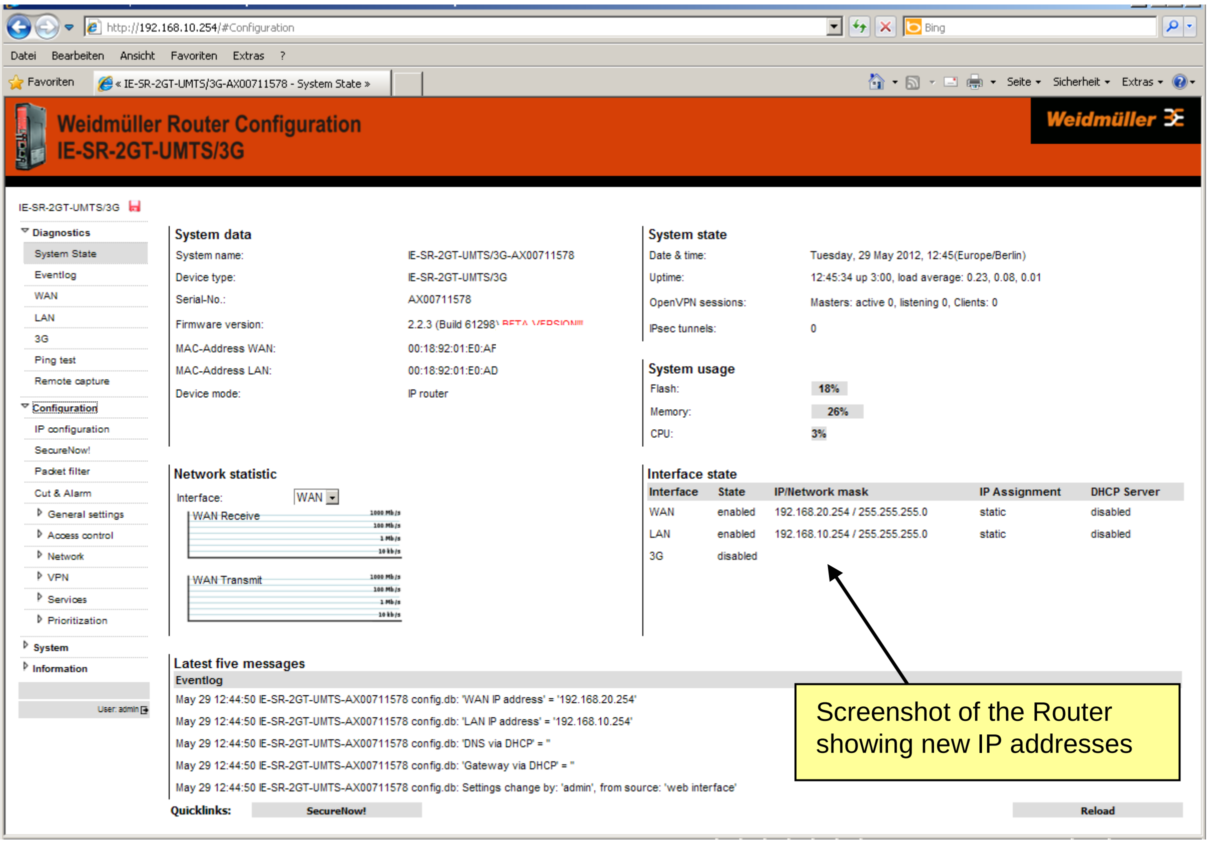
► To reconnect to the Router now set the IP address of the PC to the new values

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



System data

System name:	IE-SR-2GT-UMTS/3G-AX00711578
Device type:	IE-SR-2GT-UMTS/3G
Serial-No.:	AX00711578
Firmware version:	2.2.3 (Build 61298) BETA VERSION!!!
MAC-Address WAN:	00:18:92:01:E0:AF
MAC-Address LAN:	00:18:92:01:E0:AD
Device mode:	IP router

System state

Date & time:	Tuesday, 29 May 2012, 12:45(Europe/Berlin)
Uptime:	12:45:34 up 3:00, load average: 0.23, 0.08, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	26%
CPU:	3%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.20.254 / 255.255.255.0	static	disabled
LAN	enabled	192.168.10.254 / 255.255.255.0	static	disabled
3G	disabled			

Latest five messages

Eventlog

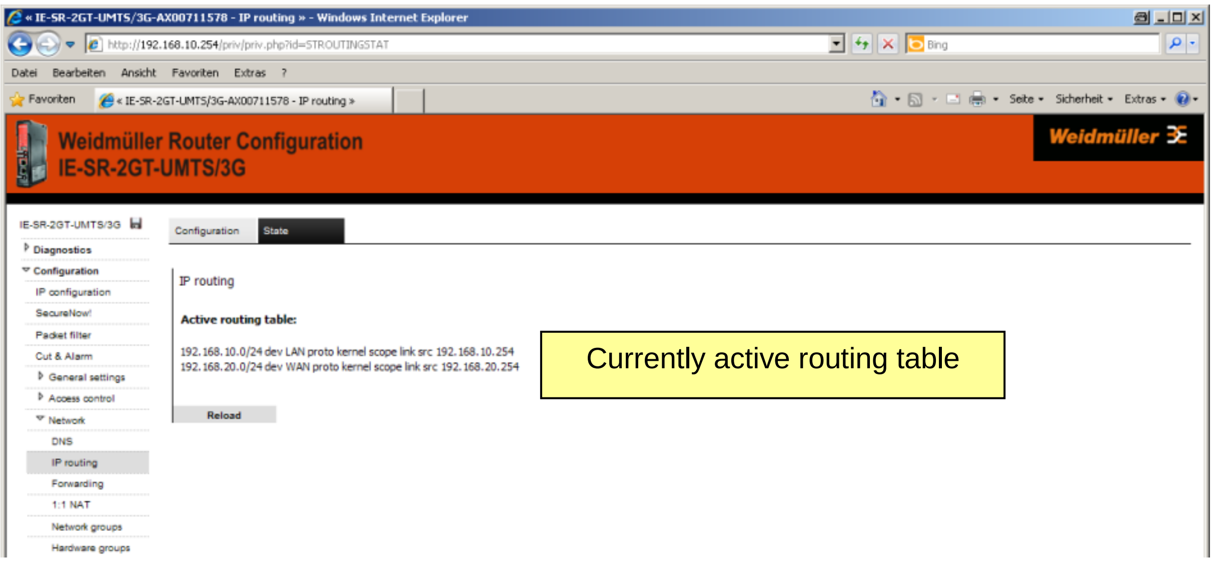
```
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'WAN IP address' = '192.168.20.254'
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'LAN IP address' = '192.168.10.254'
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'DNS via DHCP' = ''
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'Gateway via DHCP' = ''
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: Settings change by: 'admin', from source: 'web interface'
```

Screenshot of the Router showing new IP addresses

Figure A1-4: Web interface after Login with change IP addresses

5. Monitoring the currently active “routes”

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



IP routing

Active routing table:

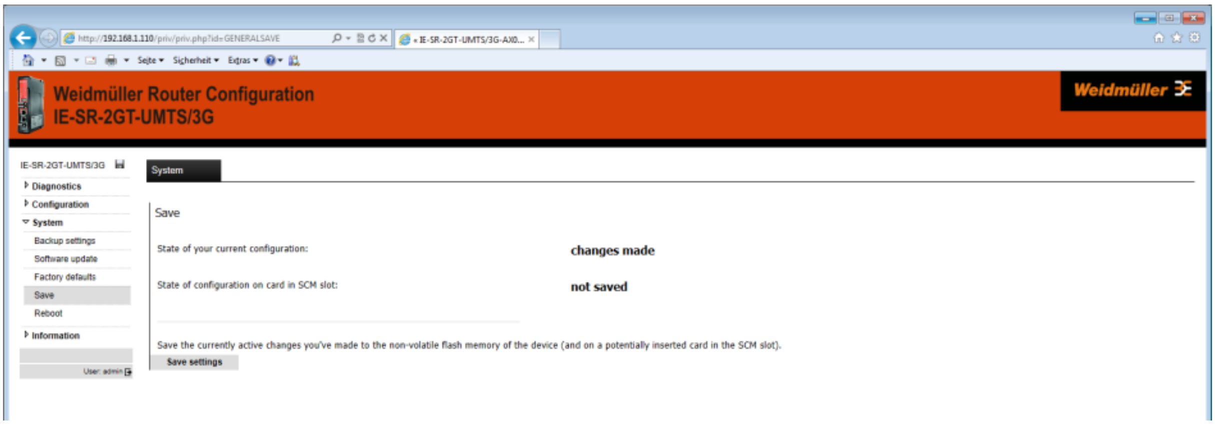
```
192.168.10.0/24 dev LAN proto kernel scope link src 192.168.10.254
192.168.20.0/24 dev WAN proto kernel scope link src 192.168.20.254
```

Currently active routing table

Figure A1-5: Menu **IP routing (Tab State)** showing the new active routing table

6. Saving the new configuration

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



Save

State of your current configuration: **changes made**

State of configuration on card in SCM slot: **not saved**

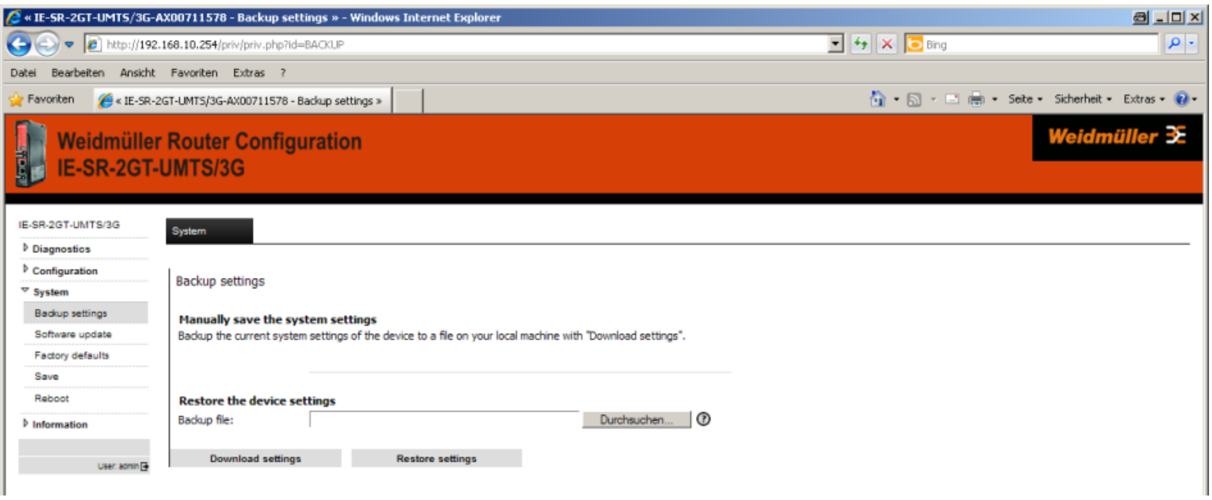
Save the currently active changes you've made to the non-volatile flash memory of the device (and on a potentially inserted card in the SCM slot).

Figure A1-6: Menu **System → Save** before saving the configuration

► 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 willbe stored on the SIM memory card.

Additionally the configuration can be stored on the file system of the PC.

► Select menu **System → Backup settings**



Backup settings

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

Restore the device settings
Backup file:

Figure A1-7: Menu **System → Backup settings** after saving the configuration

► 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 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)

A2 - Connecting 2 Ethernet networks with activated NAT masquerading and using IP address forwarding

This Technical Note applies to the Weidmüller Industrial Router IE-SR-2GT-LAN and IE-SR-2GT-UMTS/3G

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.
No special firewall filter rules shall be configured.

Solution:

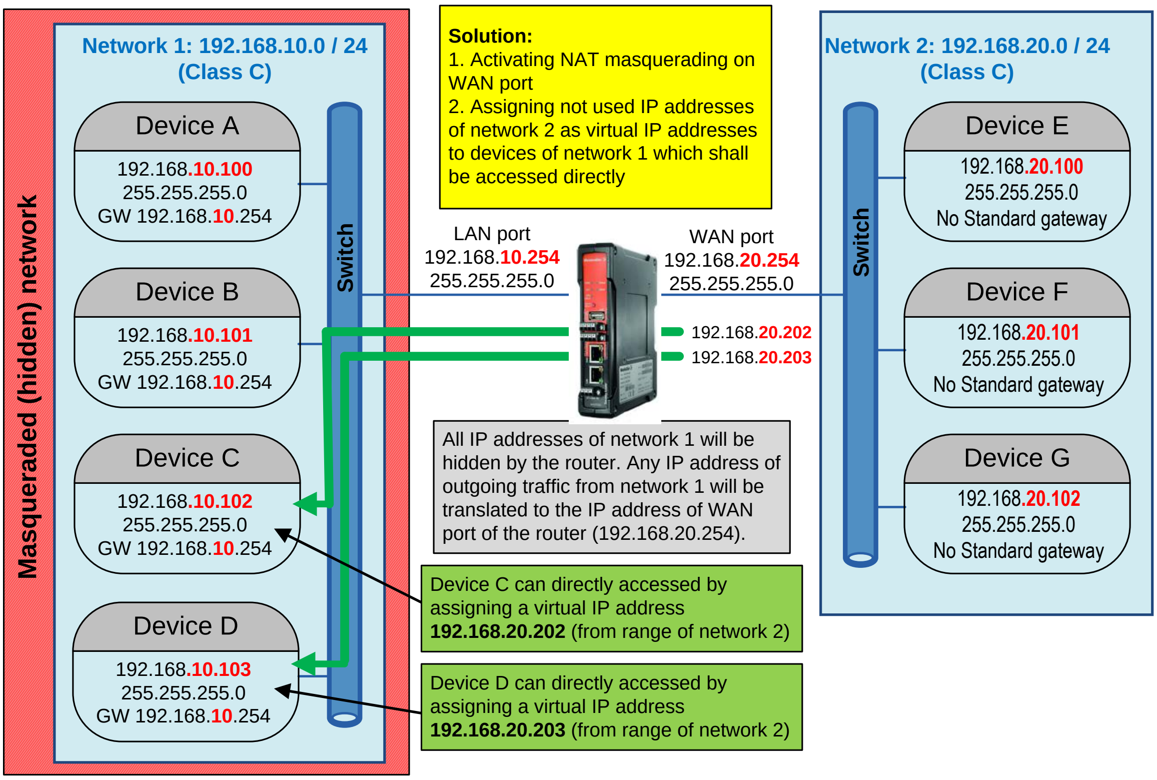
1. Activating “NAT masquerading” at **WAN** port of the Router which is connected to network 2. As result the sender IP addresses of any outgoing traffic at WAN port – initiated by devices of network 1 connect to LAN port – will be translated to the IP address of the Router’s WAN port. From the perspective 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 has to 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

Tasks: 1. Hiding the IP addresses of network 1 by activating NAT masquerading at router’s WAN port
2. As an exception devices C and D should be accessed directly by assigning a virtual IP address from the IP range of network 2



Solution:
1. Activating NAT masquerading on WAN port
2. Assigning not used IP addresses of network 2 as virtual IP addresses to devices of network 1 which shall be accessed directly

All IP addresses of network 1 will be hidden by the router. Any IP address of outgoing traffic from network 1 will be translated to the IP address of WAN port of the router (192.168.20.254).

Device C can directly accessed by assigning a virtual IP address **192.168.20.202** (from range of network 2)

Device D can directly accessed by assigning a virtual IP address **192.168.20.203** (from range of network 2)

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).

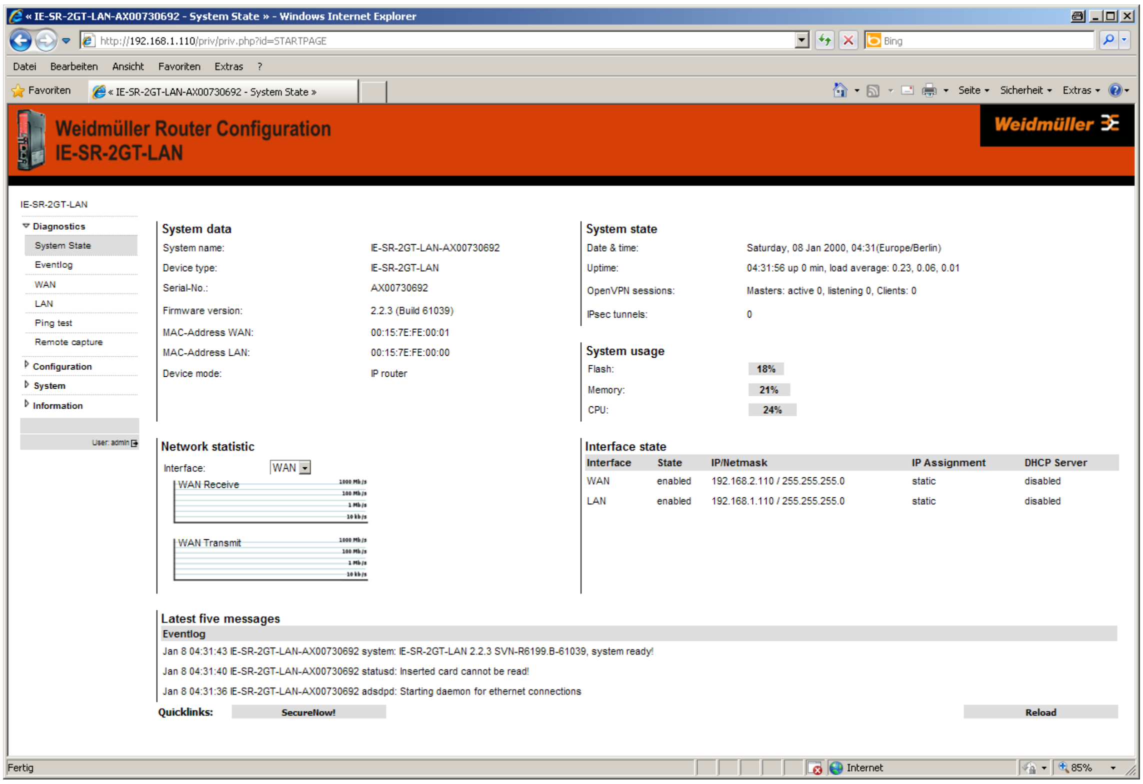
Note: Use autonegotiation on the Ethernet Interface of the PC

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
	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



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:31(Europe/Berlin)
Uptime:	04:31:56 up 0 min, load average: 0.23, 0.06, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	21%
CPU:	24%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled

Latest five messages

Eventlog

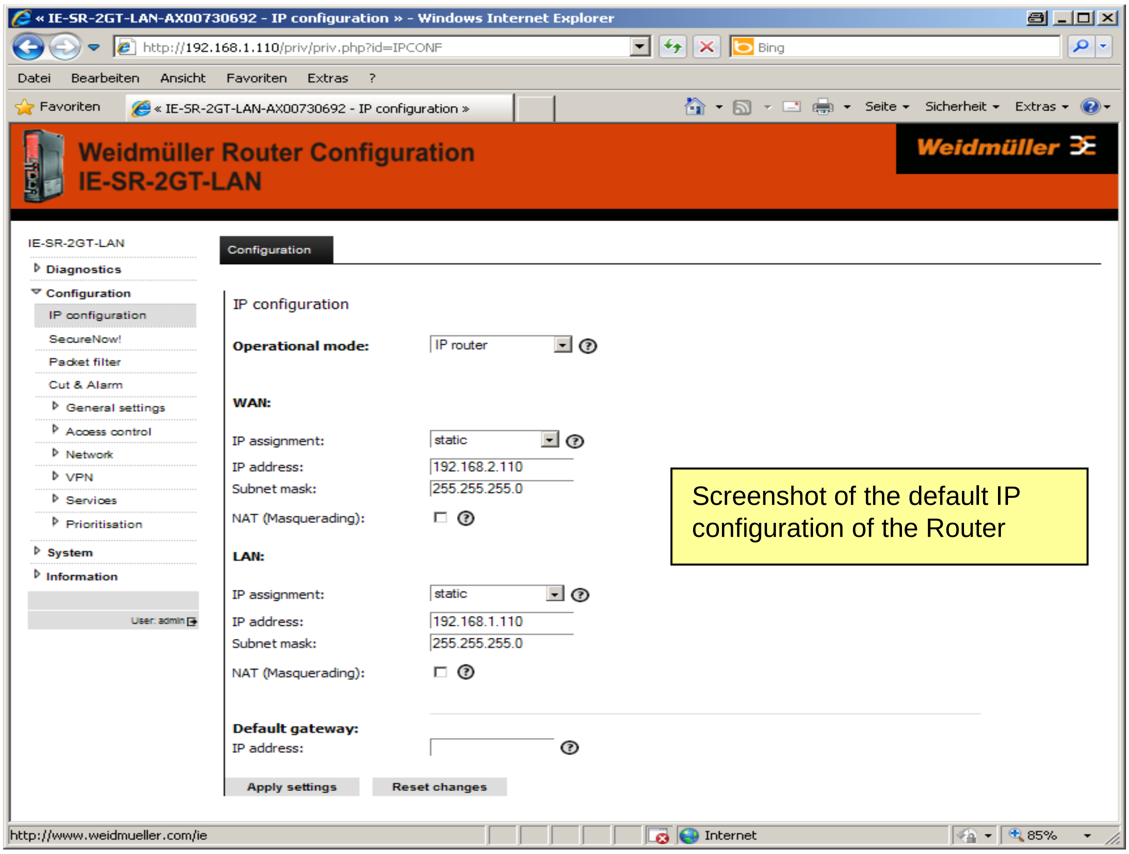
```
Jan 8 04:31:43 IE-SR-2GT-LAN-AX00730692 system: IE-SR-2GT-LAN 2.2.3 SVN-R6199.B-61039, system ready!
Jan 8 04:31:40 IE-SR-2GT-LAN-AX00730692 statusd: Inserted card cannot be read!
Jan 8 04:31:36 IE-SR-2GT-LAN-AX00730692 adsdpd: Starting daemon for ethernet connections
```

Quicklinks:

Figure A2-1: Login page of the Router (equivalent with menu Diagnostics → System State)

4. Set the basic IP configuration and activate NAT masquerading

► Select menu **Configuration → IP configuration**



« IE-SR-2GT-LAN-AX00730692 - IP configuration » - Windows Internet Explorer

http://192.168.1.110/priv/priv.php?id=IPCONF

IP configuration

Operational mode: IP router

WAN:

IP assignment: static

IP address: 192.168.2.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

LAN:

IP assignment: static

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

Default gateway:

IP address:

Screenshot of the default IP configuration of the Router

Figure A2-2: Default factory settings of menu **IP configuration**

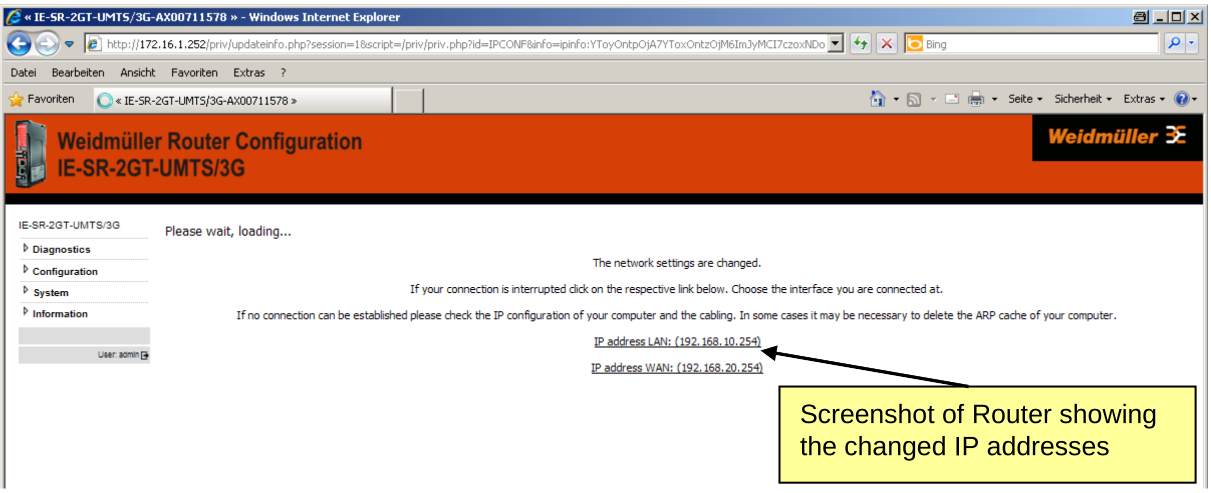
► Configure the menu entries as below described

Operational mode:	IP Router
IP address parameters **WAN** Port:	static
	192.168.**20**.254
	255.255.255.0 (Class C)
	Click and Set the checkbox NAT (masquerading)
IP address parameters **LAN** Port:	static
	192.168.**10**.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
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 A2-3.

Please keep in mind that you now have lost the Router connection due to changing the IP address range of your connected LAN port.



« IE-SR-2GT-UMTS/3G-AX00711578 » - Windows Internet Explorer
http://172.16.1.252/priv/updateinfo.php?session=1&script=/priv/priv.php?id=IPCONF&info=ipinfo:YToyOntpOjA7YToxOntzOjM6ImJyMCI7czoxNDo
Bing
Datei
Bearbeiten
Ansicht
Favoriten
Extras
?
Favoriten
« IE-SR-2GT-UMTS/3G-AX00711578 »
Seite
Sicherheit
Extras
Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G
Weidmüller
IE-SR-2GT-UMTS/3G
Diagnostics
Configuration
System
Information
User: admin

Please wait, loading...

The network settings are changed.

If your connection is interrupted click on the respective link below. Choose the interface you are connected at.

If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.

IP address LAN: (192.168.10.254)

IP address WAN: (192.168.20.254)

Screenshot of Router showing the changed IP addresses

Figure A2-3: Display of activated new IP addresses of LAN and WAN 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

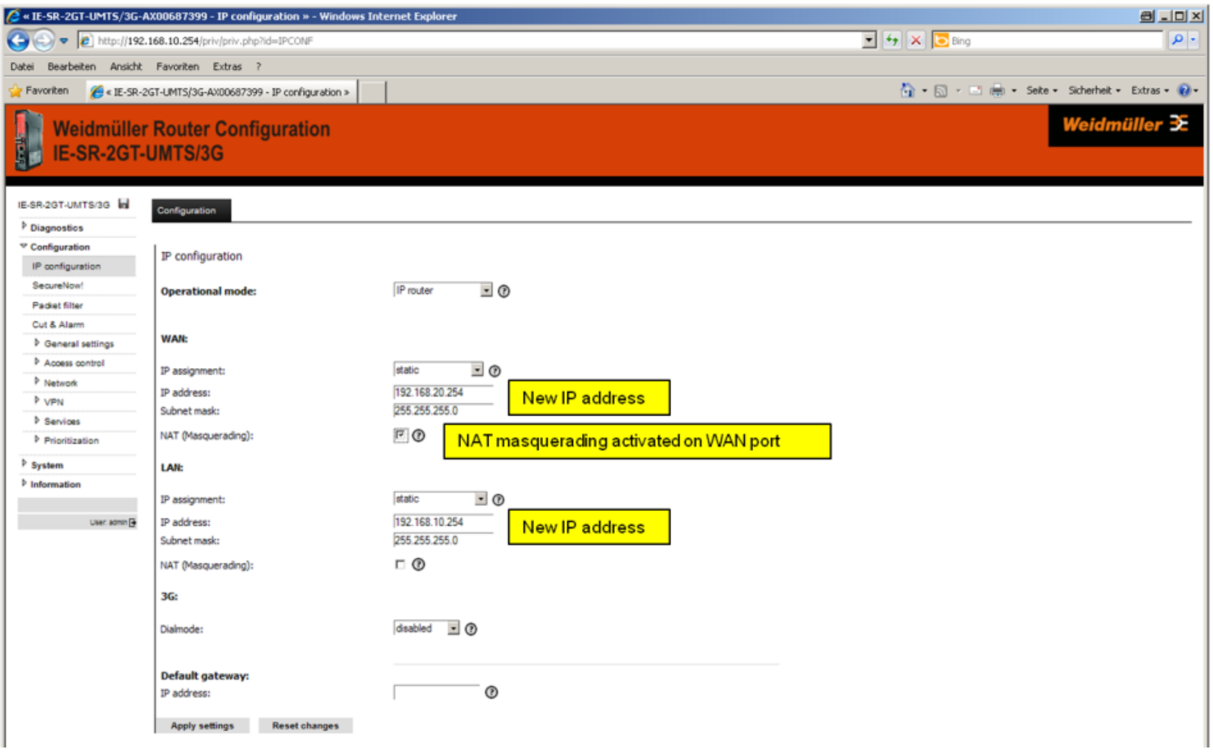
6. Again login into the Web interface of the Router using a Web browser

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

User:	admin
Password:	Detmold

7. Verify that configured parameters are valid

► Select menu **Configuration → IP configuration**



« IE-SR-2GT-UMTS/3G-AX00687399 - IP configuration » - Windows Internet Explorer

http://192.168.10.254/priv/priv.php?id=IPCONF

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Configuration

IP configuration

Operational mode: IP router

WAN:

IP assignment: static

IP address: 192.168.20.254 — New IP address

Subnet mask: 255.255.255.0

NAT (Masquerading): ☑ — NAT masquerading activated on WAN port

LAN:

IP assignment: static

IP address: 192.168.10.254 — New IP address

Subnet mask: 255.255.255.0

NAT (Masquerading): ☐

3G:

Dialmode: disabled

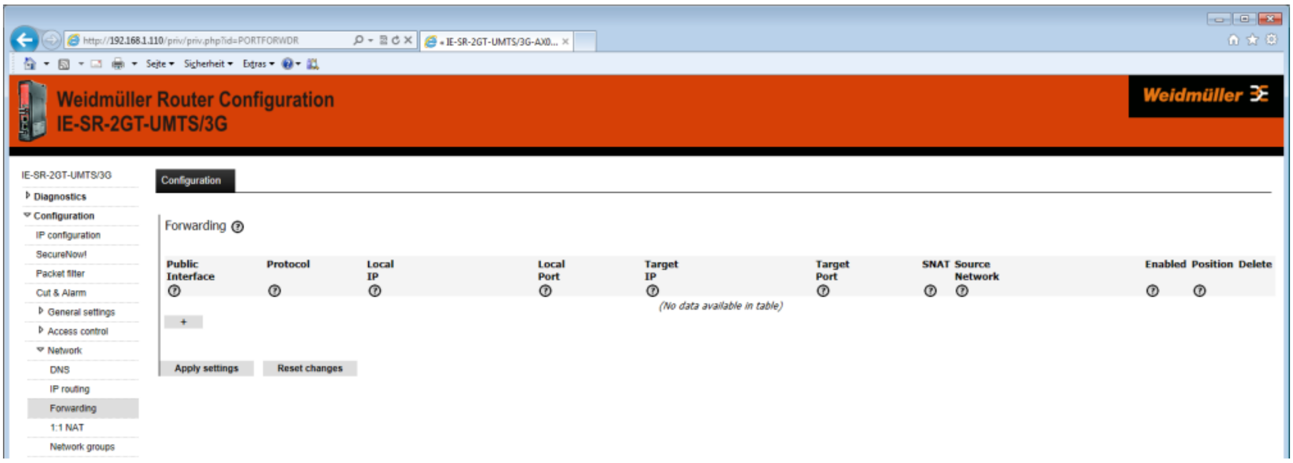
Default gateway:

IP address:

Figure A2-4: Changed settings of menu **IP configuration**

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

► Select menu **Configuration → Forwarding**



http://192.168.1.110/priv/priv.php?id=PORTFORWDR

Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G

Configuration

Forwarding

Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT	Source Network	Enabled	Position	Delete
				(No data available in table)						

Figure A2-5: Empty Forwarding table of menu **Forwarding**

► 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 6.

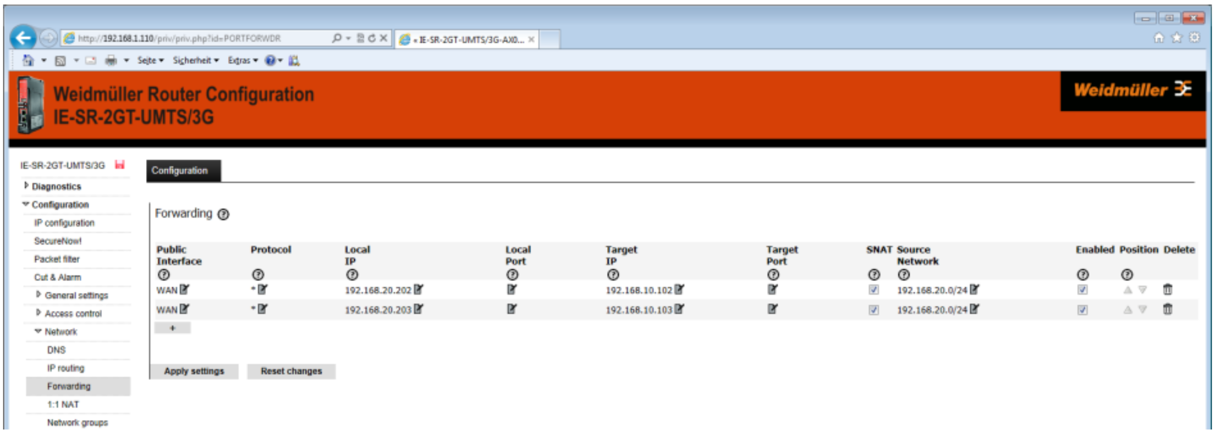
→ Ensure that each input will be completed by clicking the icon ☑.

► Click again icon **+** to add a second line to enter the next IP forwarding values.

► Select or fill the values as shown in the lower entry of figure 6.

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

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



Public Interface	Protocol	Local IP	Local Port	Target IP	Target Port	SNAT	Source Network	Enabled	Position	Delete
WAN	*	192.168.20.202		192.168.10.102		☑	192.168.20.0/24	☑	△ ▽	🗑
WAN	*	192.168.20.203		192.168.10.103		☑	192.168.20.0/24	☑	△ ▽	🗑

Figure A2-6:: Forwarding table with activated IP address forwardings

Now the configuration of the Router is finished!

Note: Don't forget to save the configuration after testing.

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 an 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 forwardings

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.

A3 - Configuring the Router to connect 2 networks with different IP address ranges and additional firewall rules

This Technical Note applies to the Weidmüller Industrial Router IE-SR-2GT-LAN and IE-SR-2GT-UMTS/3G

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).

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

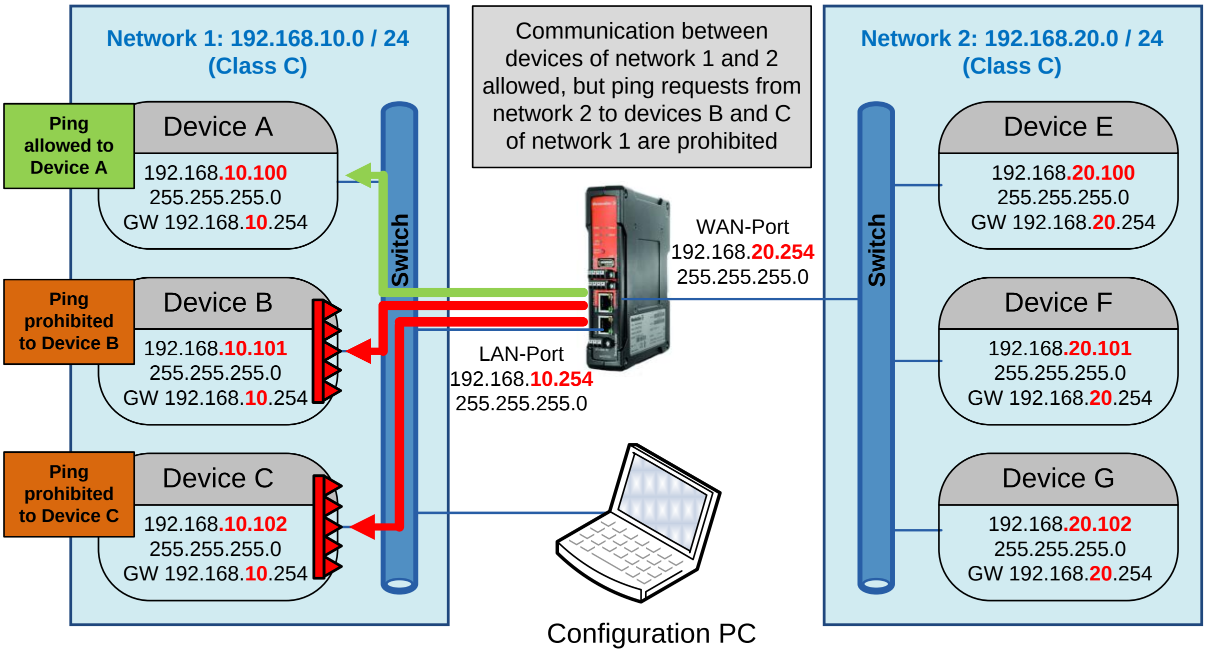
In this example the IP address ranges are set to

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 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

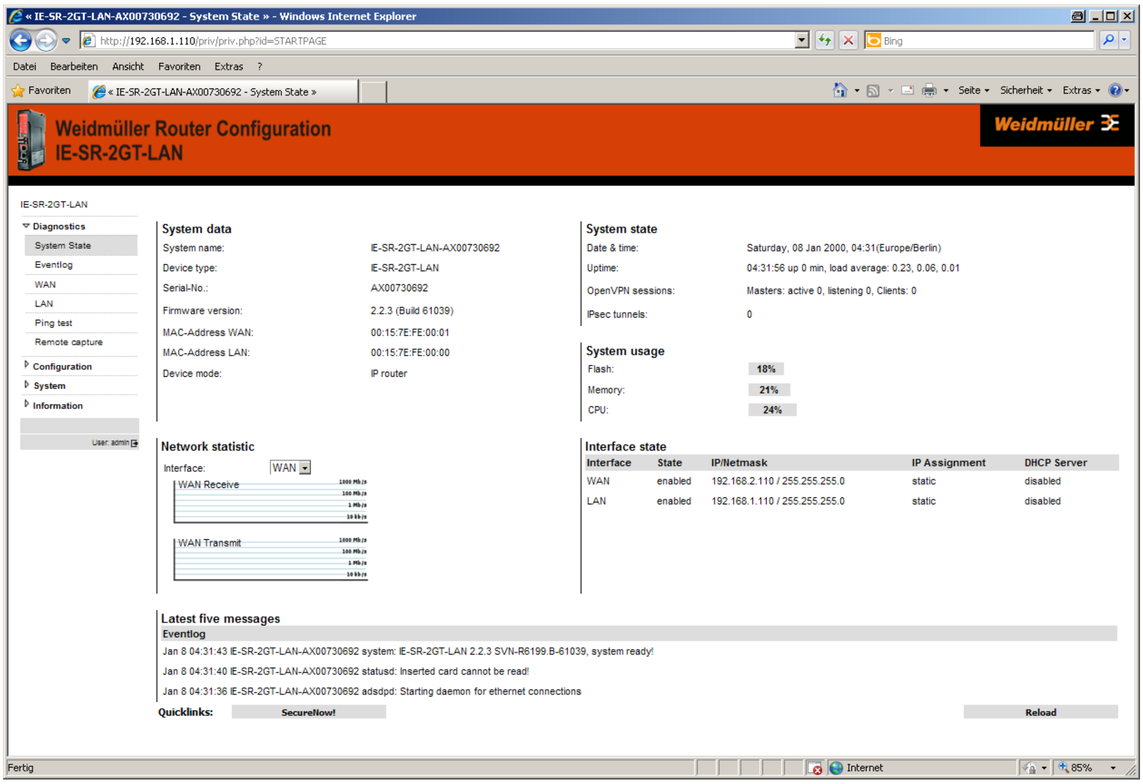
2. Change the IP address of the PC to one of the range 192.168.1.0 / 24

→ e.g.	IP address	192.168.1.99
	Subnet mask	255.255.255.0
	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



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:31(Europe/Berlin)
Uptime:	04:31:56 up 0 min, load average: 0.23, 0.06, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	21%
CPU:	24%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled

Latest five messages

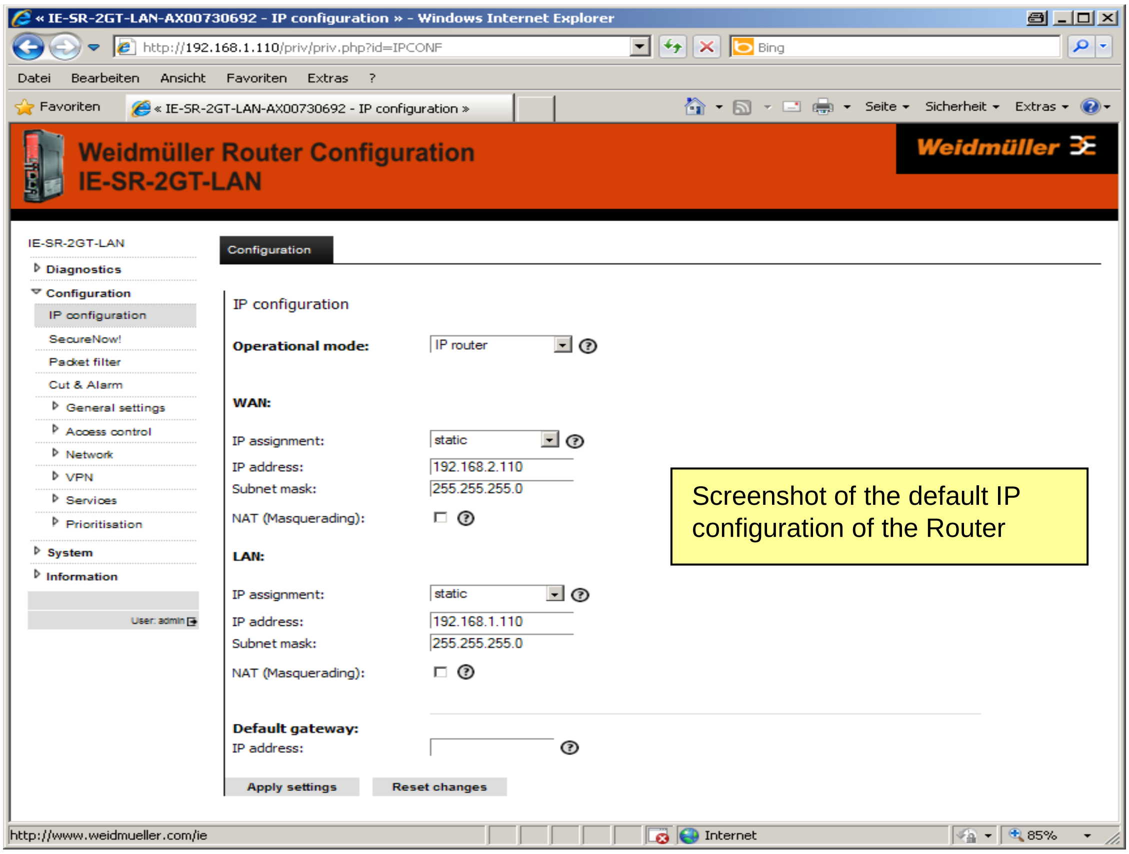
Eventlog

```
Jan 8 04:31:43 IE-SR-2GT-LAN-AX00730692 system: IE-SR-2GT-LAN 2.2.3 SVN-R6199.B-61039, system ready!
Jan 8 04:31:40 IE-SR-2GT-LAN-AX00730692 statusd: Inserted card cannot be read!
Jan 8 04:31:36 IE-SR-2GT-LAN-AX00730692 adsdpd: Starting daemon for ethernet connections
```

Figure A3-1: Login page of the Router (equivalent with menu Diagnostics → System State)

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

► Select menu **Configuration → IP configuration**



IP configuration

Operational mode: IP router

WAN:

IP assignment: static

IP address: 192.168.2.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

LAN:

IP assignment: static

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

Default gateway:

IP address:

Screenshot of the default IP configuration of the Router

Figure A3-2: Default values of menu **IP configuration**

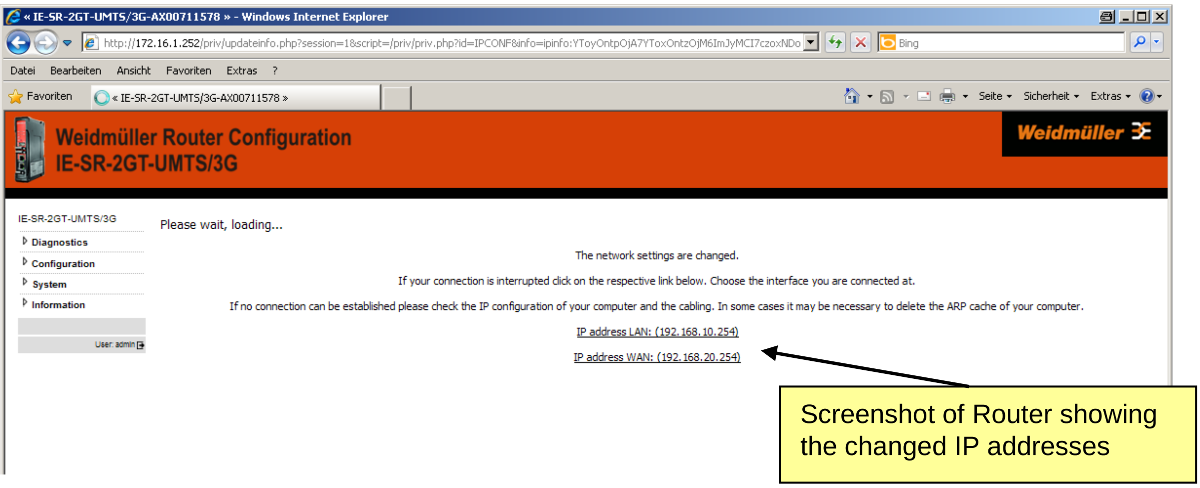
► Configure the menu entries as following shown

Operational mode:	IP Router
IP address parameters **WAN** Port:	static
	192.168.**20**.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
IP address parameters **LAN** Port:	static
	192.168.**10**.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
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 now have lost the Router connection due to changing the IP address range of your connected LAN port.


« IE-SR-2GT-UMTS/3G-AX00711578 » - Windows Internet Explorer
http://172.16.1.252/priv/updateinfo.php?session=1&script=/priv/priv.php?id=IPCONF&info=ipinfo:YToyOntpOjA7YToxOntzOjM6ImJyMCI7czoxNDo
Bing
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
« IE-SR-2GT-UMTS/3G-AX00711578 »
Seite Sicherheit Extras
Weidmüller Router Configuration
IE-SR-2GT-UMTS/3G
Weidmüller
IE-SR-2GT-UMTS/3G
Diagnostics
Configuration
System
Information
User: admin

Please wait, loading...

The network settings are changed.

If your connection is interrupted click on the respective link below. Choose the interface you are connected at.

If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.

IP address LAN: (192.168.10.254)

IP address WAN: (192.168.20.254)

Screenshot of Router showing the changed IP addresses

Figure A3-3: Display of activated new IP addresses of LAN and WAN port

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

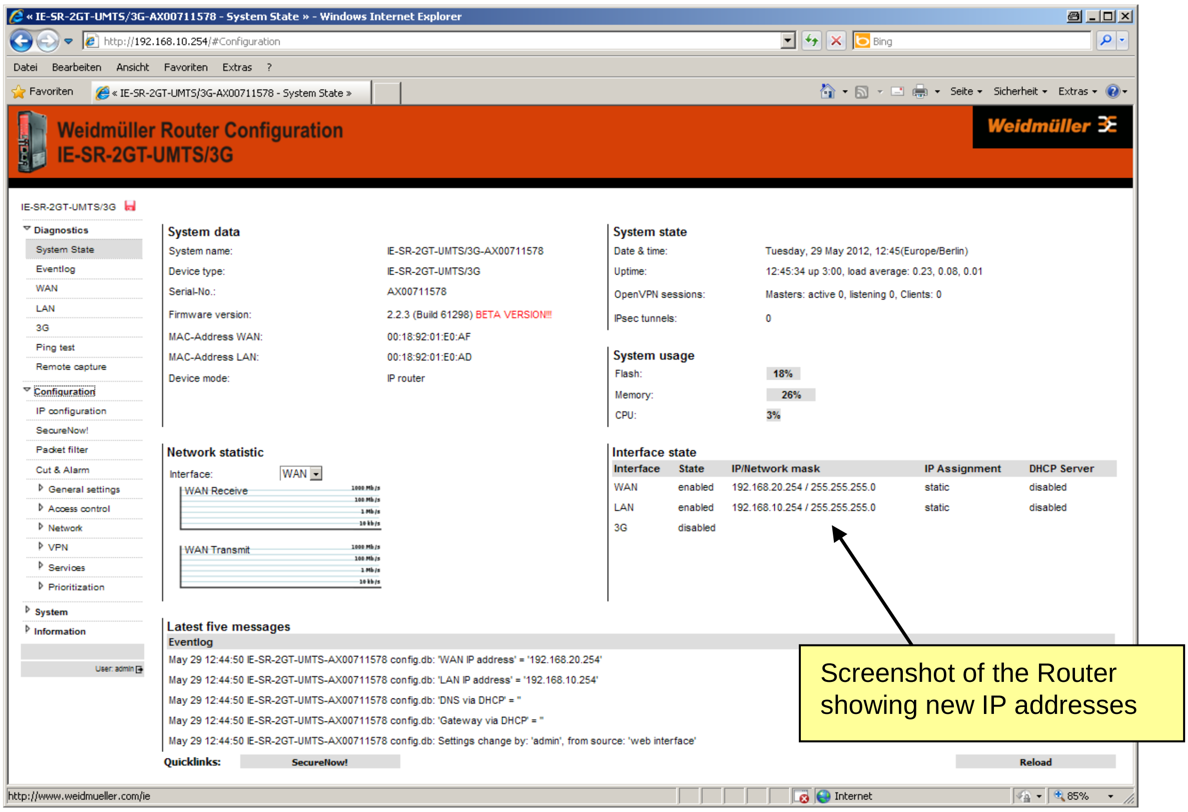
► To reconnect to the Router now set the IP address of the PC to the new values

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



System data

System name:	IE-SR-2GT-UMTS/3G-AX00711578
Device type:	IE-SR-2GT-UMTS/3G
Serial-No.:	AX00711578
Firmware version:	2.2.3 (Build 61298) BETA VERSION!!!
MAC-Address WAN:	00:18:92:01:E0:AF
MAC-Address LAN:	00:18:92:01:E0:AD
Device mode:	IP router

System state

Date & time:	Tuesday, 29 May 2012, 12:45(Europe/Berlin)
Uptime:	12:45:34 up 3:00, load average: 0.23, 0.08, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	26%
CPU:	3%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Network mask	IP Assignment	DHCP Server
WAN	enabled	192.168.20.254 / 255.255.255.0	static	disabled
LAN	enabled	192.168.10.254 / 255.255.255.0	static	disabled
3G	disabled			

Latest five messages

Eventlog

```
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'WAN IP address' = '192.168.20.254'
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'LAN IP address' = '192.168.10.254'
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'DNS via DHCP' = ''
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: 'Gateway via DHCP' = ''
May 29 12:44:50 IE-SR-2GT-UMTS-AX00711578 config.db: Settings change by: 'admin', from source: 'web interface'
```

Screenshot of the Router showing new IP addresses

Figure A3-4: Web interface after login with changed IP addresses

5. 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 hierachical 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

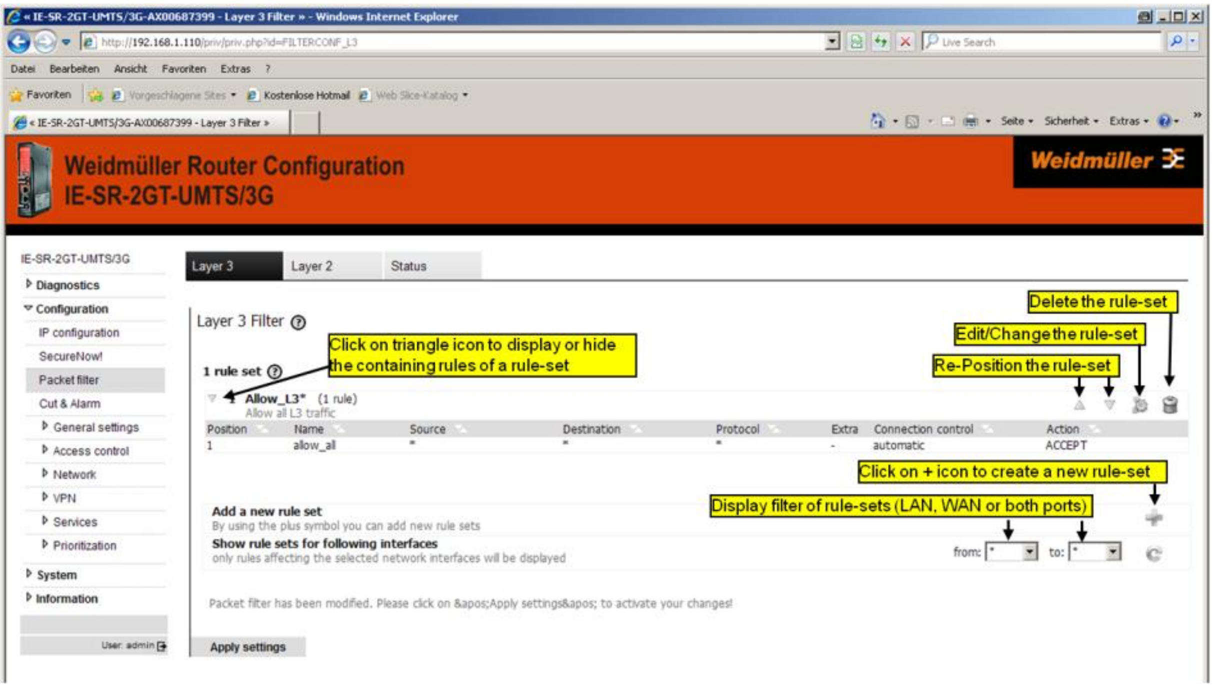
Several configured rule-sets will be applicated top-down. That means every data traffic will first be checked by the top-most displayed rule-set with its containing rules.

If a defined rule match the inspected data the filter rule will be applicated. 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 do **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.

6. Setup the firewall rules

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



Layer 3 Filter

1 rule set

Allow_L3* (1 rule)
Allow all L3 traffic

Position	Name	Source	Destination	Protocol	Extra	Connection control	Action
1	allow_all	*	*	*	-	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 &apos;Apply settings&apos; to activate your changes!

Delete the rule-set

Edit/Change the rule-set

Re-Position the rule-set

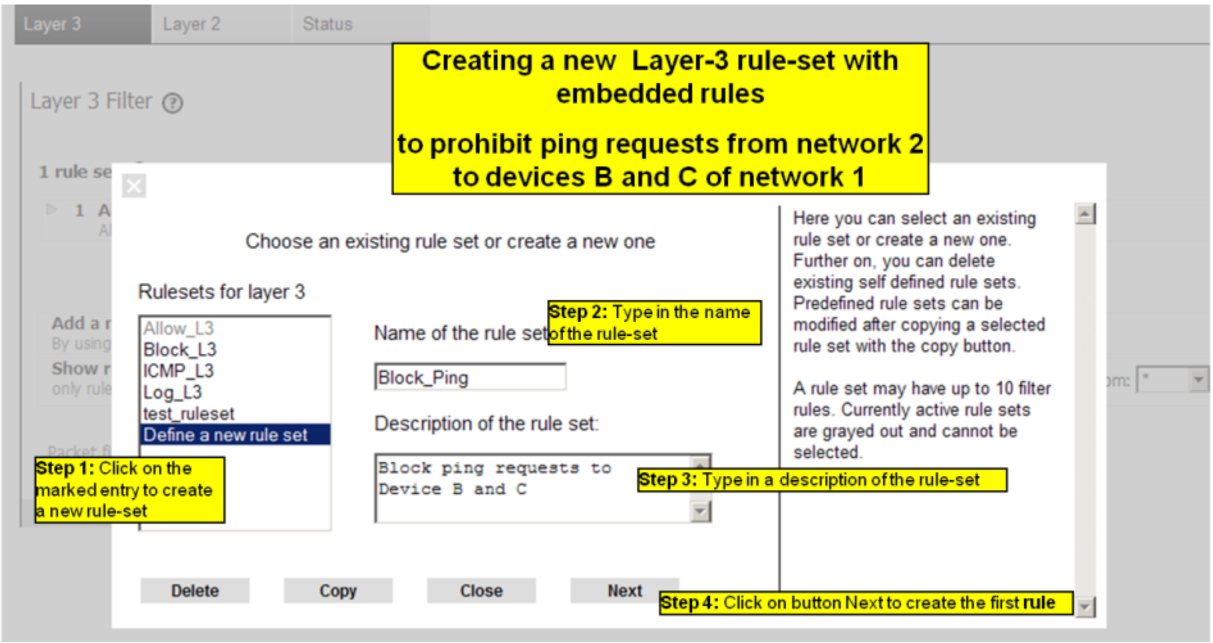
Click on triangle icon to display or hide the containing rules of a rule-set

Click on + icon to create a new rule-set

Display filter of rule-sets (LAN, WAN or both ports)

Figure A3-5: Menu **Packet filter (Tab Layer 3)** showing the factory default settings

► 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)



Creating a new Layer-3 rule-set with embedded rules

to prohibit ping requests from network 2 to devices B and C of network 1

Choose an existing rule set or create a new one

Rulesets for layer 3

- Allow_L3
- Block_L3
- ICMP_L3
- Log_L3
- test_ruleset
- Define a new rule set

Name of the rule set: Block_Ping

Description of the rule set:

```
Block ping requests to
Device B and C
```

Here you can select an existing rule set or create a new one. Further on, you can delete existing self defined rule sets. Predefined rule sets can be modified after copying a selected rule set with the copy button.

A rule set may have up to 10 filter rules. Currently active rule sets are grayed out and cannot be selected.

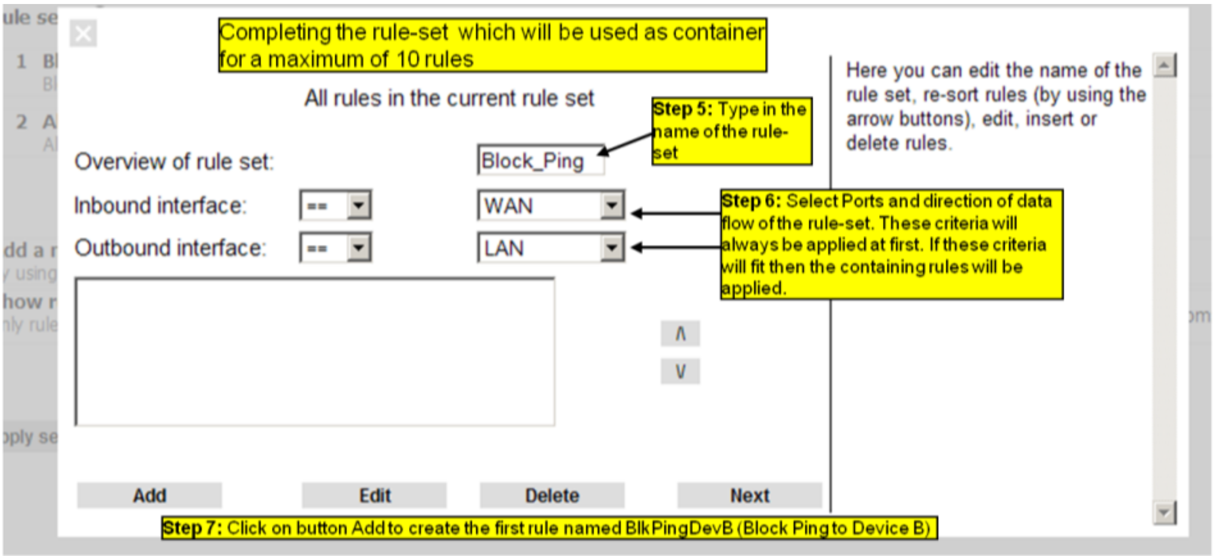
Step 1: Click on the marked entry to create a new rule-set

Step 2: Type in the name of the rule-set

Step 3: Type in a description of the rule-set

Step 4: Click on button Next to create the first **rule**

Figure A3-6: Define a new rule-set according described steps 1 to 4



Completing the rule-set which will be used as container for a maximum of 10 rules

All rules in the current rule set

Overview of rule set: Block_Ping

Inbound interface: == WAN

Outbound interface: == LAN

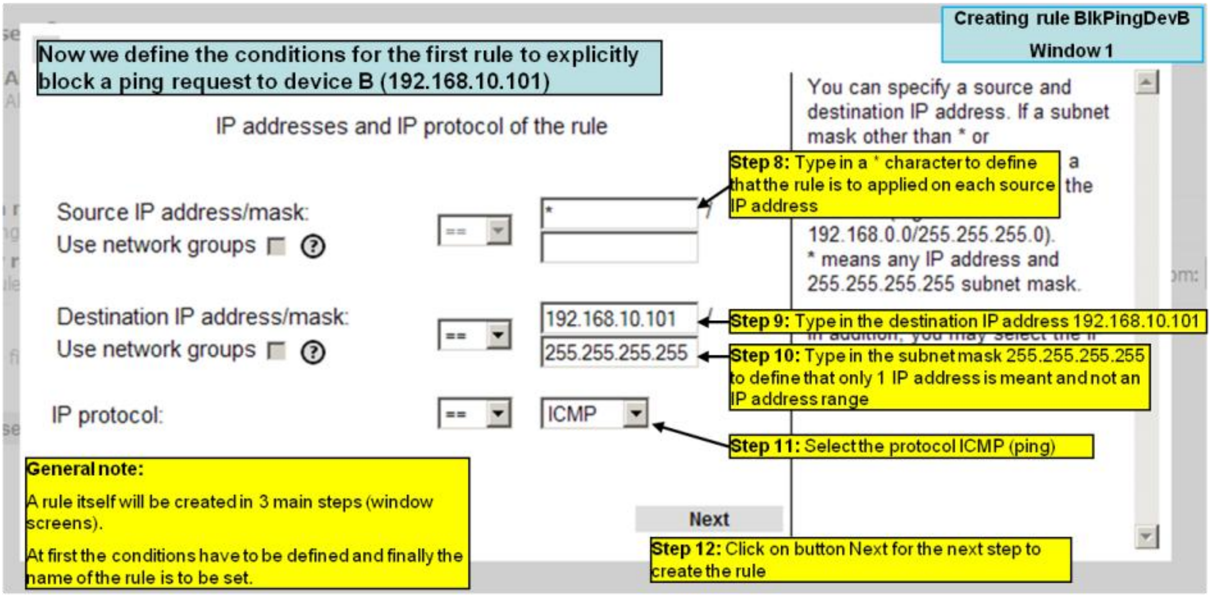
Here you can edit the name of the rule set, re-sort rules (by using the arrow buttons), edit, insert or delete rules.

Step 5: Type in the name of the rule-set

Step 6: Select Ports and direction of data flow of the rule-set. These criteria will always be applied at first. If these criteria will fit then the containing rules will be applied.

Step 7: Click on button Add to create the first rule named BlkPingDevB (Block Ping to Device B)

Figure A3-7: Define additional parameters of the new rule-set according described steps 5 to 7



Creating rule BlkPingDevB
Window 1

Now we define the conditions for the first rule to explicitly block a ping request to device B (192.168.10.101)

IP addresses and IP protocol of the rule

Source IP address/mask: == *
Use network groups □

Destination IP address/mask: == 192.168.10.101 / 255.255.255.255
Use network groups □

IP protocol: == ICMP

You can specify a source and destination IP address. If a subnet mask other than * or a the 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.

Step 8: Type in a * character to define that the rule is to applied on each source IP address

Step 9: Type in the destination IP address 192.168.10.101

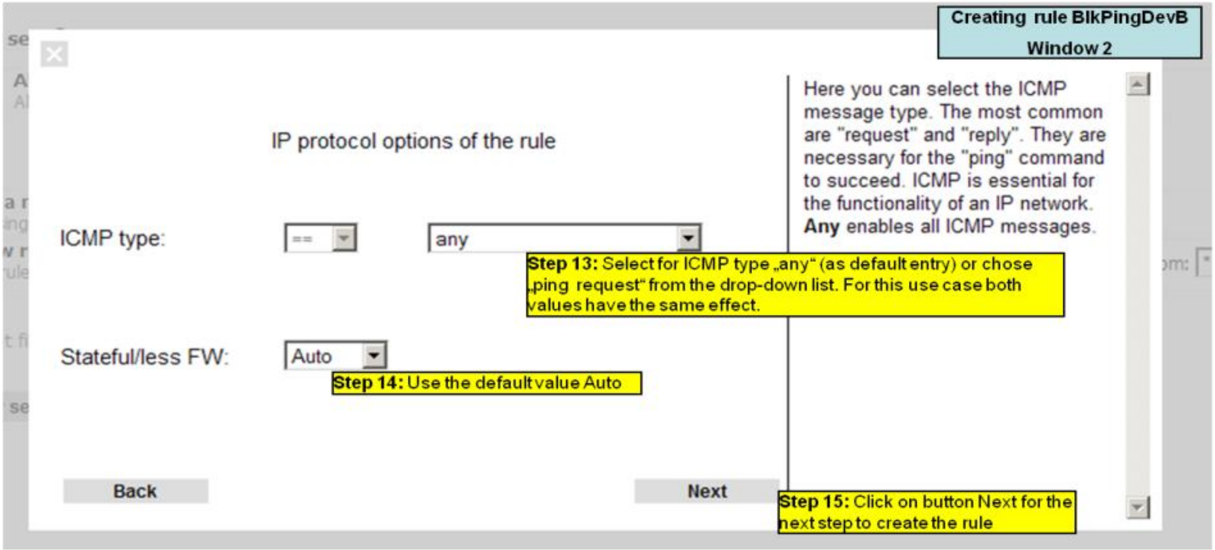
Step 10: Type in the subnet mask 255.255.255.255 to define that only 1 IP address is meant and not an IP address range

Step 11: Select the protocol ICMP (ping)

Step 12: Click on button Next for the next step to create the rule

General note:
A rule itself will be created in 3 main steps (window screens).
At first the conditions have to be defined and finally the name of the rule is to be set.

Figure A3-8: Define the first rule according described steps 8 to 12



Creating rule BlkPingDevB
Window 2

IP protocol options of the rule

ICMP type: == any

Stateful/less FW: Auto

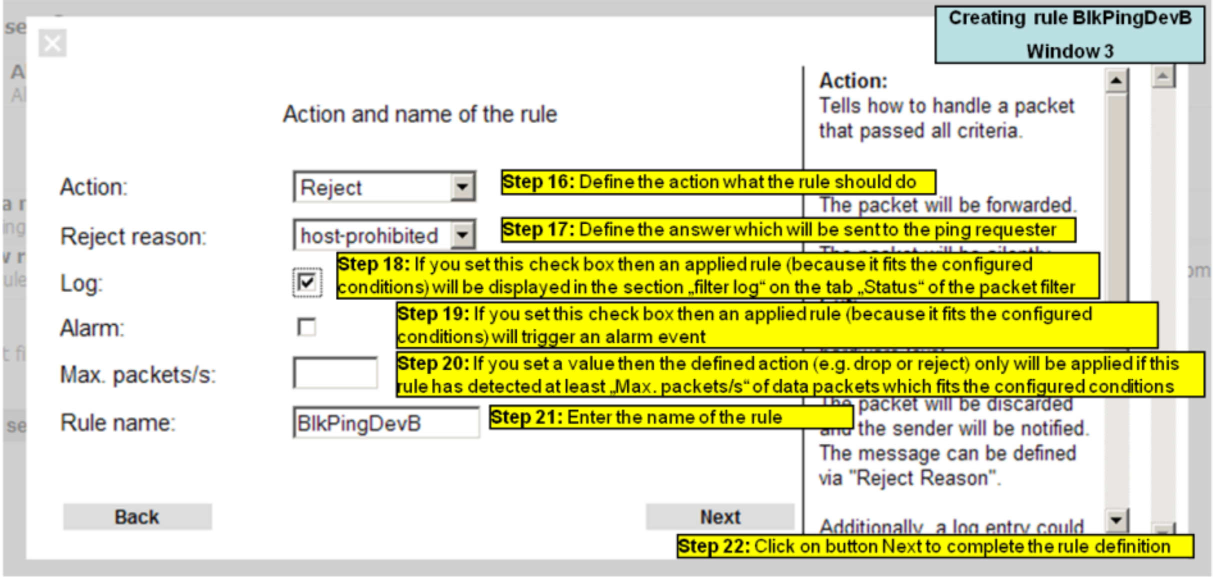
Here you can select the ICMP message type. The most common are "request" and "reply". They are necessary for the "ping" command to succeed. ICMP is essential for the functionality of an IP network. **Any** enables all ICMP messages.

Step 13: Select for ICMP type „any" (as default entry) or chose „ping request" from the drop-down list. For this use case both values have the same effect.

Step 14: Use the default value Auto

Step 15: Click on button Next for the next step to create the rule

Figure A3-9: Define additional parameters of the first rule according described steps 13 to 15



Creating rule BlkPingDevB
Window 3

Action and name of the rule

Action: Reject
Reject reason: host-prohibited
Log: ☑
Alarm: □
Max. packets/s:
Rule name: BlkPingDevB

Action:
Tells how to handle a packet that passed all criteria.
The packet will be forwarded.
packet will be discarded and the sender will be notified. The message can be defined via "Reject Reason".
Additionally, a log entry could

Step 16: Define the action what the rule should do

Step 17: Define the answer which will be sent to the ping requester

Step 18: If you set this check box then an applied rule (because it fits the configured conditions) will be displayed in the section „filter log" on the tab „Status" of the packet filter

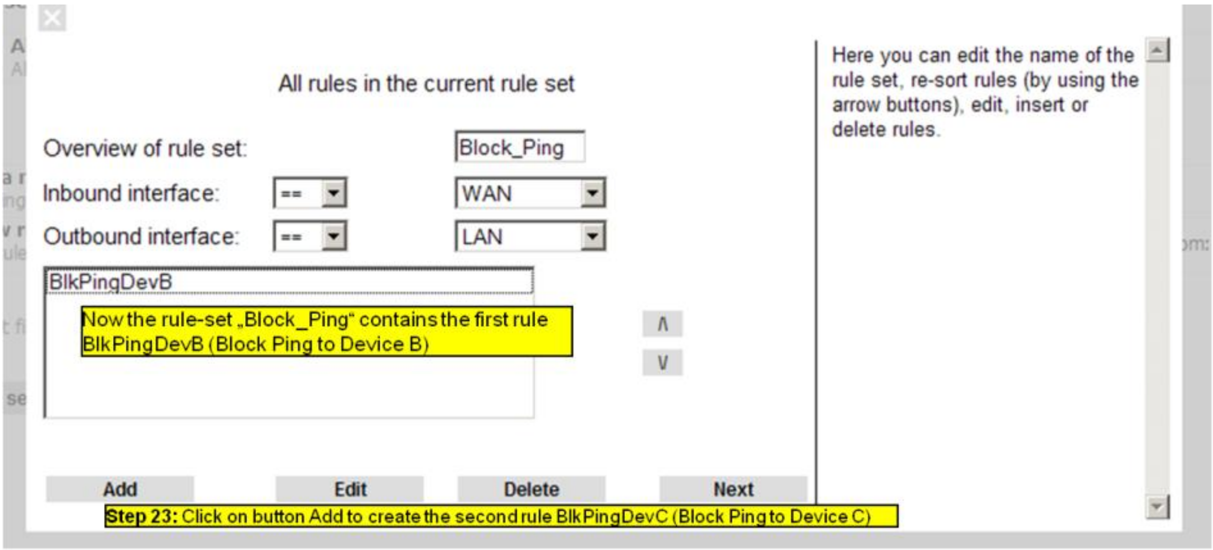
Step 19: If you set this check box then an applied rule (because it fits the configured conditions) will trigger an alarm event

Step 20: If you set a value then the defined action (e.g. drop or reject) only will be applied if this rule has detected at least „Max. packets/s" of data packets which fits the configured conditions

Step 21: Enter the name of the rule

Step 22: Click on button Next to complete the rule definition

Figure A3-10: Define additional parameters of the first rule according described steps 16 to 22



All rules in the current rule set

Overview of rule set: Block_Ping

Inbound interface: == WAN

Outbound interface: == LAN

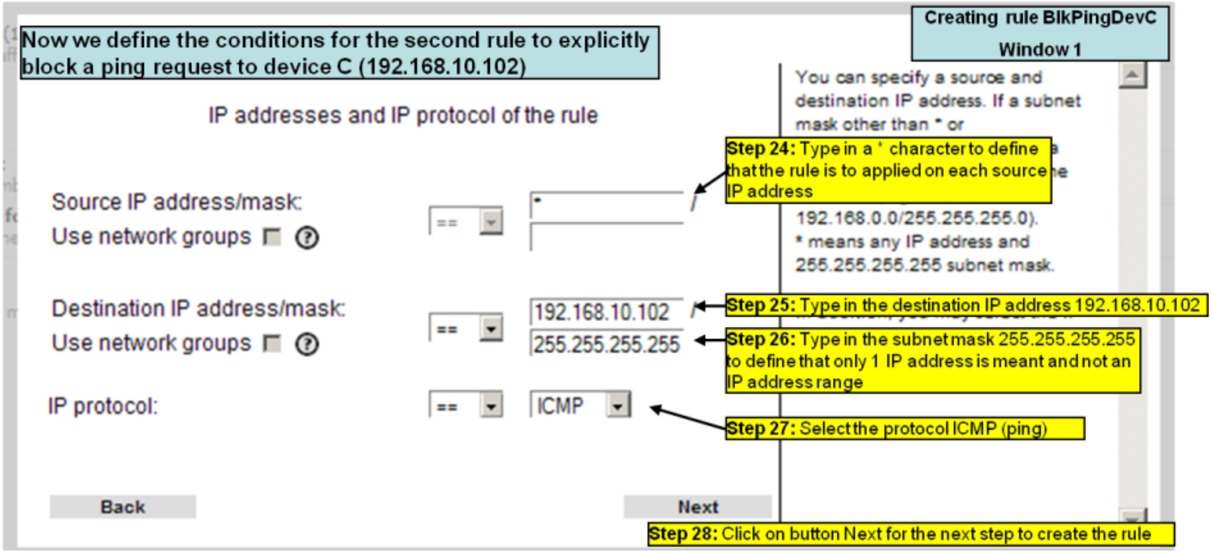
BlkPingDevB

Now the rule-set „Block_Ping" contains the first rule BlkPingDevB (Block Ping to Device B)

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

Step 23: Click on button Add to create the second rule BlkPingDevC (Block Ping to Device C)

Figure A3-11: Creation of first rule completed



Creating rule BlkPingDevC Window 1

Now we define the conditions for the second rule to explicitly block a ping request to device C (192.168.10.102)

IP addresses and IP protocol of the rule

Source IP address/mask: == *

Use network groups □

Destination IP address/mask: == 192.168.10.102 255.255.255.255

Use network groups □

IP protocol: == ICMP

You can specify a source and destination IP address. If a subnet mask other than * or ... 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.

Step 24: Type in a * character to define that the rule is to applied on each source IP address

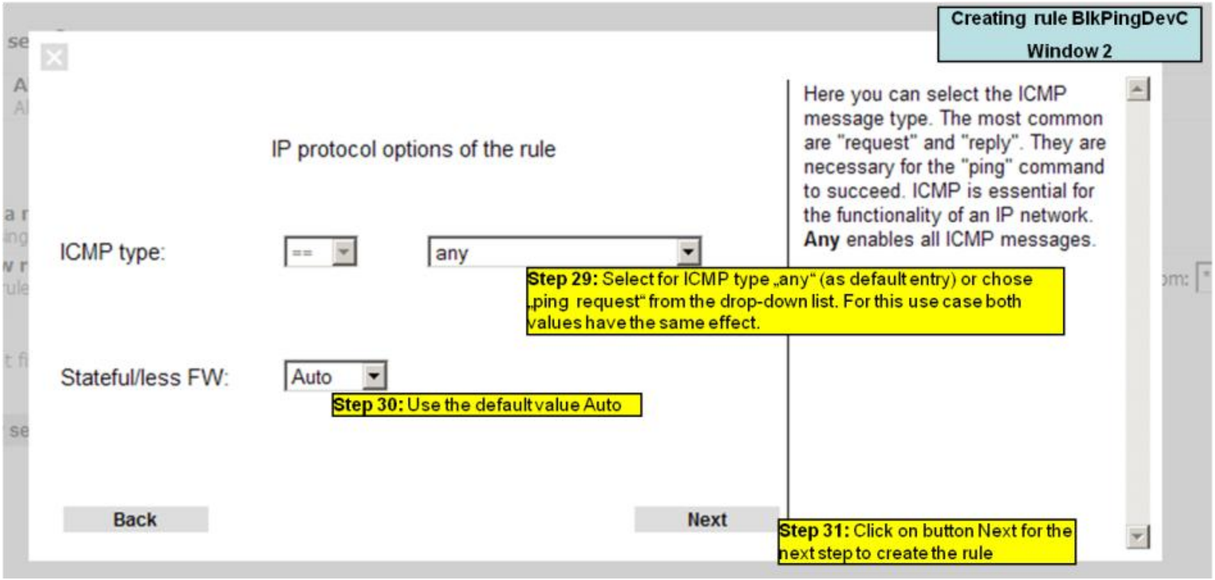
Step 25: Type in the destination IP address 192.168.10.102

Step 26: Type in the subnet mask 255.255.255.255 to define that only 1 IP address is meant and not an IP address range

Step 27: Select the protocol ICMP (ping)

Step 28: Click on button Next for the next step to create the rule

Figure A3-12: Define of second rule according described steps 24 to 28



Creating rule BlkPingDevC Window 2

IP protocol options of the rule

ICMP type: == any

Stateful/less FW: Auto

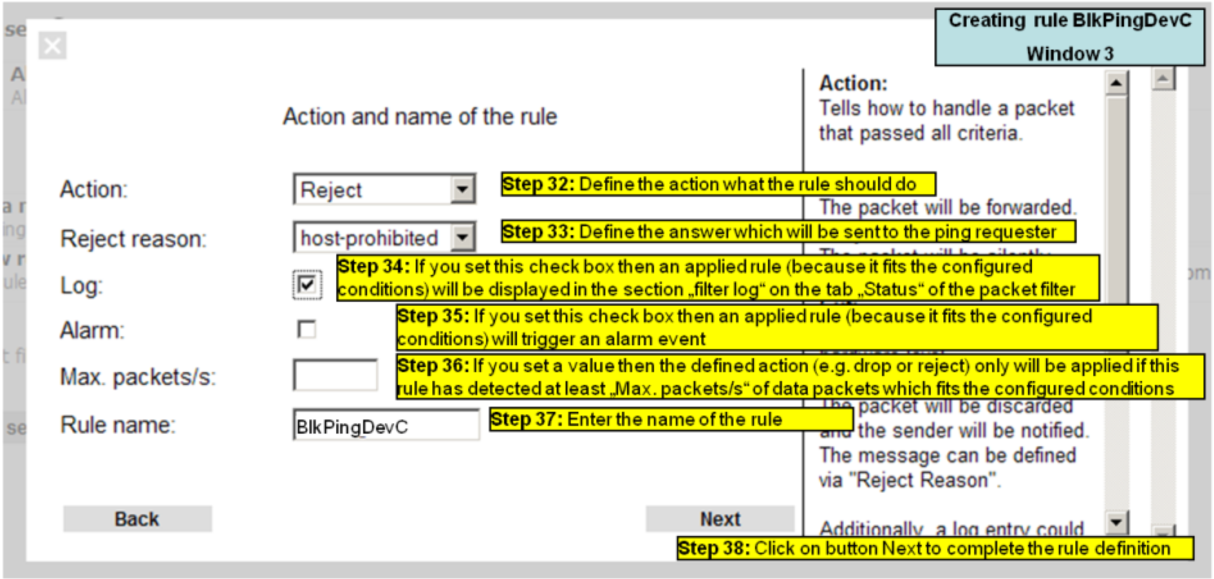
Here you can select the ICMP message type. The most common are "request" and "reply". They are necessary for the "ping" command to succeed. ICMP is essential for the functionality of an IP network. **Any** enables all ICMP messages.

Step 29: Select for ICMP type „any" (as default entry) or chose „ping request" from the drop-down list. For this use case both values have the same effect.

Step 30: Use the default value Auto

Step 31: Click on button Next for the next step to create the rule

Figure A3-13: Define additional parameters of the second rule according described steps 29 to 31



Creating rule BlkPingDevC
Window 3

Action and name of the rule

Action: Reject

Reject reason: host-prohibited

Log: ☑

Alarm: □

Max. packets/s:

Rule name: BlkPingDevC

Step 32: Define the action what the rule should do

Step 33: Define the answer which will be sent to the ping requester

Step 34: If you set this check box then an applied rule (because it fits the configured conditions) will be displayed in the section „filter log“ on the tab „Status“ of the packet filter

Step 35: If you set this check box then an applied rule (because it fits the configured conditions) will trigger an alarm event

Step 36: If you set a value then the defined action (e.g. drop or reject) only will be applied if this rule has detected at least „Max. packets/s“ of data packets which fits the configured conditions

Step 37: Enter the name of the rule

Step 38: Click on button Next to complete the rule definition

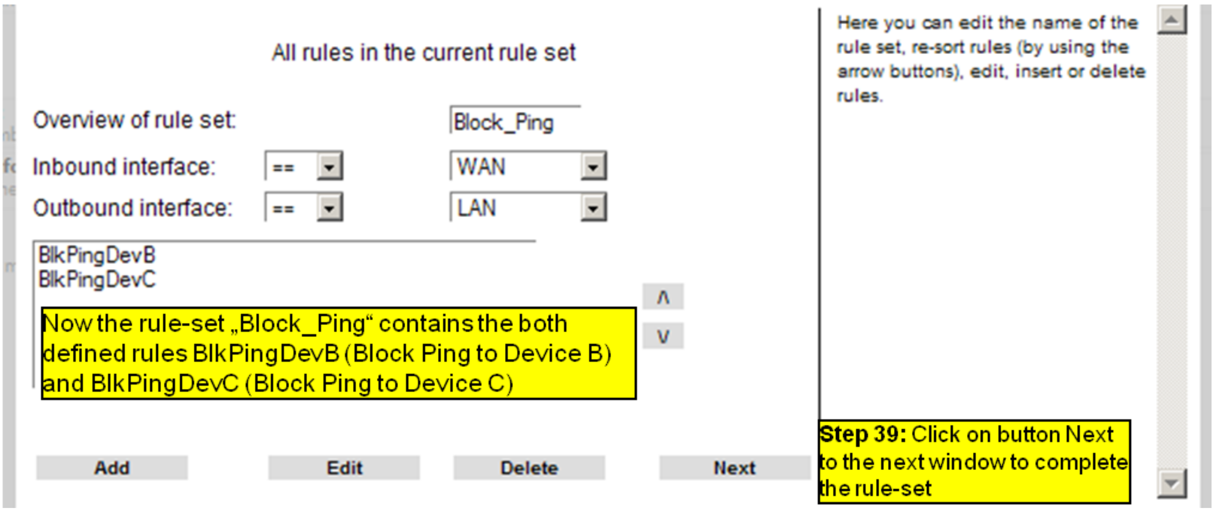
Action: Tells how to handle a packet that passed all criteria.

The packet will be forwarded.

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

Additionally, a log entry could

Figure A3-14: Define additional parameters of the second rule according described steps 32 to 38



All rules in the current rule set

Overview of rule set: Block_Ping

Inbound interface: == WAN

Outbound interface: == LAN

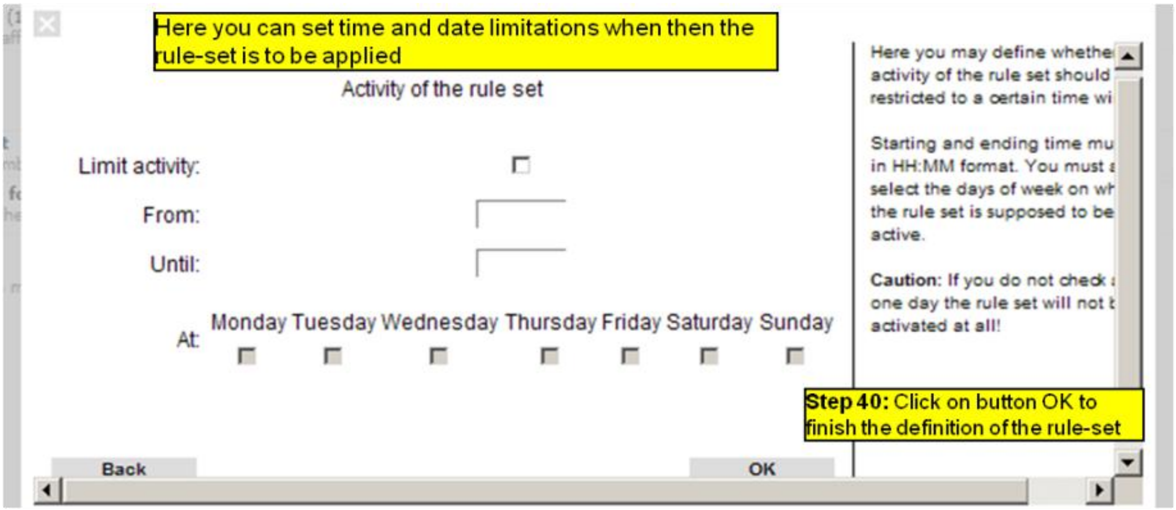
BlkPingDevB
BlkPingDevC

Now the rule-set „Block_Ping“ contains the both defined rules BlkPingDevB (Block Ping to Device B) and BlkPingDevC (Block Ping to Device C)

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

Step 39: Click on button Next to the next window to complete the rule-set

Figure A3-15: Creation of second rule completed



Here you can set time and date limitations when then the rule-set is to be applied

Activity of the rule set

Limit activity: □

From:

Until:

At: Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday □

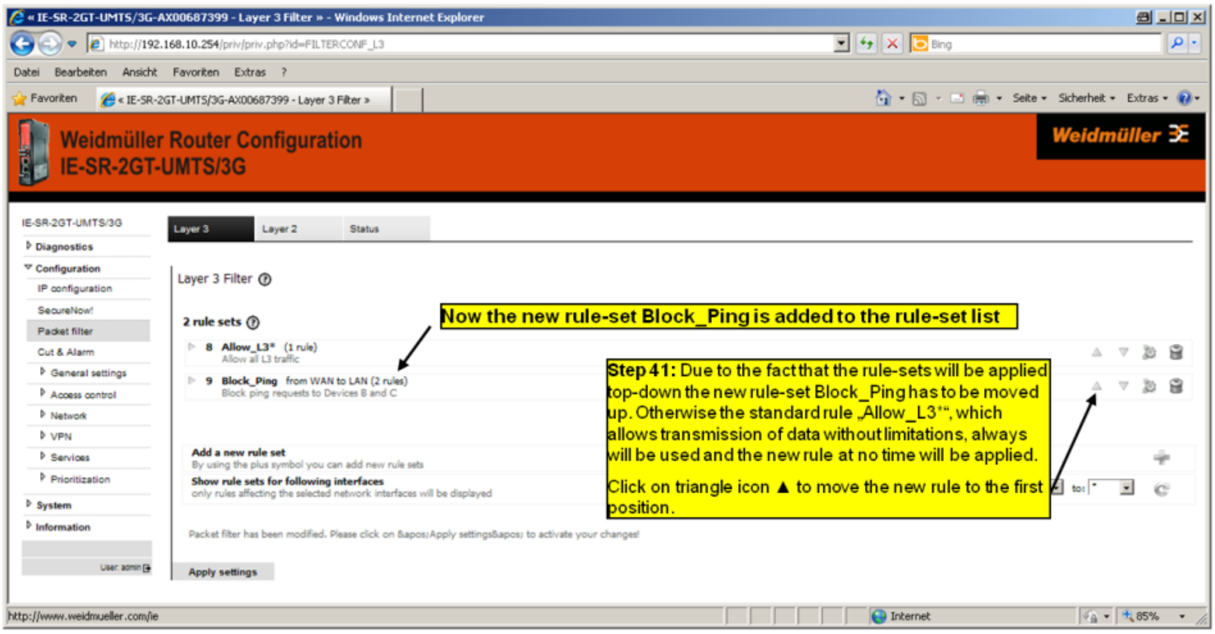
Here you may define whethe activity of the rule set should restricted to a certain time wi

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

Caution: If you do not check a one day the rule set will not b activated at all!

Step 40: Click on button OK to finish the definition of the rule-set

Figure A3-16: Setting optional date and time limitations of the rule-set



Layer 3 Filter

2 rule sets

8 Allow_L3* (1 rule)
Allow all L3 traffic

9 Block_Ping from WAN to LAN (2 rules)
Block ping requests to Devices B and C

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

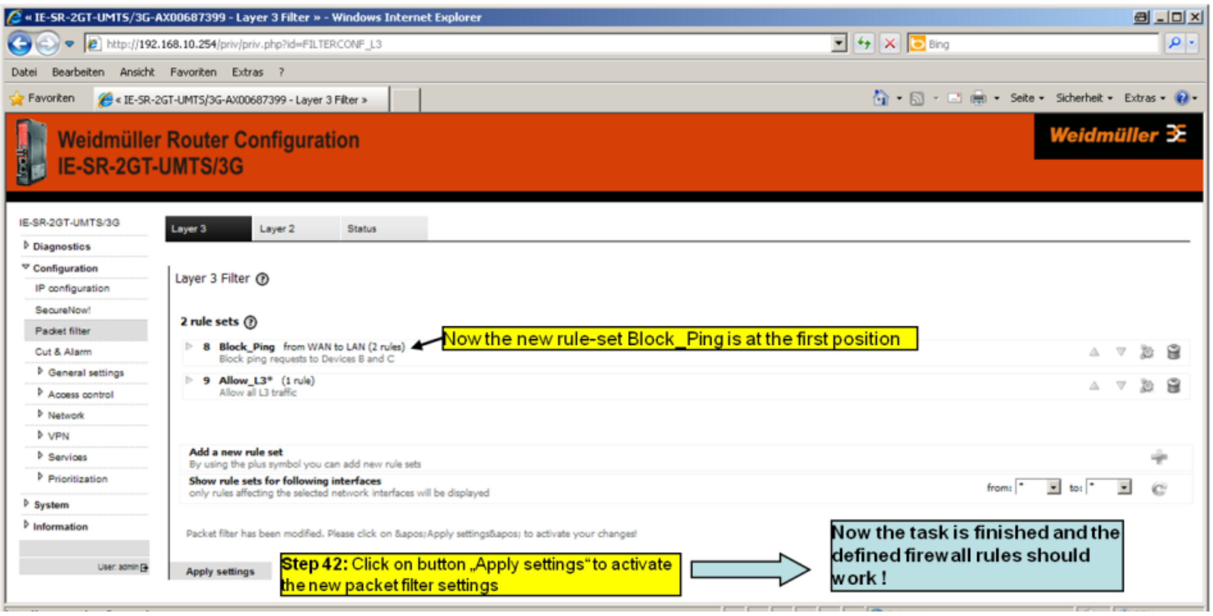
Packet filter has been modified. Please click on &apos;Apply settings&apos; to activate your changes!

Now the new rule-set Block_Ping is added to the rule-set list

Step 41: Due to the fact that the rule-sets will be applied top-down the new rule-set Block_Ping has to be moved up. Otherwise the standard rule „Allow_L3*“, which allows transmission of data without limitations, always will be used and the new rule at no time will be applied.

Click on triangle icon ▲ to move the new rule to the first position.

Figure A3-17: Creation of new rule-set is completed and added to the rule-set list. Move the new rule-set to top position



Layer 3 Filter

2 rule sets

8 Block_Ping from WAN to LAN (2 rules)
Block ping requests to Devices B and C

9 Allow_L3* (1 rule)
Allow all L3 traffic

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

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

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

Now the new rule-set Block_Ping is at the first position

Step 42: Click on button „Apply settings“ to activate the new packet filter settings

Now the task is finished and the defined firewall rules should work !

Figure A3-18: Activate the changes

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)

A4 - Connecting 2 Ethernet networks with the same IP address range to another network using 1:1 NAT address translation

This Technical Note applies to the Weidmüller Industrial Router IE-SR-2GT-LAN and IE-SR-2GT-UMTS/3G

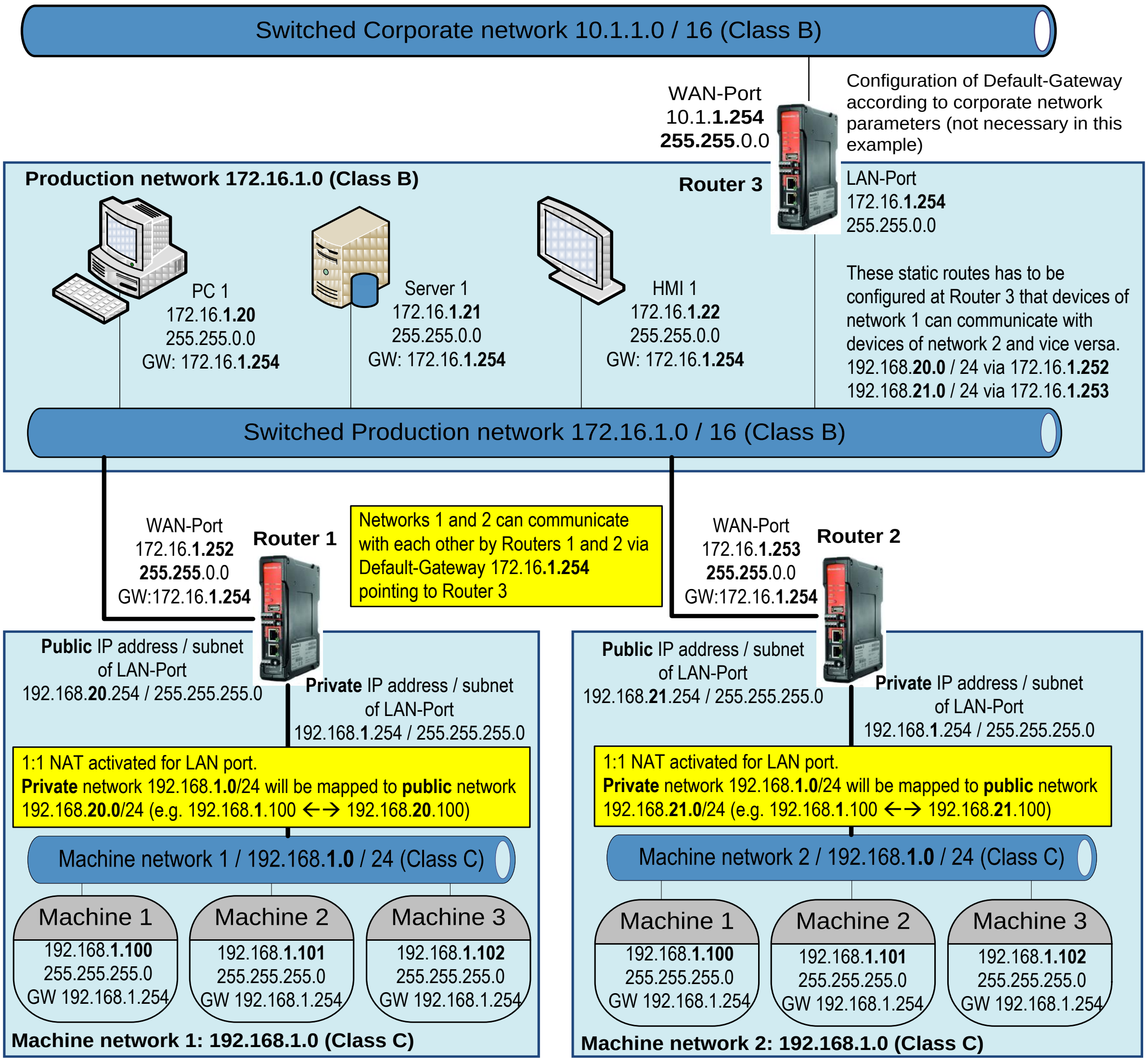
Application scenario:

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

Task and solution:

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

1:1 NAT means that IP addresses (**private**) of devices connected to the LAN port, internally will be translated to a new IP address (**public**) if they communicate with IP addresses connected to the WAN network. 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.


Switched Corporate network 10.1.1.0 / 16 (Class B)
WAN-Port
10.1.1.254
255.255.0.0
Configuration of Default-Gateway according to corporate network parameters (not necessary in this example)
Production network 172.16.1.0 (Class B)
Router 3
LAN-Port
172.16.1.254
255.255.0.0
PC 1
172.16.1.20
255.255.0.0
GW: 172.16.1.254
Server 1
172.16.1.21
255.255.0.0
GW: 172.16.1.254
HMI 1
172.16.1.22
255.255.0.0
GW: 172.16.1.254
These static routes has to be configured at Router 3 that devices of network 1 can communicate with devices of network 2 and vice versa.
192.168.20.0 / 24 via 172.16.1.252
192.168.21.0 / 24 via 172.16.1.253
Switched Production network 172.16.1.0 / 16 (Class B)
WAN-Port
172.16.1.252
255.255.0.0
GW:172.16.1.254
Router 1
Networks 1 and 2 can communicate with each other by Routers 1 and 2 via Default-Gateway 172.16.1.254 pointing to Router 3
WAN-Port
172.16.1.253
255.255.0.0
GW:172.16.1.254
Router 2
Public IP address / subnet of LAN-Port
192.168.20.254 / 255.255.255.0
Private IP address / subnet of LAN-Port
192.168.1.254 / 255.255.255.0
Public IP address / subnet of LAN-Port
192.168.21.254 / 255.255.255.0
Private IP address / subnet of LAN-Port
192.168.1.254 / 255.255.255.0
1:1 NAT activated for LAN port.
Private network 192.168.1.0/24 will be mapped to public network 192.168.20.0/24 (e.g. 192.168.1.100 <-> 192.168.20.100)
1:1 NAT activated for LAN port.
Private network 192.168.1.0/24 will be mapped to public network 192.168.21.0/24 (e.g. 192.168.1.100 <-> 192.168.21.100)
Machine network 1 / 192.168.1.0 / 24 (Class C)
Machine network 2 / 192.168.1.0 / 24 (Class C)
Machine 1
192.168.1.100
255.255.255.0
GW 192.168.1.254
Machine 2
192.168.1.101
255.255.255.0
GW 192.168.1.254
Machine 3
192.168.1.102
255.255.255.0
GW 192.168.1.254
Machine 1
192.168.1.100
255.255.255.0
GW 192.168.1.254
Machine 2
192.168.1.101
255.255.255.0
GW 192.168.1.254
Machine 3
192.168.1.102
255.255.255.0
GW 192.168.1.254
Machine network 1: 192.168.1.0 (Class C)
Machine network 2: 192.168.1.0 (Class C)

Machine networks 1 and 2 uses the same IP address range

This document describes an application scenario using 3 Routers. But for a simple test of the feature “1:1 NAT” you only need 1 Router (configured as Router 1 of machine network 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:

Both Routers of machine network 1 and 2 have to be connected by WAN port to the production network 172.16.1.0. The IP addresses of the WAN ports will be set to

172.16.1.252 / 255.255.0.0 for Router 1 and

172.16.1.253 / 255.255.0.0 for Router 2

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

In this example – using the feature 1:1 NAT at **LAN port** –

the **public** IP addresses will be set to

192.168.**20**.254 / 255.255.255.0 for Router 1 and

192.168.**21**.254 / 255.255.255.0 for Router 2

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

192.168.**1**.254 / 255.255.255.0 for Router 1 and

192.168.**1**.254 / 255.255.255.0 for Router 2

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 between devices of LAN and WAN network the **public** IP addresses of LAN devices have to be 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 of Router's LAN port**	**Configured Public IP address and subnet of Router's LAN port**	**Resulting Public IP address and subnet of 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 WAN network
192.168.1.**100** / 255.255.255.0	192.168.1.254 / 255.255.255.0	192.168.21.254 / 255.255.255.0	192.168.21.**100** / 255.255.255.0
192.168.1.**101** / 255.255.255.0			192.168.21.**101** / 255.255.255.0
172.16.1.**101** / 255.255.255.0	172.16.1.1 / 255.255.255.0	192.168.100.1 / 255.255.255.0	192.168.100.**101** / 255.255.255.0
10.8.**1.10** / 255.255.0.0	10.8.1.1 / **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
Note: In a class C network with subnet mask 255.255.255.0 only the last segment of an IP address is translated			
Note: In a class B network with subnet mask 255.255.0.0 the last 2 segments of an IP address are translated			

How to configure Router 1 (Machine network 1), Router 2 (Machine network 2) and Router 3 (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 3 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 and Router 2 (connected at LAN port) 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 3 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 at the end of this document in chapter A5.

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 by IP address 192.168.2.110.

Due to the fact that the machine network Routers 1 and 2 have to 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 autonegotiation on the Ethernet Interface of the PC

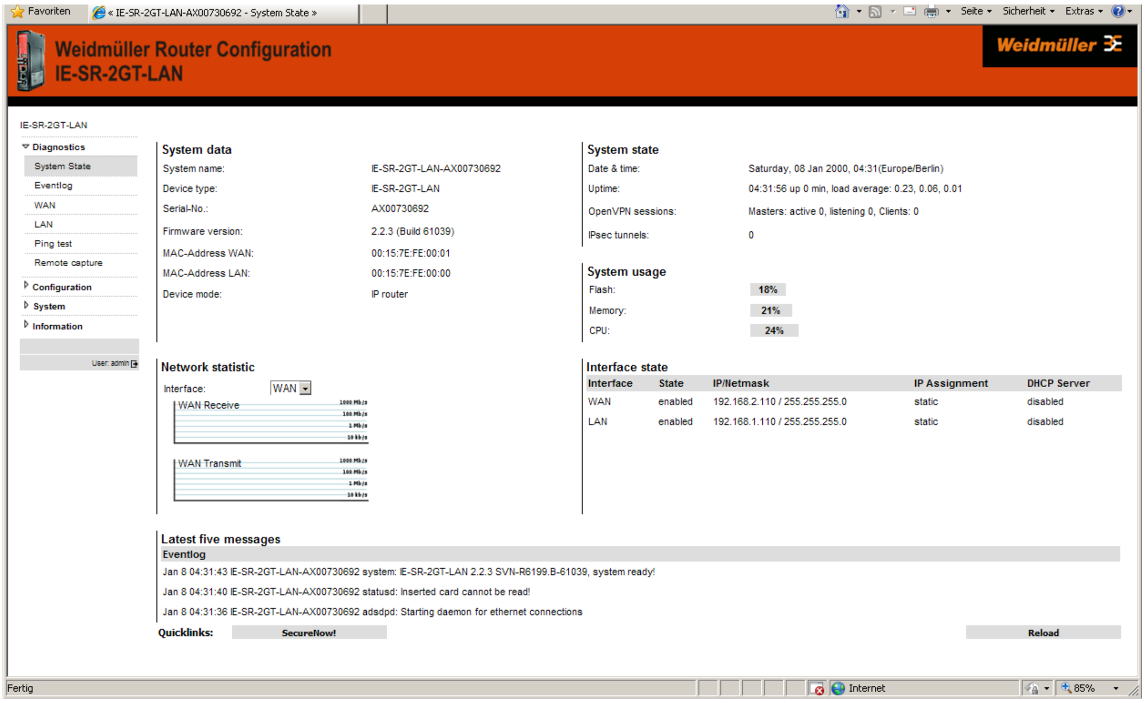
2. Change the IP address of the PC to one of the range 192.168.2.0

→ e.g.	IP address	192.168.2.100
	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 server of Router (http://192.168.2.110)

User: admin

Password: Detmold



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:31(Europe/Berlin)
Uptime:	04:31:56 up 0 min, load average: 0.23, 0.06, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	21%
CPU:	24%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled

Latest five messages

Eventlog

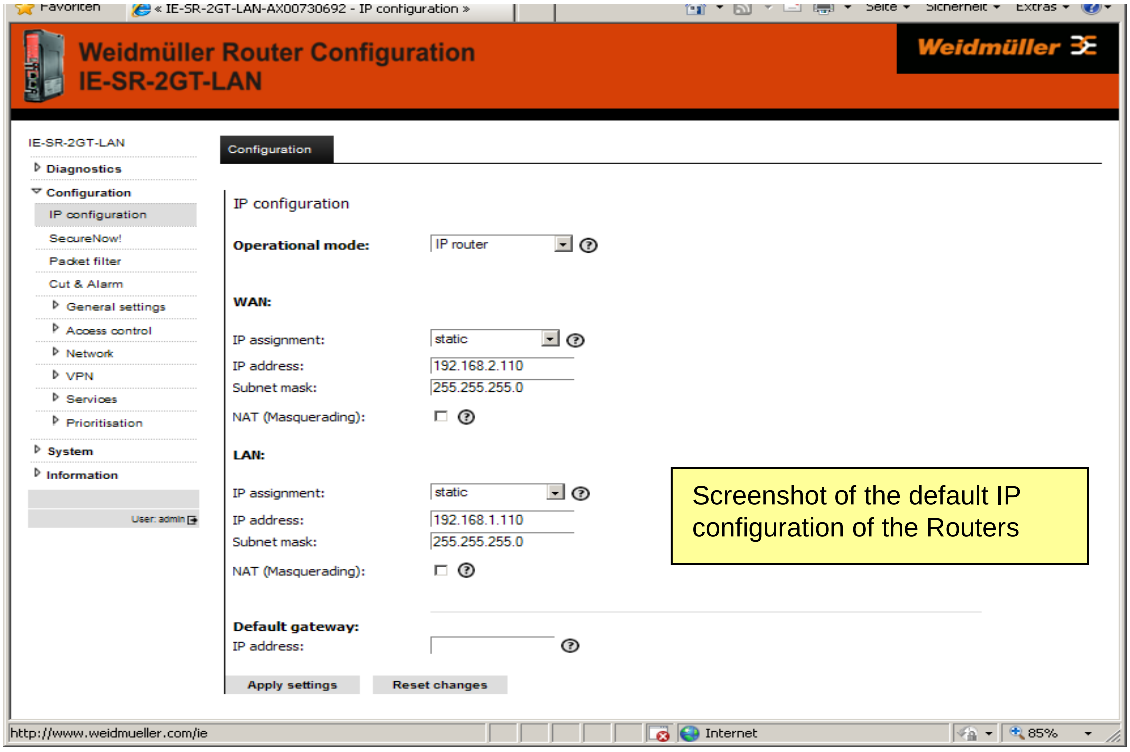
```
Jan 8 04:31:43 IE-SR-2GT-LAN-AX00730692 system: IE-SR-2GT-LAN 2.2.3 SVN-R6199.B-61039, system ready!
Jan 8 04:31:40 IE-SR-2GT-LAN-AX00730692 statusd: Inserted card cannot be read!
Jan 8 04:31:36 IE-SR-2GT-LAN-AX00730692 adsdpd: Starting daemon for ethernet connections
```

Quicklinks:

Figure A4-1: Login page of the Router (equivalent with menu Diagnostics → System State)

4. Set the basic IP configuration

► Select menu **Configuration → IP configuration**



IP configuration

Operational mode: IP router

WAN:

IP assignment: static

IP address: 192.168.2.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

LAN:

IP assignment: static

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

NAT (Masquerading): □

Default gateway:

IP address:

Screenshot of the default IP configuration of the Routers

Figure A4-2: Default values of menu **IP configuration**

► Configure the menu entries as following shown

Only for Router 1

Operational mode:	IP Router
IP address parameters WAN Port:	static
	172.16.1.252
	255.255.0.0 (Class B)
	NAT (masquerading) not set (leave checkbox empty)
IP address parameters LAN Port:	static
	192.168.20.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
Default gateway	172.16.1.254 (Router of the production network)

Leave „Default gateway“ empty if you test the „simple scenario“ with only 1 Router

Only for Router 2

Operational mode:	IP Router
IP address parameters WAN Port:	static
	172.16.1.253
	255.255.0.0 (Class B)
	NAT (masquerading) not set (leave checkbox empty)
IP address parameters LAN Port:	static

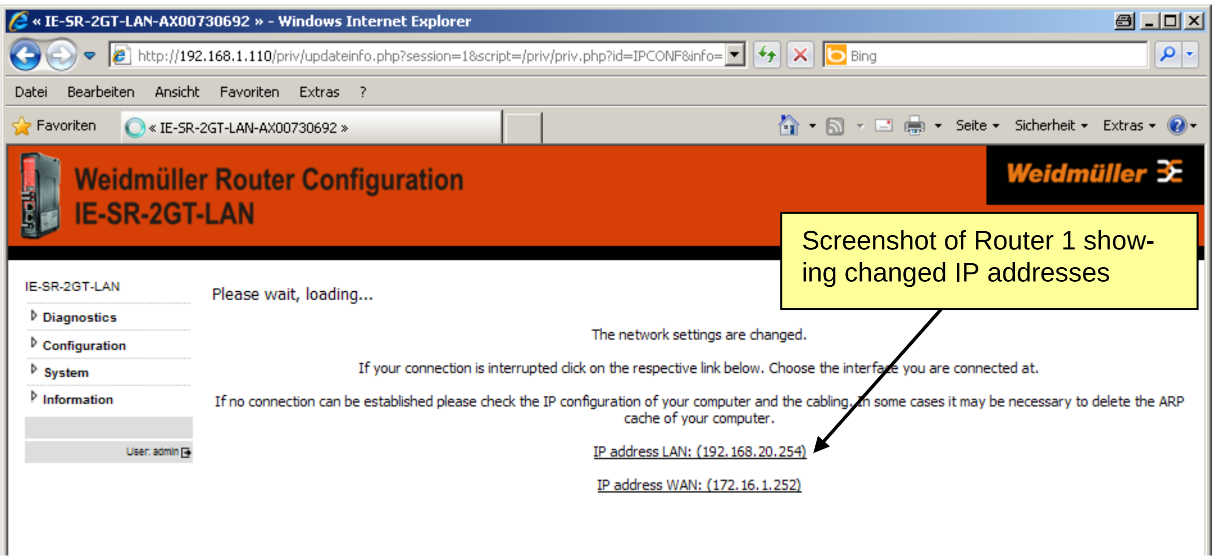
	192.168.21.254
	255.255.255.0 (Class C)
	NAT (masquerading) not set (leave checkbox empty)
Default gateway	172.16.1.254 (Router of the production network)

Only for Router 3

Operational mode:	IP Router
IP address parameters WAN Port:	static
	10.1.1.254
	255.255.0.0 (Class B)
	NAT (masquerading) not set (leave checkbox empty)
IP address parameters LAN Port:	static
	172.16.1.254
	255.255.0.0 (Class B)
	NAT (masquerading) not set (leave checkbox empty)
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.


« IE-SR-2GT-LAN-AX00730692 » - Windows Internet Explorer
http://192.168.1.110/priv/updateinfo.php?session=1&script=/priv/priv.php?id=IPCONF&info=
Bing
Datei
Bearbeiten
Ansicht
Favoriten
Extras
?
Favoriten
« IE-SR-2GT-LAN-AX00730692 »
Seite
Sicherheit
Extras
Weidmüller Router Configuration
IE-SR-2GT-LAN
Weidmüller
IE-SR-2GT-LAN
Diagnostics
Configuration
System
Information
User: admin

Please wait, loading...

The network settings are changed.

If your connection is interrupted click on the respective link below. Choose the interface you are connected at.

If no connection can be established please check the IP configuration of your computer and the cabling. In some cases it may be necessary to delete the ARP cache of your computer.

IP address LAN: (192.168.20.254)

IP address WAN: (172.16.1.252)

Screenshot of Router 1 showing changed IP addresses

Figure A4-3: Display of activated new IP addresses of LAN and 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 172.16.1.0/16

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 3 you also can chose e.g. IP address 172.16.1.100 (subnet mask 255.255.0.0) but you have to change the cable connection from WAN to LAN port due to the fact that Router 3 is connected to the production network by LAN port (see network diagram). Otherwise you have to use an IP address of the WAN port range 10.1.0.0.

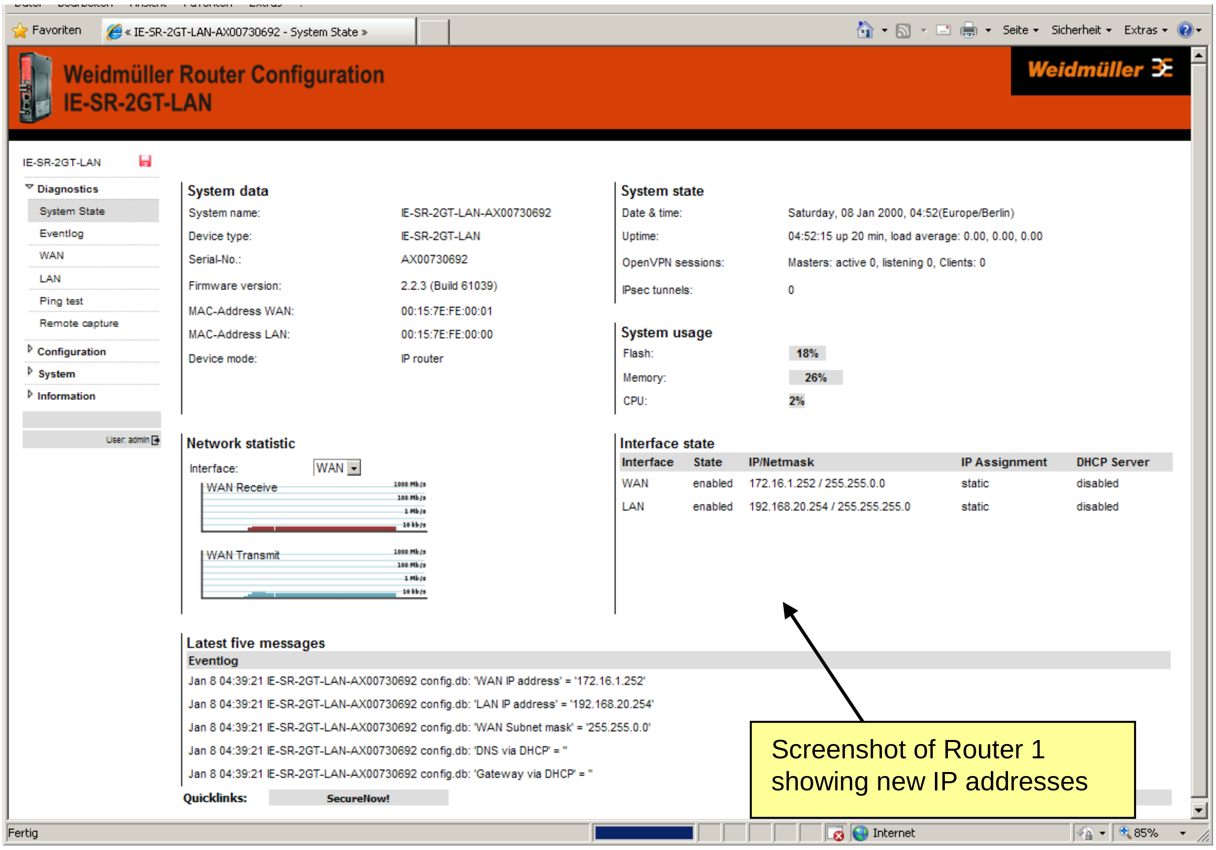
► Again login into the web interface of the Router using a web browser

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

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

Only for Router 3 : Use IP address 172.16.1.254 (http://172.16.1.254) on **LAN** port

User: admin
Password: Detmold



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:52(Europe/Berlin)
Uptime:	04:52:15 up 20 min, load average: 0.00, 0.00, 0.00
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	26%
CPU:	2%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	172.16.1.252 / 255.255.0.0	static	disabled
LAN	enabled	192.168.20.254 / 255.255.255.0	static	disabled

Latest five messages

Eventlog

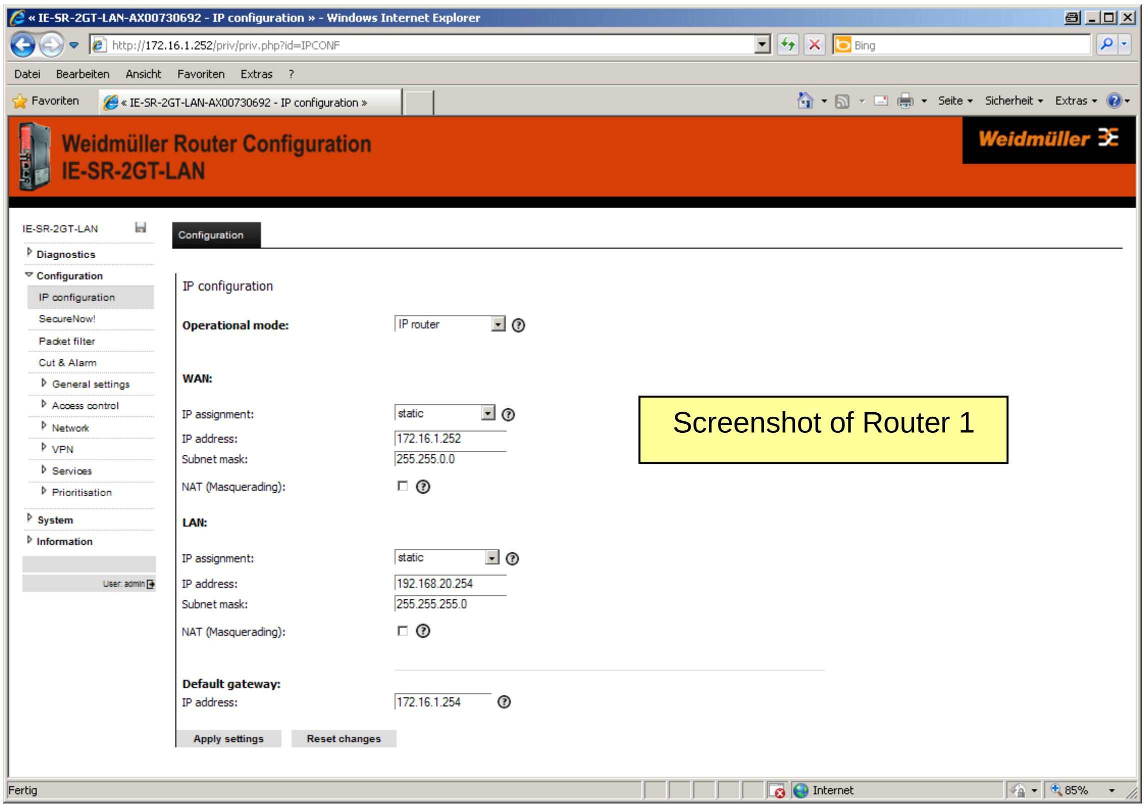
```
Jan 8 04:39:21 IE-SR-2GT-LAN-AX00730692 config.db: 'WAN IP address' = '172.16.1.252'
Jan 8 04:39:21 IE-SR-2GT-LAN-AX00730692 config.db: 'LAN IP address' = '192.168.20.254'
Jan 8 04:39:21 IE-SR-2GT-LAN-AX00730692 config.db: 'WAN Subnet mask' = '255.255.0.0'
Jan 8 04:39:21 IE-SR-2GT-LAN-AX00730692 config.db: 'DNS via DHCP' = ''
Jan 8 04:39:21 IE-SR-2GT-LAN-AX00730692 config.db: 'Gateway via DHCP' = ''
```

Quicklinks: SecureNow!

Screenshot of Router 1 showing new IP addresses

Figure A4-4: Web interface after login with changed IP addresses

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



« IE-SR-2GT-LAN-AX00730692 - IP configuration » - Windows Internet Explorer

http://172.16.1.252/priv/priv.php?id=IPCONF

Weidmüller Router Configuration
IE-SR-2GT-LAN

IP configuration

Operational mode: IP router

WAN:

IP assignment: static
IP address: 172.16.1.252
Subnet mask: 255.255.0.0
NAT (Masquerading): □

LAN:

IP assignment: static
IP address: 192.168.20.254
Subnet mask: 255.255.255.0
NAT (Masquerading): □

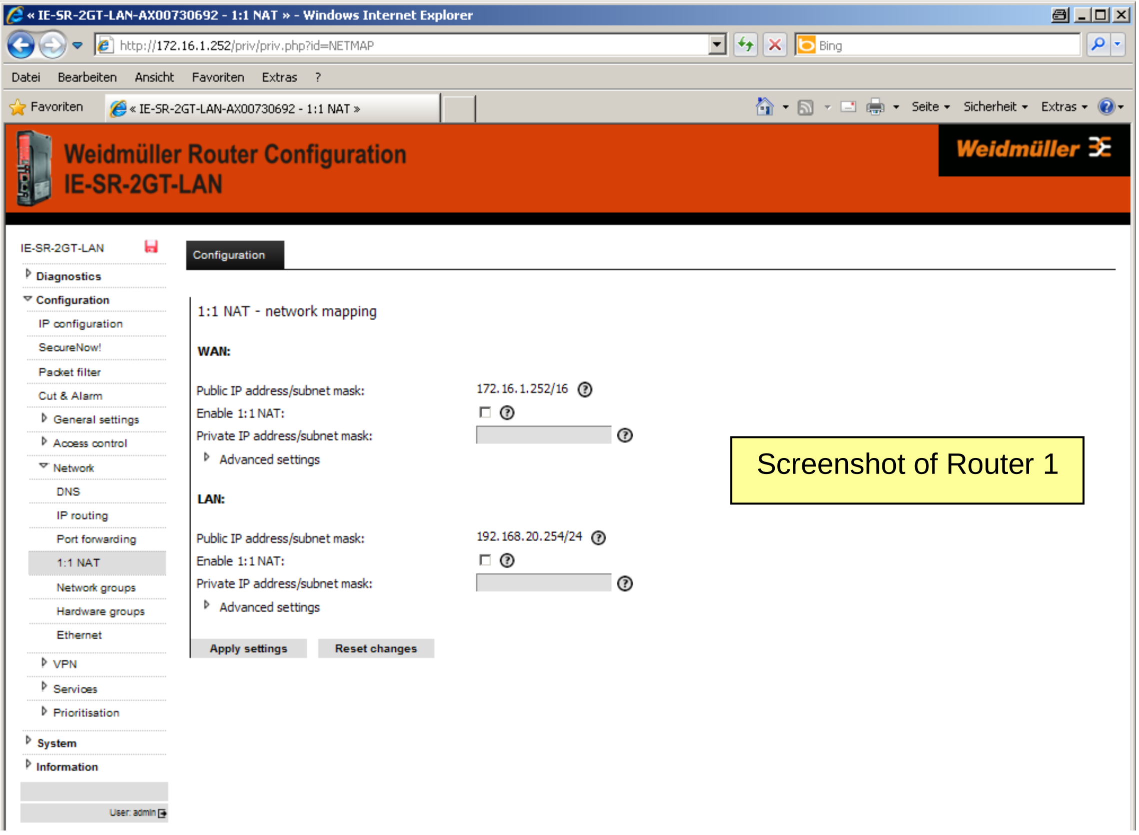
Default gateway:
IP address: 172.16.1.254

Screenshot of Router 1

Figure A4-5: New values of menu **IP configuration**

6. Configuring 1:1 NAT address translation (Do this only for Routers 1 and 2)

► Select menu Configuration → Network → 1:1 NAT



« IE-SR-2GT-LAN-AX00730692 - 1:1 NAT » - Windows Internet Explorer

http://172.16.1.252/priv/priv.php?id=NETMAP

Weidmüller Router Configuration
IE-SR-2GT-LAN

1:1 NAT - network mapping

WAN:

Public IP address/subnet mask: 172.16.1.252/16
Enable 1:1 NAT: □
Private IP address/subnet mask:
Advanced settings

LAN:

Public IP address/subnet mask: 192.168.20.254/24
Enable 1:1 NAT: □
Private IP address/subnet mask:
Advanced settings

Screenshot of Router 1

Figure A4-6: Default values of menu **1:1 NAT configuration**

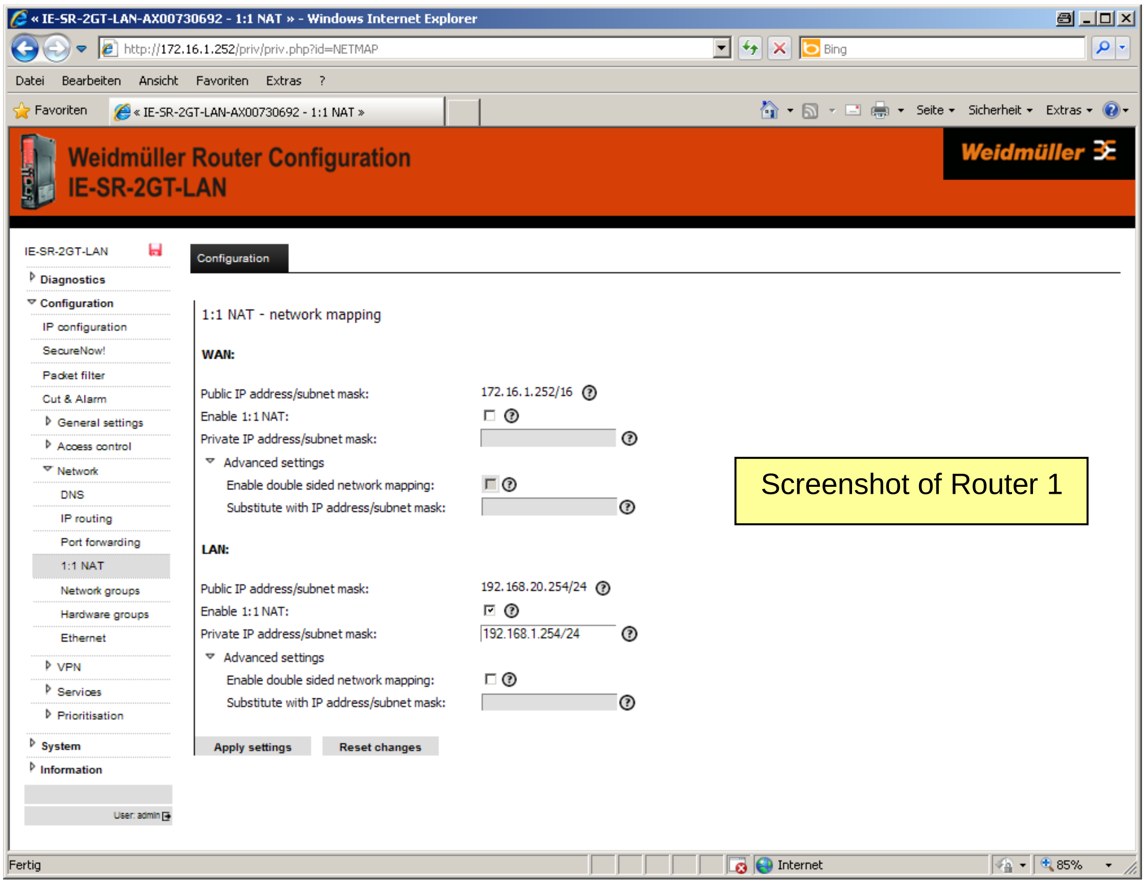
Configure below described entries on **both Routers 1 and 2** in the section **LAN:** of the “1:1 NAT configuration menu”.

► 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.



1:1 NAT - network mapping

WAN:

Public IP address/subnet mask: 172.16.1.252/16

Enable 1:1 NAT: □

Private IP address/subnet mask:

Advanced settings

Enable double sided network mapping: □

Substitute with IP address/subnet mask:

LAN:

Public IP address/subnet mask: 192.168.20.254/24

Enable 1:1 NAT: ☑

Private IP address/subnet mask: 192.168.1.254/24

Advanced settings

Enable double sided network mapping: □

Substitute with IP address/subnet mask:

Screenshot of Router 1

Figure A4-7: Changed values of menu **1:1 NAT configuration**

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 have to 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 1 of network 1 (**IP 192.168.1.1**) can be accessed by **public IP 192.168.20.1** from production network

Machine 2 of network 1 (**192.168.1.2**) can be accessed by **public IP 192.168.20.2** from production network

Machine N of network 1 (**192.168.1.n**) can be accessed by **public IP 192.168.20.n** from production network

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

Machine 1 of network 1 (**IP 192.168.1.1**) can be accessed by **public IP 192.168.21.1** from production network

Machine 2 of network 1 (**192.168.1.2**) can be accessed by **public IP 192.168.21.2** from production network

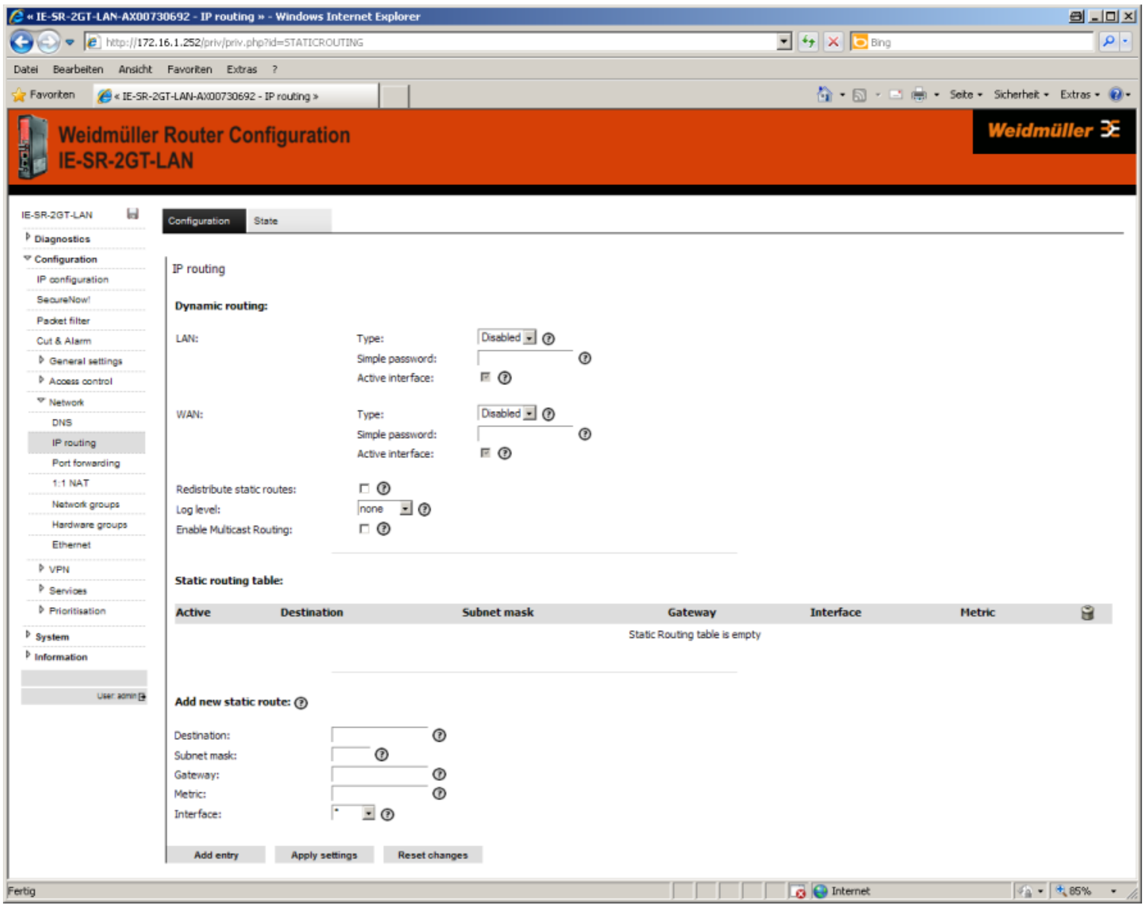
Machine N of network 1 (**192.168.1.n)** can be accessed by **public IP 192.168.21.n** from production network

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

7. Configuring static routes (Only for Router 3, skip if you test the"Ssimple scenario" with only 1 Router)

Next 2 static routes have to be configured on Router 3 that all Ethernet devices of machine networks networks 1 and 2 (behind LAN port of Routers 1 and 2) can get access to each other.

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



IP routing

Dynamic routing:

LAN:
Type: Disabled
Simple password:
Active interface: ☑

WAN:
Type: Disabled
Simple password:
Active interface: ☑

Redistribute static routes: □
Log level: none
Enable Multicast Routing: □

Static routing table:

Active	Destination	Subnet mask	Gateway	Interface	Metric

Static Routing table is empty

Add new static route:

Destination:
Subnet mask:
Gateway:
Metric:
Interface: *

Figure A4-8: Default values of menu **IP routing (Tab Configuration)**

Configure below described entries in the area **Add new static route** of the menu:

Only for Router 3 (This Router has 2 static routes)

Values for the first route:

- Destination network: 192.168.20.0 (Public address range of machine network 1 at LAN port of Router 1)
- Subnet mask : 24 (Class C)
- Gateway: 172.16.1.252 (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)

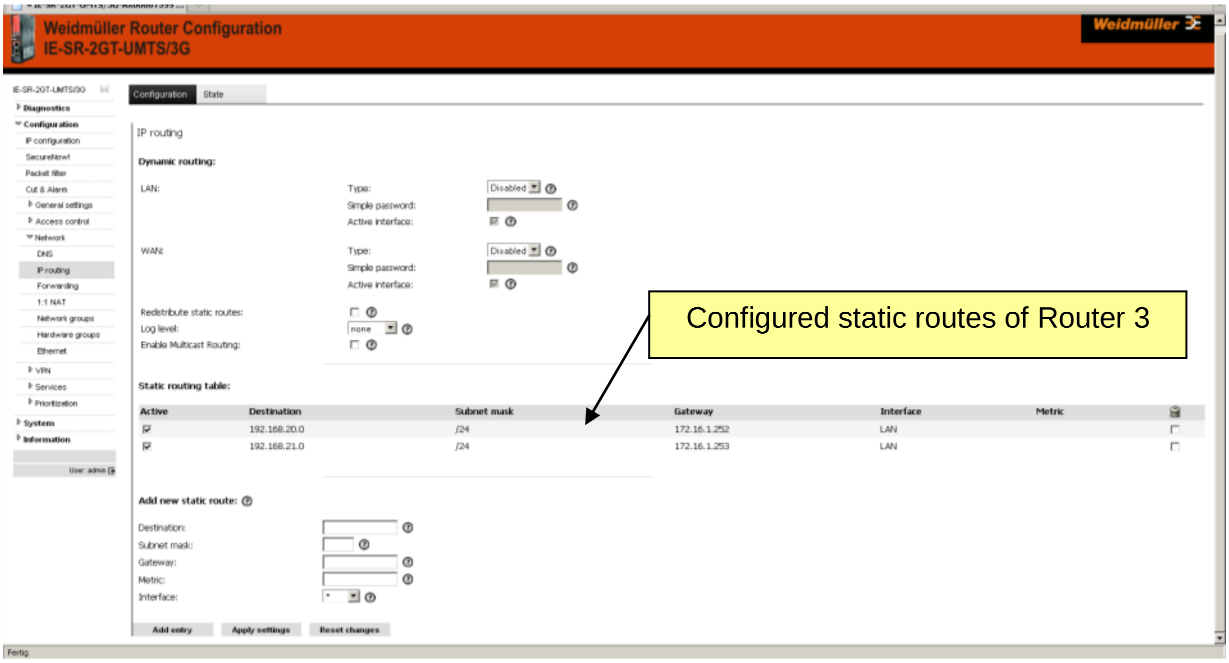
►Click button “Add entry” to add the new static route to the routing table.

Values for the second route:

- Destination network: 192.168.21.0 (Public address range of machine network 2 at LAN port of Router 2)
- Subnet mask: 24 (Class C)
- Gateway: 172.16.1.253 (Public address of WAN port of Router 2)
- Metric: Can be left blank (only one route, therefore no need for prioritization)
- Interface: **LAN** (Router 2 can be reached by LAN port)

►Click button “Add entry” to add the new static route to the routing table.

►Then click button “Apply settings” to activate the new settings.



IP routing

Dynamic routing:

LAN: Type: Disabled; Simple password: ; Active interface: ☑

WAN: Type: Disabled; Simple password: ; Active interface: ☑

Redistribute static routes: ☐
Log level: none
Enable Multicast Routing: ☐

Static routing table:

Active	Destination	Subnet mask	Gateway	Interface	Metric	
☑	192.168.20.0	/24	172.16.1.252	LAN		☐
☑	192.168.21.0	/24	172.16.1.253	LAN		☐

Add new static route:

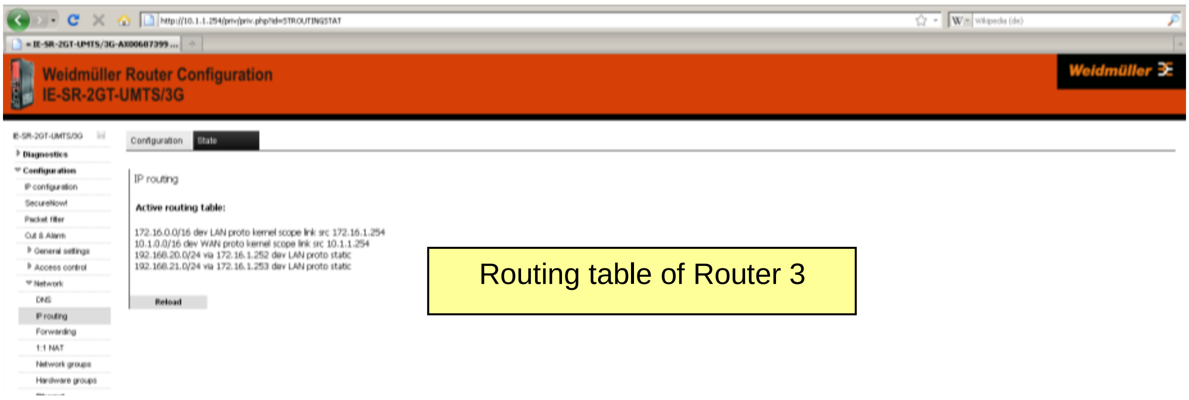
Destination:
Subnet mask:
Gateway:
Metric:
Interface: *

Configured static routes of Router 3

Figure A4-9: Changed values of menu **IP routing (Tab Configuration)** displaying 2 new static routes

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

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



IP routing

Active routing table:

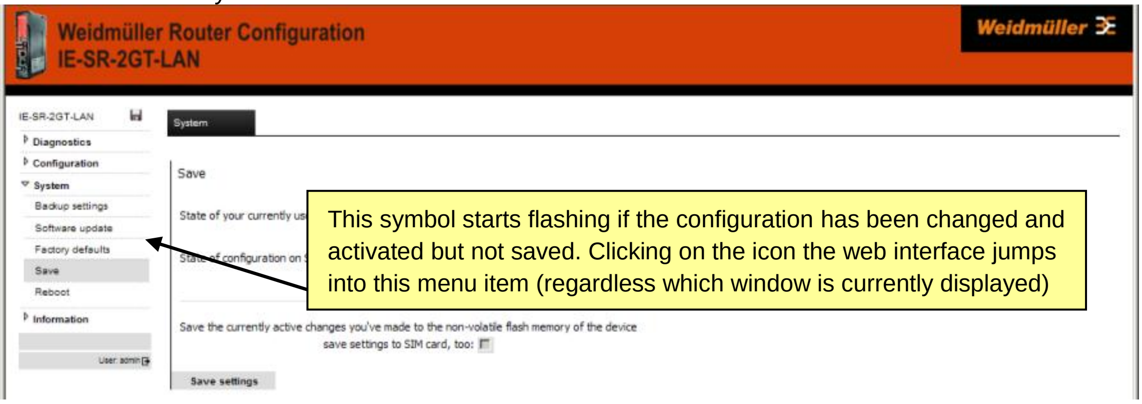
```
172.16.0.0/16 dev LAN proto kernel scope link src 172.16.1.254
10.1.0.0/16 dev WAN proto kernel scope link src 10.1.1.254
192.168.20.0/24 via 172.16.1.252 dev LAN proto static
192.168.21.0/24 via 172.16.1.253 dev LAN proto static
```

Routing table of Router 3

Figure A4-10: Menu **IP routing (Tab State)** showing the new active routing table

9. Saving the new configuration

► Select menu System → Save



Save

State of your currently us

State of configuration on S

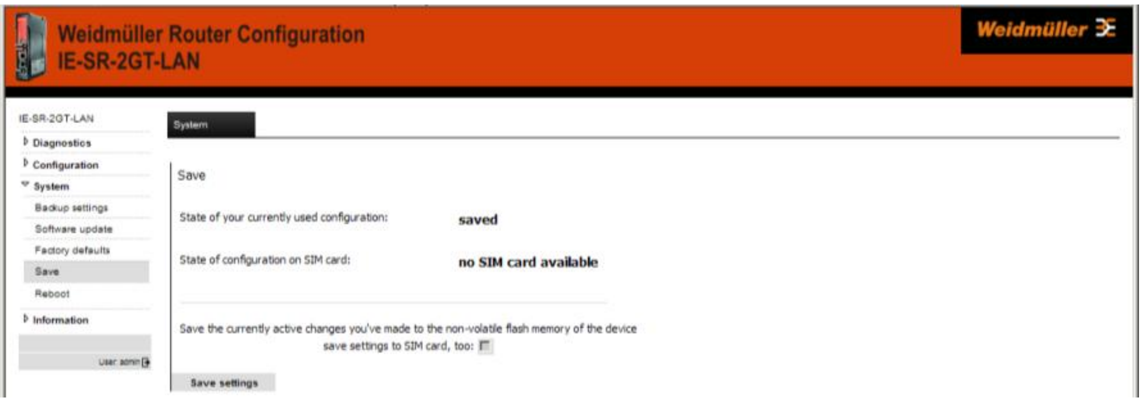
Save the currently active changes you've made to the non-volatile flash memory of the device

save settings to SIM card, too: □

This 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 which window is currently displayed)

Figure A4-11: Menu **System → Save** before saving the configuration

► 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.



Save

State of your currently used configuration: **saved**

State of configuration on SIM card: **no SIM card available**

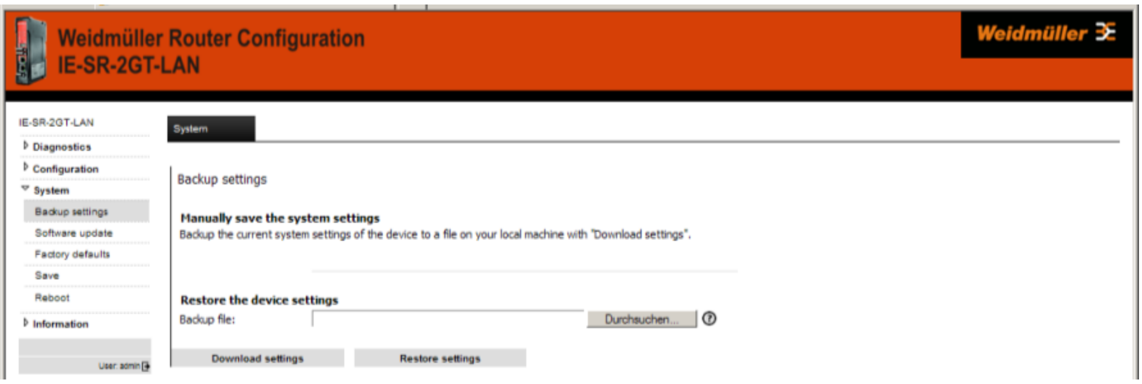
Save the currently active changes you've made to the non-volatile flash memory of the device

save settings to SIM card, too: □

Figure A4-12: Menu **System → Save** after saving the configuration

Additionally the configuration can be stored on the file system of the PC.

► Select menu **System → Backup settings**



Backup settings

Manually save the system settings

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

Restore the device settings

Backup file:

Figure A4-13: Menu **System → Backup settings** after saving the configuration

► 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!

Testing the configured feature 1:1 NAT

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 1 of network 1 is configured using following parameters:

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

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

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

1.1 Try to to send a ping request from machine **1** (192.168.1.100) of network **1** to PC of production network (172.16.1.20).

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

1.2 Try to to send a ping request from PC of production network (172.16.1.20) to machine **1** (192.168.1.100) of network **1** by using the public IP address 192.168.**20**.100.

Result: Machine 1 of network 2 should reply the “ping request” with reply IP address 192.168.**20**.100 (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 **1** (192.168.1.100) of network **1** to machine **1** (same IP 192.168.1.100) of network **2** by using the public IP address 192.168.**21**.100.

Result: Machine **1** of network **2** should reply the “ping request” with reply IP address 192.168.**21**.100 (due to configured 1:1 NAT).

2.2 Try to send a ping request from machine **1** (192.168.1.100) of network **2** to machine **1** (same IP 192.168.1.100) of network **1** by using the public IP address 192.168.**20**.100.

Result: Machine **1** of network **2** should reply the “ping request” with reply IP address 192.168.**20**.100 (due to configured 1:1 NAT).

Note: If you perform the “ping” test please ensure that the firewall configuration of the PC is not blocking the test.

A5 - Using dynamic IP routing as an alternative for manually configuring static routes

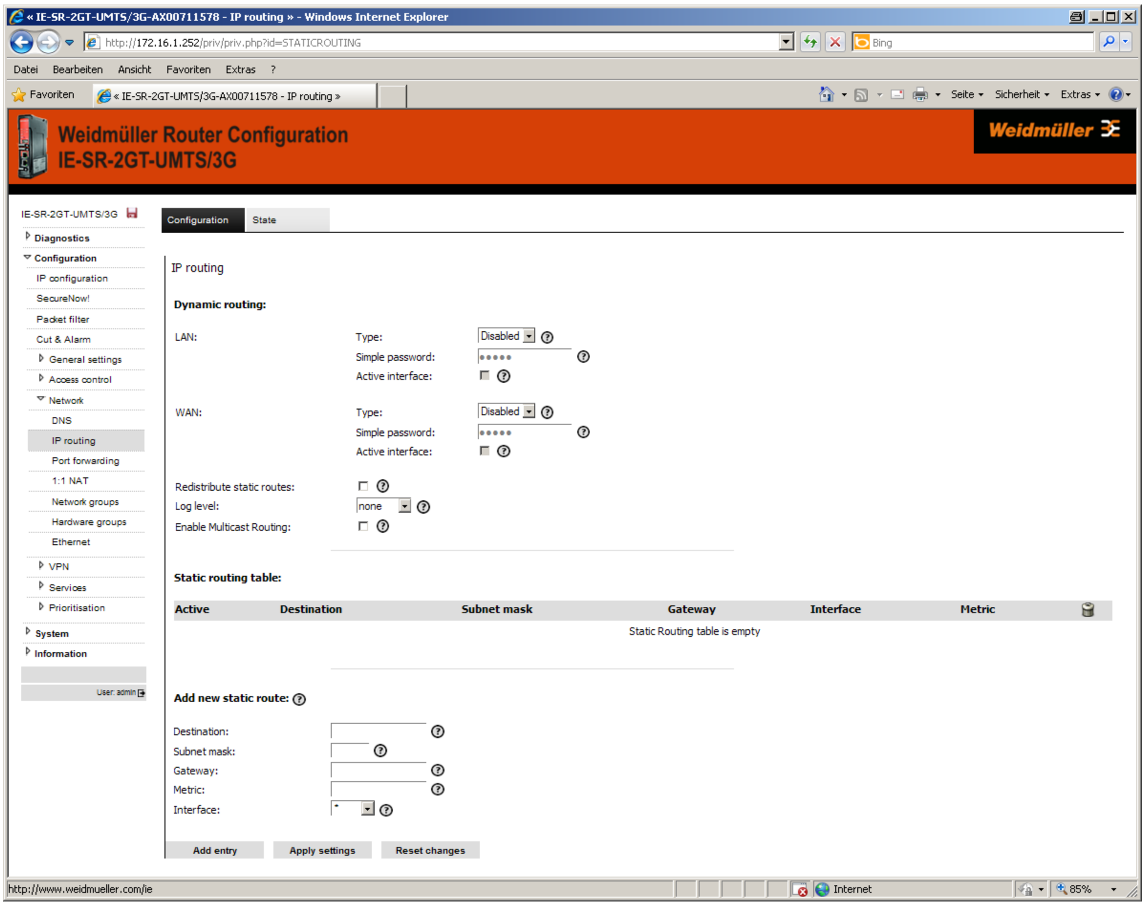
Instead of configuring static routes on Router 3 it is more comfortable to use the “dynamic IP routing” feature to announce the routes of all Router network interfaces to each Router. For announcing the routing information the protocols RIP or OSPF can be used.

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 chose alternatively the “newer” protocol OSPF (Open shortest path first). Both are working properly.

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



IP routing

Dynamic routing:

LAN: Type: Disabled
Simple password: •••••
Active interface: □

WAN: Type: Disabled
Simple password: •••••
Active interface: □

Redistribute static routes: □
Log level: none
Enable Multicast Routing: □

Static routing table:

Active	Destination	Subnet mask	Gateway	Interface	Metric

Static Routing table is empty

Add new static route:

Destination:
Subnet mask:
Gateway:
Metric:
Interface: *

Figure A5-1: Default values of menu **IP routing (Tab Configuration)** → Dynamic routing is disabled

Configure below described entries in the section Dynamic routing of the menu:

→ Configure the below described parameters for all Routers 1, 2 and 3

LAN:	● Type:	Select “RIP”
	● Simple password:	Free text **Note:** If there are several Routers with activated RIP but only the Routers 1, 2 and 3 should exchange their routing tables, then you have to use the same password for each Router.
	● Active interface:	Activate the checkbox if the Router shall send the routing table to the **LAN** port (to other Routers)

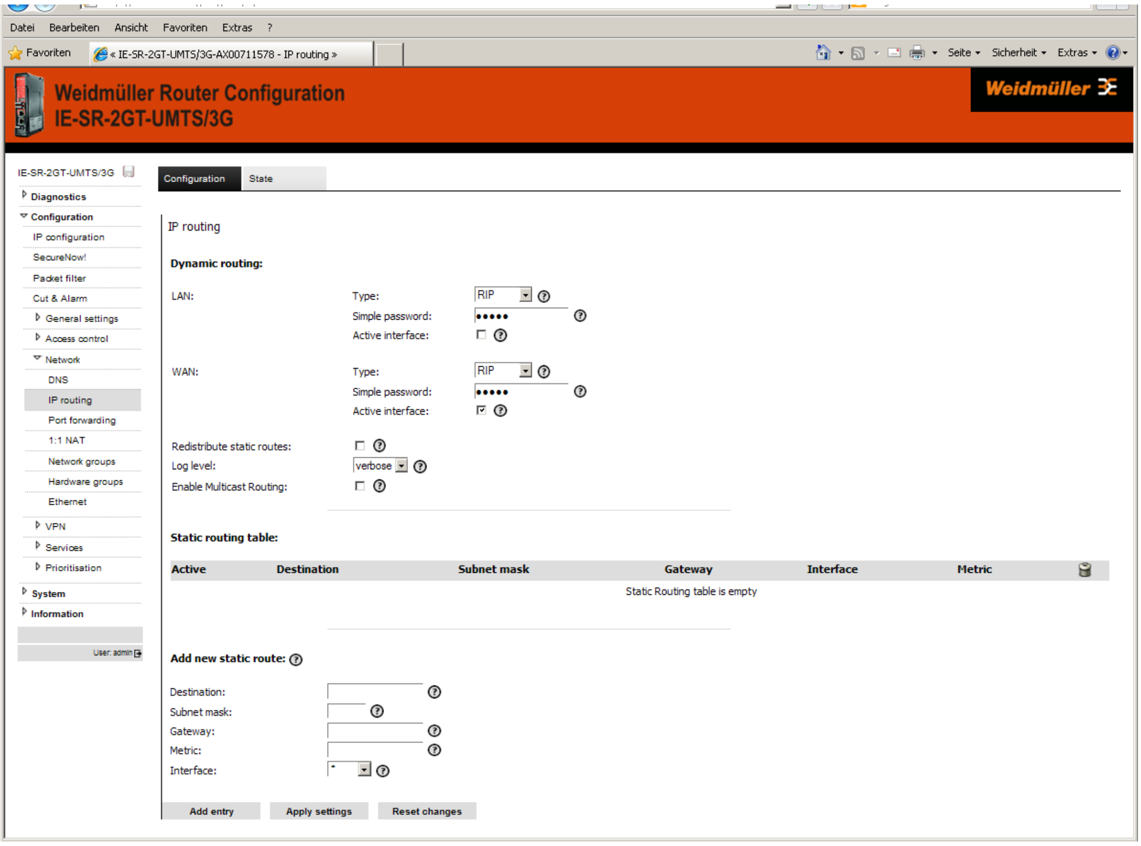
WAN:	● Type:	Select “RIP”
	● Simple password:	→ see explanation above
	● Active interface:	Activate the checkbox if the Router shall send the routing table to the **WAN** port (to other Routers)

Note:

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 chose how detailed information about RIP will be shown in the menu Eventlog.

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



IP routing

Dynamic routing:

LAN: Type: RIP
Simple password: •••••
Active interface: □

WAN: Type: RIP
Simple password: •••••
Active interface: ☑

Redistribute static routes: □
Log level: verbose
Enable Multicast Routing: □

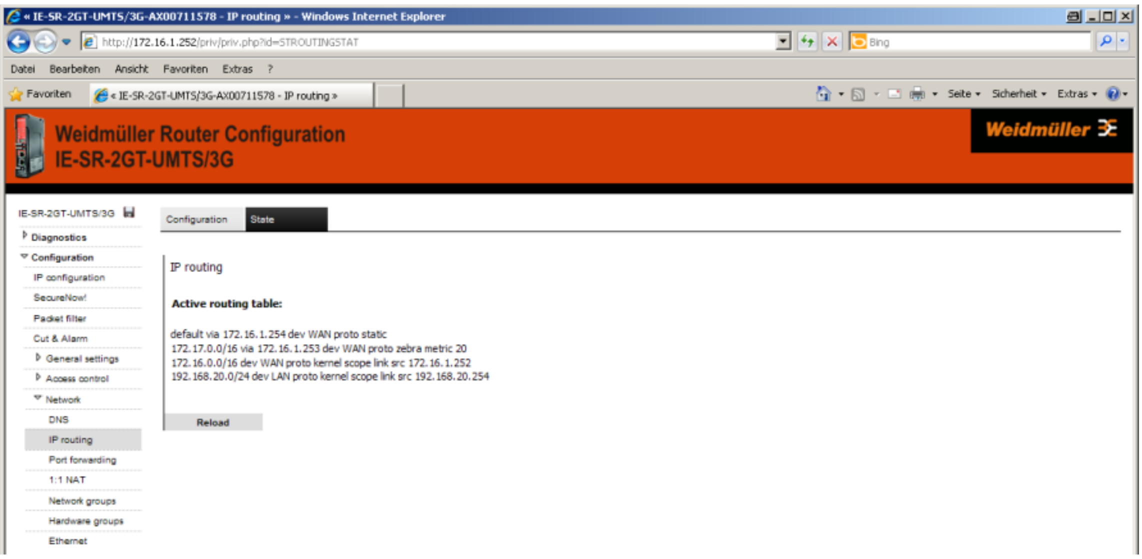
Static routing table:

Active	Destination	Subnet mask	Gateway	Interface	Metric
Static Routing table is empty					

Add new static route:

Destination:
Subnet mask:
Gateway:
Metric:
Interface: *

Figure A5-2: Configured dynamic IP routing



IP routing

Active routing table:

```
default via 172.16.1.254 dev WAN proto static
172.17.0.0/16 via 172.16.1.253 dev WAN proto zebra metric 20
172.16.0.0/16 dev WAN proto kernel scope link src 172.16.1.252
192.168.20.0/24 dev LAN proto kernel scope link src 192.168.20.254
```

Figure A5-3: Menu **IP routing (Tab State)** showing the new active routing table

Testing the accessibility between Ethernet Devices of network 1 and 2

1. Send a ping request from Machine 1 of Network 1 to Machine 1 of Network 2
   Send “ping 192.168.21.100” (this ist the public IP address of Machine 1 of Network 2, translated by
   1:1 NAT from 192.168.1.100 to from 192.168.21.100)

1. Send a ping request from Machine 1 of Network 2 to Machine 1 of Network 1
   Send “ping 192.168.20.100” (this ist the public IP address of Machine 1 of Network 1, translated by
   1:1 NAT from 192.168.1.100 to from 192.168.20.100)

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).

B. Application scenarios (Uses cases) for VPN (Virtual private networks)

B1 - OpenVPN based remote access application via "Meeting Point"

Description of a remote access application to allow a communication between protected, not directly accessible machine networks and remote Service-PC's by using a public OpenVPN-Server as „Meeting-Point"

Please **download** this technical note from the Weidmüller website using the following path:

1. Open http://www.weidmueller.com/IE
2. Select section „Industrial Ethernet" → „Documents"
3. Scroll down to section „Technical Notes"
4. Download the file „TechNote-RemoteAccess_via_Router_and_MeetingPoint_V1_??.pdf"

B2 - Configuring an OpenVPN remote access scenario using a Weidmüller Router as OpenVPN-Server

Please **download** this technical note from the Weidmüller website using the following path:

1. Open http://www.weidmueller.com/IE
2. Select section „Industrial Ethernet" → „Documents"
3. Scroll down to section „Technical Notes"
4. Download the file „TechNote-RemoteAccess_via_Router_as_OpenVPN_Server_V1_??.pdf"

B3 - Configuring an IPsec scenario between 2 Routers (Client and Server)

This document is currently in preparation. Please check if this technical note is available from the Weidmüller website using the following path:

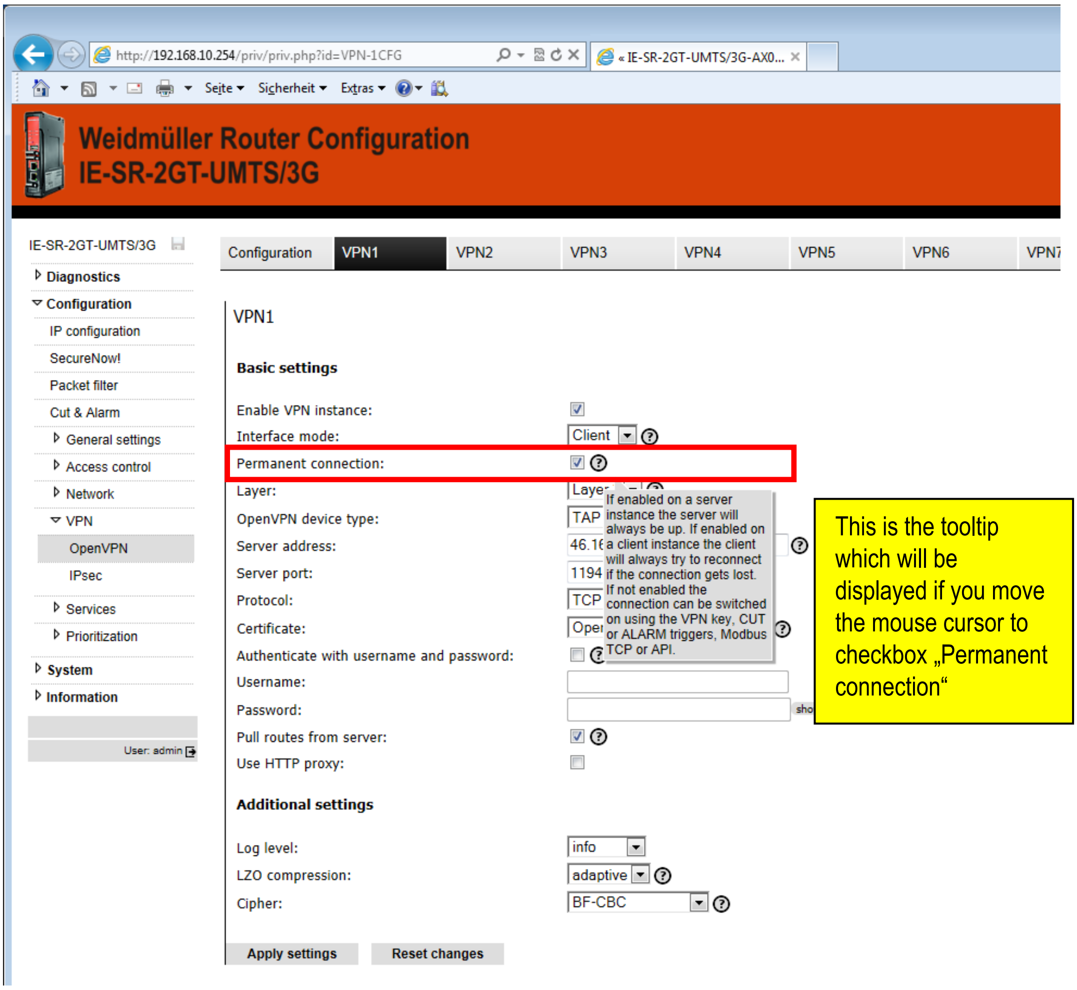
1. Open http://www.weidmueller.com/IE
2. Select section „Industrial Ethernet" → „Documents"
3. Scroll down to section „Technical Notes"

C. Additional application notes

C1- How to start and stop a pre-defined OpenVPN connection by external 24 VDC input

In this example a pre-defined OpenVPN client connection (at tab VPN1) will be configured to be started and stopped by external 24 VDC input.

C1.1 Go into the Web-Interface and select OpenVPN menu.
C1.2 Select the configured VPN session (here tab VPN1 as shown below).



VPN1

Basic settings

Enable VPN instance: ☑
Interface mode: Client
Permanent connection: ☑
Layer: Laye
OpenVPN device type: TAP
Server address: 46.16
Server port: 1194
Protocol: TCP
Certificate: Ope
Authenticate with username and password: □
Username:
Password:
Pull routes from server: ☑
Use HTTP proxy: □

If enabled on a server instance the server will always be up. If enabled on a client instance the client will always try to reconnect 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.

Additional settings

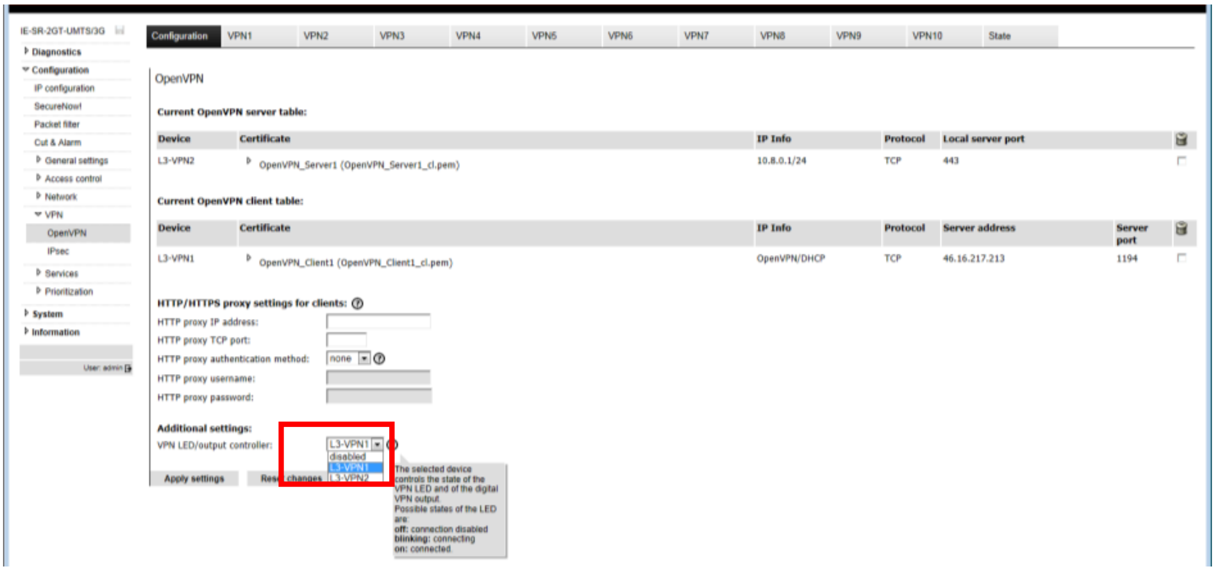
Log level: info
LZO compression: adaptive
Cipher: BF-CBC

This is the tooltip which will be displayed if you move the mouse cursor to checkbox „Permanent connection“

C1.3 Disable (Clear) checkbox “Permanent connection”.
→ Now the OpenVPN-Client configuration will not automatically try to connect an OpenVPN-Server but it will start a connection by external 24 VDC input (connector “VPN initiate”). A connected OpenVPN tunnel will be stopped by removing the external 24 VDC input.

C1.4 Click “Apply settings”.

C1.5 If a connected OpenVPN tunnel shall be signalized by LED “VPN” and digital output connector “VPN active”, select tab “Configuration” of OpenVPN menu, goto field “VPN LED / Output Controller” and select the desired VPN tunnel (below screenshot shows selected L3-VPN1 session).



OpenVPN

Current OpenVPN server table:

Device	Certificate	IP Info	Protocol	Local server port	
L3-VPN2	OpenVPN_Server1 (OpenVPN_Server1_cl.pem)	10.8.0.1/24	TCP	443	□

Current OpenVPN client table:

Device	Certificate	IP Info	Protocol	Server address	Server port	
L3-VPN1	OpenVPN_Client1 (OpenVPN_Client1_cl.pem)	OpenVPN/DHCP	TCP	46.16.217.213	1194	□

HTTP/HTTPS proxy settings for clients:

HTTP proxy IP address:

HTTP proxy TCP port:

HTTP proxy authentication method: none

HTTP proxy username:

HTTP proxy password:

Additional settings:

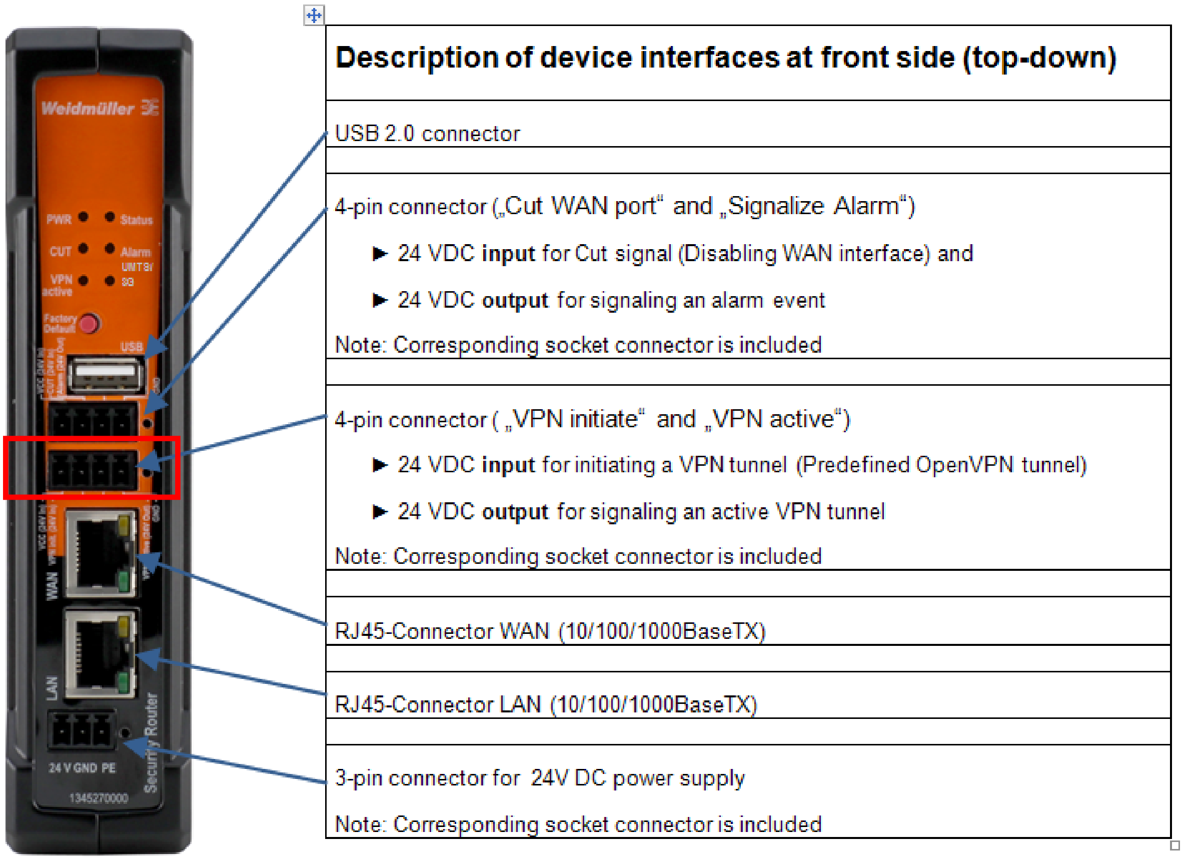
VPN LED/output controller: L3-VPN1 (disabled / L3-VPN1 / L3-VPN2)

The selected device controls the state of the VPN LED and of the digital VPN output.
Possible states of the LED are:
off: connection disabled
blinking: connecting
on: connected

C1.6 Click “Apply settings”

C1.7 To activate the “not permanent” configured OpenVPN connection provide 2 pins of the 4-pin con nector named “VPN initiate / VPN active” with 24 VDC. If you disconnect the power then the VPN tunnel will be closed.

See below described pin assigment.



Description of device interfaces at front side (top-down)

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

Note: Corresponding socket connector is included

4-pin connector („VPN initiate“ and „VPN active“)

- 24 VDC **input** for initiating a VPN tunnel (Predefined OpenVPN tunnel)
- 24 VDC **output** for signaling an active VPN tunnel

Note: Corresponding socket connector is included

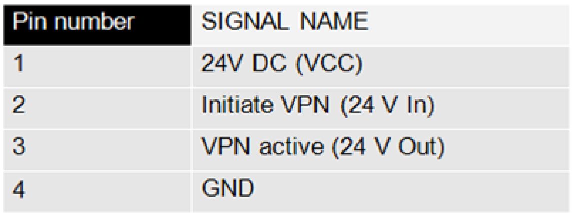
RJ45-Connector WAN (10/100/1000BaseTX)

RJ45-Connector LAN (10/100/1000BaseTX)

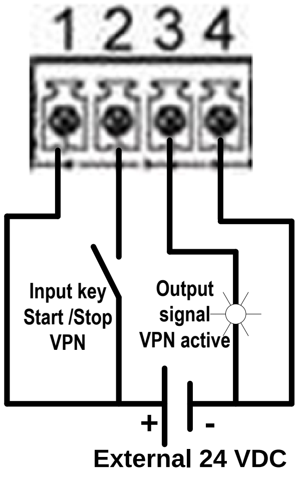
3-pin connector for 24V DC power supply

Note: Corresponding socket connector is included

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



C2- Description how to disable the Ethernet connection at WAN port

The Ethernet WAN port can physically disabled using several methods:

Method 1: Hardware-based disconnection (Cut) by external digital input

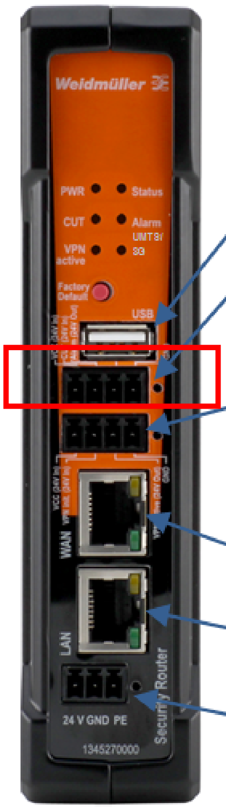
Method 2: Software-based disconnection by a Firewall-rule

Method 3: Software-based disconnection by feature “Client monitoring”

Method 1: Hardware-based disconnection of WAN port by external digital input

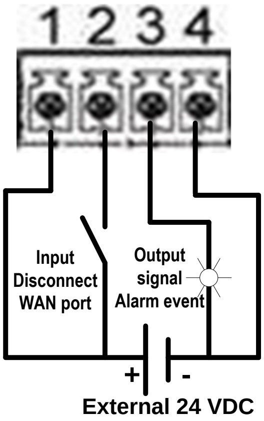
To disconnect the WAN port provide 2 pins of the 4-pin connector named “CUT Wan port / Signalize Alarm” with 24 VDC. If you disconnect the power then the WAN port will be activated again. See below described pin assigment.

Note: Disconnecting the WAN port by digital input overrules the software-based CUT events.



Description of device interfaces at front side (top-down)
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 Note: Corresponding socket connector is included
4-pin connector („VPN initiate“ and „VPN active“) ► 24 VDC **input** for initiating a VPN tunnel (Predefined OpenVPN tunnel) ► 24 VDC **output** for signaling an active VPN tunnel Note: Corresponding socket connector is included
RJ45-Connector WAN (10/100/1000BaseTX)
RJ45-Connector LAN (10/100/1000BaseTX)
3-pin connector for 24V DC power supply Note: Corresponding socket connector is included

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

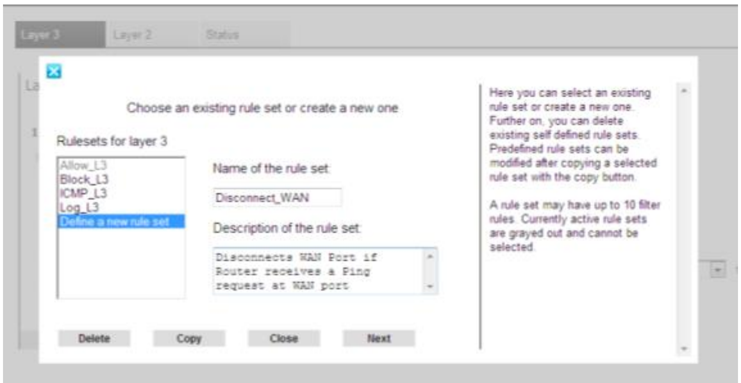


Method 2: Software-based disconnection of WAN port by Firewall-rule

Inside of a Firewall-rule it can be configured that the WAN port will be disconnected if this Firewall-rule matches.

As an example below we create a Firewall-rule which will deactivate the WAN port if a device is sending a ping request incoming into the WAN port and outgoing to a device connected at the LAN port.

C2.1 Goto menu Configuration → Packet filter
C2.2 Click the “+” icon (Add a new rule-set)
C2.3 Mark Define a new rule-set and enter the name and the description of the rule-set as shown below



Choose an existing rule set or create a new one

Rulesets for layer 3

- Allow_L3
- Block_L3
- ICMP_L3
- Log_L3
- Define a new rule set

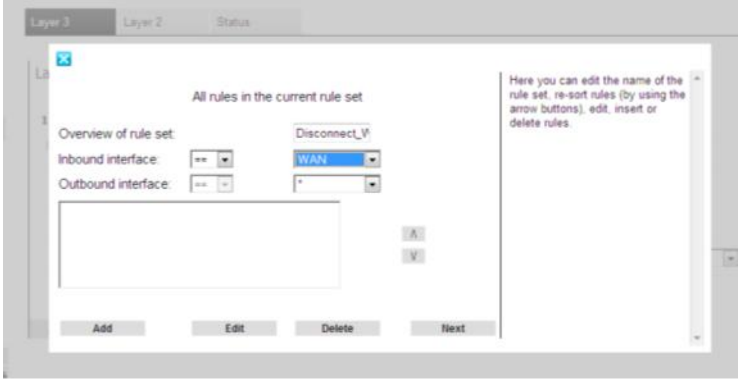
Name of the rule set: Disconnect_WAN

Description of the rule set: Disconnects WAN Port if Router receives a Ping request at WAN port

Here you can select an existing rule set or create a new one. Further on, you can delete existing self defined rule sets. Predefined rule sets can be modified after copying a selected rule set with the copy button.

A rule set may have up to 10 filter rules. Currently active rule sets are grayed out and cannot be selected.

C2.4 Click button “Next”



All rules in the current rule set

Overview of rule set: Disconnect_V

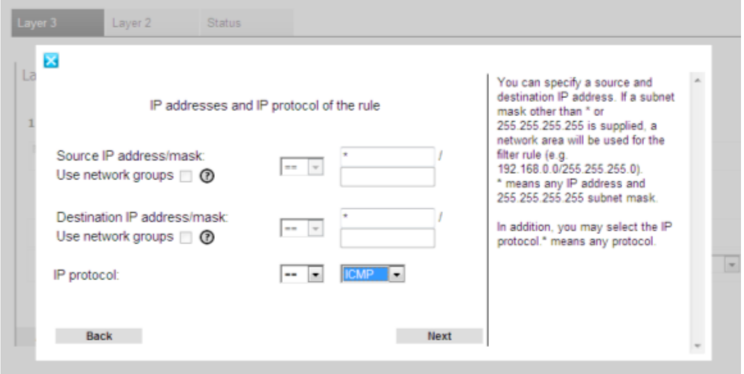
Inbound interface: -- WAN

Outbound interface: -- *

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

C2.5 Select Inbound Interface = WAN

C2.6 Click button “Add” to create the first rule of the rule-set “Disconnect_WAN”



IP addresses and IP protocol of the rule

Source IP address/mask: -- * /

Use network groups □

Destination IP address/mask: -- * /

Use network groups □

IP protocol: -- ICMP

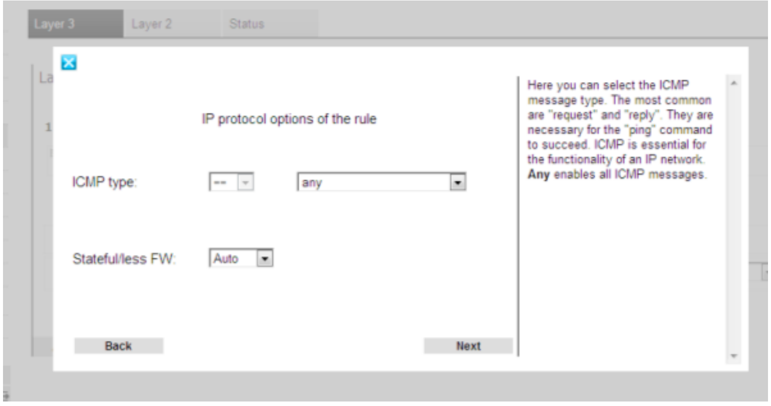
You can specify a source and destination IP address. If a subnet mask other than * or 255.255.255.255 is supplied, a network area will be used for the filter rule (e.g. 192.168.0.0/255.255.255.0). * means any IP address and 255.255.255.255 subnet mask.

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

C2.7 Enter * in both fields “Source IP address” and “Destination IP address”

C2.8 Select IP protocol = ICMP

C2.9 Click button “Next”



IP protocol options of the rule

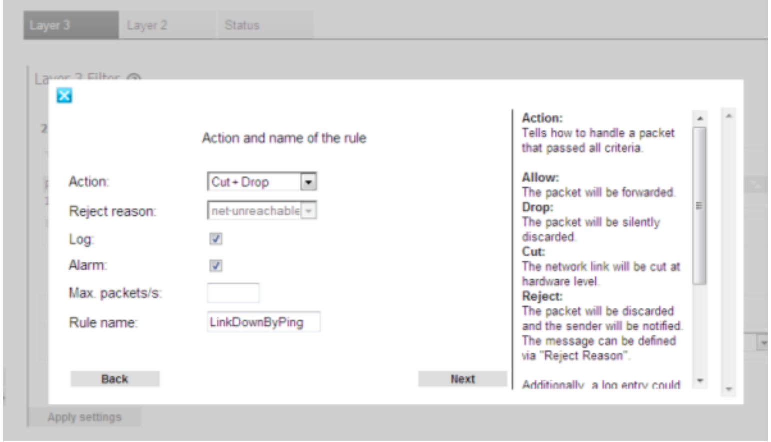
ICMP type: -- any

Stateful/less FW: Auto

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.

C2.10 Leave “ICMP type” as default (any)

C2.11 Click button “Next”



Action and name of the rule

Action: Cut + Drop

Reject reason: net-unreachable

Log: ☑

Alarm: ☑

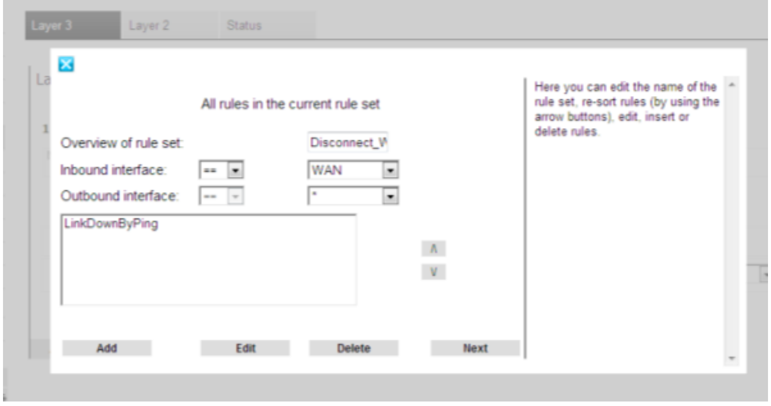
Max. packets/s:

Rule name: LinkDownByPing

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

C2.12 Select “Action” = Cut + Drop
C2.13 Enable checkboxes Log and Alarm to signalize a CUT in the Event-Log and to switch-on the Alarm-LED at frontside of the Router
C2.14 Enter the name of the rule (max. 15 characters)
C2.15 Click button “Next”



All rules in the current rule set

Overview of rule set: Disconnect_W

Inbound interface: -- WAN

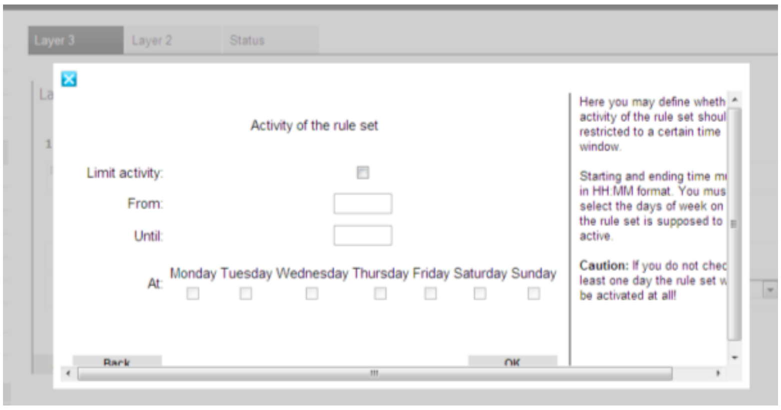
Outbound interface: -- *

LinkDownByPing

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 rule “LinkDownByPing” is created. We do not need any further rules.

C2.16 Click button Next to finish creating the rule-set



Activity of the rule set

Limit activity: □

From:

Until:

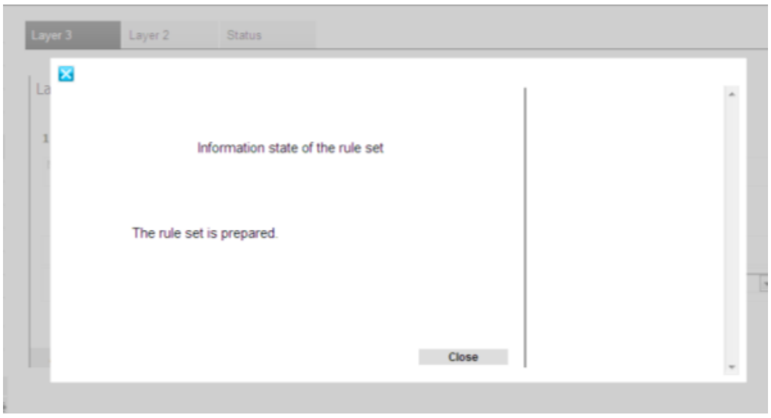
At: Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday □

Here you may define wheth activity of the rule set shoul restricted to a certain time window.

Starting and ending time mu in HH:MM format. You mus select the days of week on the rule set is supposed to active.

Caution: If you do not chec least one day the rule set w be activated at all!

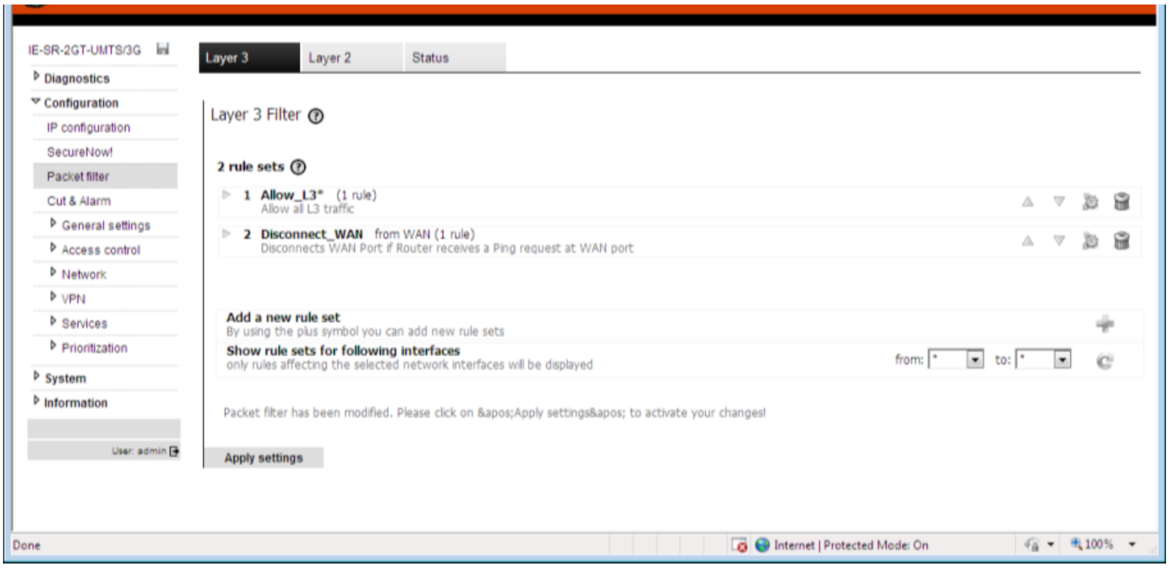
C2.17 Click button “OK” cause we do not set any time limits



Information state of the rule set

The rule set is prepared.

C2.18 Click button “Close” to finish the rule-set creation



Layer 3 Filter

2 rule sets

1 **Allow_L3*** (1 rule)
Allow all L3 traffic

2 **Disconnect_WAN** from WAN (1 rule)
Disconnects WAN Port if Router receives a Ping request at WAN port

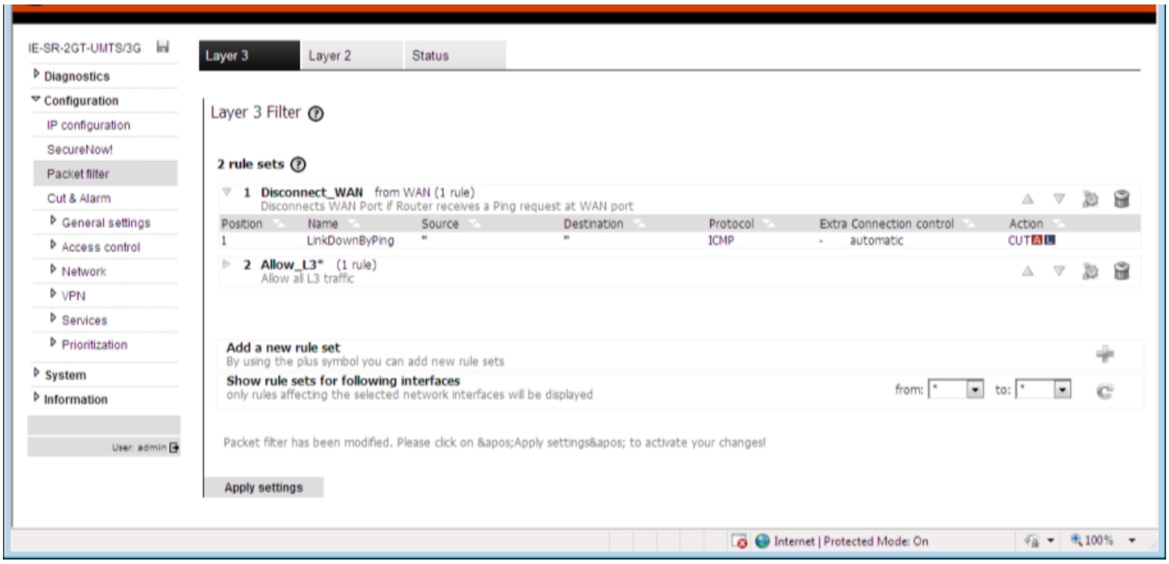
Add a new rule set
By using the plus symbol you can add new rule sets

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 &apos;Apply settings&apos; to activate your changes!

Apply settings

Now the new rule-set Disconnect_WAN will be displayed in the Layer3-Filter-table. We need to change the position of the new rule-set to top-most cause the Packet filter (Firewall) checks the rules from top to bottom. Due to the fact that the default filter rule “Allow_L3” is always matching for each traffic the new rule-set never would be used.



Layer 3 Filter

2 rule sets

1 **Disconnect_WAN** from WAN (1 rule)
Disconnects WAN Port if Router receives a Ping request at WAN port

Position	Name	Source	Destination	Protocol	Extra	Connection control	Action
1	LinkDownByPing	*	*	ICMP	-	automatic	CUT

2 **Allow_L3*** (1 rule)
Allow all L3 traffic

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

Show rule sets for following interfaces
only rules affecting the selected network interfaces will be displayed
from: * to: *

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

Apply settings

C2.19 Change the position of rule-set “Disconnect_WAN” to be the topmost by clicking the arrow-icon

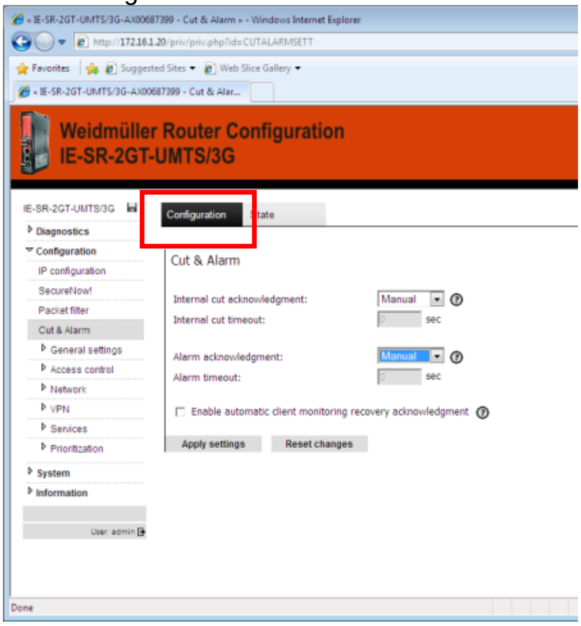
C2.20 Click button “Apply settings” to activate the new firewall-filter

Important:
Before testing the CUT function we have to determine how to re-activate a disconnected WAN port. This has to be done in the menu Cut & Alarm.

C2.21 Select menu Configuration → Cut & Alarm

By default a triggered CUT or Alarm event has to be **re-set** manually as shown below left. To re-set manually triggered events change to tab State and click buttons “Reset cut signal” and/or “Reset alarm signal”

Tab “Configuration”



Cut & Alarm

Internal cut acknowledgment: Manual

Internal cut timeout: 0 sec

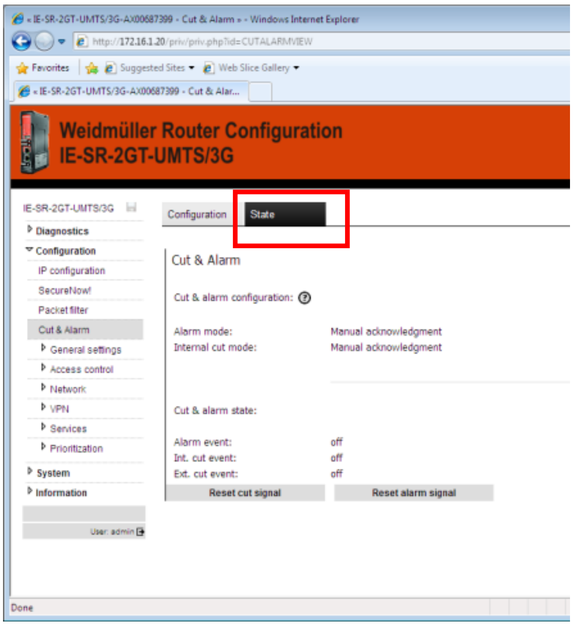
Alarm acknowledgment: Manual

Alarm timeout: 0 sec

☐ Enable automatic client monitoring recovery acknowledgment

Apply settings Reset changes

Tab “State”



Cut & Alarm

Cut & alarm configuration:

Alarm mode: Manual acknowledgment

Internal cut mode: Manual acknowledgment

Cut & alarm state:

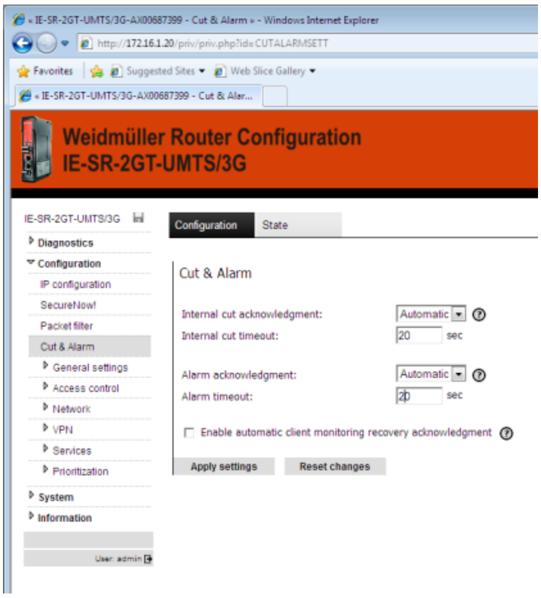
Alarm event: off

Int. cut event: off

Ext. cut event: off

Reset cut signal Reset alarm signal

Alternatively the **re-set** of events can be configured automatically with a selectable time-delay.
The 2 screenshots below show a configured “automatic mode”



Cut & Alarm

Internal cut acknowledgment: Automatic

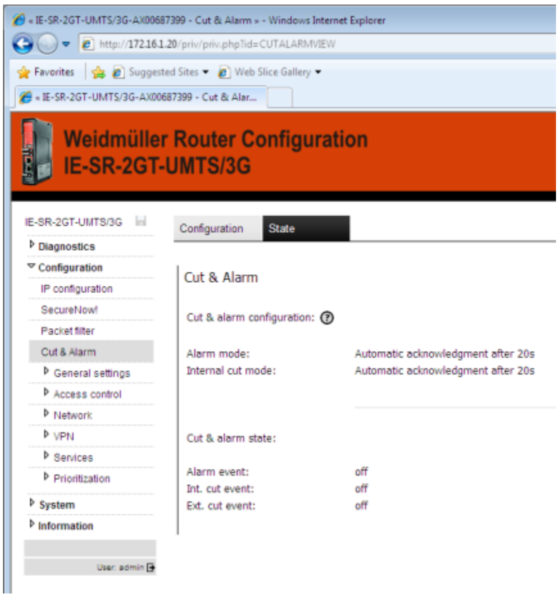
Internal cut timeout: 20 sec

Alarm acknowledgment: Automatic

Alarm timeout: 20 sec

☐ Enable automatic client monitoring recovery acknowledgment

Apply settings Reset changes



Cut & Alarm

Cut & alarm configuration:

Alarm mode: Automatic acknowledgment after 20s

Internal cut mode: Automatic acknowledgment after 20s

Cut & alarm state:

Alarm event: off

Int. cut event: off

Ext. cut event: off

C2.22 Set the modes for CUT and Alarm acknowledgement to Automatic

After finishing configuration and applying (don't forget) of the behaviour how to re-set the event, a test of the configured CUT-Firewall-rule can be started.

C2.23 Connect a PC at WAN-Port of the Router.

C2.24 Connect a second PC at LAN-Port of the Router to check what happens when the CUT-event is triggered.

C2.25 Send a Ping request from PC-WAN to PC-LAN.

As result the WAN port should be disabled immediately. In automatic mode you have to wait the delay time until the WAN port is re-activating. In manual mode goto to Routers Web-Interface with PC-LAN, select menu Cut & Alarm, change to tab "State" and click buttons "Reset cut signal" and/or "Reset alarm signal".

Note: Please keep in mind that "pinging" the **IP address of Router's LAN-Port from WAN-network** will **not** trigger the configured Firewall-rule. The Layer-3-Firewall is only working for data packets which have to be transmitted from Router's inbound to outbound interfaces to an external device.

Method 3: Software-based WAN port disconnection by feature "Client monitoring"

The Router has a builtin feature named "Client monitoring" which can be used to test if a connected device is still alive. This will be done by periodically sending a block of 5 ping requests every 50 seconds. If a monitored device is no longer answering then either an internal CUT (disconnect WAN port) or an Alarm (24 VDC digital output) can be triggered.

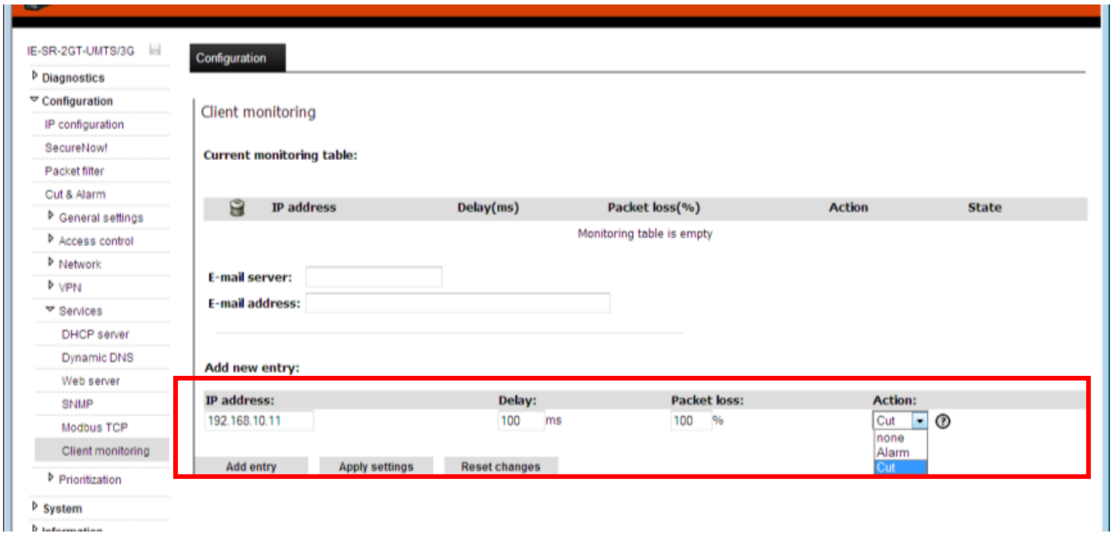
As an example (as shown in the screenshot below) we create an entry to monitor a device with the IP address 192.168.10.11.

C3.1 Goto menu Configuration → Services → Client monitoring

C3.2 Enter into the line of section "Add a new entry" the parameters to monitor a device

- IP address → Device which will be monitored
- Delay (ms) → The Router sends every 50 seconds a block of 5 ping requests to the monitored device. If the average response time (based on 5 ping requests) is longer than the configured Delay-time then this trigger condition will match.
- Packet loss(%) → If the lost share (no response) of 5 ping requests is greater than this configured value then this trigger condition will match.
- Action → As an action "CUT"-WAN-Port or an "Alarm" can be defined. An action will be triggered if one of the parameters *Delay (ms)* or *Packet loss(%)* exceeds the configured values.

Note: If you select the action "CUT" it makes only sense to monitor devices at LAN port due to the fact that the WAN port will be disabled in case of a lost connection.



Client monitoring

Current monitoring table:

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

E-mail server:

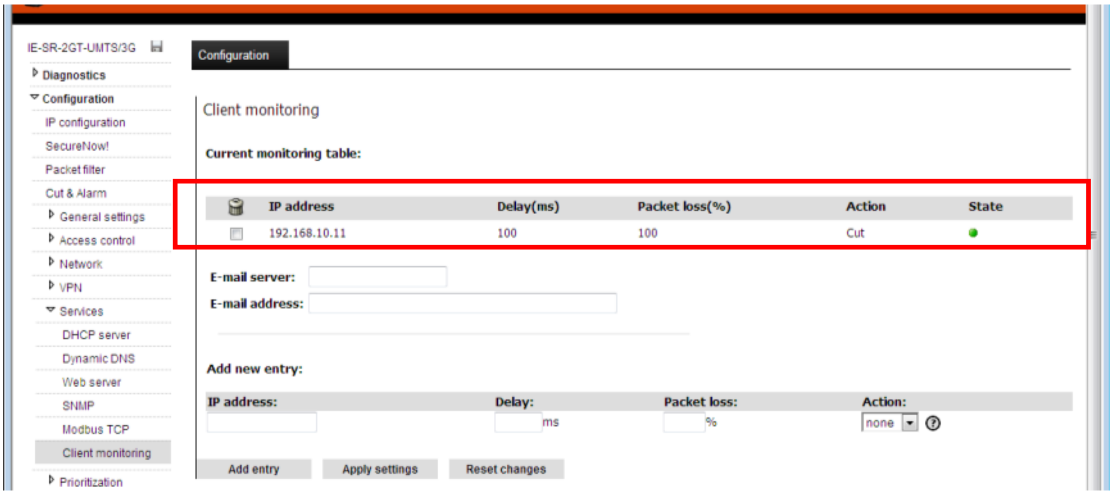
E-mail address:

Add new entry:

IP address:	Delay:	Packet loss:	Action:
192.168.10.11	100 ms	100 %	Cut none Alarm Cut

C3.3 Click button “Add entry”

C3.4 Click button “Apply settings” to activate the new entry



Client monitoring

Current monitoring table:

	IP address	Delay(ms)	Packet loss(%)	Action	State
□	192.168.10.11	100	100	Cut	●

E-mail server:

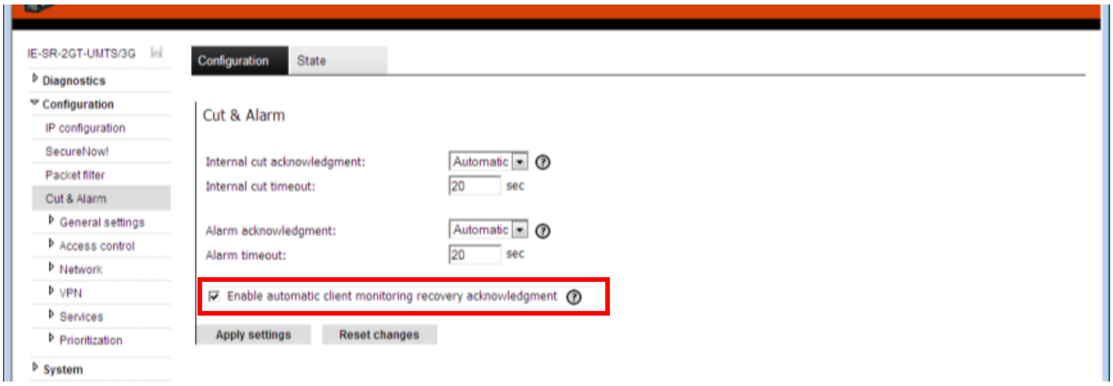
E-mail address:

Add new entry:

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

Note: The behaviour of re-setting a triggered (CUT or Alarm) depends on the configuration of the menu Configuration → Cut & Alarm.

Additionally, if the parameter “Enable automatic client monitoring recovery acknowledgment” is activated then the Router will automatically re-activate the WAN port if the monitored device (at LAN port) is accessible again (cause the Router is still checking every 50 seconds by ping request).



Cut & Alarm

Internal cut acknowledgment: Automatic

Internal cut timeout: 20 sec

Alarm acknowledgment: Automatic

Alarm timeout: 20 sec

☑ Enable automatic client monitoring recovery acknowledgment

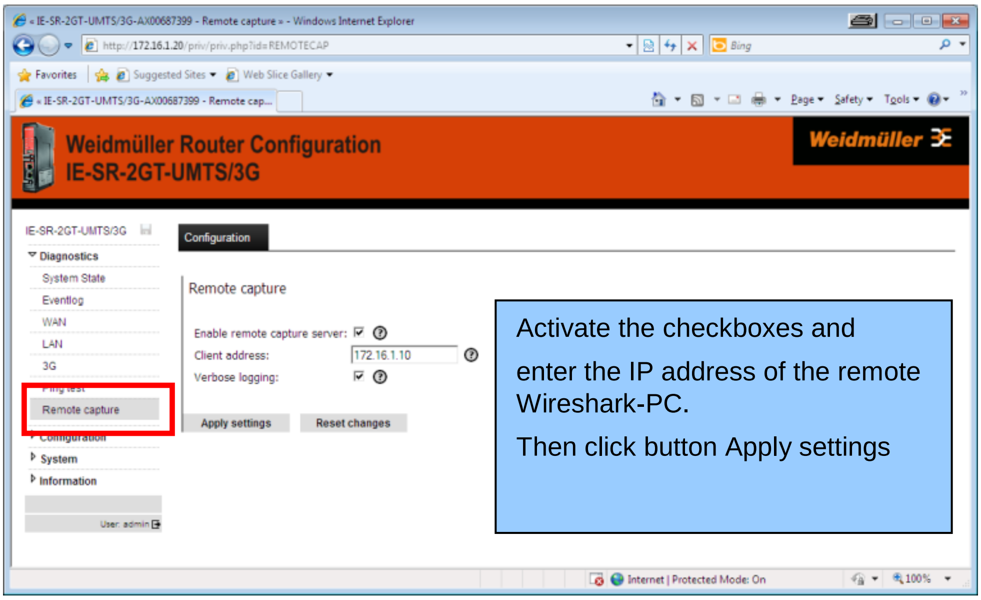
C3- Description how to use the feature “Remote Capture” with Wireshark to analyze the LAN/WAN traffic of the Router

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

C3.1 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 deactive this feature if you no longer need to analyze the traffic because it has an impact on the performance of the Router.



Remote capture

Enable remote capture server: ☑

Client address: 172.16.1.10

Verbose logging: ☑

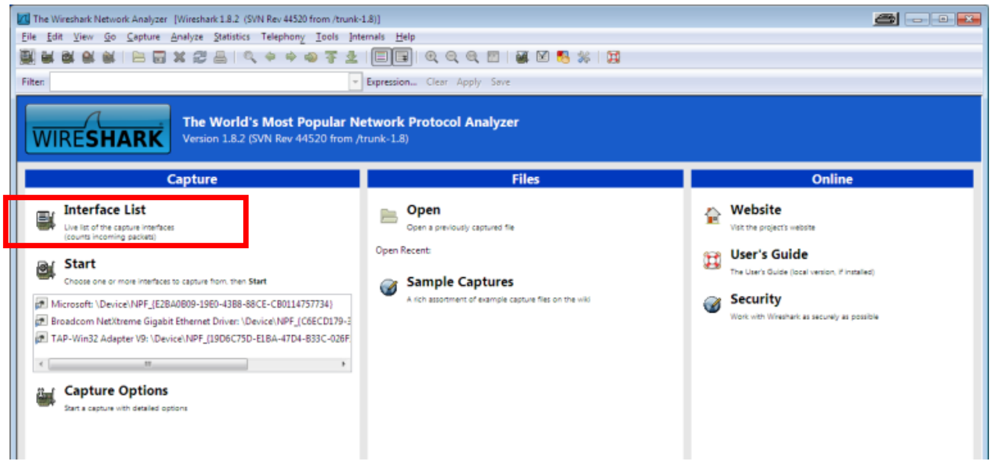
Activate the checkboxes and

enter the IP address of the remote Wireshark-PC.

Then click button Apply settings

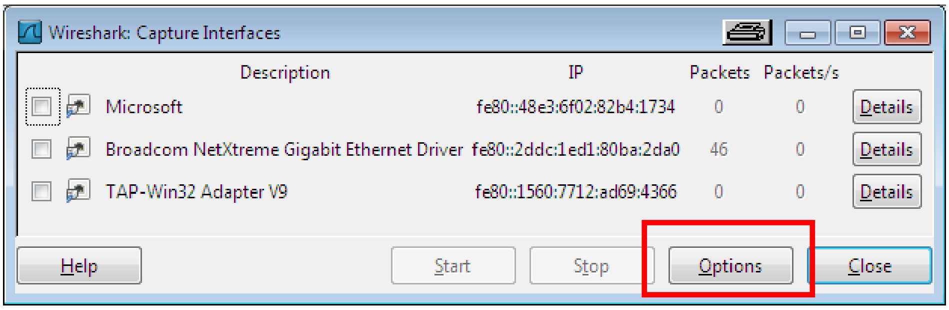
C3.2 Start Wireshark at your PC

C3.3 Click “Interface list” or alternatively select in the menu “Capture” → “Interfaces”


The Wireshark Network Analyzer [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible

Microsoft: \Device\NPF_{E2BA0B09-19E0-43B8-88CE-CB0114757734}
Broadcom NetXtreme Gigabit Ethernet Driver: \Device\NPF_{C6ECD179-3
TAP-Win32 Adapter V9: \Device\NPF_{19D6C75D-E1BA-47D4-B33C-026F

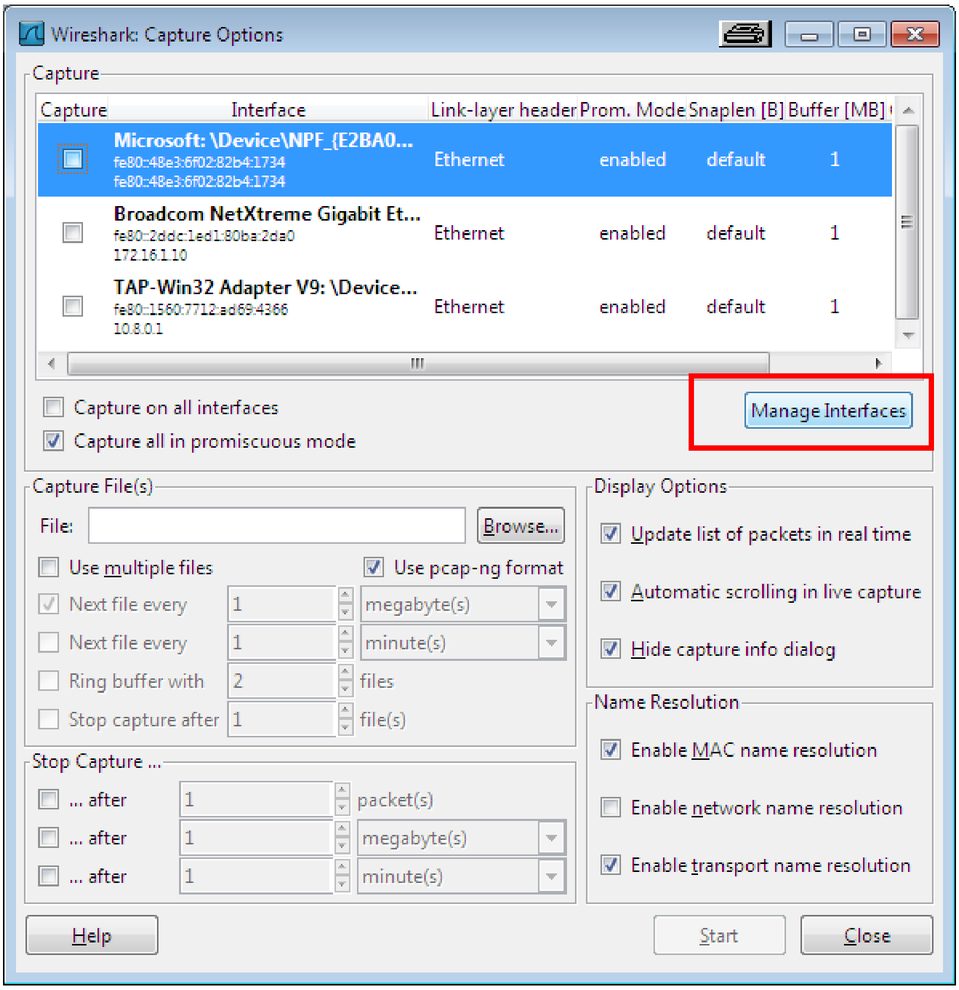
The local Ethernet Interfaces of the computer will be displayed.



Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	
□	Microsoft	fe80::48e3:6f02:82b4:1734	0	0	Details
□	Broadcom NetXtreme Gigabit Ethernet Driver	fe80::2ddc:1ed1:80ba:2da0	46	0	Details
□	TAP-Win32 Adapter V9	fe80::1560:7712:ad69:4366	0	0	Details

C3.4 Click button “Options”



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]
□	Microsoft: \Device\NPF_{E2BA0... fe80::48e3:6f02:82b4:1734 fe80::48e3:6f02:82b4:1734	Ethernet	enabled	default	1
□	Broadcom NetXtreme Gigabit Et... fe80::2ddc:1ed1:80ba:2da0 172.16.1.10	Ethernet	enabled	default	1
□	TAP-Win32 Adapter V9: \Device... fe80::1560:7712:ad69:4366 10.8.0.1	Ethernet	enabled	default	1

□ Capture on all interfaces

☑ Capture all in promiscuous mode

Capture File(s)

File:

□ Use multiple files ☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

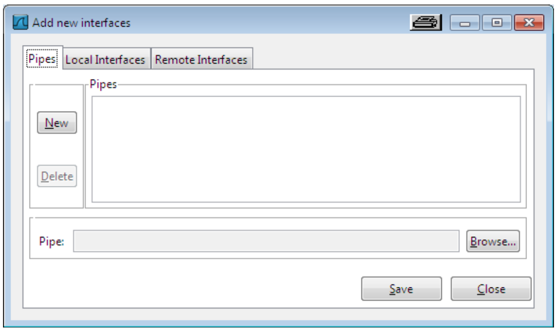
Name Resolution

☑ Enable MAC name resolution

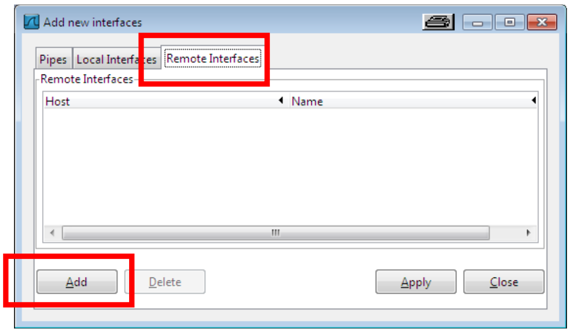
□ Enable network name resolution

☑ Enable transport name resolution

C3.5 Click button “Manage Interfaces” and change to tab “Remote Interfaces”

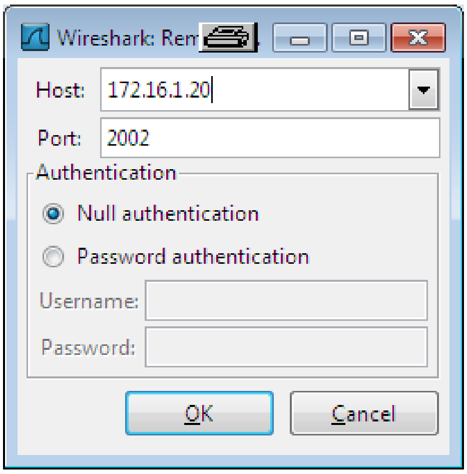


Add new interfaces



Add new interfaces

C3.6 Click button “Add”



Host: 172.16.1.20

Port: 2002

● Null authentication

○ Password authentication

Username:

Password:

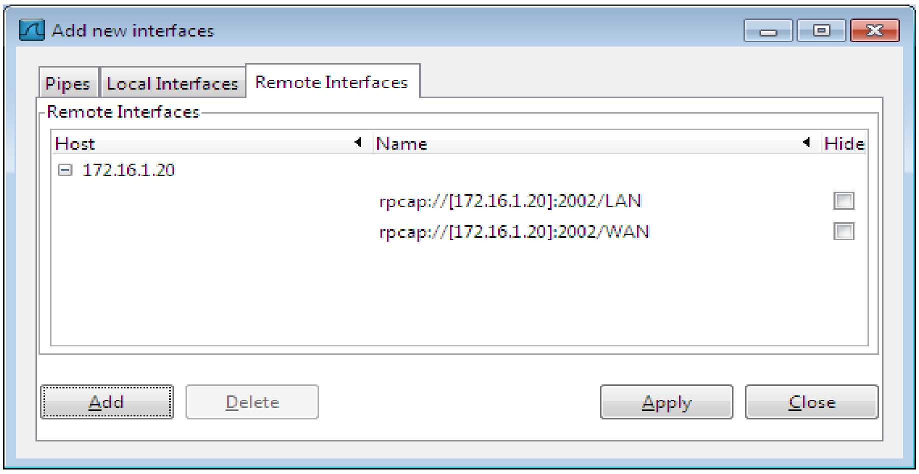
C3.7 Enter into field “Host” the IP address of the Router

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

C3.8 Enter into field “Port” the value 2002 (will be filled automatically if you enter an IP address)

C3.9 Click button OK

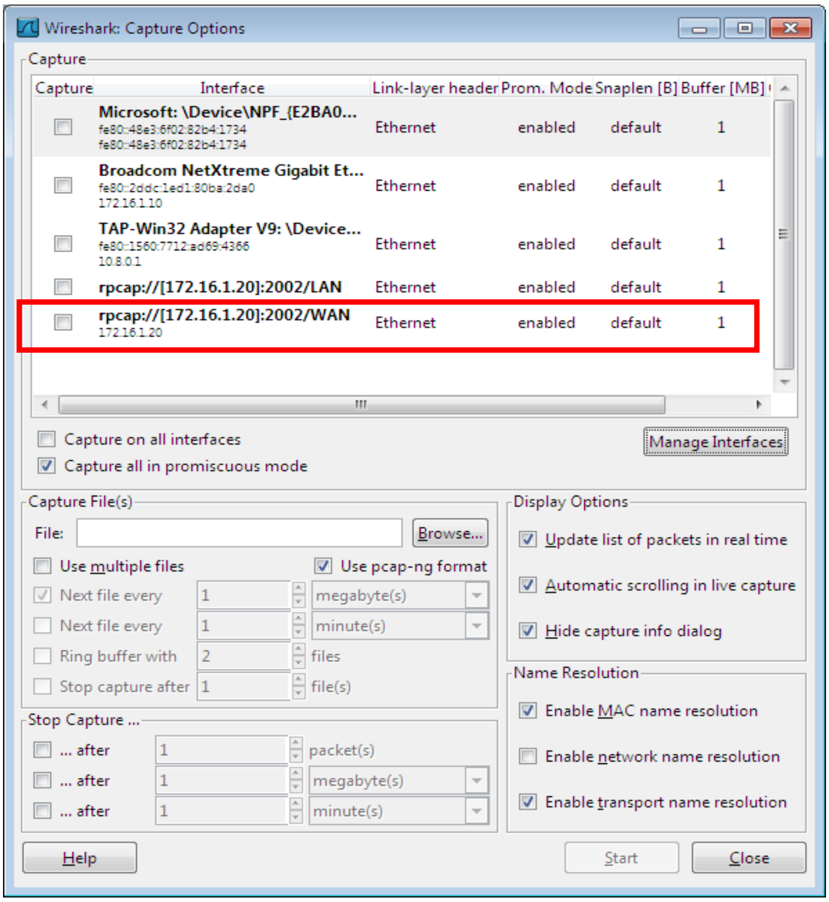
Now both Interfaces of the Router (= Host 172.16.1.20) should be displayed.



Host	Name	Hide
⊟ 172.16.1.20		
	rpcap://[172.16.1.20]:2002/LAN	□
	rpcap://[172.16.1.20]:2002/WAN	□

C3.10 Click button Close

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



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]
□	Microsoft: \Device\NPF_{E2BA0... fe80::48e3:6f02:82b4:1734 fe80::48e3:6f02:82b4:1734	Ethernet	enabled	default	1
□	Broadcom NetXtreme Gigabit Et... fe80::2ddc:1ed1:80ba:2da0 172.16.1.10	Ethernet	enabled	default	1
□	TAP-Win32 Adapter V9: \Device... fe80::1560:7712:ad69:4366 10.8.0.1	Ethernet	enabled	default	1
□	rpcap://[172.16.1.20]:2002/LAN	Ethernet	enabled	default	1
□	rpcap://[172.16.1.20]:2002/WAN 172.16.1.20	Ethernet	enabled	default	1

□ Capture on all interfaces

☑ Capture all in promiscuous mode

Capture File(s)

File:

☐ Use multiple files ☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

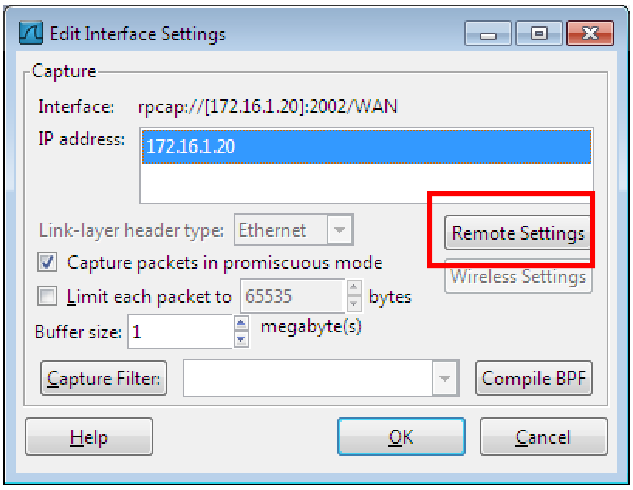
☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

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

C3.11 Double-Click the line **rpcap//[172.16.1.20]:2002/WAN**



Edit Interface Settings

Capture

Interface: rpcap://[172.16.1.20]:2002/WAN

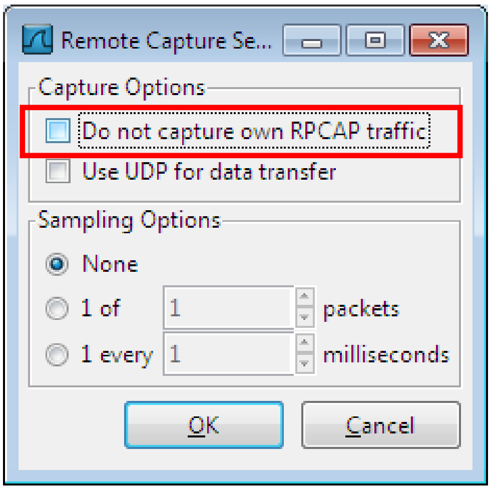
IP address: 172.16.1.20

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

□ Limit each packet to 65535 bytes

Buffer size: 1 megabyte(s)



Remote Capture Se...

Capture Options

□ Do not capture own RPCAP traffic

□ Use UDP for data transfer

Sampling Options

● None

○ 1 of 1 packets

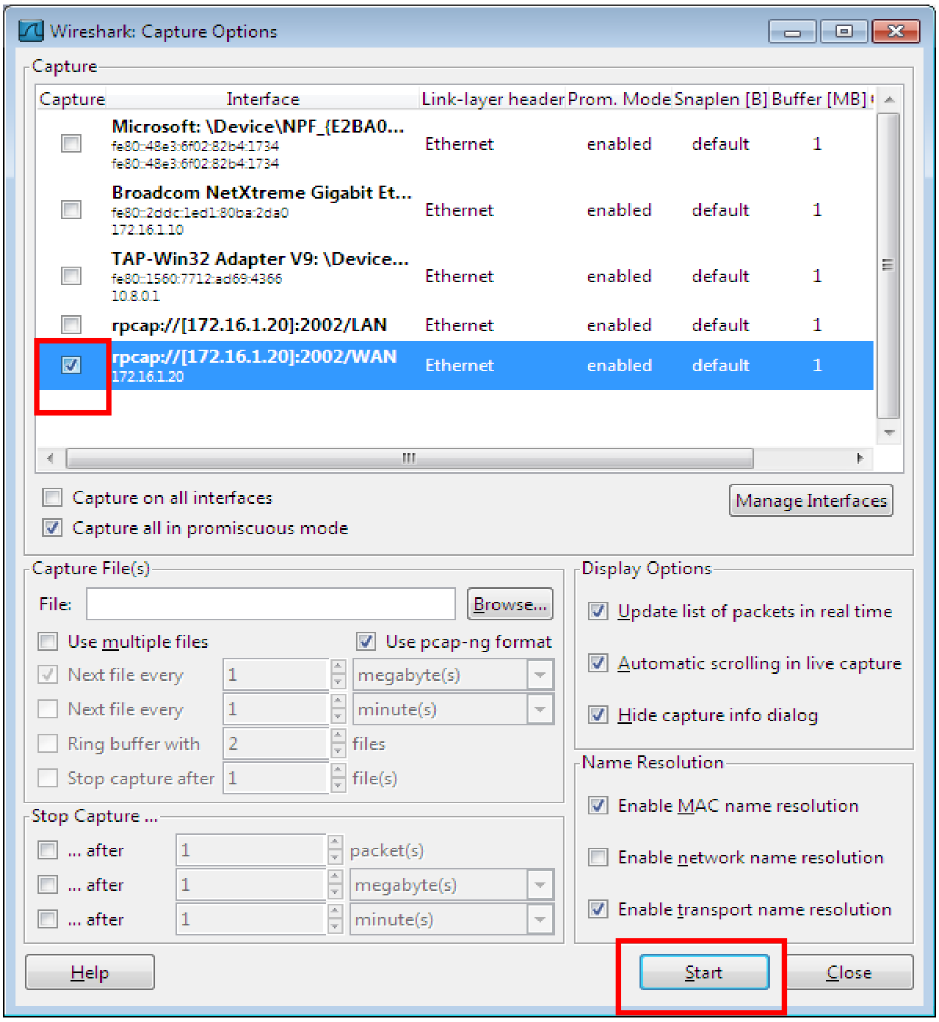
○ 1 every 1 milliseconds

C3.12 Click button “Remote Settings”

C3.13 **Clear** the checkbox “Do not capture own RPCAP traffic”

C3.14 Click button “OK”

C3.15 Again click button “OK” to close the window “Edit Interface Settings”



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]
□	**Microsoft: \Device\NPF_{E2BA0...** fe80::48e3:6f02:82b4:1734 fe80::48e3:6f02:82b4:1734	Ethernet	enabled	default	1
□	**Broadcom NetXtreme Gigabit Et...** fe80::2ddc:1ed1:80ba:2da0 172.16.1.10	Ethernet	enabled	default	1
□	**TAP-Win32 Adapter V9: \Device...** fe80::1560:7712:ad69:4366 10.8.0.1	Ethernet	enabled	default	1
□	**rpcap://[172.16.1.20]:2002/LAN**	Ethernet	enabled	default	1
☑	**rpcap://[172.16.1.20]:2002/WAN** 172.16.1.20	Ethernet	enabled	default	1

□ Capture on all interfaces

☑ Capture all in promiscuous mode

Manage Interfaces

Capture File(s)

File: Browse...

□ Use multiple files ☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

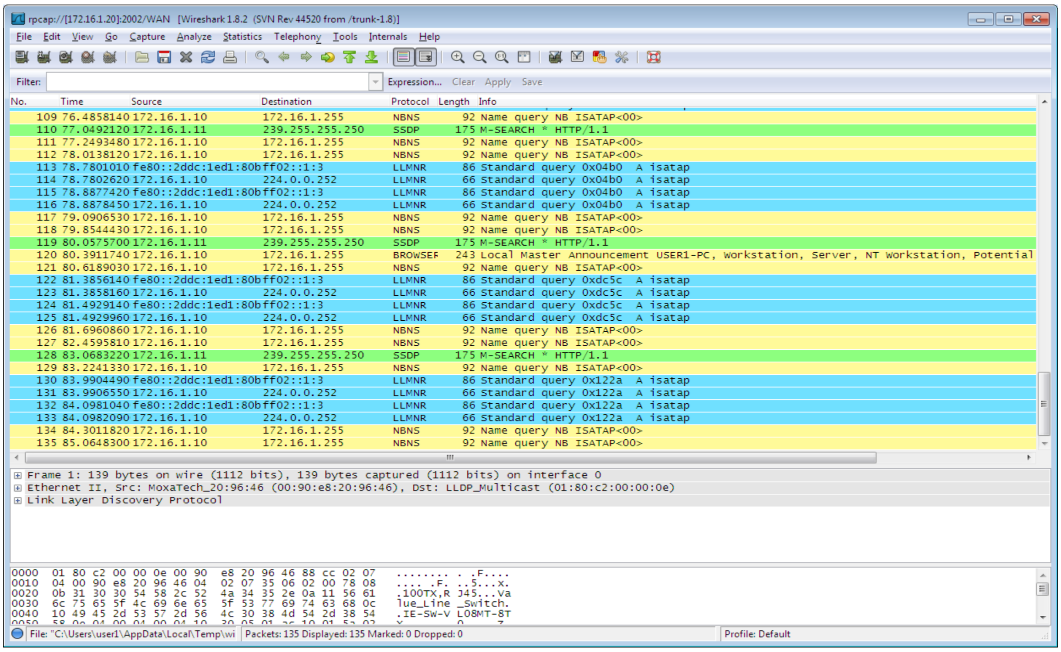
□ Enable network name resolution

☑ Enable transport name resolution

Help Start Close

C3.16 Activate the checkbox in line **rpcap//[172.16.1.20]:2002/WAN**

C3.17 Click button “Start” to record the traffic at Routers WAN port



rpcap://[172.16.1.20]:2002/WAN [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source                    Destination       Protocol  Length Info
 109 76.4858140 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 110 77.0492120 172.16.1.11                239.255.255.250   SSDP      175 M-SEARCH * HTTP/1.1
 111 77.2493480 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 112 78.0138120 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 113 78.7801010 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0x04b0  A isatap
 114 78.7802620 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0x04b0  A isatap
 115 78.8877420 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0x04b0  A isatap
 116 78.8878450 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0x04b0  A isatap
 117 79.0906530 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 118 79.8544430 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 119 80.0575700 172.16.1.11                239.255.255.250   SSDP      175 M-SEARCH * HTTP/1.1
 120 80.3911740 172.16.1.10                172.16.1.255      BROWSEF   243 Local Master Announcement USER1-PC, Workstation, Server, NT Workstation, Potential
 121 80.6189030 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 122 81.3856140 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0xdc5c  A isatap
 123 81.3858160 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0xdc5c  A isatap
 124 81.4929140 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0xdc5c  A isatap
 125 81.4929960 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0xdc5c  A isatap
 126 81.6960860 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 127 82.4595810 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 128 83.0683220 172.16.1.11                239.255.255.250   SSDP      175 M-SEARCH * HTTP/1.1
 129 83.2241330 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 130 83.9904490 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0x122a  A isatap
 131 83.9906550 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0x122a  A isatap
 132 84.0981040 fe80::2ddc:1ed1:80bff02::1:3                 LLMNR      86 Standard query 0x122a  A isatap
 133 84.0982090 172.16.1.10                224.0.0.252       LLMNR      66 Standard query 0x122a  A isatap
 134 84.3011820 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
 135 85.0648300 172.16.1.10                172.16.1.255      NBNS       92 Name query NB ISATAP<00>
```

```
⊞ Frame 1: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
⊞ Ethernet II, Src: MoxaTech_20:96:46 (00:90:e8:20:96:46), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
⊞ Link Layer Discovery Protocol
```

```
0000  01 80 c2 00 00 0e 00 90  e8 20 96 46 88 cc 02 07   ........ . .F....
0010  04 00 90 e8 20 96 46 04  02 07 35 06 02 00 78 08   .... .F. ..5...x.
0020  0b 31 30 30 54 58 2c 52  4a 34 35 2e 0a 11 56 61   .100TX,R J45...Va
0030  6c 75 65 5f 4c 69 6e 65  5f 53 77 69 74 63 68 0c   lue_Line _Switch.
0040  10 49 45 2d 53 57 2d 56  4c 30 38 4d 54 2d 38 54   .IE-SW-V L08MT-8T
```

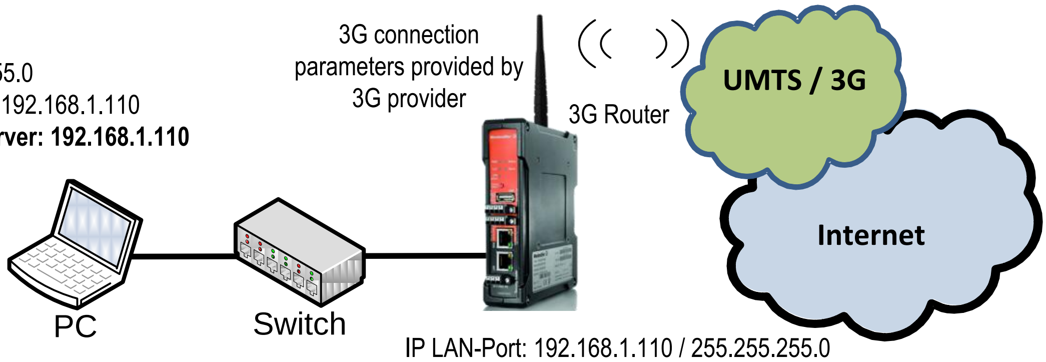
File: "C:\Users\user1\AppData\Local\Temp\wi | Packets: 135 Displayed: 135 Marked: 0 Dropped: 0 | Profile: Default

C4- Description how to configure the Internet access of a PC via a 3G Router

This description applies to the Weidmüller Industrial Router IE-SR-2GT-UMTS/3G

Illustration of the application scenario

IP: 192.168.1.99
Subnet: 255.255.255.0
Standard gateway: 192.168.1.110
Preferred DNS-Server: 192.168.1.110



IP LAN-Port: 192.168.1.110 / 255.255.255.0
Default gateway: can be left blank for 3G Internet access

Note: If the 3G connection is online then the default gateway automatically is set to 3G provider. As long as the Router is connected to the Internet a manually configured default gateway will be not used.

Starting situation

- The Router has inserted a SIM card of your local Internet provider (slot labeled 3G at rear side of the Router).
- The Router is set to factory default configuration and connected to the PC via Router's LAN port (IP address 192.168.1.110).

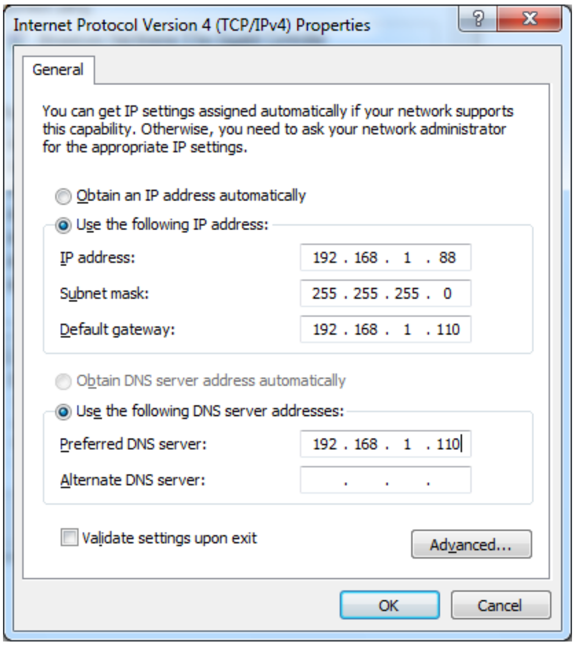
C4.1 Connect the Configuration-PC to Router's LAN port

→ Use autonegotiation on the Ethernet Interface of the PC

C4.2 Change the IP address of the PC to one out of the range 192.168.1.0

→ e.g.	IP address	192.168.1.88
	Subnet mask	255.255.255.0
	Standardgateway	192.168.1.110
	Preferred DNS-Server	**192.168.1.110**

(Do not forget to enter the Router IP address as preferred DNS-Server, otherwise you cannot access Web pages by DNS name, Router is acting as DNS forwarder)



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 88
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 110

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 110
Alternate DNS server: . . .

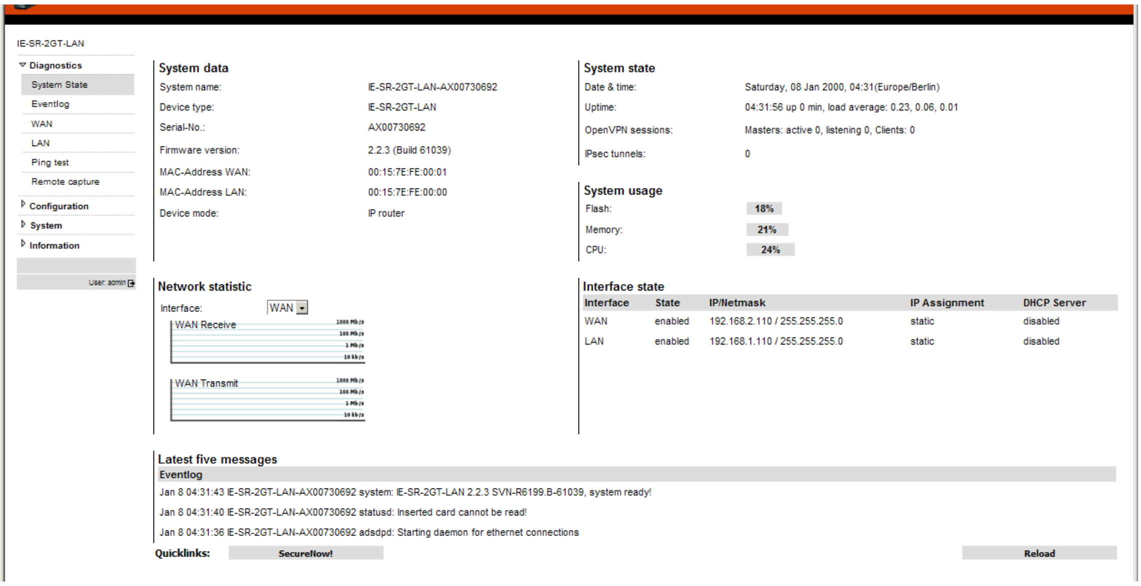
□ Validate settings upon exit

Figure C1: IP settings of PC's LAN interface

C4.3 Start a Web browser and login into the Router Web interface (http://192.168.1.110)

User: admin

Password: Detmold



System data

System name:	IE-SR-2GT-LAN-AX00730692
Device type:	IE-SR-2GT-LAN
Serial-No.:	AX00730692
Firmware version:	2.2.3 (Build 61039)
MAC-Address WAN:	00:15:7E:FE:00:01
MAC-Address LAN:	00:15:7E:FE:00:00
Device mode:	IP router

System state

Date & time:	Saturday, 08 Jan 2000, 04:31(Europe/Berlin)
Uptime:	04:31:56 up 0 min, load average: 0.23, 0.06, 0.01
OpenVPN sessions:	Masters: active 0, listening 0, Clients: 0
IPsec tunnels:	0

System usage

Flash:	18%
Memory:	21%
CPU:	24%

Network statistic

Interface: WAN

Interface state

Interface	State	IP/Netmask	IP Assignment	DHCP Server
WAN	enabled	192.168.2.110 / 255.255.255.0	static	disabled
LAN	enabled	192.168.1.110 / 255.255.255.0	static	disabled

Latest five messages

Eventlog

```
Jan 8 04:31:43 IE-SR-2GT-LAN-AX00730692 system: IE-SR-2GT-LAN 2.2.3 SVN-R6199.B-61039, system ready!
Jan 8 04:31:40 IE-SR-2GT-LAN-AX00730692 statusd: Inserted card cannot be read!
Jan 8 04:31:36 IE-SR-2GT-LAN-AX00730692 adsdpd: Starting daemon for ethernet connections
```

Figure C2: Login page of the Router (equivalent with menu Diagnostics → System State)

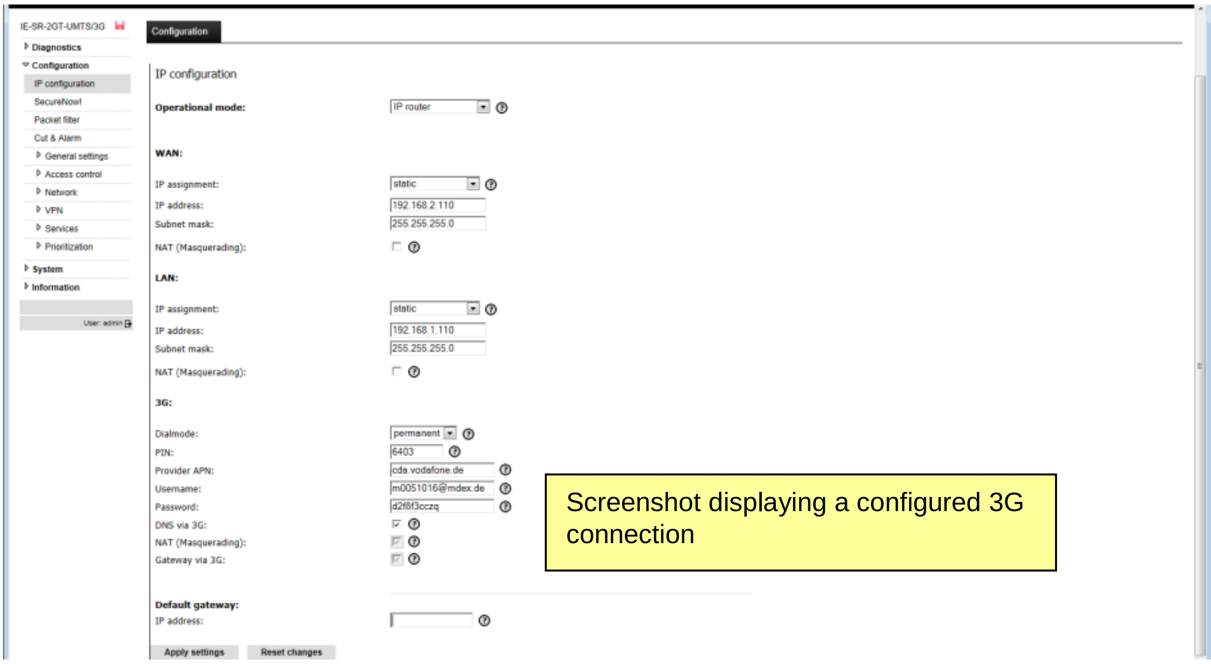
C4.4 Configure the 3G connection

► Select menu **Configuration → IP configuration**

► Configure the 3G connection according to the data provided by Internet provider (normally PIN and APN)

Note: In many cases you don't need to fill values into fields „username“ and „password“. If your provider does not use „username“ and „password“ please leave them blank.

You don't have to configure a Default gateway because the default gateway automatically is set to 3G provider if the 3G connection is online. As long as the Router is connected to the Internet (Status = online) a manually configured default gateway will be not used.



IP configuration

Operational mode:	IP router
WAN:	
IP assignment:	static
IP address:	192.168.2.110
Subnet mask:	255.255.255.0
NAT (Masquerading):	☐
LAN:	
IP assignment:	static
IP address:	192.168.1.110
Subnet mask:	255.255.255.0
NAT (Masquerading):	☐
3G:	
Dialmode:	permanent
PIN:	6403
Provider APN:	cda.vodafone.de
Username:	m0051016@mdex.de
Password:	d2f8f3cczq
DNS via 3G:	☑
NAT (Masquerading):	☑
Gateway via 3G:	☑
Default gateway:	
IP address:	

Screenshot displaying a configured 3G connection

Figure C3: Screenshot of menu **IP configuration**

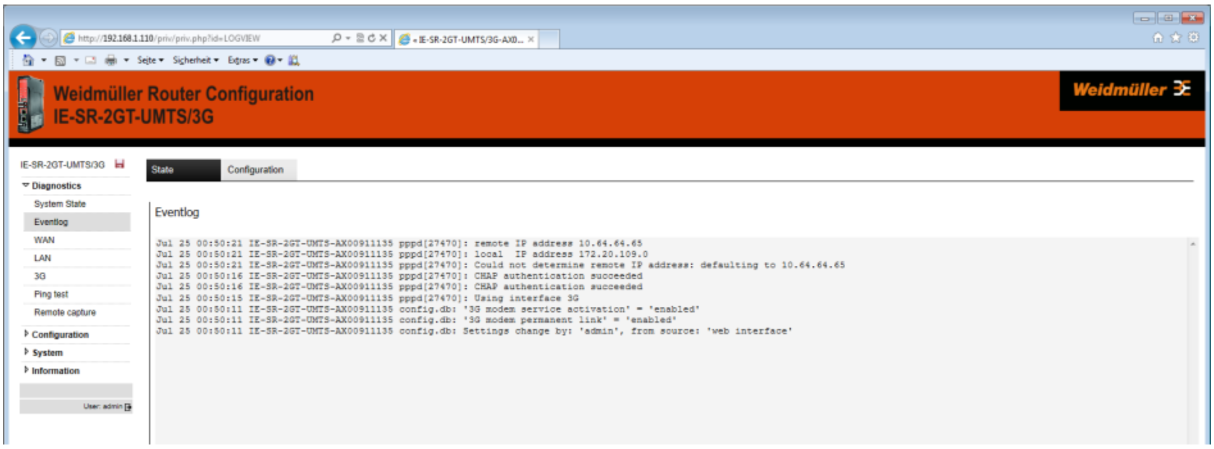
- ► Click button "Apply settings" to activate the new settings.

Now the Router tries to connect to the Internet. Please wait some seconds.

C4.5 Evaluating a successful Internet connection

- ► Select menu **Diagnostics → Event**

The event log displays the result of initiating the 3G Internet connection.



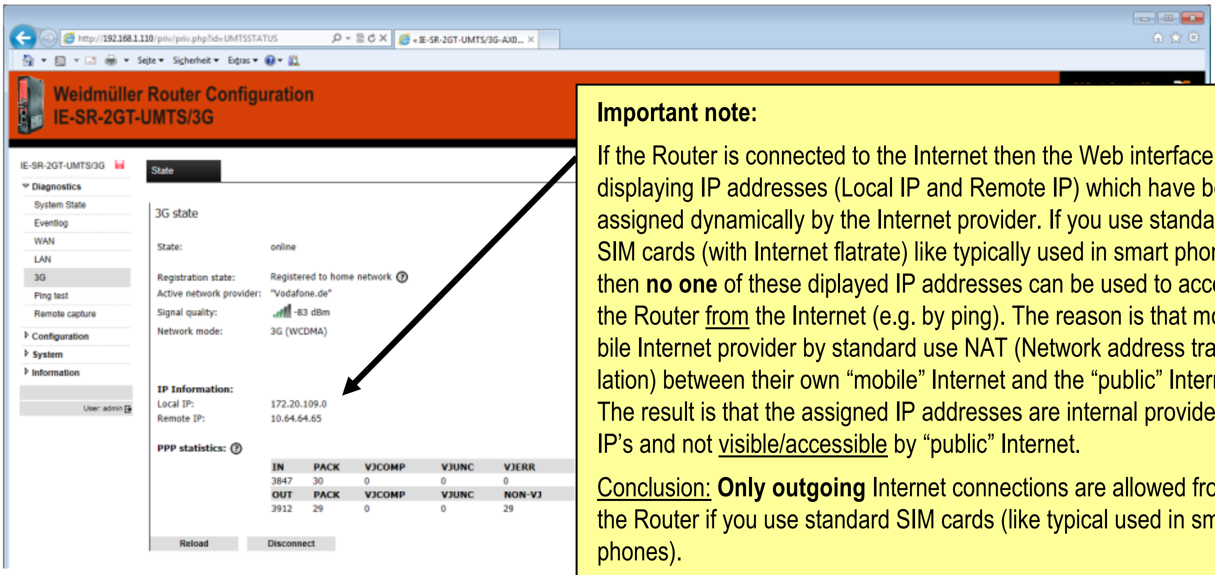
Eventlog

```
Jul 25 00:50:21 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: remote IP address 10.64.64.65
Jul 25 00:50:21 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: local  IP address 172.20.109.0
Jul 25 00:50:21 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: Could not determine remote IP address: defaulting to 10.64.64.65
Jul 25 00:50:16 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: CHAP authentication succeeded
Jul 25 00:50:16 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: CHAP authentication succeeded
Jul 25 00:50:15 IE-SR-2GT-UMTS-AX00911135 pppd[27470]: Using interface 3G
Jul 25 00:50:11 IE-SR-2GT-UMTS-AX00911135 config.db: '3G modem service activation' = 'enabled'
Jul 25 00:50:11 IE-SR-2GT-UMTS-AX00911135 config.db: '3G modem permanent link' = 'enabled'
Jul 25 00:50:11 IE-SR-2GT-UMTS-AX00911135 config.db: Settings change by: 'admin', from source: 'web interface'
```

Figure C4: Screenshot of event log

- ► Select menu **Diagnostics → 3G**

This menu shows the current status of the 3G connection.



3G state

State: online

Registration state: Registered to home network
Active network provider: "Vodafone.de"
Signal quality: -83 dBm
Network mode: 3G (WCDMA)

IP Information:
Local IP: 172.20.109.0
Remote IP: 10.64.64.65

PPP statistics:

IN	PACK	VJCOMP	VJUNC	VJERR
3847	30	0	0	0
OUT	PACK	VJCOMP	VJUNC	NON-VJ
3912	29	0	0	29

Figure C5: Screenshot of status of 3G connection

Important note:

If the Router is connected to the Internet then the Web interface is displaying IP addresses (Local IP and Remote IP) which have been assigned dynamically by the Internet provider. If you use standard SIM cards (with Internet flatrate) like typically used in smart phones then **no one** of these diplayed IP addresses can be used to access the Router from the Internet (e.g. by ping). The reason is that mobile Internet provider by standard use NAT (Network address translation) between their own "mobile" Internet and the "public" Internet. The result is that the assigned IP addresses are internal provider IP's and not visible/accessible by "public" Internet.

Conclusion: **Only outgoing** Internet connections are allowed from the Router if you use standard SIM cards (like typical used in smart phones).

If the 3G-Router needs to be accessed **from** the Internet (eg. beeing a VPN server) then you have to use a SIM Card which explicitly is assigned with a static and public accessible IP address by the provider (eg. m2m SIM cards for machine-to-machine communication). Please clarify with your local mobile providers what they are offering regarding data SIM cards with a static and public accessible IP address.

If the Router successfully is connected to the Internet (online) you now can try to open any Internet Web page by the connected PC.