Weidmüller

Industrial Security Router

IE-SR-2TX-WL (Part number 2682590000)
IE-SR-2TX-WL-4G-EU (Part number 2682560000)
IE-SR-2TX-WL-4G-US-V (Part number 2682580000)

User Manual

Edition 1.0
2022-11-25

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 document 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
Klingenbergstrasse 26
32758 Detmold
Germany
Phone +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

1. Introduction

1.1 About

Weidmüller Routers of series IE-SR-2TX-WL-(4G) are reliable and cost-effective Industrial Security Routers, providing a versatile and redundant Internet / WAN connectivity. The devices are equipped with

- 2 x 10/100Base T(X) ports (LAN /WAN)
- 1 x WLAN interface (IEEE 802.11 b/g/n)
- 1 x Serial interface (RS232/422/485)
- 1 x LTE/4G CAT4 modem (Models IE-SR-2TX-WL-4G-EU and IE-SR-2TX-WL-4G-US-V)
  - Model IE-SR-2TX-WL-4G-EU covers bands LTE-FDD:B1/B3/B7/B8/B20/B28A, LTE-TDD:B38/B40/B41, WCDMA:B1/B8 and GSM:B3/B8. It is primarily intended for use in region EMEA.
  - Model IE-SR-2TX-WL-4G-US-V covers bands LTE-FDD:B2/B4/B5/B12/B13/B14/B66/B71 and WCDMA:B2/B4/B5. It is applicable for mobile operators of region North America. Additionally, it is certified by cellphone provider Verizon.

The devices can be used in a variety of applications like IP-Routing, Firewalling, IP address management (NAT), secured VPN connections or Ethernet/Serial data conversion.

IE-SR-2TX-WL

IE-SR-2TX-WL-4G-EU
IE-SR-2TX-WL-4G-US-V

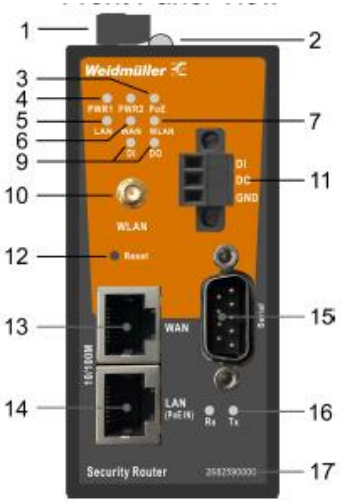
1.2 Overview Software Features

IP Routing	IPv4 Routing.
Stateful Inspection Firewall	IP-based Layer 3 packet filtering.
DHCP-Server and DNS relay	Provides DHCP/DNS services for devices connected to LAN network.
Time Server	NTP time synchronization and NTP time server relay.
WLAN Connectivity	Configurable as Access Point (Client assignment to LAN network) or Wireless Client (providing WAN / Internet access via connection to a remote Access Point).
Cellular Connectivity	Integrated LTE/4G modem configurable as primary or failover Internet connection.
Versatile Internet/WAN connectivity (LTE/4G models)	Option 1: WAN Port (Wired connection), Failover via Cellular Interface Option 2: Cellular Interface (Dual SIM, Failover from SIM1 to SIM2) Option 3: Wireless Interface (Client mode), Failover via Cellular Interface
Network Address Translation	Source / Destination NAT, variable configurable and related to a Port number, IP address (single Host) or IP subnet (Network).
VPN	OpenVPN (Server or Client), IPSec (Server or Client), Authentication X.509v3, PSK
Event-based Warning	Event-triggered Information and alert management via Digital IO, eMail, SNMP Traps or SMS (only LTE/4G models).
Serial Interface Functions	Ethernet/Serial converter functions providing services modes 'Virtual COM Port', 'TCP Client', 'TCP Server' and 'UDP Client / Server Mode'.

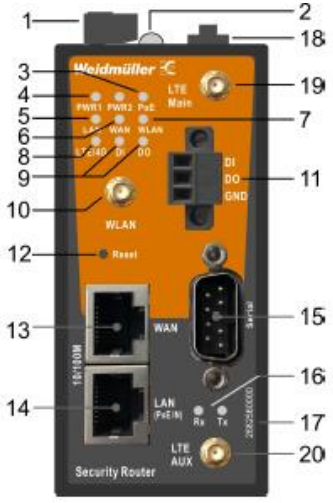
2. Overview Hardware (1 / 3)

2.1 Panel Views

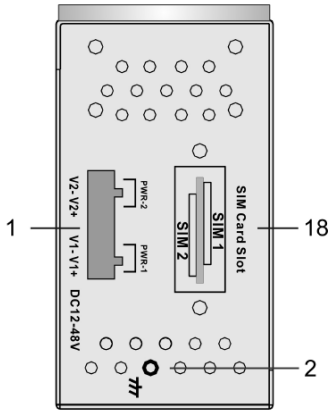
IE-SR-2TX-WL
Front Panel View



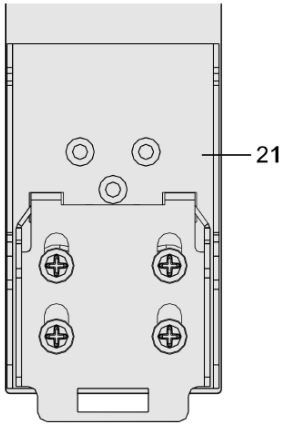
IE-SR-2TX-WL-4G-EU
IE-SR-2TX-WL-4G-US-V
Front Panel View



Top Panel View



Rear Panel View



Item Descriptions

1. 4-Pin Terminal block power input PWR1 / PWR2
2. Grounding screw / Frame ground (Note: The shielding ground of LAN and WAN port is electrically connected to the grounding screw)
3. PoE Indicator (powered via PoE)
4. Power input LEDs (PWR1 / PWR2)
5. LAN port Link/Activity LED
6. WAN port Link/Activity LED
7. WLAN Link/Activity LED
8. LTE/4G Connection Status LED (only LTE/4G models)
9. Digital I/O ports Status LEDs (ON/OFF)
10. WLAN antenna connector **(RP-SMA female)**
11. Terminal block for Digital Input and Output
12. Reset Button
    Pressing < 5 seconds: Reboots the device (Warm Start) and sets IP of LAN port to Factory Default IP.
    Pressing >= 5 seconds: Resets the device completely to factory default settings.
13. WAN Port 10/100Base-T(X)
14. LAN port 10/100Base-T(X) / **PoE (Powered Device)**
15. Serial Port (RS 232 connector)
16. LEDs TX/RX Status of Serial Port
17. Article Number
18. Slot for 2 SIM Cards with **format Mini SIM** (only LTE/4G models)
19. Main Antenna LTE/4G Interface (**SMA-female**)
20. AUX Antenna LTE/4G Interface (**SMA-female**)
21. DIN-rail Clip

2. Overview Hardware (2 / 3)

2.2 Technical Specifications

Product Properties

Technology	
Ethernet Standards	IEEE 802.3 for 10BASE-T IEEE 802.3u for 100BASE-TX IEEE 802.3af for Power-over-Ethernet IEEE 802.11b/g/n for Wireless LAN
Interfaces	
RJ45 Ports	10/100BASE-T(X) auto negotiation speed, F/H duplex mode and auto MDI/MDI-X connection
Serial Port	1x DB9 connector
Cellular Interface	2G (GSM / GPRS / EGPRS / EDGE), 3G (WCDMA / HSDPA / HSUPA), 4G/LTE
WLAN Interface	IEEE802.11b/g/n
SIM-Card slots	2x Mini-SIM (ID-000 format)
Connector for antennas	1x RP-SMA female 2x SMA female (LTE/4G models only)
DI/DO (Dry Contact)	1x DI (1: 5~30V, 0: 0~2V), 1x DO (Max.: 30V / 20 mA)
LED Indicators	PWR1, PWR2, PoE (active), LAN/WAN Port Link / Activity, WLAN Link, LTE/4G Link, DI / DO Status; Serial Port Data Transmitting
Power supply	
Input Voltage	24 V DC (12 to 48 V DC), 2 redundant inputs or 48 V DC Power-over-Ethernet on LAN Port (IEEE802.3af compliant)
Input Power	5.5 W (typical)
Connection	One removable 4-pin terminal block, Wiring cable 12-24AWG
Overload Current Protection	Present
Reverse Polarity Protection	Present
Physical Characteristics	
Housing	IP30 protection, metal
Dimension (W x H x D)	45 x 95 x 81 mm (1.77 x 3.74 x 3.19 inch)
Weight	395 g
Installation	DIN-rail
Environmental conditions	
Operating Temperature	-25 to 70°C (-13 to 158°F)
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5 to 95% (non-condensing)
Altitude	up to 2000 m
Regulatory Approvals	
Safety	UL 61010-1; UL 61010-2-201; EN 62311
EMC	EN 55032, EN 55024, FCC Part 15 Subpart B Class A, IEC 61000-4-2 ESD IEC 61000-4-3 RS IEC 61000-4-4 EFT IEC 61000-4-5 Surge IEC 61000-4-6 CS
Radio	EN 301 489-1/-17; EN 300 328, EN 301 511; EN 301 908-1
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-31
Vibration	IEC 60068-2-6
MTBF	
Time	IE-SR-2TX-WL: 381.084 hrs IE-SR-2TX-WL-4G-EU: 355.921 hrs IE-SR-2TX-WL-4G-US: 353.679 hrs
Database	Telcordia SR332
Warranty	
Time Period	5 years

LED Indicators

LED	Color	Status	Description
PWR1	Green	On	Power is being supplied to power input PWR1.
PWR2	Green	On	Power is being supplied to power input PWR2.
PoE	Green	On	The device is powered via PoE.
LAN / WAN	Green	On	LAN/WAN Port Link / Activity LED
		Blinking	Data is transmitted.
WLAN	Green	On	Linked to a Wireless network (Client Mode)
	Green	Blinking	Operating in mode Access Point
LTE/4G	Green	On	Mobile connection established (Online)
DI / DO	Green	On	Input / Output status set to logical 1
		Off	Input / Output status set to logical 0

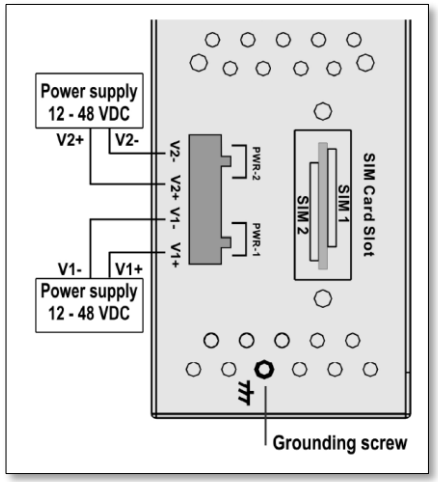
Pinouts DB-9 Connector (Serial Interface)

Pin #	RS-232 (DTE Device)	RS-422	RS-485(4-wire)	RS-485 (2-wire)	
1	DCD	TX-	TX-	DATA-	
2	RXD	TX+	TX+	DATA+	
3	TXD	RX+	RX+	---	
4	DTR	RX-	RX-	---	
5	GND	GND	GND	GND	
6	DSR	---	---	---	
7	RTS	---	---	---	
8	CTS	---	---	---	
9	RI	---	---	---	

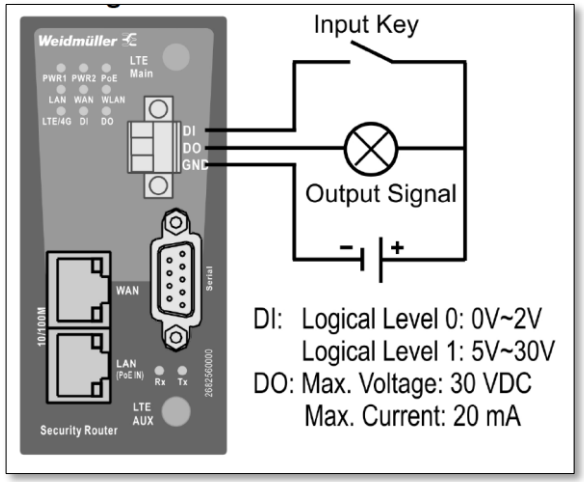
2. Overview Hardware (3 / 3)

2.3 Wiring and SIM Card installation

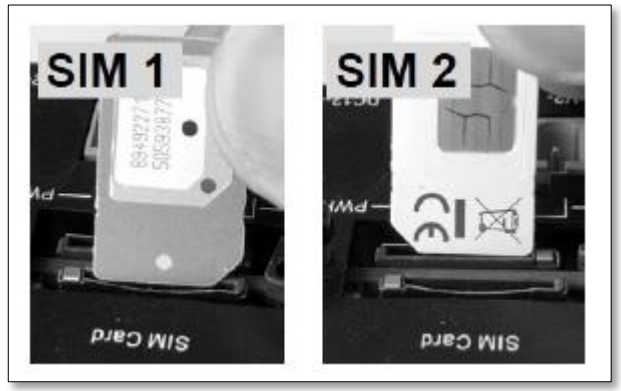
Power Wiring



Wiring Digital Input and Output



SIM Card Installation (only for 4G models)



SIM card installation:

1. Ensure that the device is powered-off.
2. Remove cover from SIM card slot on top of the housing.
3. Insert SIM card(s) with **Mini** format as illustrated.

Note: For using SIM cards with format Nano or Micro use a frame from attached SIM card adapter set.

Attention: For device installation and for safety notice refer to document 'Hardware Installation Guide' for Router series IE-SR-2TX-WL-xx (Part No. 2682560000, 2682580000, 2682590000).
The document can be downloaded from the Weidmüller Online Product Catalogue. Select or search for device name **IE-SR-2TX-WL** or part numbers and refer to section 'Downloads'.

3. Getting Started

3.1 Hardware Installation

- Install and power-up the device according to 'Hardware Installation Guide' for Router series IE-SR-2TX-WL-xx (downloadable from Weidmüller Online Product Catalogue).
- **Consider the safety notices mentioned in the Hardware Installation Guide!**

3.2 Factory Default Settings

- Factory Default Settings:
- IP LAN port: 192.168.1.110 / 255.255.255.0 (static)
- IP WAN port: DHCP
- Wireless LAN: Disabled
- Mobile Interface: Disabled (only available for LTE/4G models)
- Username: admin
- Password: Weidmueller
- Web Access: HTTPS via LAN port

3.3 General Device Access and Configuration

- IE-SR-2TX-WL-xx devices needs to be configured via the configuration pages of the integrated Web server.
- For Linux respectively OpenWRT-skilled users the Router additionally can be released for low-level root access via SSH or Telnet by enabling related checkboxes in section 'Access Settings' of configuration page 'Administration → System Settings' (Goto chapter '4.36 Administration → System Settings' for more detailed information).
- For using the Serial-to-Ethernet converter function 'Virtual Com Port', applicable to the RS232/485 interface, the software 'ComServer / Modbus Gateway Utility' can be used to install a virtual COM-Port driver on a Windows PC as counterpart to the Router (downloadable from the Weidmüller Online Product Catalogue).

3.4 Web Interface Access

- By factory default, the Router **only** can be accessed via the **HTTPS-secured** web interface and being connected to the wired **LAN Port**. All other access modes (HTTP, Telnet, SSH) and any access from other interfaces are not allowed by default. Granting additional access modes can be configured via section 'Access Settings' of configuration page 'Administration → System Settings.

- Login credentials (Factory default settings):
  - IP address / Netmask: 192.168.1.110 / 255.255.255.0
  - Username: admin
  - Password: Weidmueller
- Connect the PC to the Ethernet port of the Converter/Gateway and set the PC's IP address to a free one of range 192.168.1.0 / 255.255.255.0.
- Start a web browser and enter the IP address of the connected device into the browser's address line (**https://192.168.1.110**).
- After the appearance of the prompt (login) enter the login credentials. After successful input of username and password home page 'System Overview' will be displayed.

Note: If the Router configuration is set to factory defaults, any HTTP access attempt to the website (via LAN port) will be redirected automatically to HTTPS.

3.5 Console Access via Telnet or SSH

- The device root level can be accessed by Telnet or SSH console login (eg. using tool PuTTY). Use for access user 'root' and same password as set for user 'admin'.

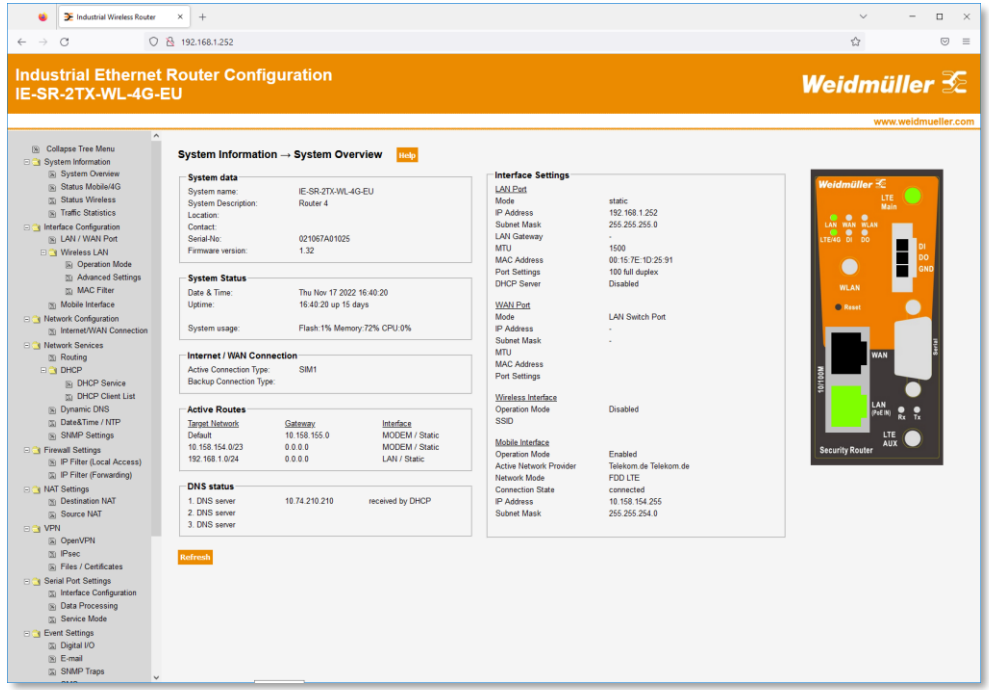
Note: When doing a device access at root level of the Linux operating system, be aware that configuration changes can have a severe impact on the functionality of the running Router application (configured via the web interface). Any change is in the user's responsibility and risk if the web-based Router application fails due to the intervention. For recovering the designed functionality based on the installed firmware reset the device to factory default settings (e.g., press external reset button larger 5 secs).

4. Web Interface Configuration

Description of Web-based device configuration

- Subsequent slides provide a detailed description about the menu structure and configuration pages of the Router's Web interface in terms of functional settings and parameter definitions.
- For access to the Web interface any browser can be used.
- Consider if the device is set to factory defaults:
  - Web interface only can be opened via secured web access (HTTPS) from LAN port.
  - Use for login IP address **192.1.68.1.110**, username **admin** and password **Weidmueller**.
- General configuration and apply behavior:
  - When pressing button 'Apply' after any configuration change (on any web page), the applied configuration becomes active immediately but will not be stored to Flash memory.
  - After applying of a changed configuration, the blue-colored note message 'Configuration changed and applied but not saved!' appears below the headline, indicating that the configuration still needs to be saved to permanent Flash memory. The note disappears after the configuration has been saved (web page 'Save Configuration').

  Note: This behavior (Apply without saving parallel saving to Flash memory) can be very helpful in case of applying an incorrect configuration which can result, for example, in an access blocking to the Router. By reboot via power down and up, the last saved configuration will be active again not having the applied misconfiguration.



Picture 1: Login page

4.1 System Information → System Overview

Login page providing status information and system overview.

Description of displayed sections

- System Data

  Provides information about system name, system description, location, contact person, serial number and firmware version.

- System Status

  Shows system time, device uptime and current system workload.

- Internet / WAN Connection

  Shows the interface currently used for Internet / WAN connection and - if configured - the failover interface (Backup connection).

- Active Routes

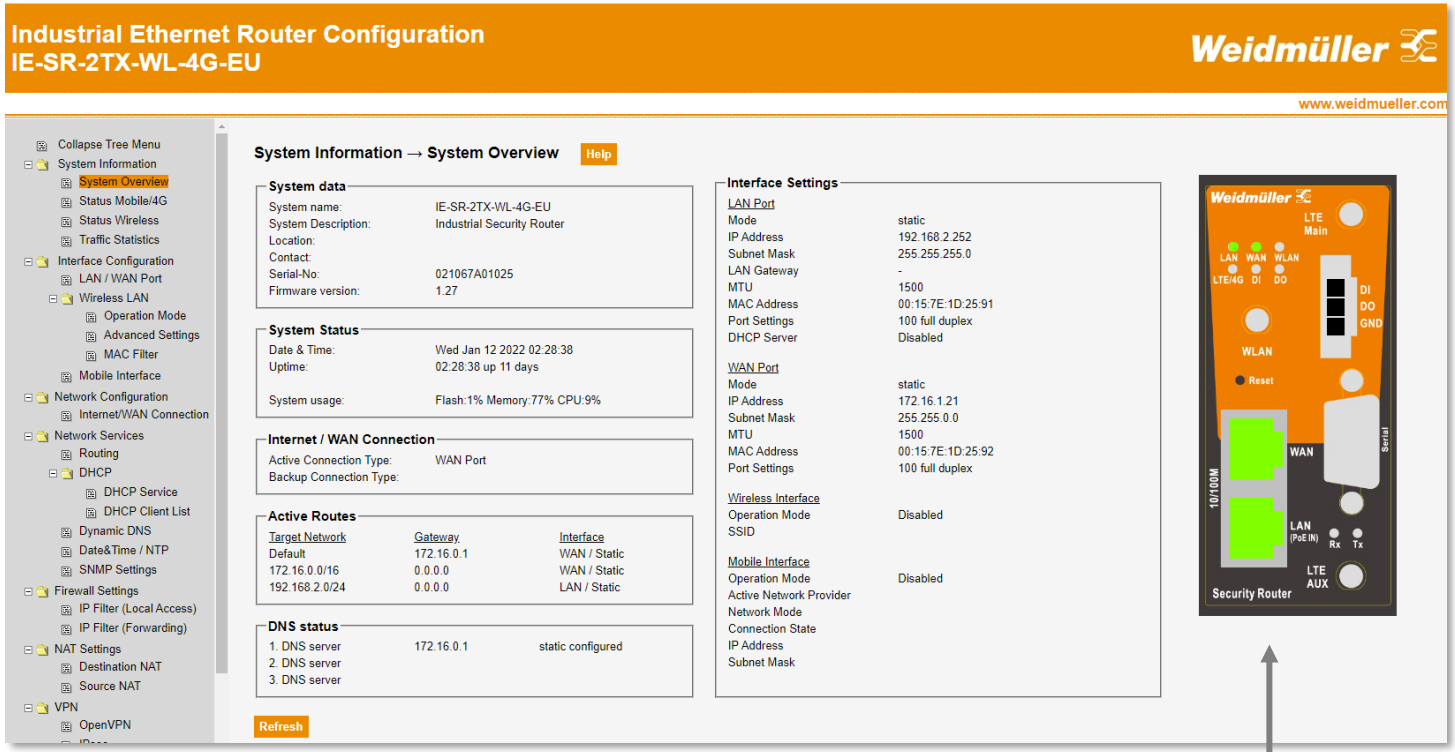
  Shows currently active routes including defined static routes.

- DNS Status

  Display of servers to be used for DNS requests.

- Interface Settings

  Provides status information about network interfaces LAN port, WAN port, Wireless Interface and Mobile Interface (only LTE/4G models).



Picture 2: Screenshot System overview (Login page).

Note about front panel view:	
LEDs for PWR1, PWR2 and PoE - available on the **real** device - are not visible on the front panel view. These LEDs are wired to the hardware directly and cannot be checked via software.	
Signaling of LEDs of Web page front panel view:	
LAN (Port) and WAN (Port)	ON (constantly) if connected (Link is established), OFF if disconnected.
WLAN	ON (constantly) if WLAN is enabled, OFF if disabled. No special signaling of the running operation mode.
LTE/4G	ON (constantly) if Mobile Interface generally is enabled, OFF if disabled. No explicit signaling of the connection state.
Digital Input (DI)	ON (constantly) if digital input is powered from 5 to 30 VDC, OFF if not connected or for power input 0 to 2 VDC.
Digital Output (DO)	ON (constantly) if digital output is set to ON, otherwise OFF.

4.2 System Information → Status Mobile/4G

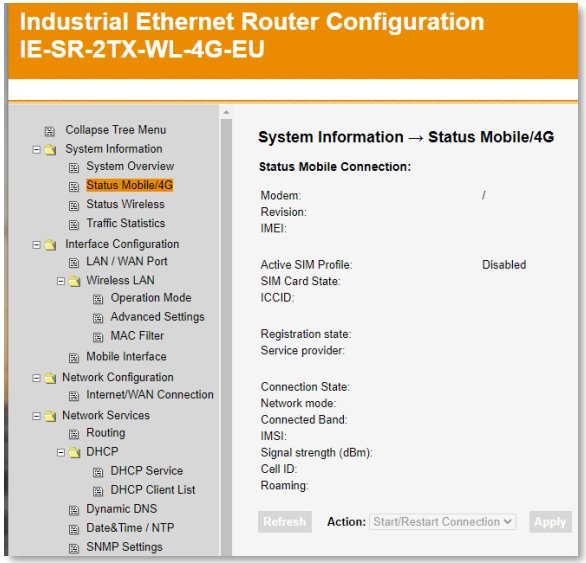
(only models IE-SR-2TX-WL-4G-EU and IE-SR-2TX-WL-4G-US-V)

This web page displays status information of the LTE/4G modem. Additionally, following modem-related actions can be triggered manually:

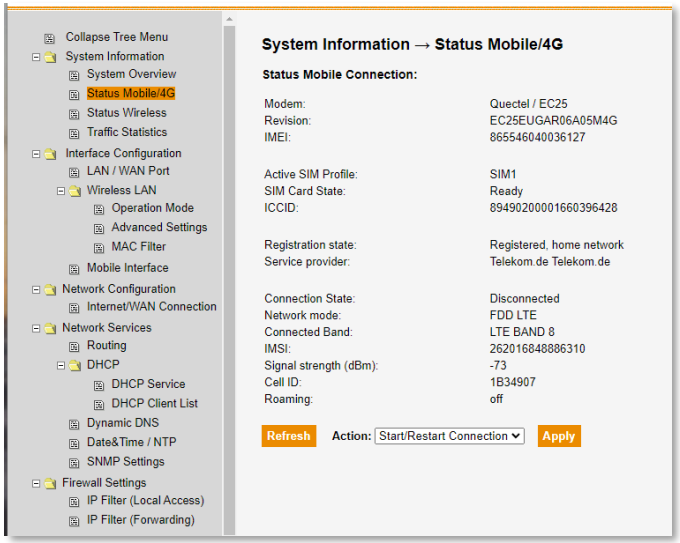
- Start/Restart Connection
- Disconnect
- Reboot Modem
- Re-Register Operator

These action types primarily are intended for diagnostic purposes in terms of evaluating the connectivity to a mobile operator.

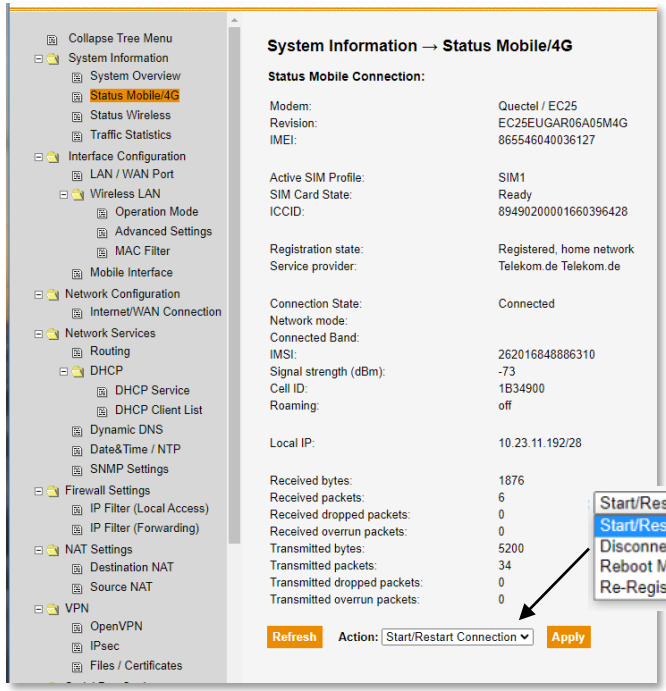
Note: Use actions 'Start/Restart Connection' and 'Disconnect' to establish/cancel a cellular connection if the connection settings of the mobile interface are set to "Manual" (Menu Interface Configuration → Mobile Interface).



Picture 3: Status information if 'Mobile Interface' is disabled.



Picture 4: Status information if 'Mobile Interface' is enabled and configured according to the inserted SIM card, but still disconnected (Offline).

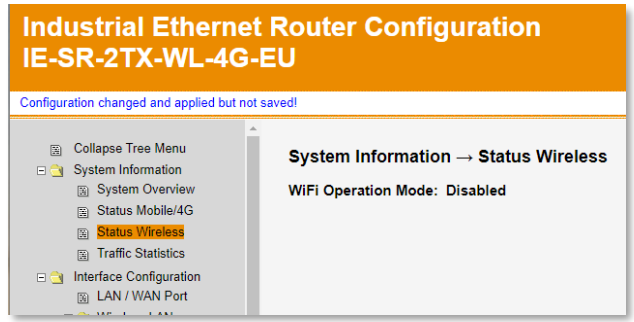


Selectable actions executable via button 'Apply'.

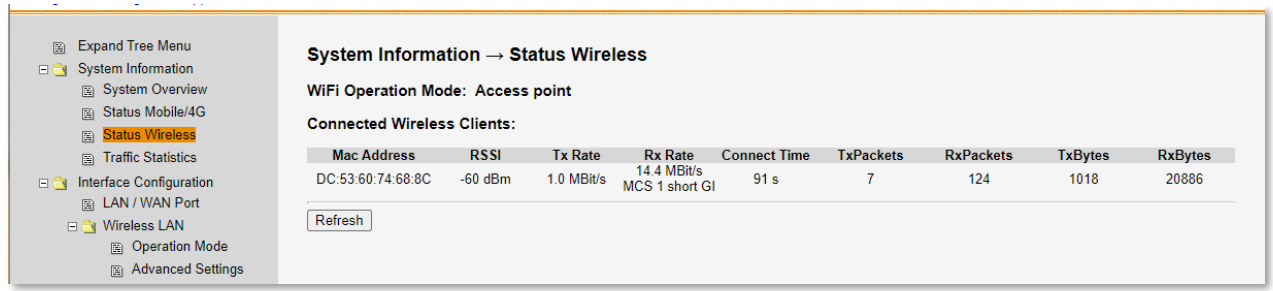
Picture 5: Status information if 'Mobile Interface' has established an Internet connection (Online).

4.3 System Information → Status Wireless

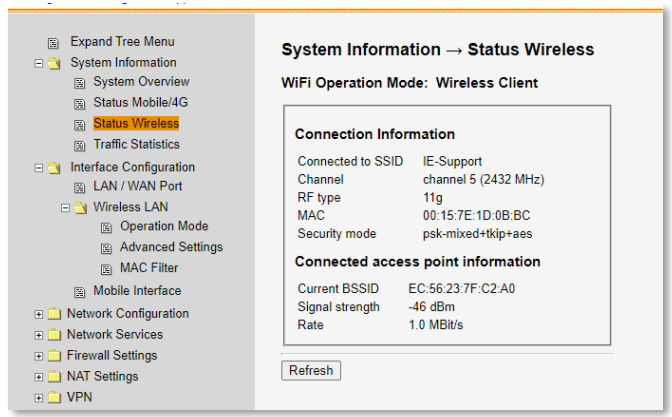
Web page displaying status information of WLAN interface dependent on the settings.



Picture 6: Example of status information if 'WLAN Interface' is disabled.



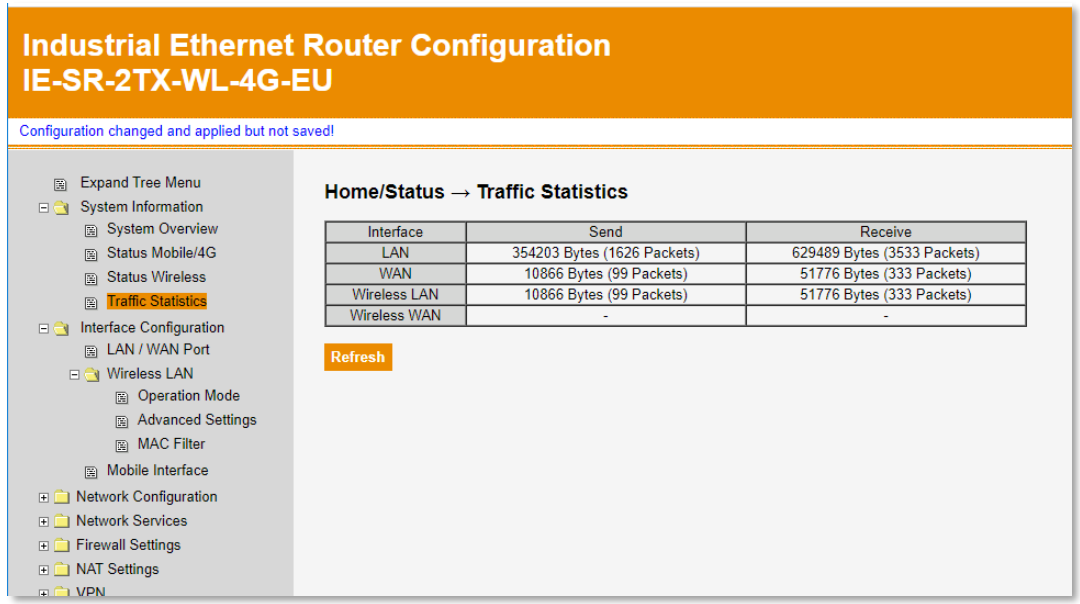
Picture 7: Example of status information if 'WLAN Interface' is running in operation mode 'Access Point' and having connected one WLAN client.



Picture 8: Example of status information if 'WLAN Interface' is running in operation mode 'Wireless Client' and being connected to an 'Access Point'.

4.4 System Information → Traffic Statistics

Displays the data traffic sent and received via device interfaces since router uptime.



Picture 9: Display of traffic statistics

4.5 Interface Configuration → LAN / WAN Port

This configuration page is used to set the IP configuration of wired LAN and WAN port.

LAN / WAN Interfaces

IP assignment: Interface can be configured using static IP, via DHCP or DHCP + Fallback. A fallback to the defined static IP will be done if DHCP fails.

Masquerade (NAT): If enabled, the source IP address of IP packets will be replaced by the Router's LAN or WAN IP when outgoing via the interface.

Default Gateway:

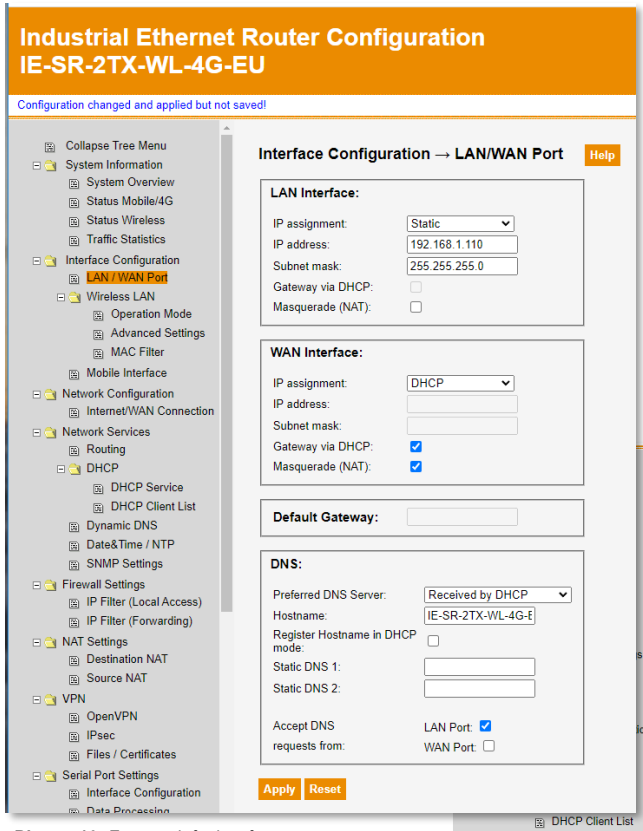
Can be configured if both interfaces LAN and WAN port are set to static IP assignment. If at least one of both interfaces is set to DHCP then this parameter is locked because default gateway will be retrieved by DHCP.

DNS:

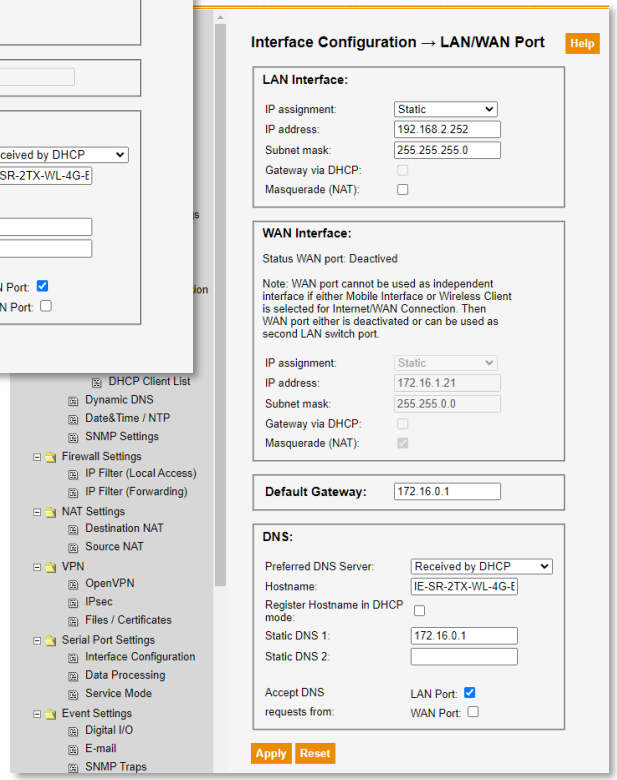
Used for configuration of DNS settings. Two static DNS servers can be configured, additional to a DNS entry retrieved by an interface with DHCP-based IP assignment.

Note about WAN Port:

For selection of the interface being the Internet/WAN connection either the wired WAN port, WLAN interface (Mode 'Wireless Client') or 'Mobile Interface' (only LTE/4G models) can be configured (refer to configuration section 'Network Configuration → Internet/WAN Connection). But there are some limitations about independent use of these interfaces. If mode 'Mobile Interface' or 'Wireless Client' is selected for Internet/WAN connection, then the wired WAN port either is deactivated or can be used as second LAN switch port.



Picture 10: Factory defaults of LAN/WAN Port settings.



Picture 11: Screenshot showing a deactivated WAN port after setting 'Internet / WAN Connection' either to connection type 'Wireless Client' or 'Mobile Interface'.

4.6 Interface Configuration → Wireless LAN → Operation Mode

Via this configuration page the WLAN interface generally can be enabled / disabled and configured for operation modes 'Access Point' or 'Wireless Client'

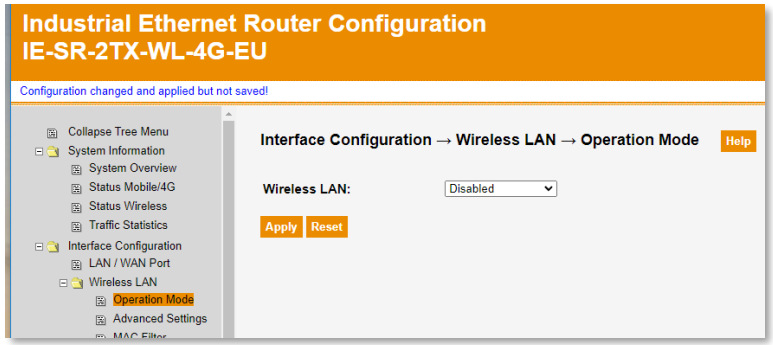
Operation Mode 'Access Point':
Running this mode, the Router provides an access point for wireless clients which will be assigned to the LAN network when connected. WLAN Clients can connect wireless based on the configured access and security settings and will be assigned to the LAN network.

Consider: Ensure that the Router's DHCP Server function is enabled and properly configured (Menu Network Service → DHCP → DHCP Service). If DHCP service is not configured, the WLAN clients connect to the 'Access Point' but do not get any IP address assignment.

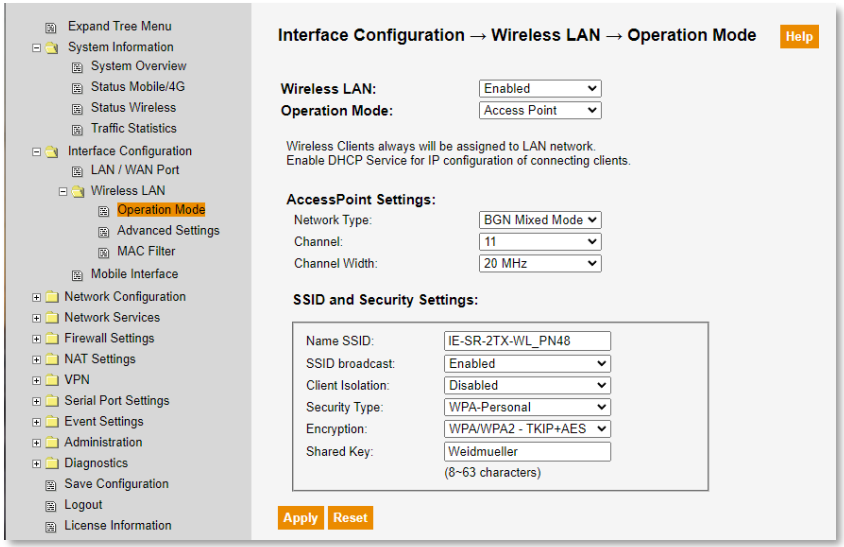
Operation Mode 'Wireless Client':
Running this mode, the interface acts as a WLAN client which connects to an 'Access Point' and provides the Internet/WAN connection via the 'Access Point' alternatively to the WAN Port. Each LAN traffic to external networks is routed via the WLAN interface which is a client of the associated 'Access Point'. The IP data assignment of the WLAN interface either is done via DHCP (received from AP) or by static configuration (if manually done, the IP of course should be in the AP's subnet). Consider: For this operation mode the WAN port either is disabled or can be used as second LAN port. For connection to an Access Point either enter the SSID of the AP manually or use button 'Site Survey' to search for an available access point. Configure the AP's security settings and the IP assignment of the WLAN interface (Either via DHCP or enter manually). Finally select the use of WAN port (either disabled or running as second LAN port) before applying the configuration.

Consider: It is highly recommended to activate 'Masquerading (NAT)' for the WLAN interface. This ensures that responses of outgoing traffic - initiated from LAN side - can be routed back to LAN devices without setting any routes in the associated 'Access Point'.

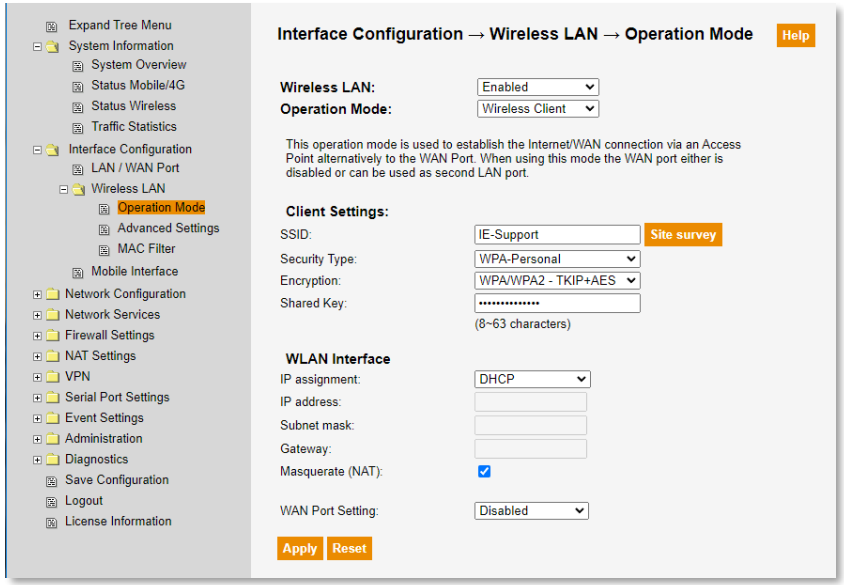
Note: If mode 'Wireless Client' will be applied, then this mode immediately becomes the current Internet/WAN connection. The previously selected interface ('WAN Port' or 'Mobile Interface' for LTE/4G models) will be replaced automatically. This behavior is caused by technical design.



Picture 12: Wireless LAN factory default settings (disabled)



Picture 13: Example of operation mode 'Access Point'

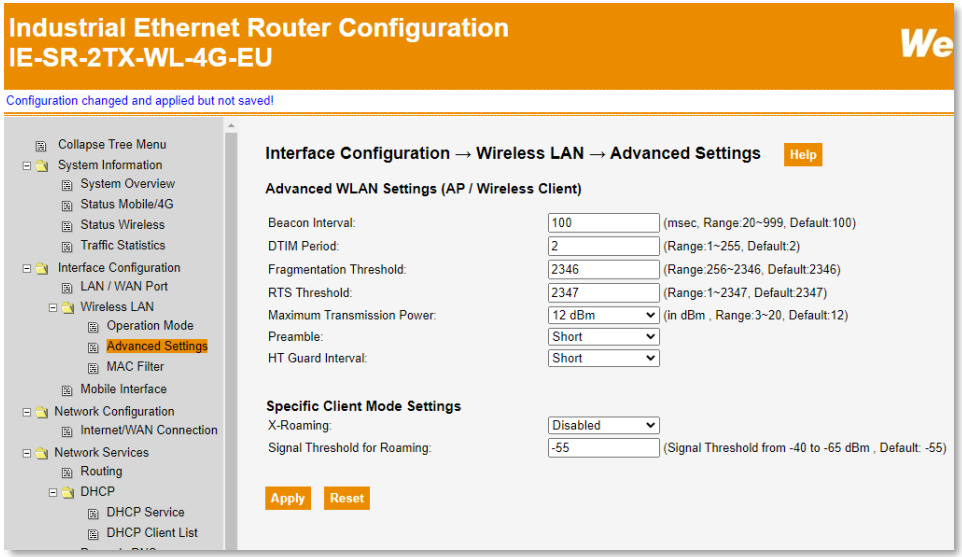


Picture 14: Example of operation mode 'Wireless Client'

4.7 Interface Configuration → Wireless LAN → Advanced Settings

Menu ‘Advanced Settings’ provides configuration of additional parameters of WLAN interface.

Advanced WLAN Settings (valid for operating modes ‘Access Point’ and ‘Wireless Client’)	
Beacon Interval	A beacon is a broadcast packet sent by the 'Access Point' to synchronize wireless devices. The beacon interval value defines the frequency interval how often the beacon is broadcast by the Router. Increasing this value reduces the number of beacons and the overhead associated with synchronization process. The default value is 100, but 50 is recommended for a reception.
DTIM Period	This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown Message (DTIM) informing clients about the next window for listening to broadcast and multicast messages. When the ‘Access Point’ has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. The associated clients hear the beacons and awaken to receive the broadcast and multicast messages. The factory default value is 2 milliseconds (Range: 1 to 255 msecs).
Fragmentation Threshold	The value specifies the maximum size of a packet before it is fragmented into multiple ones. It ranges from packet size 256 bytes up to 2346, it is recommended to remain at the default size of 2346 bytes. If you experience a high packet error rate, you may slightly decrease the value. Setting the value too low may result in poor network performance. Only minor modifications of this value are recommended..
RTS Threshold	The RTS (Request to Send) threshold is the amount of time a wireless device, attempting to send, will wait for a recipient to acknowledge that it is ready. Normally, an access point sends a RTS frame to a station and negotiates the sending of data. After receiving RTS frame, the station responds with a CTS (Clear to Send) frame to acknowledge the right to begin transmission. To ensure communication, the maximum value should be used, which is the default value 2347 (Range: 0 to 2347 bytes). If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.
Maximum Transmission Power	This parameter allows you to change the power output level. Default value is 12 dBm (Range: 3 dBm to 20 dBm). A 'Maximum Transmission Power' value of 12 dBm (around 60% of maximum) is probably suitable for most user applications. Higher power settings are not recommended for users due to excess heat generated by the radio chipset, which can affect the life of the device.
Preamble	Two different preamble types (long or short) can be selected. A long preamble uses additional data header strings to check data transmission errors. A short preamble is faster because it adds less data when checking transmission errors. Default setting is a short preamble enabling an increased overall throughput. However, if any wireless device does not support short preamble, then it will not be able to communicate within the wireless network. In this case select a long preamble.



Picture 15: Factory default settings of advanced wireless parameters

HT Guard Interval	When doing a wireless transmission, RF signals can reach the receiving antenna by two or more paths resulting in an interference and degradation of the signal. Parameter 'Guard Interval' is intended to avoid signal loss from multipath effect, the value can be set to 'short' or 'long'. By default, a short 'HT Guard Interval' is active, it can increase the data rate by roughly 10%. Note: This parameter is only valid for wireless standard 802.11n (HT is equivalent to 802.11n and means High Throughput).
Specific Client Mode Settings	
X-Roaming	For operation mode 'Wireless Client' parameter 'X-Roaming' can be enabled to shorten the time for handover from a connected access point to another one. This feature is disabled by default.
Signal Threshold for Roaming	If 'X-Roaming' is enabled, this parameter determines when to start looking for new access point candidates. If the current connection quality (Signal Strength) is lower than the specified threshold, the Router will start background scanning and look for the next-hop candidate. Default signal threshold for roaming is 55 dBm (Range: -40 to -65 dBm).

4.8 Interface Configuration → Wireless LAN → MAC Filter

Function 'MAC Filter' for Wireless LAN can be used to control the access of wireless clients if the Router is running in mode 'Access Point'.

If MAC Filter is enabled, WLAN client connections either are allowed or rejected dependent on the selected policy and if being a member of the MAC filter table.

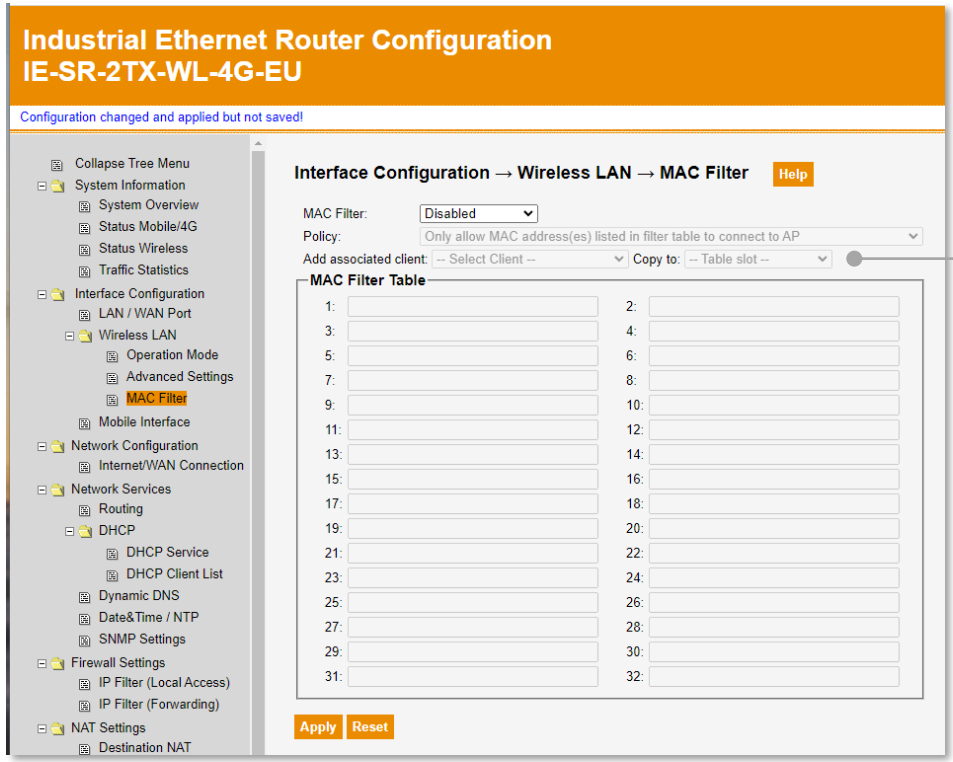
General Activation / Deactivation
MAC Filter: Enables or disables access control by MAC address generally.

Selectable Policy Settings

- Only allow MAC address(es) listed in filter table to connect to 'Access Point'.
  As stated, only clients having a MAC address listed in the MAC filter table may connect to the Router. This access policy is working as a "white" list.
- Only deny MAC address(es) listed in filter table to connect to 'Access Point'.
  As stated, all clients having a MAC address listed in the MAC filter table are rejected for connection. This access policy is working as a "black" list.

MAC Filter Table
This table contains the MAC addresses which are controlled according to the policy setting. Up to 32 client MAC addresses can be managed via the MAC filter table.

Note: When entering a MAC address manually use format xx:xx:xx:xx:xx:xx.



Picture 16: Factory default settings of MAC filter table

Consider:

1. Function 'Add associated client' can be used for an easy MAC address takeover of already connected clients into the MAC filter table. The preferred method is to do this as long the Router is running with disabled MAC Filter because only this status lists connected clients (still not controlled by MAC filter) in the drop-down selection box for take-over (Copy to).

2. When starting to configure, first set parameter 'MAC Filter' to enabled. Next select an associated client and then select the table slot (Number 1 to 32) via the drop-down list box. When clicking on the desired table slot, the MAC address automatically will be copied to the MAC filter table.

3. Please keep in mind that this method only is reasonable for policy setting 'Only allow MAC address(es) listed in filter table to connect to AP'. Otherwise, already connected clients which just have been added to the MAC filter table, will be rejected for access immediately if the configuration will be applied.

4.9 Interface Configuration → Mobile Interface

Via this configuration page the 'Mobile interface' generally can be enabled / disabled and configured providing a 4G/LTE connection. The device is equipped with one radio module but supports the use of 2 SIM cards (Dual SIM). Each SIM can be configured with its own provider profile. One is selectable as primary connection and the other one as failover connection in case of an operator-dependent connection loss.

Mobile Interface: Enables or disables the use of the mobile interface generally.

Network Scan: Click button to detect available network providers in the (environment of the Router's location and to retrieve information about their accessibility based on the inserted SIM card(s).
Note: Starting a network scan interrupts an established connection (Online) and can take several minutes to get a response.

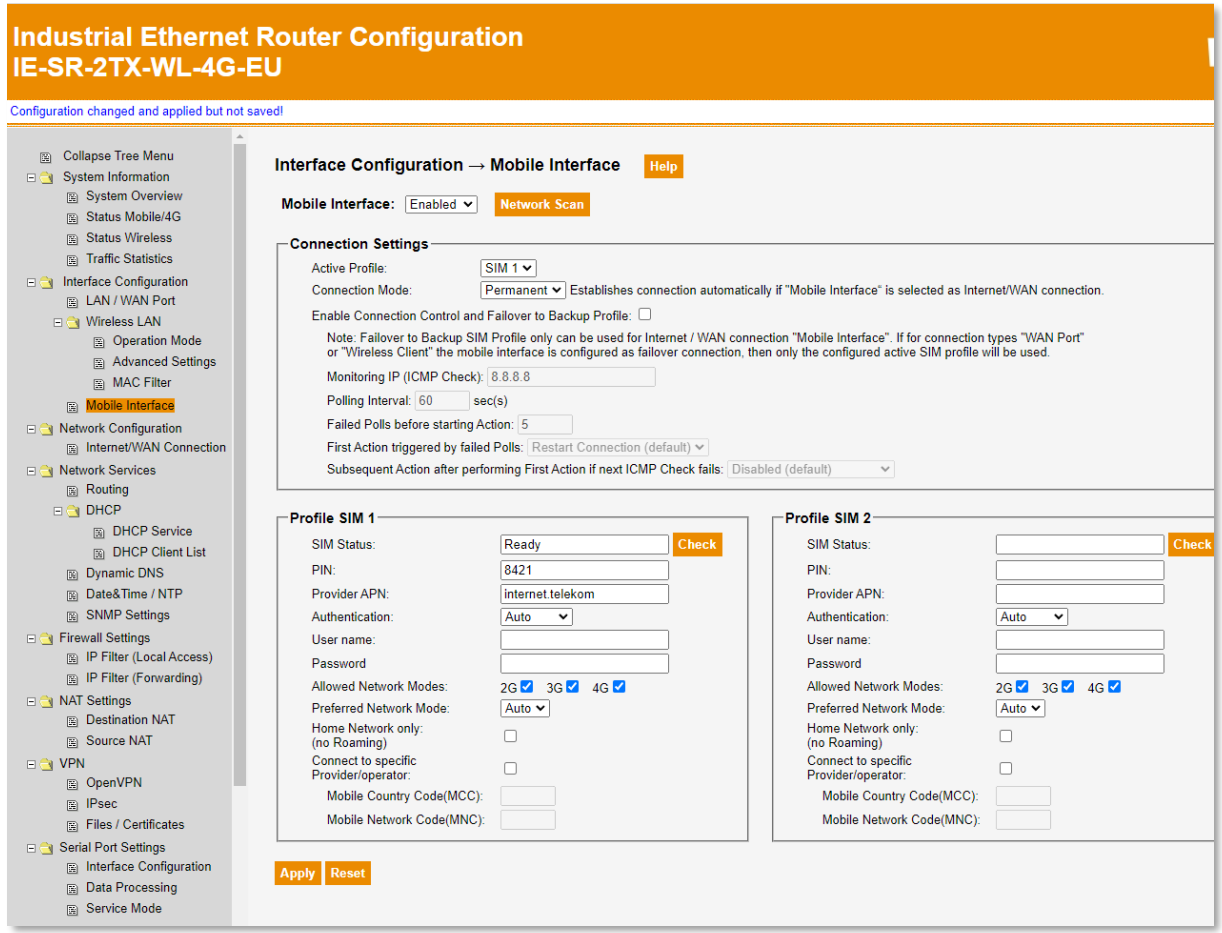
Section 'Connection Settings'

Active Profile: The primary mobile connection (SIM1 or SIM 2) is selected by parameter 'Active Profile'. The other SIM profile can be used as backup connection but only if 'Mobile Interface' is selected for the Internet/WAN connection.

Connection Mode: Defines when to establish a provider connection. If set to 'Permanent', the Router tries to establish the connection automatically at boot time if the Internet/WAN connection is set to 'Mobile Interface'. For connection mode 'Manual' the mobile connection can be established/canceled manually via menu 'System Information → Status Mobile/4G'.

Failover to Backup Profile: The failover from the active SIM card to the backup SIM profile only is possible if the Internet/WAN connection is set to 'Mobile Interface'. The failover behavior can be configured when enabling checkbox 'Enable Connection Control and Failover to Backup Profile'.

Sections 'Profile SIM 1' / 'Profile SIM 2'
Use these sections for configuration of inserted SIM card(s) for connection to the mobile operator.



Picture 17: Example of enabled and configured mobile interface (Profile SIM 1)

Notes:

- If 'Internet/WAN Connection' is set to 'WAN Port' or 'Wireless Client' and if the 'Mobile Interface' is set as backup connection, then always the selected 'Active SIM Profile' (primary) is used. A subsequent changeover to the backup SIM profile, in case that the primary SIM profile also fails, is not implemented. The failover function from primary to backup SIM card only is possible if 'Internet/WAN Connection' is set to 'Mobile Interface'.
- After applying of the configuration, the connection status of the mobile interface can be checked on website 'System Information → Status Mobile/4G'.

4.10 Network Configuration → Internet/WAN Connection (1 / 2)

Selection of the network interface (connection type) to be used for Internet/WAN connection.

Via this configuration page the connectivity to the Internet or to an upper-level network (WAN) will be defined.

For establishing an Internet/WAN connection one of the interfaces
- WAN port (wired)
- WLAN interface (Mode Wireless Client)
- Mobile interface (only for LTE/4G models)

can be selected.

By factory default the RJ45 WAN port is selected as the active Internet / WAN connection.

General configuration hints:

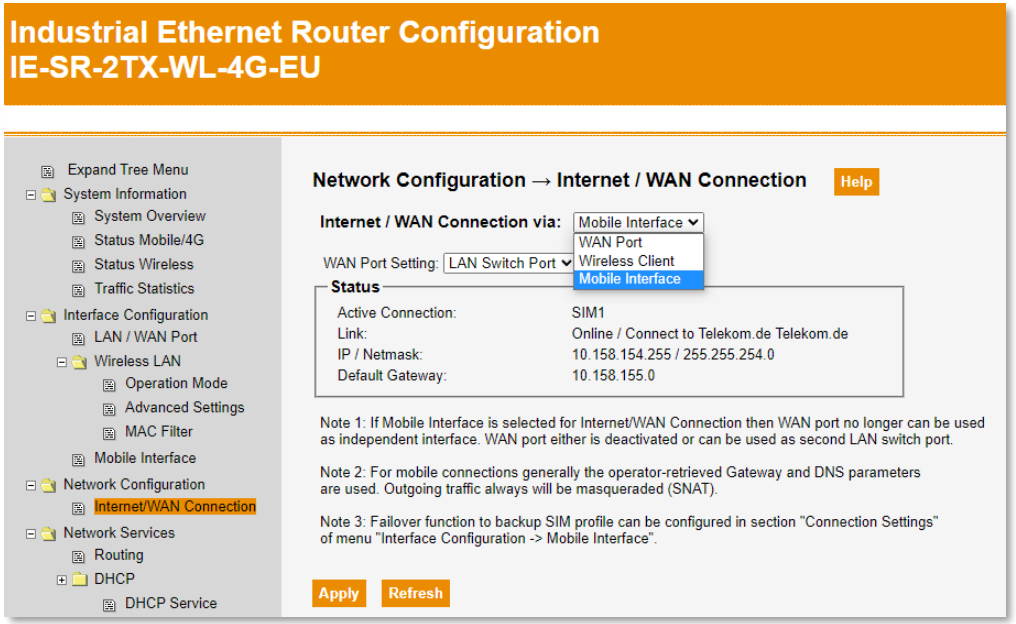
1. The WAN port (wired) always can be selected to be used for the Internet / WAN connection.

2. Interfaces 'Mobile Interface' or 'Wireless Client' cannot be selected for the Internet / WAN connection as long the interface is not enabled or not yet configured (Error message is displayed). Before selection, you need to enable and configure the desired interface in section 'Interface Configuration' to be useable for Internet / WAN connectivity.

3. If WLAN interface (Mode 'Wireless Client') will be configured (Menu Interface Configuration → Wireless LAN → Operation Mode), then after applying mode 'Wireless Client' immediately and automatically becomes the active Internet/WAN connection (replacing previous setting 'WAN Port' or 'Mobile Interface'). This is caused by technical design.

4. 'Mobile Interface' can be configured independent of the selected interface for Internet / WAN connection and needs to be set as active Internet / WAN connection explicitly.

5. If either 'Wireless Client' or 'Mobile Interface' is selected for Internet / WAN connectivity, then the wired WAN port either is disabled or can be configured as additional (switched) LAN port. In this condition the WAN port related configuration parameters (Interface Configuration → LAN/WAN Port) are locked. If WAN port shall be used again for Internet / WAN connectivity, then select 'WAN Port' as active Internet / WAN connection.

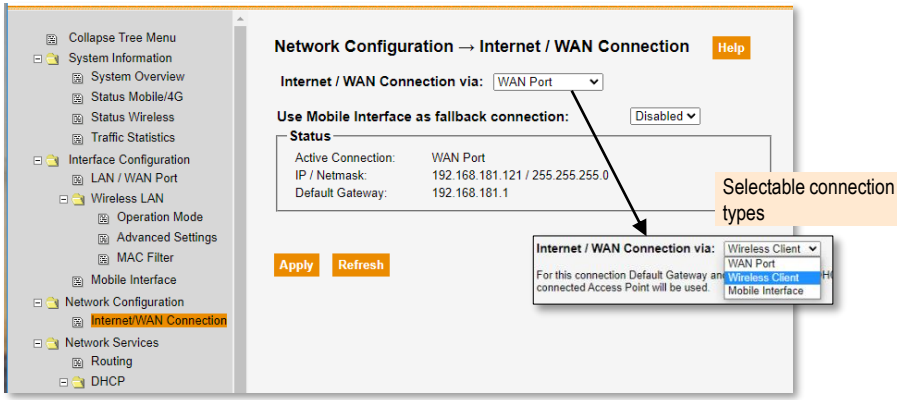


Picture 18: Example of an established Internet / WAN connection via 'Mobile Interface'.

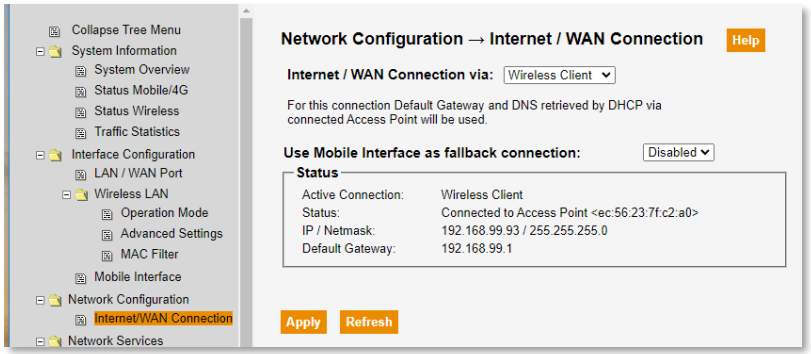
Selectable combinations for Internet / WAN connectivity:		
Primary connection	**Configurable Fallback Connection**	**Restrictions / Limitations / Impact**
WAN Port (wired)	Mobile Interface (Active SIM profile)	WLAN can only be used in mode Access Point. Connecting clients will be assigned to LAN network.
WLAN Interface (Mode Wireless Client)	Mobile Interface (Active SIM profile)	WAN port (wired) either disabled or useable as additional LAN port.
Mobile Interface (Active SIM profile)	Mobile Interface (Backup SIM profile)	WAN port (wired) either disabled or useable as additional LAN port.

4.10 Network Configuration → Internet/WAN Connection (2 / 2)

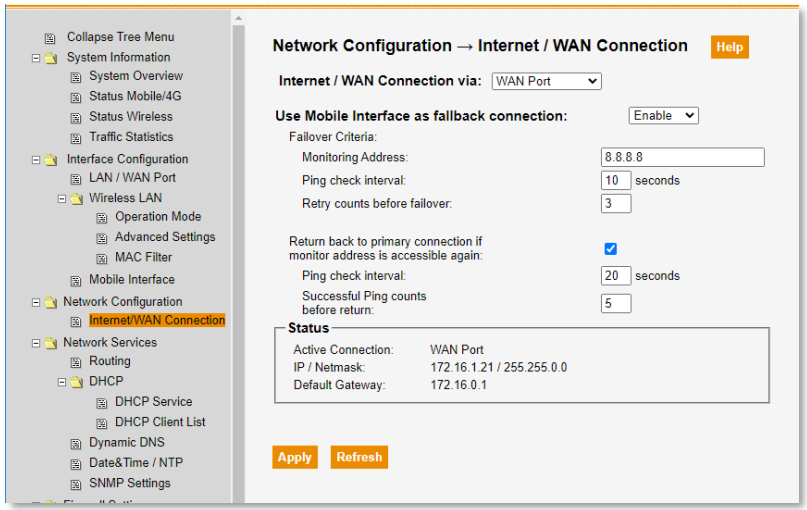
Examples of selection of a network interface (connection type) to be used for Internet / WAN connection.



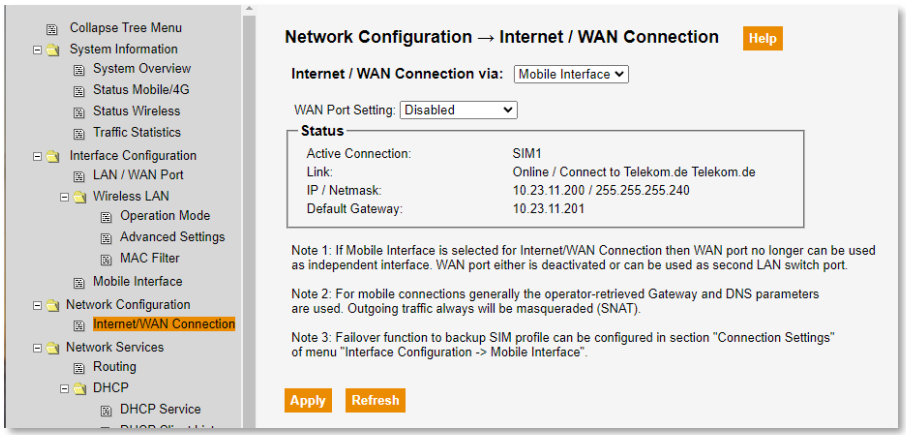
Picture 19: Example of WAN Port selected for Internet / WAN connection. No connection failover to 'Mobile Interface' (Backup) configured.



Picture 21: Example of WLAN interface (Mode 'Wireless Client') selected for Internet / WAN connection. No connection failover to 'Mobile Interface' (Backup) configured.



Picture 20: Example of WAN Port selected for Internet / WAN connection. 'Mobile Interface' is configured as failover connection (Backup).



Picture 22: Example of mobile interface selected for Internet / WAN connection and currently connected (Online) to the operator via profile 'SIM 1'.

Note: If - for example - profile 'SIM 2' also is activated and configured for failover (backup), then in case of a connection changeover profile 'SIM 2' would be displayed here as active connection.

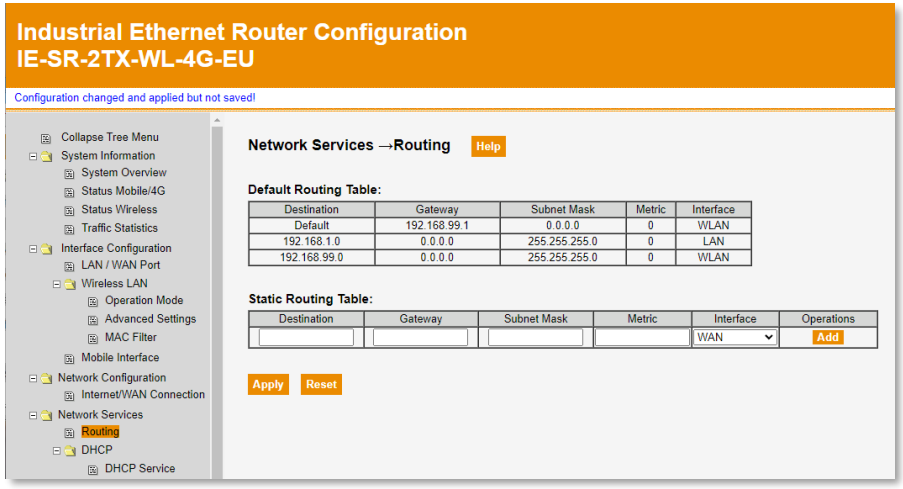
4.11 Network Services → Routing

This web page shows all active routing entries of the device and can be used for definition of static routes.

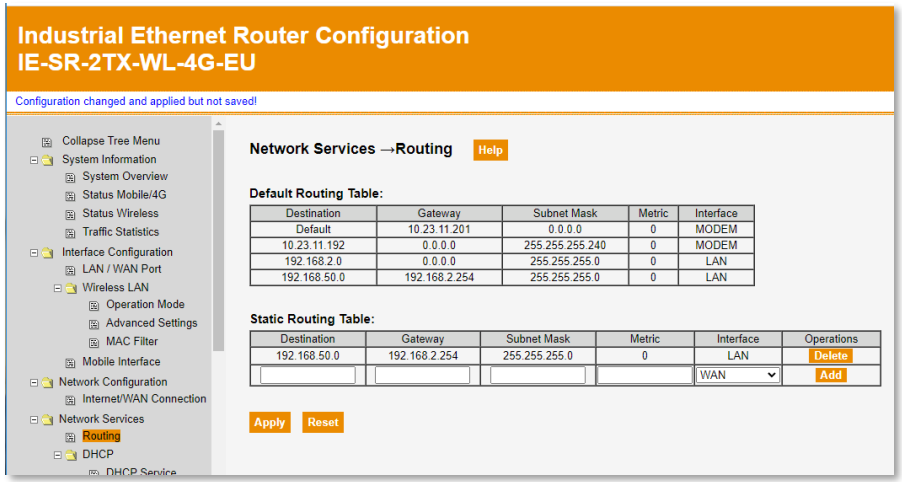
The 'Default Routing Table' lists the default network routes based on the active router interfaces.

Via the “Static Routing Table” additional routes can be configured manually. A static route will become active immediately after adding and applying. Several static routes can be added before clicking 'Apply' button to activate them.

The default metric for static routes is zero (0) having the highest priority. If necessary for any reason, change the metric to a higher value to decrease the priority of this entry.



Picture 23: Example of routing entries for an Internet / WAN connection via WLAN Interface (Operation mode ‘Wireless Client’)



Picture 24: Example of routing entries for an Internet / WAN connection via Mobile Interface (4G/LTE modem) and one additionally configured static route.

4.12 Network Services → DHCP → DHCP Service

The Router supports features 'DHCP Server' and 'DHCP Relay' exclusively for LAN network members.

DHCP Server

Provides IP data assignment for DHCP clients when connecting to the LAN interface. The DHCP service operates on the wired LAN port and for connecting WLAN clients if the Router's WLAN interface is running in operation mode 'Access Point'.

IP address data for DHCP clients will be assigned according to the configurable parameters, for Gateway and DNS current Router settings will be provided to clients.

Additionally, static IP assignment of connecting clients based on their MAC addresses can be assigned.

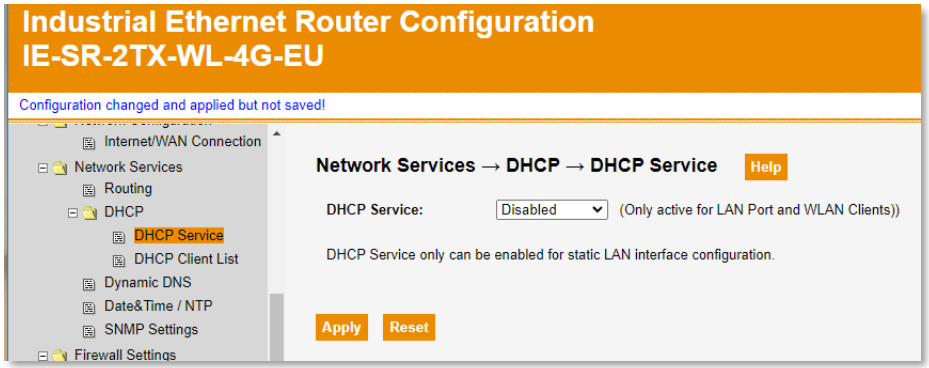
DHCP Relay

In this mode the Router acts as a gateway between a requesting DHCP client at LAN side (wired LAN port or WLAN Client) and a remote DHCP server accessible by the configured 'Target DHCP Server IP'.

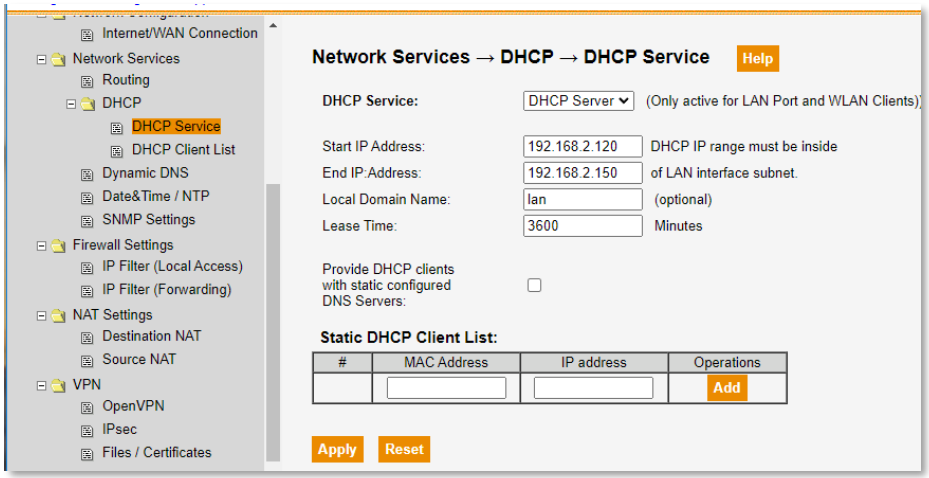
If activated, DHCP requests will be forwarded to a DHCP Server having the specified IP address and the responses from DHCP server will sent back to the requesting DHCP client.

Notes:

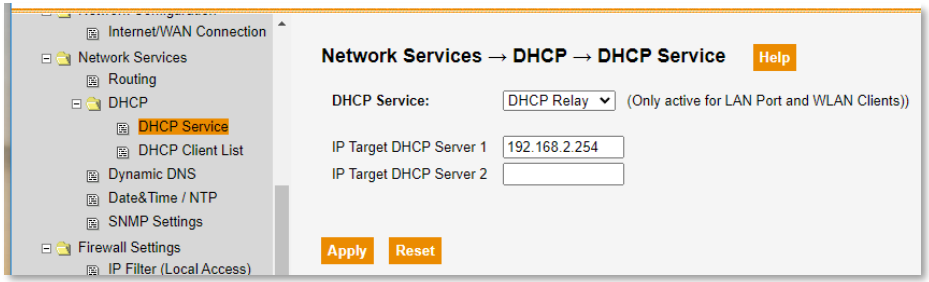
- Both services 'DHCP Server' and 'DHCP Relay' only can be applied for DHCP clients connecting either via wired LAN port or via wireless LAN if the Router is running as Access Point.
- If the Router's WLAN interface is running in operation mode 'Access Point', do not forget to activate ''DHCP Server' to ensure that connecting WLAN clients (configured with DHCP) will get their IP address data.



Picture 25: Example for disabled DHCP service



Picture 26: Example for enabled DHCP server

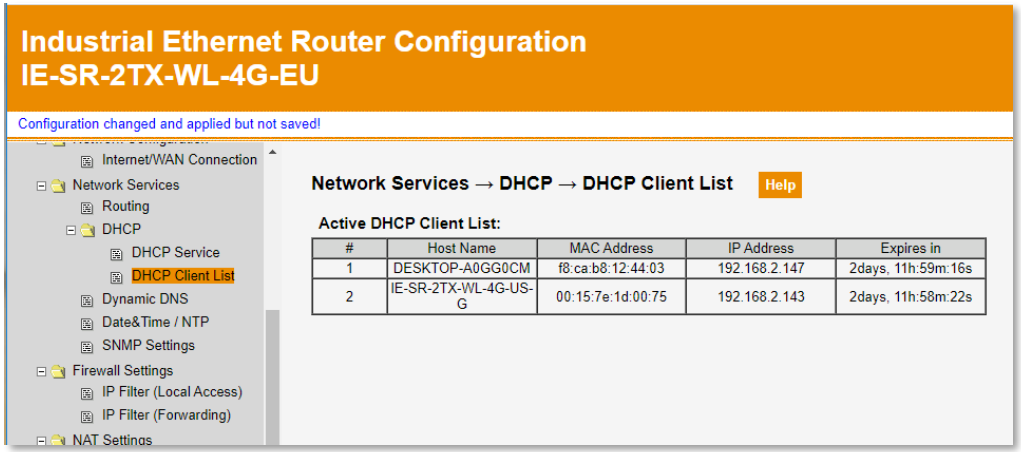


Picture 27: Example for an enabled DHCP relay service

4.13 Network Services → DHCP → DHCP Client List

This table shows all DHCP clients having received a DHCP lease from the Router's DHCP service.

Listed DHCP clients either are devices connected to the wired LAN port or WLAN clients (also members of the LAN network) if the Router is configured running operation mode 'Access Point'.

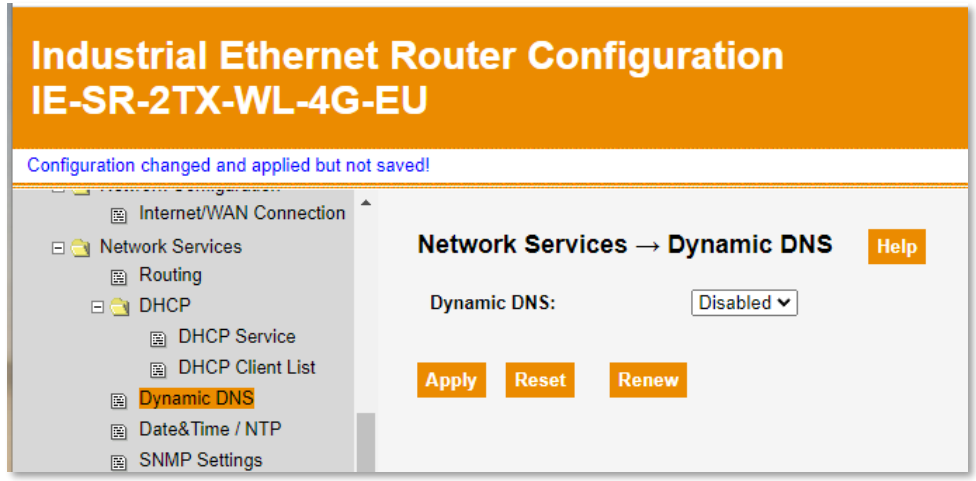


Picture 28: Example showing 2 DHCP clients which have been received IP data from the Router's DHCP service.

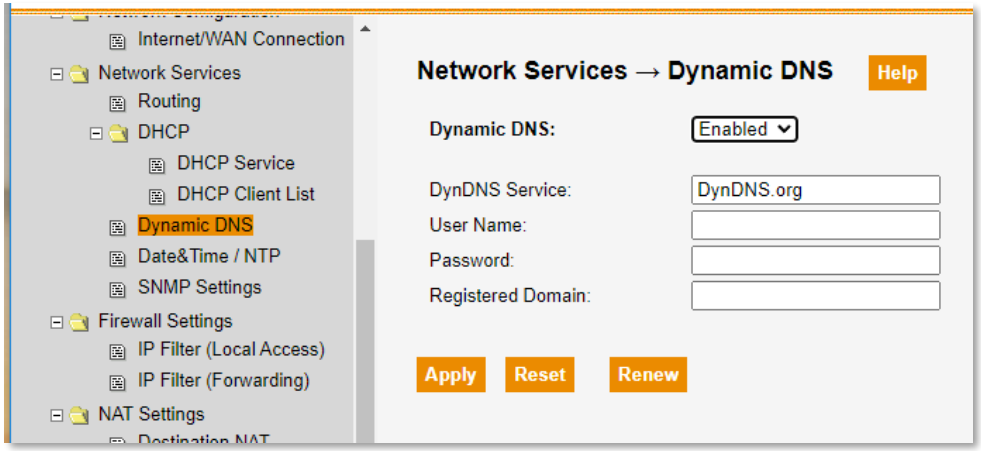
4.14 Network Services → Dynamic DNS

DDNS (Dynamic Domain Name System) allows you to configure a domain name for your IP address which is dynamically assigned by your Internet Service Provider. Therefore, you can use a static domain name that always points to the current dynamic IP address.

Note: Currently the Router only supports provider 'DynDNS.org' for dynamic DNS service. Prerequisite for using this function is having an existing account at 'DynDNS.org'.



Picture 29: Disabled Dynamic DNS (Factory default)



Picture 30: Enabled Dynamic DNS. Currently only provider 'DynDNS.org' is supported.

4.15 Network Services → Date & Time / NTP

This web page can be used

- to set the Router's system time manually,
- to configure NTP time synchronization getting date and time from an external NTP server,
- to configure NTP time server relay function allowing NTP clients requesting date and time from the Router.

Note: The Router is equipped with an internal clock (not battery buffered) which needs to be set when powered-up or rebooted to show correct date and time values. At power-up or if the Router will be rebooted, the system time always starts with date 01 January 2022 and time 00:00:00 plus offset (from UTC) related to the configured time zone.

Manual Date / Time Settings

- Enter data for date and time input fields or click button 'Get Browser Data' to fill the input fields with current settings of the connected PC.
- Click button 'Set System Time' to update the system time with content of the date and time input fields.

Note: Button 'Set System Time' updates the system time exactly according to the input fields. The setting of the time zone will not be considered.
For manual date / time setting it is recommended to select first the right time zone, then click button Apply, then click button 'Get Browser Data' and finally click “Set System Time’.

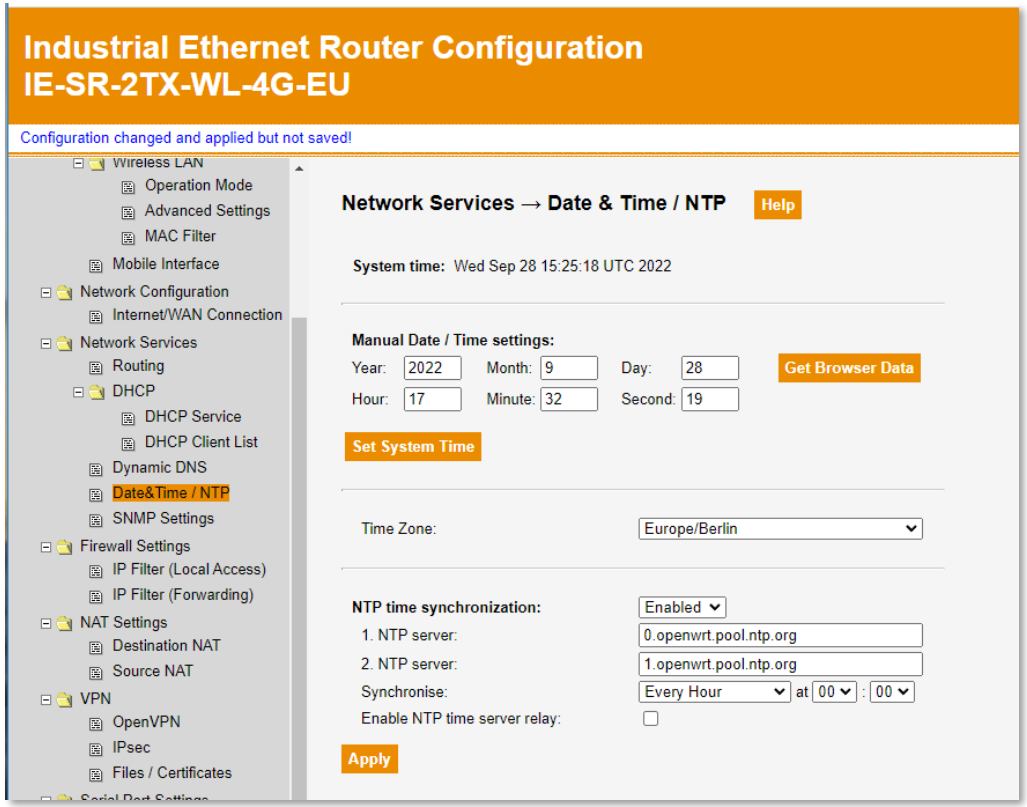
Time Zone Setting

- Select the time zone according to the Router's location.

Note: If the time zone has been changed and button 'Apply' will be clicked, then the system time will be adapted with the offset between previous and selected time zone.

NTP Time Synchronization

Via this section a periodic time synchronization with an external NTP server can be configured. If NTP time synchronization is enabled, the Router additionally can serve as NTP server (Checkbox ‘NTP time server relay’) providing date and time information for other NTP clients.



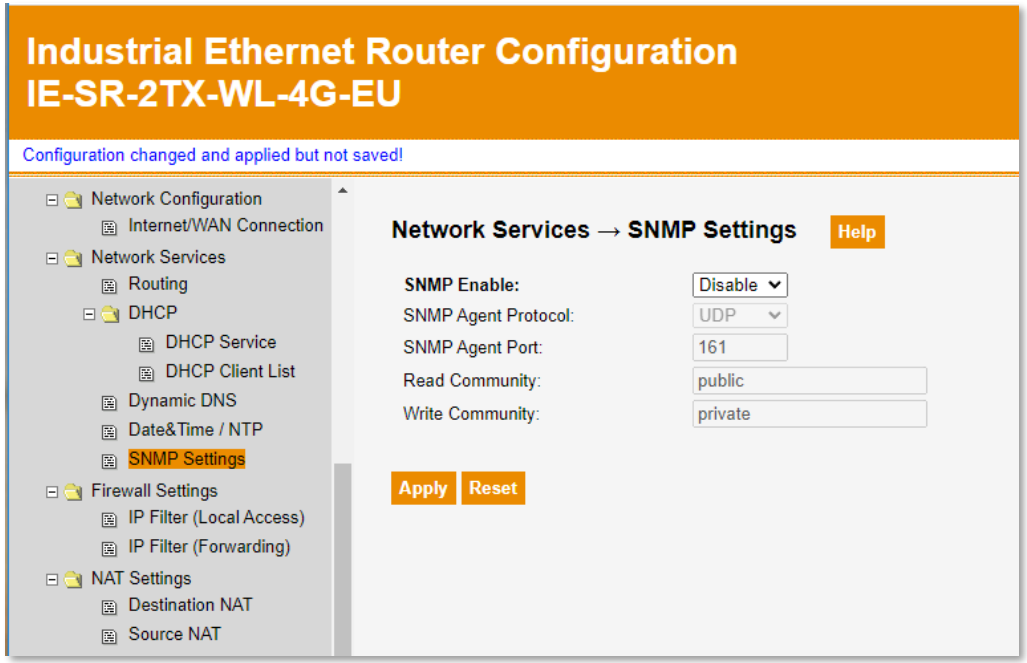
Picture 31: Example of Date & Time settings having NTP time synchronization enabled.

4.16 Network Services → SNMP Settings (Simple Network Management Protocol)

This webpage is used to enable/disable the Router's SNMP agent and for configuration of the SNMP communication settings.

SNMP requests will be provided for common parameters based on standards SNMPv2-MIB, RFC1213-MIB, TCP-MIB and UDP-MIB.

Note: Currently the Router supports only SNMP v2.



Picture 32: SNMP factory default settings.

4.17 Firewall Settings → IP Filter (Local Access)

Web page **IP Filter (Local Access)** is used to define filter rule settings for **incoming** traffic terminating on the Router itself and is assigned to the 'input chain' of the iptables firewall.

Each incoming IP packet - having a destination IP address of any of the Router interfaces (LAN IP, WAN IP, etc.) - do pass this 'Local Access' filter and can be controlled by rules defined in the active IP filter table.

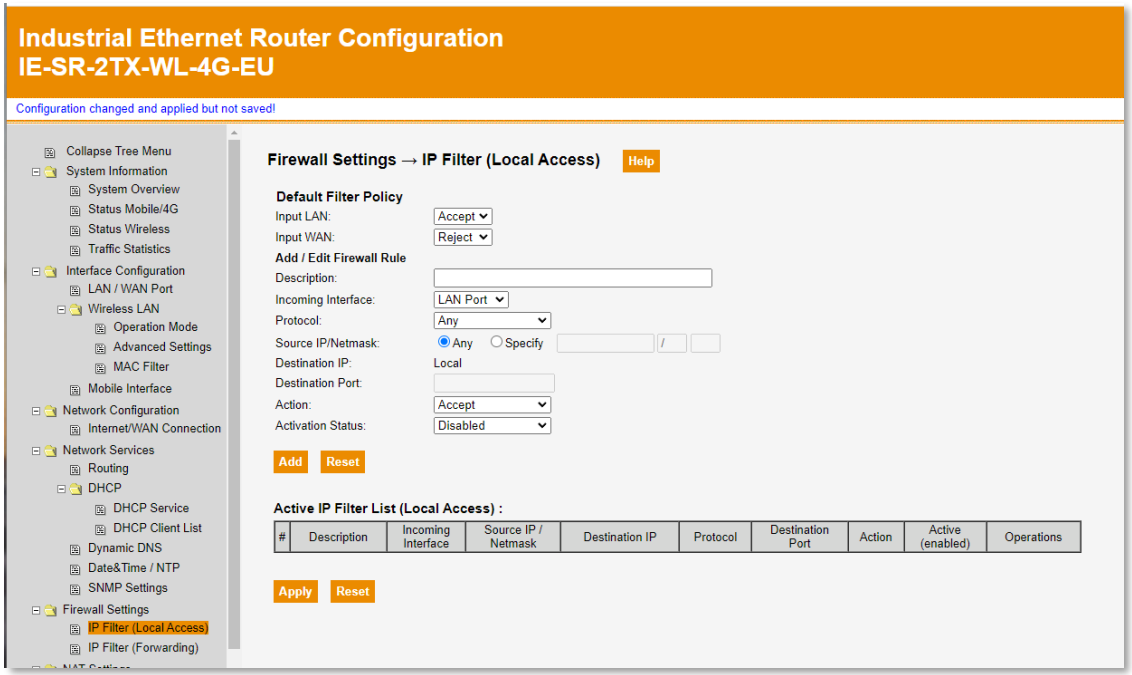
For example, typical applications for definitions of 'Local Access' rules can be:
- Allow access to the Web interface only for specific IP addresses.
- Allow use of Ethernet/Serial converter functions only for specific (source) IP addresses.

Default Filter Policy (LAN and WAN input):
These parameters determine the default handling of packets incoming at LAN respective WAN port and targeted to the Router itself. It will be applied for ingress packets not matching any rule specified in the 'Active IP Filter List (Local Access)'.

Section 'Add / Edit Firewall Rule':
Use for creation / adaption of specific firewall rules. Several rules can be defined and added before they become active by clicking button 'Apply'.

Table 'Active IP Filter List (Local Access)':
This table contains all configured rules, either being enabled (active) or disabled. Active rules will be checked from top to bottom. If a rule matches, the defined action (Accept, Reject, Drop) will be done, and the rule check will be canceled immediately. If no rule matches, the default filter policy will be applied.

Note: Rules for device access like Web interface access via HTTP(S), Telnet, SSH Console or Ping to WAN port IP, do not need to be configured as special local access rule. These access settings can be configured easily via checkbox settings in configuration menu 'Administration → System Settings'.



Picture 33: Default settings of IP Filter (Local Access).

4.18 Firewall Settings → IP Filter (Forwarding)

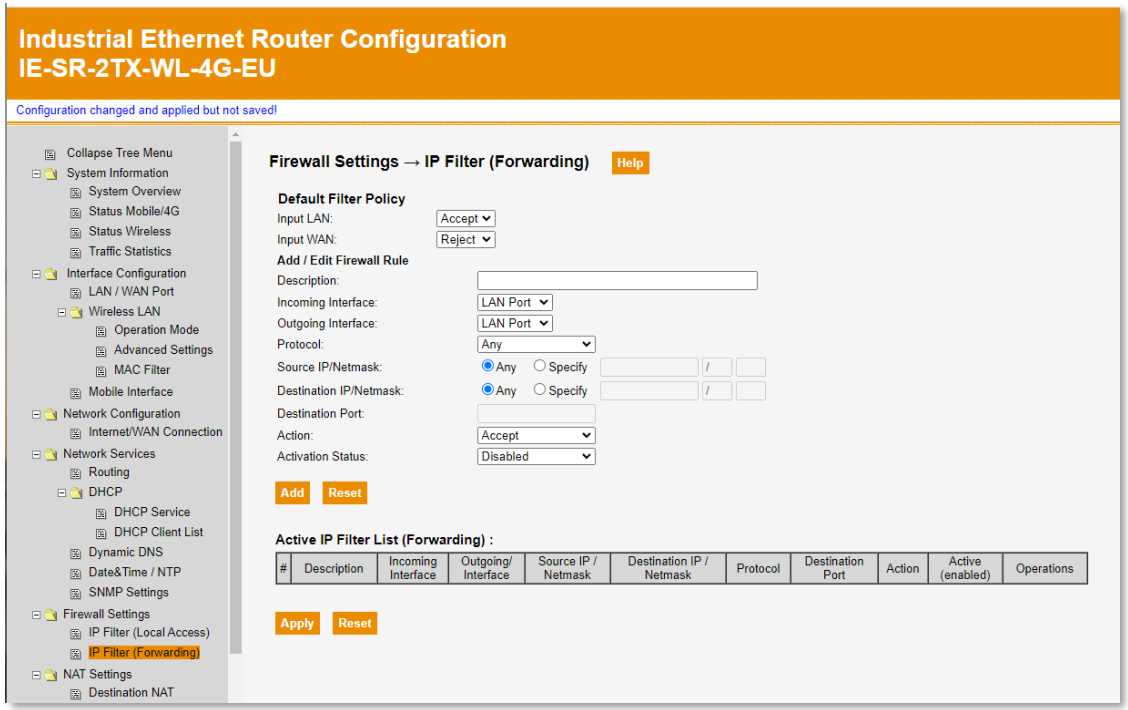
Web page **IP Filter (Forwarding)** is used to define filter rules for control of IP packets passing the Router incoming at any interface and outgoing at any other interface. This IP filter is assigned to the 'forward chain' of the iptables firewall.

Each incoming IP packet with a destination IP that can be routed is checked according to the criteria defined in the rules and - depending on the result - either discarded (Rejected or dropped) or forwarded (Accepted) to the destination address.

Default Filter Policy (LAN and WAN input):
These parameters define the default handling of packets incoming at LAN respective WAN port and trying to pass the Router outgoing to any interface. It will be applied for packets not matching any rule of the 'Forwarding IP Filter List'.

Section 'Add / Edit Firewall Rule':
Creation / Adaption of specific firewall rules for incoming packets targeted to external (routable) IP addresses.

Table 'Active IP Filter List (Forwarding) ':
This table contains all configured rules, either being enabled (active) or disabled. Active rules will be checked from top to bottom. If a rule matches, the defined action (Accept, Reject, Drop) will be done, and the rule check will be canceled immediately. If no rule matches, the default filter policy will be applied.



Picture 34: Default settings of IP Filter (Forwarding).

4.19 NAT Settings → Destination NAT

Web page **Destination NAT (Forwarding)** is used to define rules for redirecting (forwarding) incoming IP packets to another destination according to the rules 'Destination IP address'. **D**estination **N**etwork **A**ddress **T**ranslation typically will be applied for data communication - initiated from the WAN side - to access hidden (private) devices located in the LAN network by a virtual public IP.

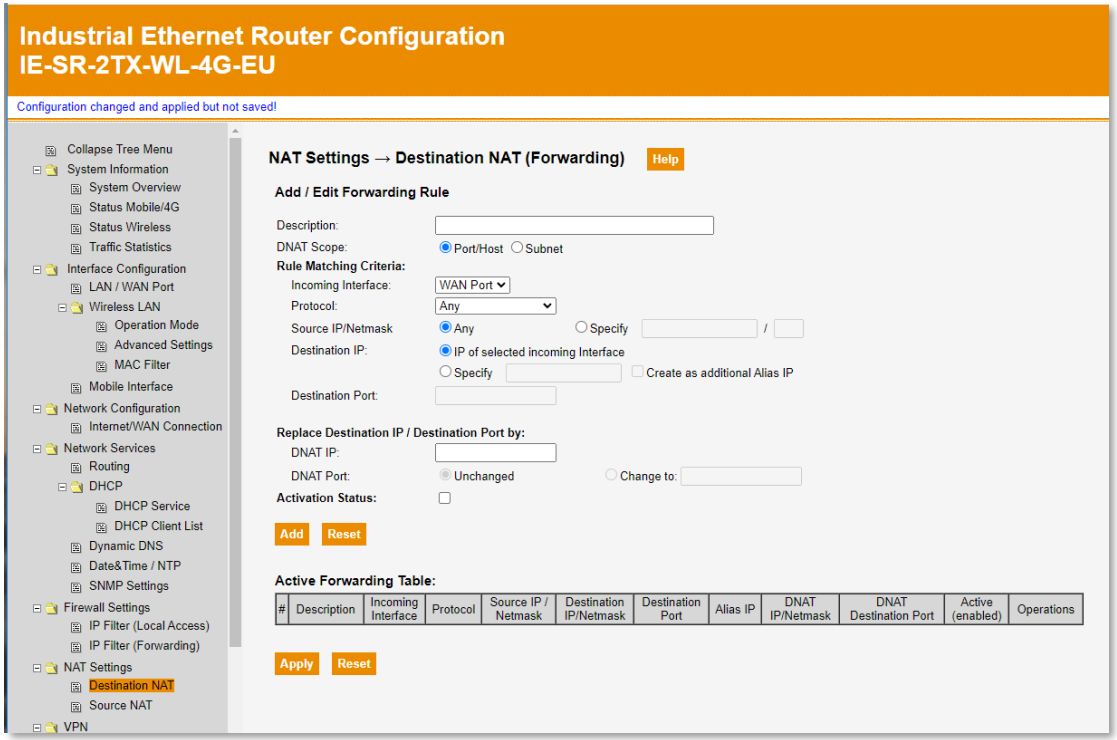
A DNAT rule replaces the original target data of an incoming IP packet (Destination IP and Destination Port) by a new IP address / Port of the rule that it can be forwarded to the device having the replaced IP address.

The Router supports following DNAT (Forwarding) features:

- Protocol / Port Forwarding (DNAT)
  - IP packets - addressed and incoming to the Router's interface (typically WAN port) will be forwarded to a LAN device dependent on the packets protocol and destination port.

- Host Forwarding (DNAT)
  - IP packets – incoming at a Router interface and matching the defined 'Rule Matching Criteria' will be forwarded (re-directed) to the device having the IP address as specified in 'DNAP IP' and possibly 'DNAT Port'. The main difference to Protocol/Port Forwarding is that at the incoming interface additional IP addresses can be defined inside of a rule that they can be targeted from other devices. Based on such rule the Router accepts IP packets addressed to those 'virtual' IPs and re-directs them according to the rule.

- Subnet Forwarding (NETMAP)
  - Similar as single 'Host Forwarding' but applies to an IP range (Subnet). IP packets - incoming at a Router interface and matching the subnet-based 'Rule Matching Criteria' - will be forwarded to devices having an IP address out of the range of the specified target DNAP IP subnet. 'Subnet Forwarding' only changes the destination IP for redirection of a packet, the used protocol and destination port always remain untouched.



Picture 35: Destination NAT configuration window (default settings).

Active Forwarding Table
This table contains the defined DNAT rules. Active rules will be checked from top to bottom. If a rule matches, the defined destination IP / Port replacement will be done, and the rule check will be canceled immediately. If no rule criterion applies, the IP packet remains untouched.

Note: DNAT rules will be applied (as first action) immediately on arrival at the incoming interface. Firewall rules defined in IP Filter (Local Access) and IP Filter (Forwarding) will be applied after processing DNAT.

Application hint:
For more detailed information how to use DNAT and SNAT features please refer to appendix A1 (Network Address Translation: Use cases and how to configure Source NAT and Destination NAT).

4.20 NAT Settings → Source NAT

Web page **Source NAT** is used to define rules for replacing the source IP of IP packets when exit an interface. Via **S**ource **N**etwork **A**ddress **T**ranslation local IP addresses (LAN) can be hidden when communicating with upper-level WAN network or Internet devices.

SNAT can be helpful to integrate series machine networks, each connected to a Router's LAN port and having the same IP address range, into an upper-level production network. By mapping the source IPs of each LAN subnet to unique virtual IPs, all members of all machine networks can communicate to each other due to having unique 'public' IP addresses.

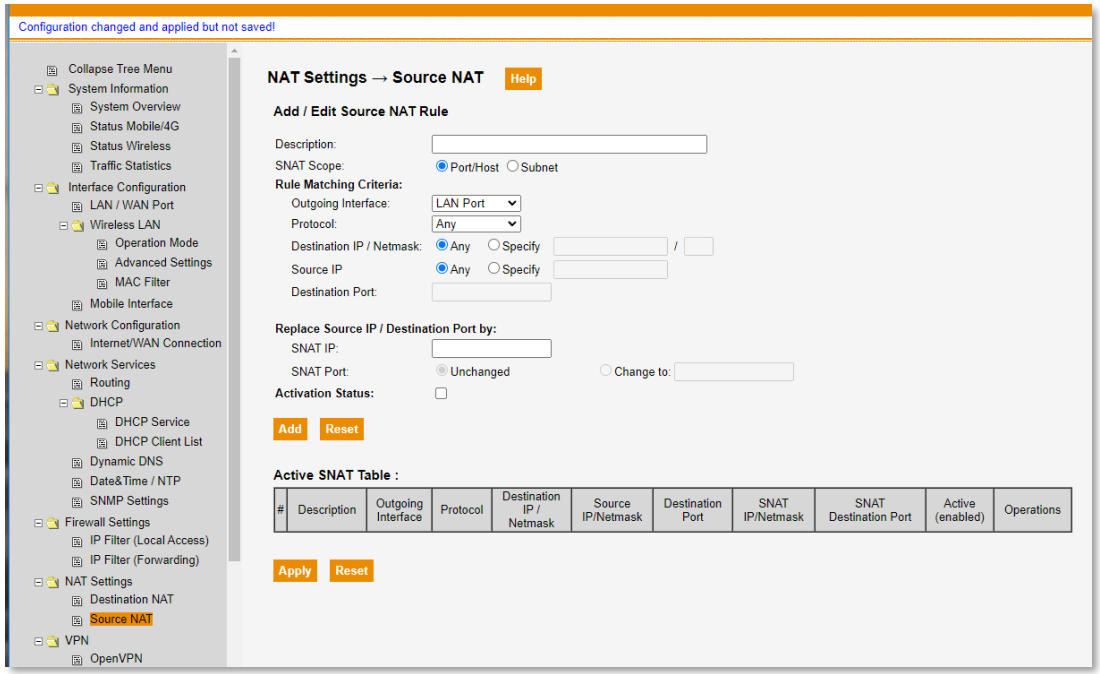
A well known SNAT rule is 'Masquerading (NAT)' which replaces the source IP of any outgoing IP packet by the outgoing interface IP hiding the original sender. It can be enabled/disabled when configuring the interface settings (checkbox 'Masquerade (NAT)' in menu 'Interface Configuration → LAN/WAN Port').

Consider: If 'Masquerading (NAT)' is active but the outgoing IP packet also matches any defined SNAT rule then only the defined rule will be applied. The setting of Masquerade (NAT) will be ignored.

Add / Edit a Source NAT rule
This section is used to create / adapt specific SNAT rules for outgoing packets with definition of filter criteria, on which packets the rules shall be applied and how the IP source data shall be changed. In case of matching the rule criteria the 'Source IP' and possibly the 'Destination Port' of the passing packet will be replaced with the specified data (SNAT IP / Port for a host respectively SNAT IP/ Netmask for a subnet).

Active SNAT Table
This table contains the defined Source NAT rules. Active rules will be checked from top to bottom. If a rule matches, the original source IP data will be replaced by the specified SNAT IP, and the rule check will be canceled immediately. The IP packet remains untouched if no rule criterion applies.

Note: SNAT rules will be applied (as last action) immediately before the IP packet exits an interface. Firewall rules defined in IP Filter (Local Access) and IP Filter (Forwarding) applies before processing SNAT.



Picture 36: Source NAT configuration window (default settings).

Hint about configuration of a '1:1 NAT' application (hiding LAN IP addresses completely with virtual 'public' IP):
1:1 NAT means that IP addresses of a local (LAN) network will be substituted (hidden) by virtual IP addresses that only these addresses will be used for bidirectional communication with (public) WAN devices and it doesn't matter who starts the TCP/IP communication. Effectively '1:1 NAT' is a combination of one SNAT and one DNAT rule. The SNAT rule replaces the (real) source IP by the virtual IP when the packet exits the Router interface, the DNAT rule forwards an incoming packet addressed to the virtual IP to the LAN device with real IP. But only one will be applied at time dependent who initiates the TCP/IP communication (from LAN or WAN side). After establishing a new TCP connection either via a SNAT rule for outgoing from a LAN device or via DNAT incoming from the WAN side a bidirectional communication via the TCP connection always can be done due to stateful firewall behavior.

Notes: If a TCP/IP communication always and only will be initiated by private LAN device – for example requesting any data from WAN sided device(s) - then only the SNAT rule needs to be configured to appear with virtual (public) IP addresses at WAN side. If the TCP connection has been established a bidirectional communication via the TCP socket is possible due to stateful firewall behavior. In this case there is no need to configure any related DNAT rule.
If a TCP/IP communication also needs to be initiated by a public WAN device addressing the virtual IP of the LAN device, then the appropriate DNAT rule must be configured additionally .

Application hint:
For more detailed information how to use DNAT and SNAT features please refer to appendix A1 (Network Address Translation: Use cases and how to configure Source NAT and Destination NAT).

4.21 VPN → OpenVPN

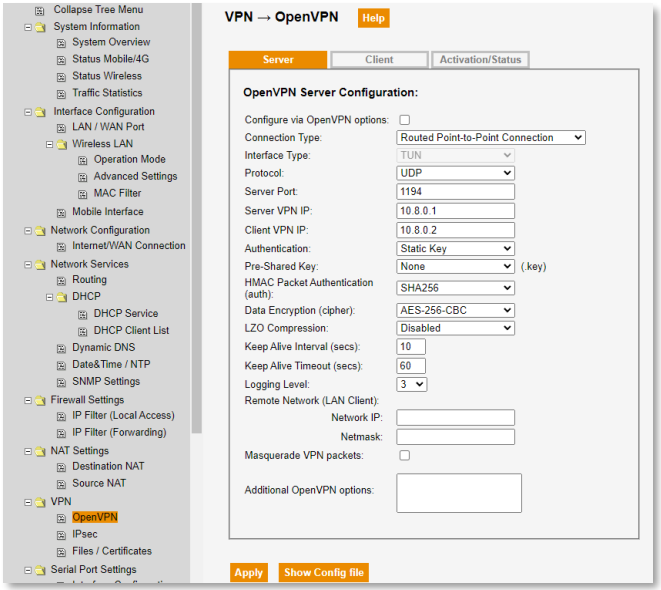
The Router supports an OpenVPN connection configurable either as OpenVPN Client or OpenVPN Server. At a time only one OpenVPN instance (either Client or Server) can be enabled for running.

The configuration for both instances can be done either via predefined selection fields or by entering the well-known OpenVPN options directly into a text input mask.

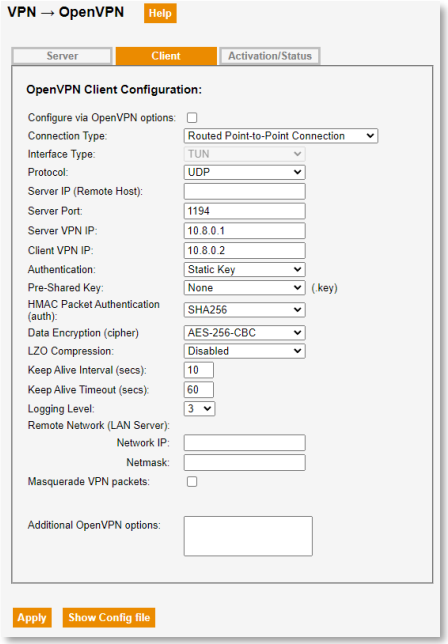
For configuration and operation section 'OpenVPN' is divided into three tabs:

- **Server** Configuration of the OpenVPN Server instance.
- **Client** Configuration of the OpenVPN Client instance.
- **Activation / Status** Activation, Deactivation and Monitoring of a configured OpenVPN instance.

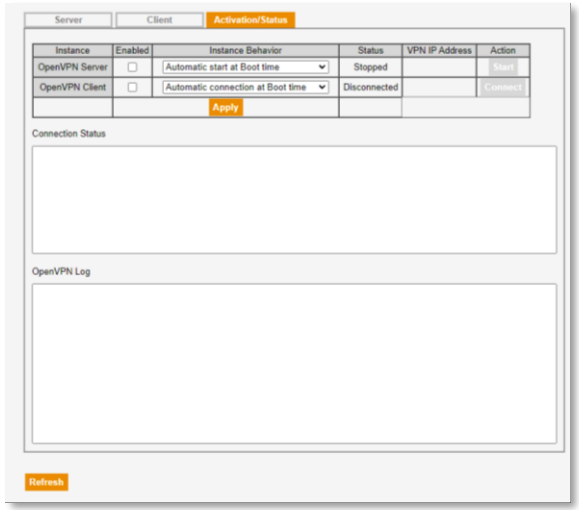
Notes:
- After applying of the configured settings, the resulting OpenVPN options can be checked via button 'Show Config file'".
- Both instances (Server and Client) can be configured and stored but only one of them may be enabled at the same time.



Picture 37: OpenVPN webpage showing **tab 'Server'** (Configuration via predefined OpenVPN parameters).



Picture 38: Web page showing **tab 'Client'** (Configuration via predefined OpenVPN parameters).



Picture 39: Web page showing **tab 'Activation / Status'**.

4.22 VPN → OpenVPN → Tab 'Server'

On tab 'Server' the settings for an OpenVPN server can be configured. If topmost parameter named 'Configure via OpenVPN options' will be enabled, the OpenVPN options can be entered into a text input mask directly. This configuration procedure is same as creating a text based OpenVPN config file containing the published OpenVPN options.

If checkbox 'Configure via OpenVPN options' is disabled, the server configuration can be done by entering data and/or value selection of the predefined fields.

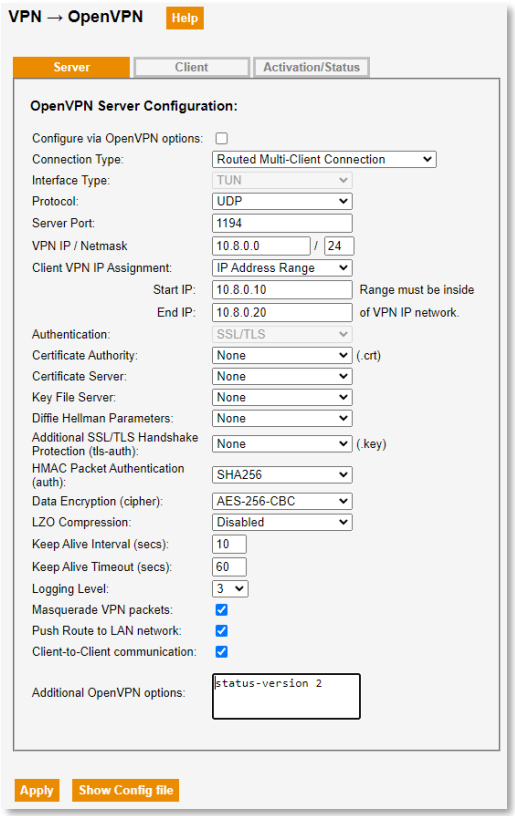
Connection Type
Selection of one of three predefined connection types how an OpenVPN client can connect to the Router (being the OpenVPN server).

- Routed Point-to-Point Connection:
  This connection type is intended to establish a simple peer-to-peer VPN connection between two devices using predefined (but changeable) parameters. In terms of security a static key file or a certificate-based SSL/TLS authentication can be used. This connection type uses default OpenVPN topology 'Net30' also enabling Windows-based OpenVPN clients for peer-to-peer communication.

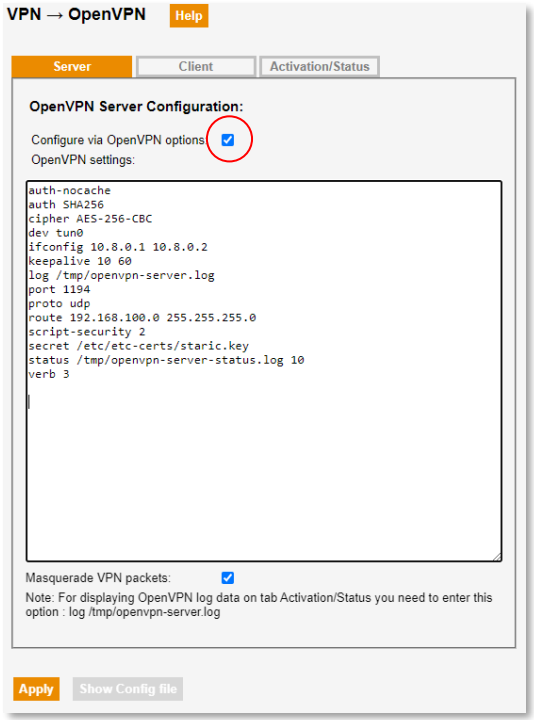
- Routed Multi-Client Connection
  Is intended that multiple OpenVPN clients can connect to the Router (being a OpenVPN Server) having access to Routers LAN network and allowing a client-to-client communication if enabled. In terms of security always certificate-based SSL/TLS authentication needs to be used. This connection type uses OpenVPN topology 'Subnet'.

- Bridged Ethernet Connection
  This mode allows connecting OpenVPN clients becoming a member of the Routers LAN network like being directly connected to the Router LAN port. The bridging mode uses interface type 'TAP' providing a secured Ethernet-based connection at Layer 2. For communication with devices connected at Router LAN port a 'bridged' client must have an IP of the Router LAN subnet. Note, that via a bridged connection also any broadcast traffic will be transferred like in a switching network.

Other listed (predefined) OpenVPN options (for data input or drop-down selection)
When selecting a 'Connection Type' some values of the parameter list (options) will be set automatically. Most of these settings are intended to be a proposal. They can be adapted as needed for the application. Only options 'Interface Type' and 'Authentication' do have a fixed assignment related to the selectable connection types.



Picture 40: OpenVPN webpage showing **tab 'Server'** (Configuration via predefined OpenVPN parameters).



Picture 41: Webpage showing **tab 'Server'** with activated checkbox for configuration via direct input of OpenVPN options.

Notes:
- For selection of necessary certificate files (CA, Server, Key) when doing a configuration via predefined parameters (left picture), the files must be uploaded before selecting via menu VPN → Files / Certificates.
- For referencing of any entered file names when configuring via text-based input mask (right picture) those files needs to be uploaded via menu VPN → Files / Certificates either in **/etc/certs-keys** or directory **/etc/files** before applying.
- After applying of the configured settings, the resulting OpenVPN options can be checked via button 'Show Config file'".

4.23 VPN → OpenVPN → Tab 'Client'

This tab is used to configure OpenVPN client settings. If topmost parameter named 'Configure via OpenVPN options' will be enabled, the OpenVPN options can be entered into a text input mask directly. This configuration procedure is same as creating a text based OpenVPN config file containing the published OpenVPN options.

If checkbox 'Configure via OpenVPN options' is disabled, the client configuration can be done by entering data and/or value selection of the predefined fields.

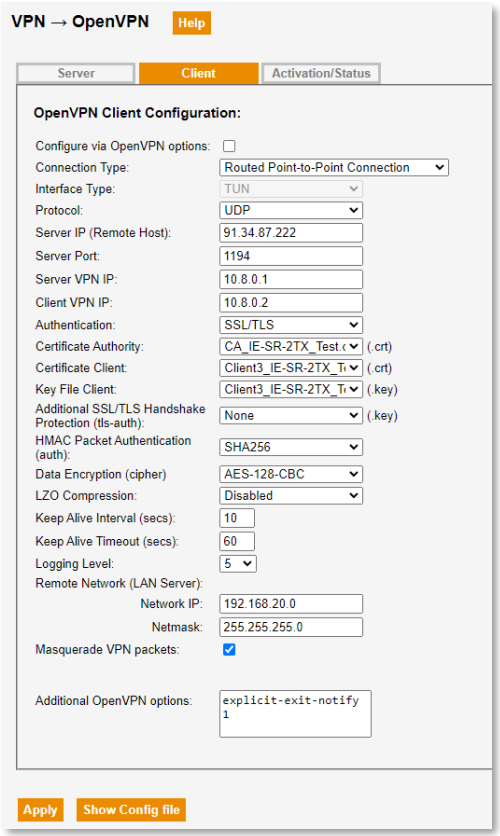
Connection Type
Selection of one of three predefined connection types how the Router - being an OpenVPN client - can connect to a remote OpenVPN server.

- Routed Point-to-Point Connection:
  This connection type is intended to establish a simple peer-to-peer VPN connection between two devices using predefined (but changeable) parameters. In terms of security a static key file or a certificate-based SSL/TLS authentication can be used. This connection type uses default OpenVPN topology 'Net30' also suitable for a peer-to-peer connection to a Windows-based OpenVPN server.

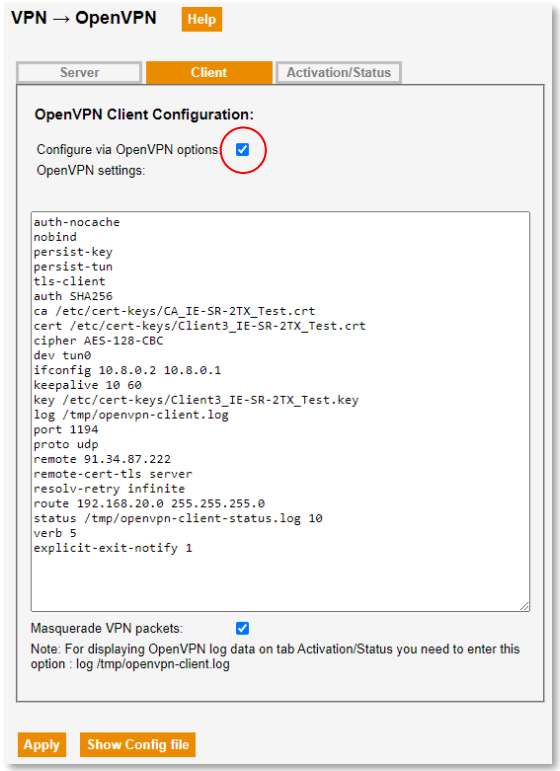
- Routed Multi-Client Connection
  This connection type is intended that the Router (OpenVPN client) may connect to a remote OpenVPN server (multi-clients) getting access to remote networks and allowing a client-to-client communication if enabled by the server. In terms of security always certificate-based SSL/TLS authentication needs to be used. This connection type uses OpenVPN topology 'Subnet'.

- Bridged Ethernet Connection
  Allows a site-to-site connection between local networks of OpenVPN Server and Client using an IP layer-2 based Ethernet bridge (TAP). Both networks behave like being in the same subnet connected via an Ethernet switch. For a bridged connection, any broadcast traffic will be transferred like in a switched network.

Other listed (predefined) OpenVPN options (for data input or drop-down selection)
When selecting a 'Connection Type' some values of the parameter list (options) will be set automatically. Most of these settings are intended to be a proposal. They can be adapted as needed for the application. Only options 'Interface Type' and 'Authentication' do have a fixed assignment related to the selectable connection types.



Picture 42: OpenVPN webpage showing **tab 'Client'** for configuration via predefined OpenVPN parameters.



Picture 43: Webpage showing **tab 'Client'** with activated checkbox for configuration via direct input of OpenVPN options.

Notes:
- For selection of necessary certificate files (CA, Client, Key) when doing a configuration via predefined parameters (left picture), the files must be uploaded before selecting via menu VPN → Files / Certificates.
- For referencing of any entered file names when configuring via text-based input mask (right picture) those files needs to be uploaded via menu VPN → Files / Certificates either in **/etc/certs-keys** or directory **/etc/files** before applying.
- After applying of the configured settings, the resulting OpenVPN options can be checked via button 'Show Config file'".

4.24 VPN → OpenVPN → Tab 'Activation / Status'

This tab is used for control and monitoring of a configured OpenVPN instance. Either function OpenVPN Server or OpenVPN Client can be enabled and run at the same time and allowing to set the instance-related behavior and action.

Additionally, this page provides information about the connection status and the OpenVPN log..

How to run a configured OpenVPN Client instance:

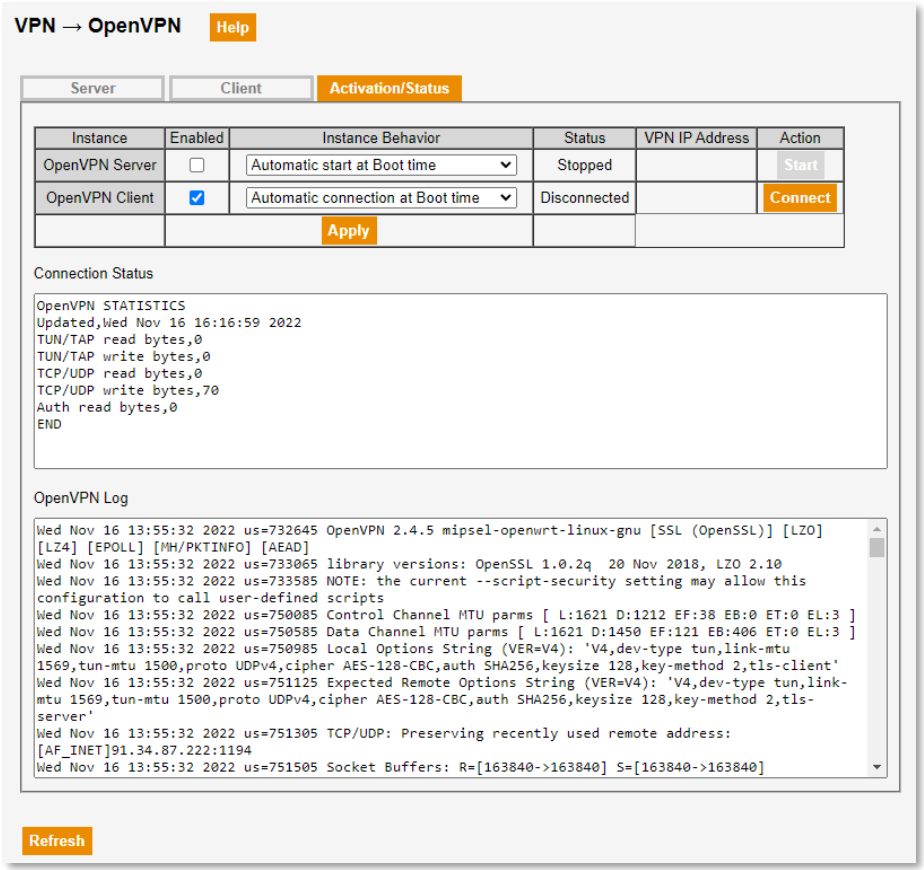
1. Activate checkbox 'Enabled' for OpenVPN client.
2. Select the desired client instance behavior
   - Automatic connection at Boot time ⇨ Tries to establish a connection after power-up or reboot
   - Connect/Disconnect triggered by DI ⇨ Initiates or cancels a connection to an OpenVPN server controlled by digital input.
   - Connect/Disconnect by Action button ⇨ Manual connection/disconnection of the VPN tunnel.
3. Click button 'Apply' to activate the OpenVPN client instance.
4. Click button 'Connect' to establish a VPN tunnel with OpenVPN server.
5. Wait some seconds, then check parameters 'Status' and 'VPN IP Address' if the connection could be established.
6. Click button 'Refresh' to show updated information.

How to run a configured OpenVPN Server instance:

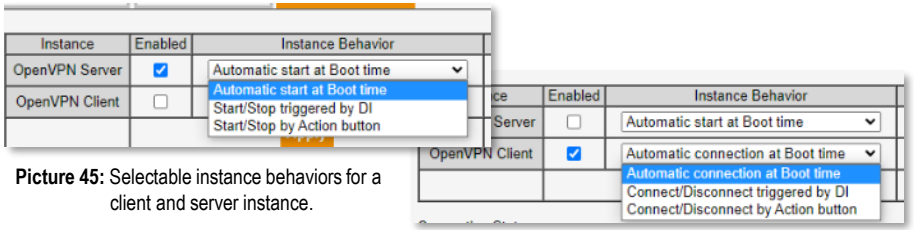
1. Activate checkbox 'Enabled' for OpenVPN server.
2. Select the desired server instance behavior
   - Automatic start at Boot time ⇨ Starts OpenVPN server after power-up or reboot if configured and enabled.
   - Start / Stop triggered by DI ⇨ Starts/Stops OpenVPN server controlled by digital input if configured and enabled.
   - Start/Stop by Action button ⇨ Start/Stop OpenVPN server instance manually.
3. Click button Apply to activate the OpenVPN server instance.
4. For functional check click button Start to run the OpenVPN server process.
5. Wait some seconds, then check parameters 'Status' and 'VPN IP Address' if the server is running.
6. Click button 'Refresh' to show updated information.

Notes:

- A defined instance behavior only works if the client or server instance is configured and enabled.
- Both windows 'Connection Status' and 'OpenVPN Log' provide information about OpenVPN instance status. If no status and log data is displayed, which can happen if the OpenVPN instance cannot be started due to a severe misconfiguration. In this case, please check 'System Log' for any OpenVPN related message.



Picture 44: Example of tab 'Activation/Status' for a configured and activated (here disconnected) OpenVPN client.

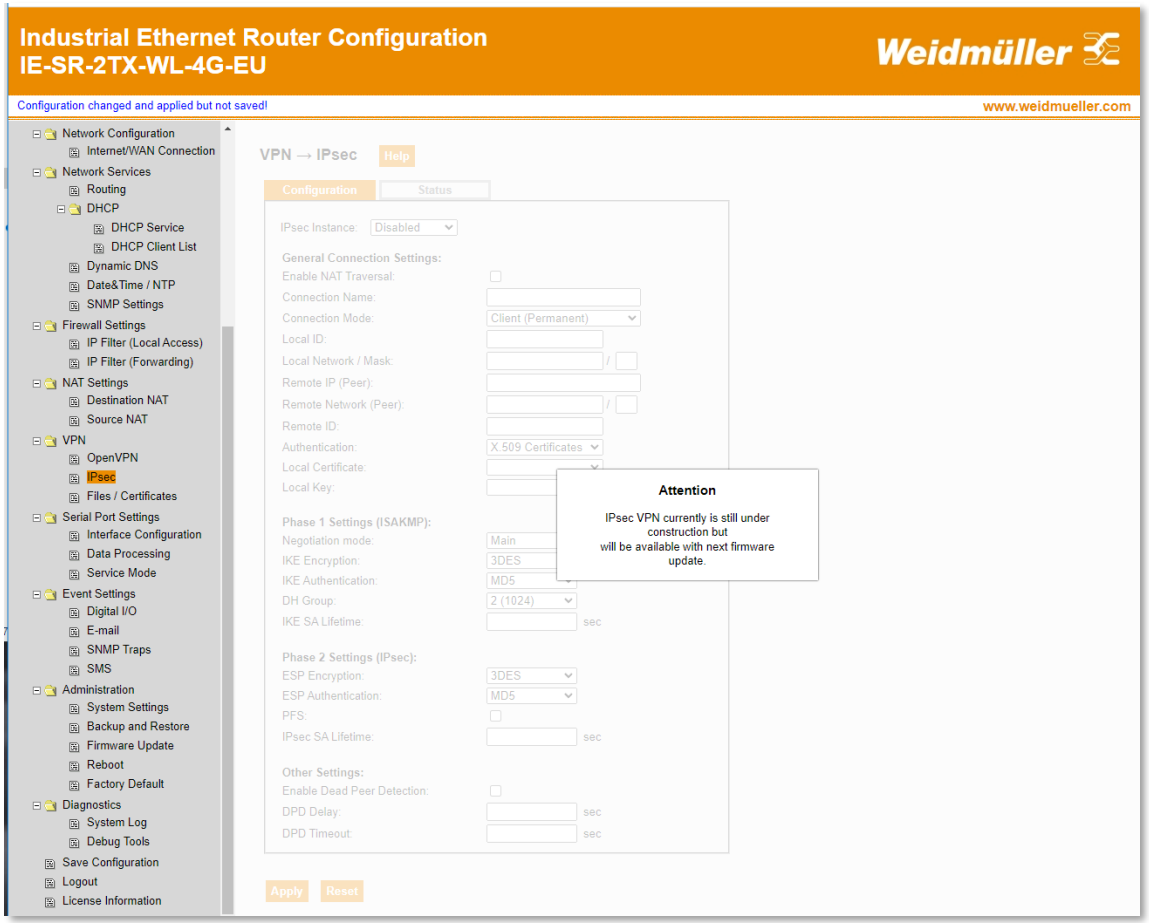


Picture 45: Selectable instance behaviors for a client and server instance.

4.25 VPN → IPSec

Attention: Firmware versions <= V1.32 do not support IPsec.

Implementation of IPsec is under construction and will be provided with next firmware upgrade!



Picture 46: Information windows that IPsec currently is still under construction.

4.26 VPN → Files / Certificates

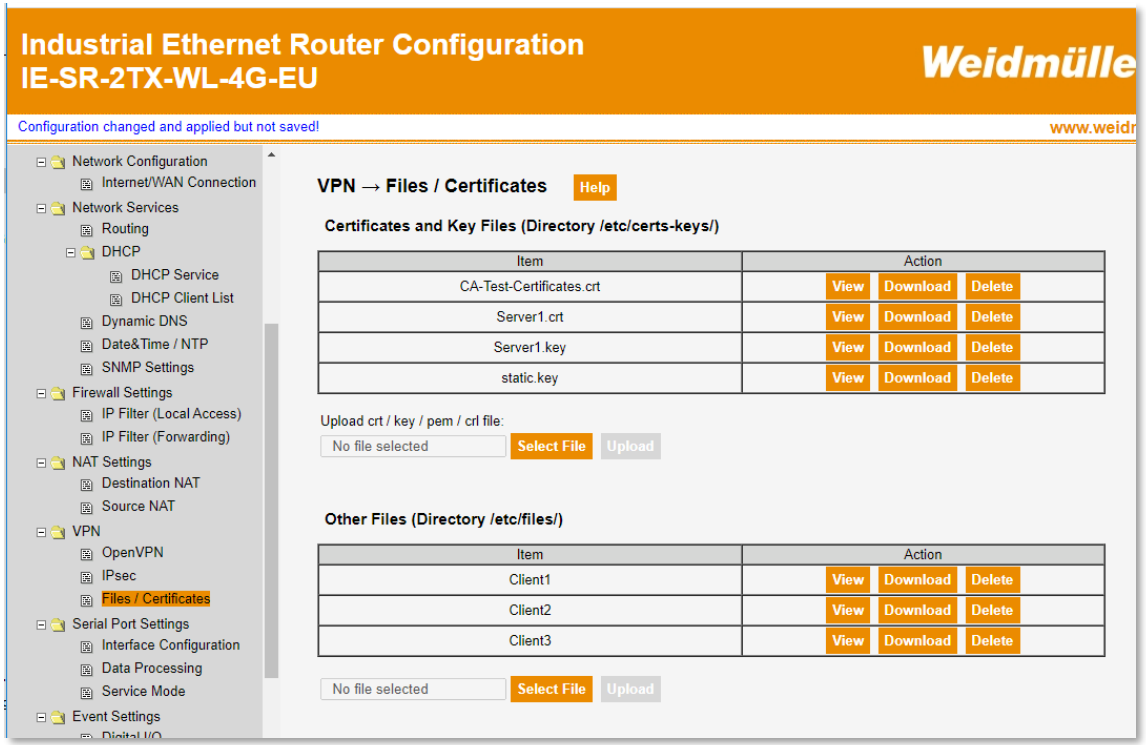
This webpage allows the management of file data primarily used for VPN applications.

Section 'Certificates and Key Files (Directory /etc/certs-keys)'

Via this section certificate and key files can be uploaded to be used for OpenVPN and IPsec applications. Each file which is uploaded to this directory (/etc/certs-keys), can be selected when configuring any file-related OpenVPN or IPsec parameter providing a drop-down selection.

Section 'Other Files (Directory /etc/files)'

This directory can be helpful to upload files to be used for individual OpenVPN applications which are configured by the text-based input (same as for an OpenVPN config file) and having any file references. For example, this file directory can be used as CCD directory containing the client specific files if the Router is running as OpenVPN server with 'client-config-dir' option (client-config-dir /etc/files).



Picture 47: Example screenshot, showing uploaded certificate and key files in the upper section. Lower section 'Other Files' contains VPN client configuration files to be used if the Router is running as OpenVPN server and refers via option **client-config-dir /etc/files** to files Client1, Client2 and Client3 (being the common names of connecting clients).

4.27 Serial Port Settings → Interface Configuration

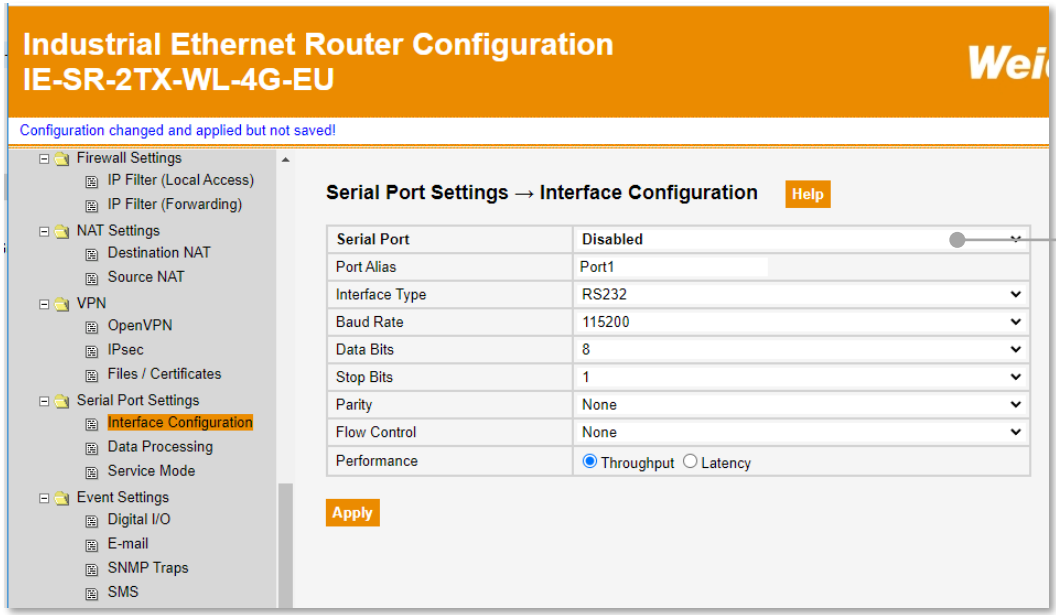
This webpage can be used to define the interface type and the transmission parameters of the serial interface. The interface settings will be applied for running one of the selectable service modes

- Virtual COM Port,
- TCP Server,
- TCP Client or
- UDP Server/Client.

These modes will be configured on webpage 'Serial Port Settings → Service Mode'.

Parameter Settings

Serial Port	Enables or disables the serial interface generally. If disabled (factory default), the serial port cannot be used for any service mode.
Port Alias	Port Alias can be used to describe or identify the connected serial device. Enter any identifying name or device description.
Interface	Choose an interface for the connected serial device. Available interfaces: RS232, RS422, RS485 (2-wires) and RS 485 (4-wires).
Baud Rate	Baud rate is the rate at which data is transferred over a serial link. The baud rate can be selected from the drop-down list which ranges from 110bps to 460800bps.
Data Bits	Choose the number of data bits (5, 6, 7 or 8) to transmit.
Stop Bits	The number of bits used to indicate the end of a byte.
Parity	Selectable values: None, Odd, Even, Mark or Space
Flow Control	Selection of hard-, software-based or deactivated flow control (XON/XOFF, RTS/CTS, DTR/DSR, None)



Picture 48: Interface settings of the serial port (Factory defaults)

Performance

- Latency: Guarantees shortest response time. This option ensures that any received character incoming at Serial Port will be sent immediately to the Ethernet network and the payload of each incoming Ethernet packet will be forwarded immediately to the serial device without any buffering.
- Throughput: Guarantees highest data throughput. This option minimizes the overall Ethernet packet overhead by using a larger payload in Ethernet frames consisting of buffered received serial data.

Consider: Parameter 'Performance' is only valid for service mode 'Virtual COM Port'.

General hint: If the serial interface is not used for the application, it is recommended to disable the port (via parameter 'Serial Port') to release some CPU resources.

4.28 Serial Port Settings → Data Processing (1 / 3)

These settings can be used to control the data processing and buffering behavior for communication between the Ethernet and the serial interface when the Router is configured to run as Serial-to-Ethernet-Converter.

The parameter settings are valid for service (converter) modes

- Virtual COM Port,
- TCP Server
- TCP Client and
- UDP Server/Client

which will be configured in menu 'Serial Port Settings → Service Mode'.

If necessary, the behavior of data processing and buffering can be adapted for Serial-to-Ethernet data transmission using parameters

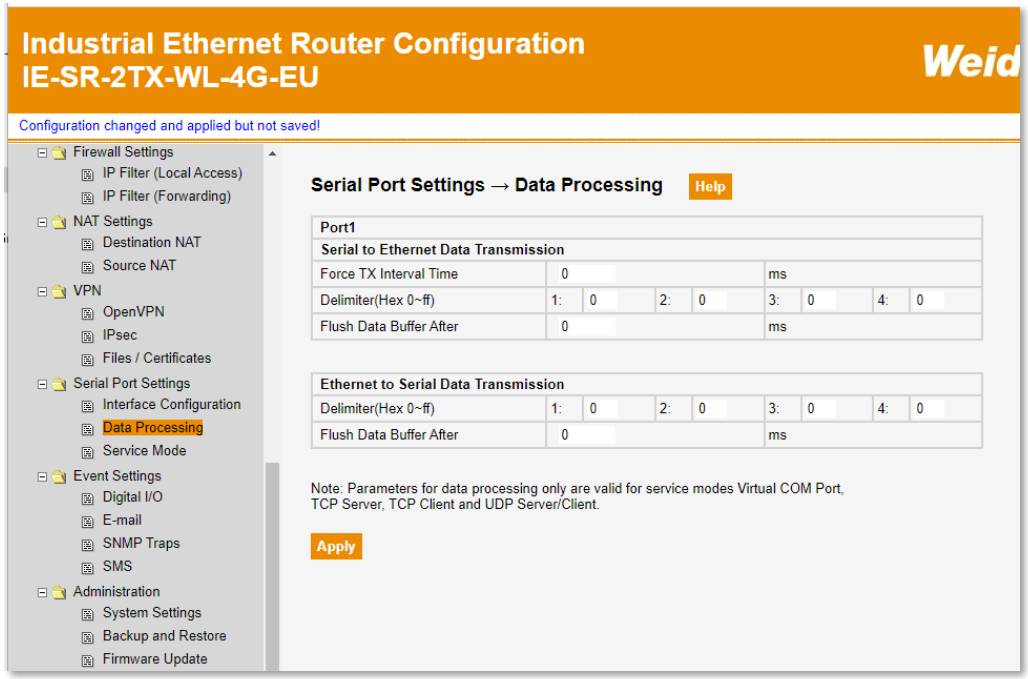
- 'Force TX Interval Time',
- 'Delimiter' characters and
- 'Flush Data Buffer After'.

For Ethernet-to-Serial data transmission only parameters

- 'Delimiter' characters and
- 'Flush Data Buffer After'

can be configured.

Please check next slides for detailed understanding of data flow and buffering and how to set parameters for Serial-to-Ethernet data transmission and vice versa.



Picture 49: Factory default settings of 'Data Processing' parameters.

4.28 Serial Port Settings → Data Processing → Behavior of Serial-to-Ethernet interface data flow (2 / 3)

Generally, the overall data flow from receiving data at serial interface (Port 1) and sending out to the Ethernet interface depends on parameters
- Delimiter (Byte value) [1]
- S2E Flush Data Buffer After (Timer) [2 *refer to picture*]
- Force TX Interval Time (Timer) [3]

which control the behavior of Serial-to-Ethernet-Input-Buffer [1 2] and Transmit-to-Ethernet-Output-Buffer [3].

Behavior of Serial-to-Ethernet-Input-Buffer:
If Delimiter byte(s) are set to 00 then input buffering always is disabled independent of setting of timer parameter "S2E Flush Data Buffer After". In this case each incoming byte from serial port will be forwarded immediately to the Transmit Buffer.

Note: If Delimiter(s) shall be applied then always use first Delimiter 1 (being not 00) followed by Delimiter 2, 3 or 4 if necessary.

If Delimiter byte(s) do have a value other than 00 AND 'S2E Flush Data Buffer After' is set to 0 (ms), then incoming bytes will be buffered as long as no Delimiter(s) will be received and match. If the delimiter condition match or if the buffer is full (4 kBytes) then data of input buffer will be forwarded to Transmit Buffer.

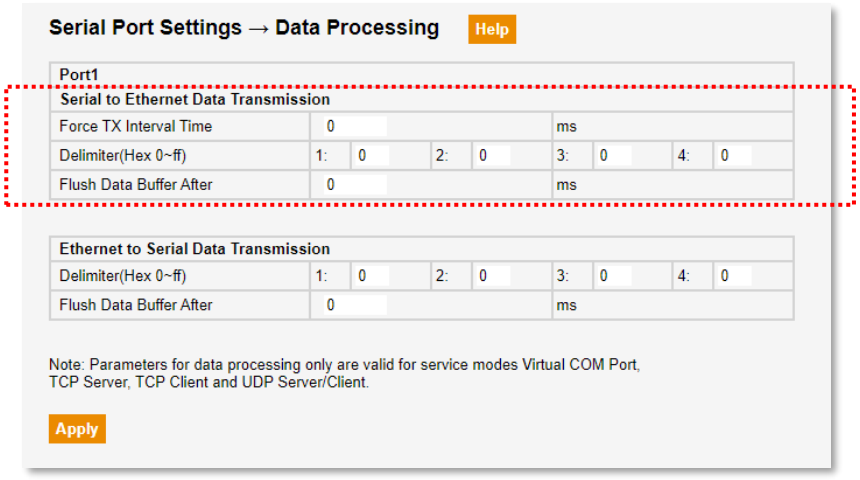
If Delimiter byte(s) do have a value other than 00 AND "S2E Flush Data Buffer After" is set > 0 (ms) then incoming bytes will be buffered as long
- delimiter settings do not match or
- elapsed time since first received byte < defined "S2E Flush Data Buffer After" time.

If one of the conditions triggers, then the buffer content will be forwarded to transmit buffer immediately.

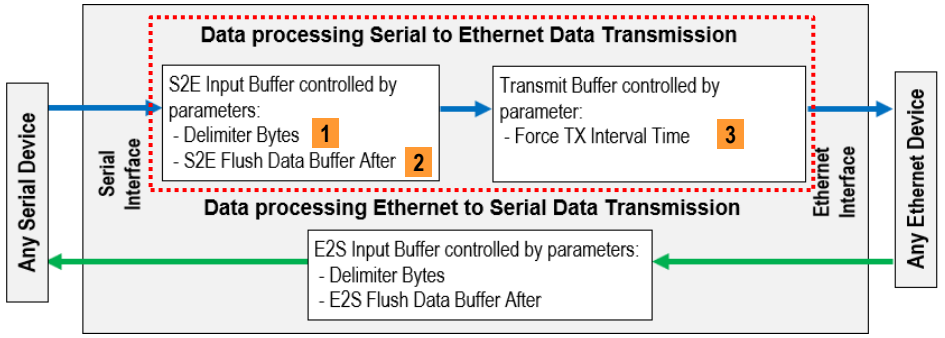
Note: Timer parameter ‚S2E Flush Data Buffer After' only can be used in combination with delimiter settings. If Delimiter byte(s) are set to 00 (disabled) then ‚S2E Flush Data Buffer After' does not have any effect. Independent of parameter settings the data always will be forwarded if the buffer is full (4kByte).

Behavior of Transmit Buffer:
If timer parameter ‚Force TX Interval Time' is set to 0, then output buffering is disabled. Each incoming byte or byte block received from S2E Input Buffer will be sent out immediately as an IP packet via Ethernet interface.

If ‚Force TX Interval Time' is set 0, then buffering is enabled. In this case the ComServer periodically sends out each defined 'Force TX Interval Time' the content of the Transmit buffer as IP packet(s) via Ethernet interface.



Picture 50: Parameters to be used for Serial-to-Ethernet data transmission.



Picture 51: Diagram of data processing and buffering for a Serial-to-Ethernet data transmission.

Note: Parameter 'Force TX Interval Time' can be used to increase the payload of an Ethernet frame by gathering more bytes of the serial input stream. But consider a possible impact on timing requirements regarding the serial application behind the Ethernet side . Independent of this parameter the data always will be sent out if the buffer is full (4kByte).

4.28 Serial Port Settings → Data Processing → Behavior of Serial-to-Ethernet interface data flow (3 / 3)

General the overall data flow from receiving the payload of an Ethernet frame and sending out at serial interface (Port 1) depends on parameters
- Delimiter (Byte value) [1 *refer to picture*]
- S2E Flush Data Buffer After (Timer) [2]

which control the behavior of Ethernet-to-Serial-Input-Buffer.

Behavior of Ethernet-to-Serial-Input-Buffer:
If Delimiter byte(s) are set to 00 then input buffering always is disabled independent of setting of timer parameter 'E2S Flush Data Buffer After'. In this case the payload of each incoming IP packet immediately will be send to the serial interface.

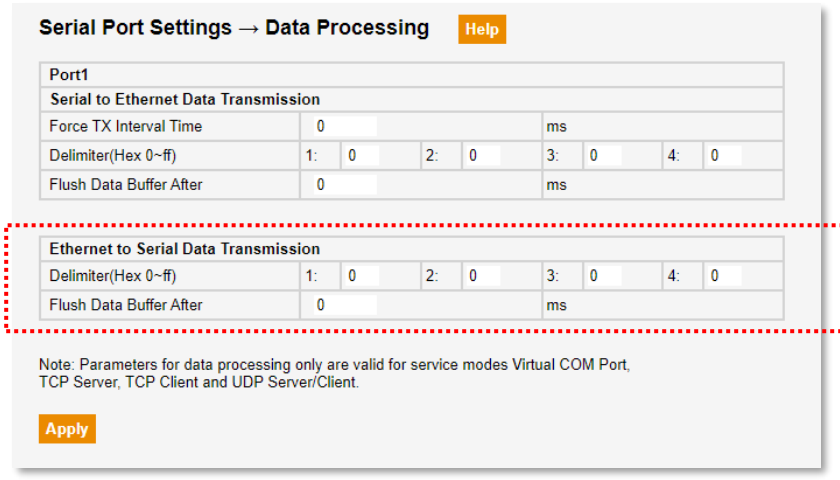
Note: If Delimiter(s) shall be applied then always use first Delimiter 1 (being not 00) followed by Delimiter 2, 3 or 4 if necessary.

If Delimiter byte(s) do have a value other than 00 AND 'E2S Flush Data Buffer After' is set to 0 (ms), then the payload of incoming IP packet(s) will be buffered as long as no delimiter byte(s) will be received and match. If the delimiter condition match or if the buffer is full (4 kBytes), then buffer data will be sent out at serial interface.

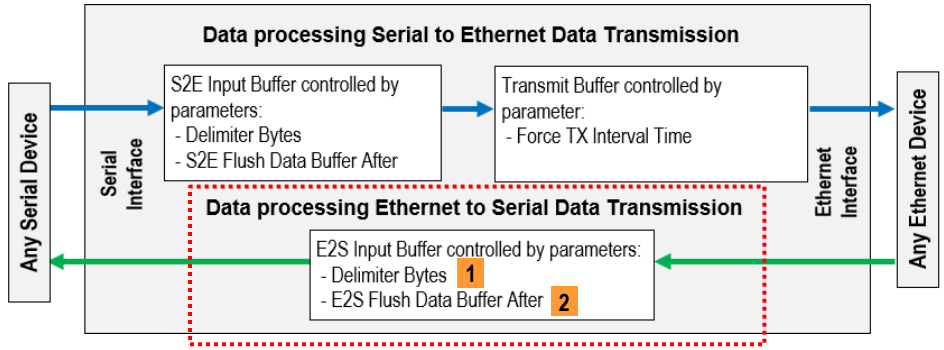
If Delimiter byte(s) do have a value other than 00 AND 'E2S Flush Data Buffer After' is set > 0 (ms), then the payload of incoming IP packet(s) will be buffered as long
- the delimiter settings do not match or
- the elapsed time since first received byte/payload has not reached defined 'E2S Flush Data Buffer After' time.

If one of the conditions triggers, then the buffer content will be sent out at the serial interface immediately.

Note: Parameter ‚E2S Flush Data Buffer After' only can be used in combination with delimiter settings. If Delimiter byte(s) are set to 00 (disabled) then 'E2S Flush Data Buffer After' does not have any effect. Independent of parameter settings the data always will be sent out if the buffer is full (4kByte).



Picture 52: Parameters to be used for Ethernet-to-Serial data transmission.



Picture 53: Diagram of data processing and buffering for a Ethernet-to-Serial data transmission.

4.29 Serial Port Settings → Overview Service Modes

This web page can be used to select the service (converter) mode for Serial-to-Ethernet respectively Ethernet-to-Serial data transmission.

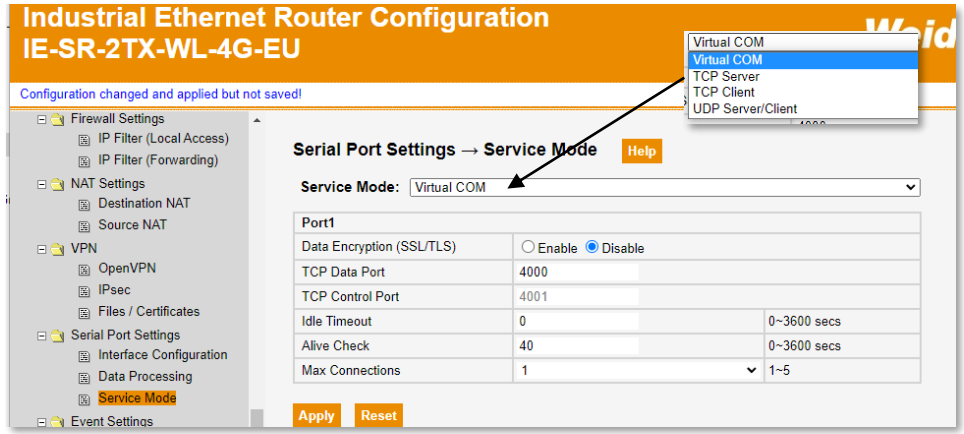
Currently the Router supports service modes

- Virtual COM Port,
- TCP Server,
- TCP Client and
- UDP Server/Client.

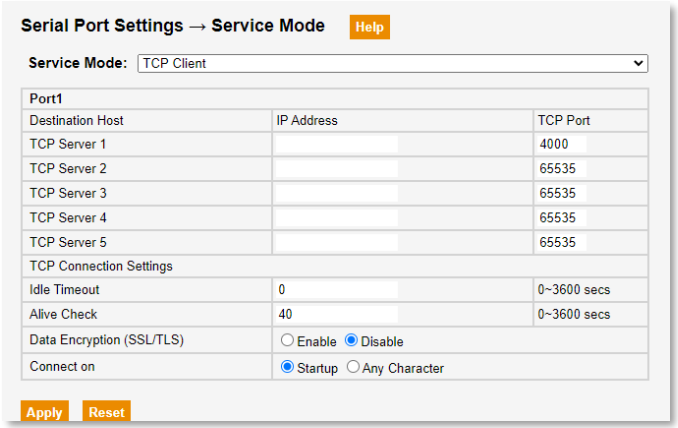
Notes:

- To run one of these service modes the serial port generally needs to be enabled on webpage 'Serial Settings →Interface Configuration → Parameter 'Serial Port'.

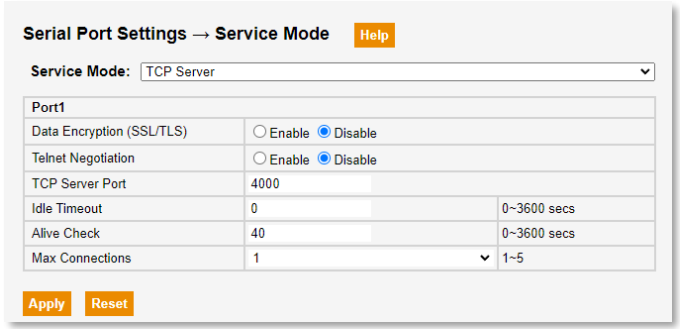
- If the serial port is not used for the application, it is recommended to set parameter 'Serial Port' to 'disabled' to release some CPU resources.



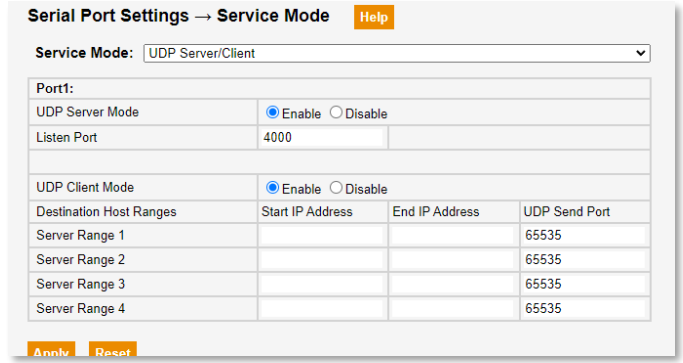
Picture 54: Service mode 'Virtual Com Port' (Factory Default)



Picture 55: Service mode 'TCP Client'



Picture 56: Service mode 'TCP Server'

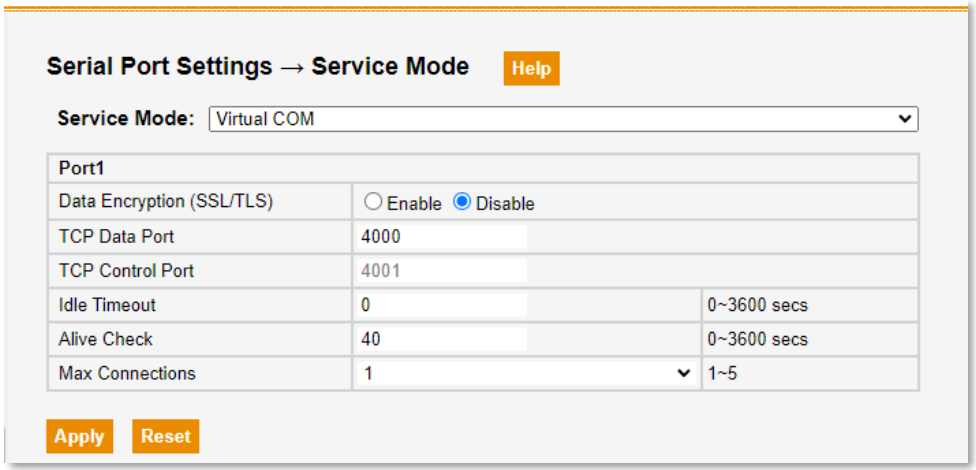


Picture 57: Service mode 'UDP Server/Client'

4.30 Serial Port Settings → Service Mode: Virtual COM Port

By using this service mode, a PC-based application - which normally communicates to a connected serial device via a physical COM port - alternatively can communicate with a (remote) serial device by using an Ethernet based communication via the Serial/Ethernet converter function of the Router.
To use this function a specific Virtual COM Port Driver (Weidmueller CS-MBGW Utility) has to be installed and configured on the PC, emulating a virtual COM port that can be selected by a software application like a physical COM port. Resulting the PC's Virtual COM Port Driver establishes a TCP/IP connection to the Routers Ethernet port. Receiving TCP/IP data will be converted to serial data and vice versa.
Mode Virtual COM Port supports up to 5 simultaneous TCP/IP connections, so that multiple hosts (each having installed a Virtual COM Port Driver) can exchange data with the same serial device at the same time.

Description of parameter settings:	
Data Encryption	Disables or enables an SSL/TLS encrypted TCP/IP communication between PC's Virtual COM Port driver and the Router.
TCP Data Port	Port number on which the Router exchanges the connection payload.
TCP Control Port	Port number on which the Router is listening for communication establishment and exchange of control data.
Idle Timeout	Disconnects established TCP/IP connection(s) after defined Idle time (seconds) if there is no further data transmission on the serial interface (due to Inactivity). If Idle Timeout = 0 seconds the Router never will terminate a consisting TCP/IP connection.
Alive Check	The Router sends according to the defined interval time (seconds) periodically TCP alive check packages to the remote host(s) to evaluate the TCP connection. If the TCP connection is no longer alive, the connection will be closed.
Max Connections	Defines the maximum number of simultaneous TCP/IP host connections.



Picture 58: Service mode 'Virtual Com Port' selected.

Note about connection between a Windows PC and the Router using service mode Virtual COM Port:

- For installation of a virtual COM port driver on the Windows PC same software (Weidmueller CS-MBGW Utility, Version 3.4 and later) can be used which primarily is intended for Virtual Com Port communication between a Windows PC and Weidmueller ComServer/Modbus Gateway IE-CS-MBGW-2TX-1COM (Article number 2682600000).
- When creating / mapping a virtual COM Port on the PC the software establishes - based on the configured communication parameters - a TCP connection to the Router.

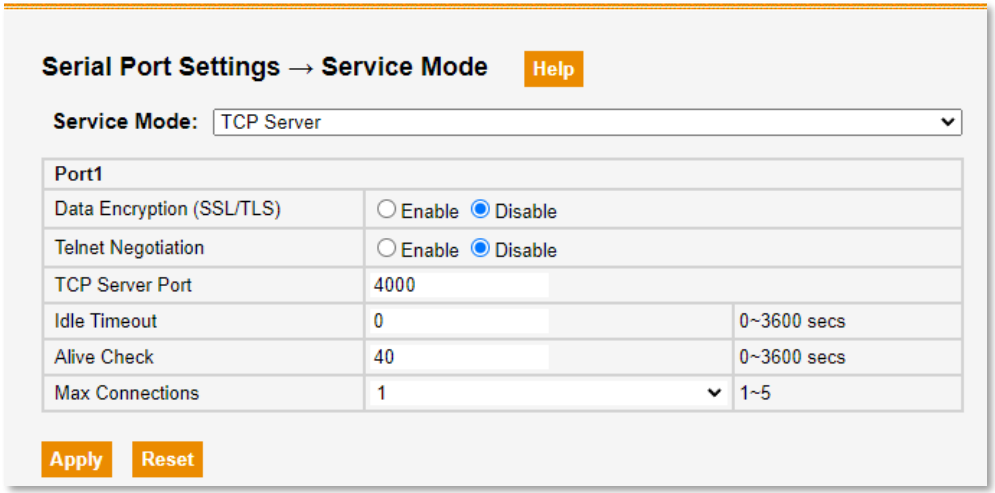
General configuration hint:

- It is not necessary to define an interface explicitly on which the Router is listening for establishing a virtual COM Port connection. The Router is accepting an incoming connection request having the configured TCP Data and Control ports on each interface as long these TCP ports are not blocked by firewall rules.
- For communication with a Virtual COM Port driver running on a remote PC, the configured TCP ports 'Data Port', 'Control Port' and 'Management Port' may not be blocked by any firewall rule.
- The 'Management Port' – used for internal communication with tool 'Weidmueller CS-MBGW Utility' - is set to 600 and cannot be configured via the webpage.

4.31 Serial Port Settings → Service Mode: TCP Server

When running mode 'TCP Server', the Router waits passively for host computer(s) to establish a TCP/IP connection to exchange data with the connected serial device. Any payload of a TCP packet will be converted into a serial data stream and vice versa. Up to 5 simultaneous connections are supported, allowing multiple hosts to exchange data with the serial device.

Description of parameter settings	
Data Encryption	Disables or enables an SSL/TLS encrypted TCP/IP communication between communication between initiating TCP Client and Router (TCP Server).
Telnet Negotiation	Disables or enables the use of Telnet protocol for establishing the TCP connection.
TCP Server Port	Port number on which the Router is listening as TCP Server. The Router is accepting an incoming connection request on each interface as long the TCP port is not blocked by firewall rules.
Idle Timeout	Disconnects existing TCP/IP connection(s) after defined Idle time (seconds) if there is no further data transmission on the serial interface (due to Inactivity). If Idle Timeout = 0 seconds the Router never will terminate a consisting TCP/IP connection.
Alive Check	The Router sends according to the defined interval time (seconds) periodically TCP alive check packages to the remote host(s) to evaluate the TCP connection. If the TCP connection is no longer alive, the connection will be closed.
Max Connections	Defines the maximum number of simultaneous TCP/IP host connections.
Note: The behavior of data processing (Latency, Buffering, etc.) between the Routers Ethernet and serial interface and vice versa can be adapted via parameters 'Force TX Interval Time', 'Delimiter' and 'Flush Data Buffer After' in menu Serial Port Setting → Data Processing.	

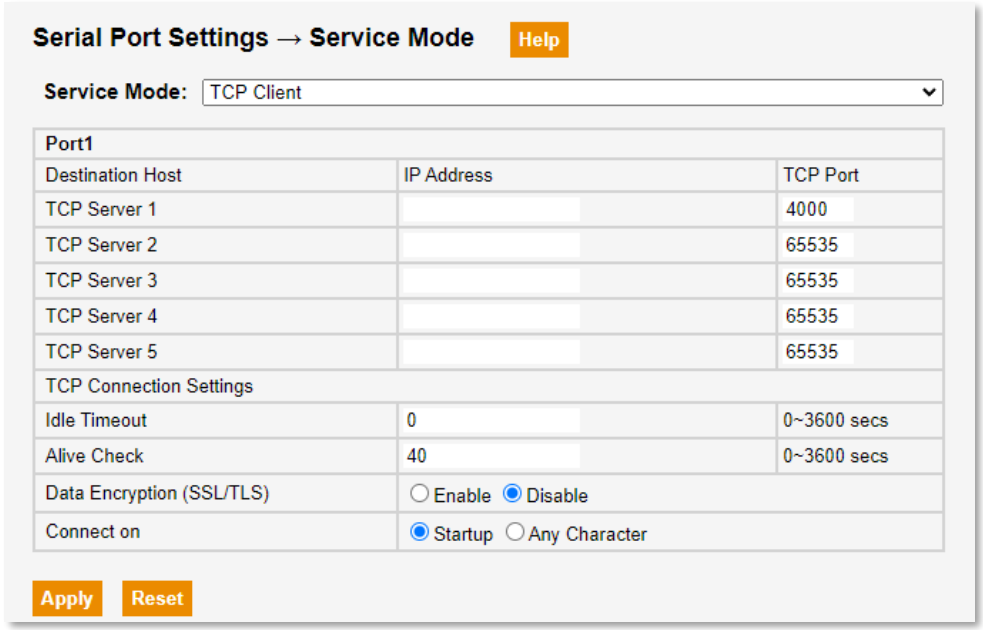


Picture 59: Service mode 'TCP Server' selected.

4.32 Serial Port Settings → Service Mode: TCP Client

In mode 'TCP Client' the Router establishes a TCP/IP connection to specified host(s) (TCP Server) to exchange data with the connected serial device. Any incoming serial data will be converted and sent as payload of a TCP packet to the defined TCP Server(s). Up to 5 simultaneous connections are supported, allowing multiple hosts to exchange data with the serial device.

Description of parameter settings:	
TCP Server 1...5	Definition of up to 5 target TCP Servers (IP address and port number) for data exchange.
Idle Timeout	Disconnects existing TCP/IP connection(s) after defined Idle time (seconds) if there is no further data transmission on the serial interface (due to Inactivity). If Idle Timeout = 0 seconds the COM-Server never will terminate an established TCP/IP connection.
Alive Check	The Router sends according to the defined interval time (seconds) periodically TCP alive check packages to the remote host to evaluate the TCP connection. If the TCP connection is not alive, the connection will be closed.
Data Encryption	Disables or enables an SSL/TLS encrypted TCP/IP communication between the initiating Router (TCP Client) and remote host (TCP Server).
Connect on	Startup: The Router establishes a TCP/IP connection to all defined TCP Server(s) automatically after start-up.
	Any Character: The Router establishes a TCP/IP connection to all defined TCP Server(s) after reception of first byte from serial interface.
Note: The behavior of data processing (Latency, Buffering, etc.) between Ethernet and serial interface and vice versa can be adapted via parameters 'Force TX Interval Time', 'Delimiter' and 'Flush Data Buffer After' in menu Serial Port Setting → Data Processing.	



Picture 60: Service mode 'TCP Client' selected.

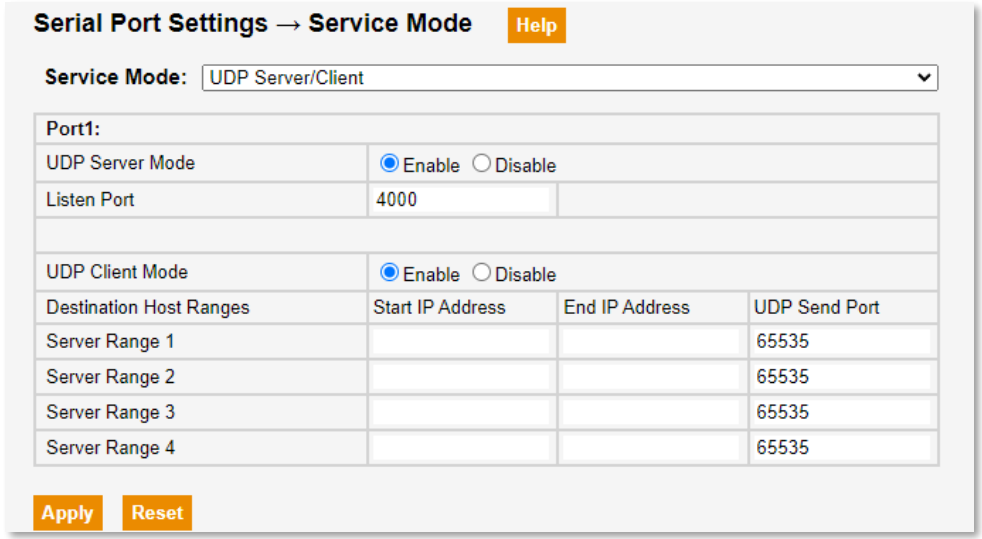
4.33 Serial Port Settings → Service Mode: UDP Server / Client

In mode 'UDP Server/Client' the Router can act as UDP Client and UDP Server simultaneously.

If mode 'UDP Server' is activated, the Router listens to incoming UDP packets at the defined port and forwards the payload to the connected serial device.

If mode 'UDP Client' is activated, any incoming serial data will be sent as payload of an UDP packet(s) to the defined Server range(s).

Description of parameter settings:	
UDP Server related settings	
UDP Server Mode	Enables or disables the UDP Server Mode.
Listen Port	Definition of UDP port on which the UDP Server listens for incoming UDP packets.
UDP Client related settings	
UDP Client Mode	Enables or disables the UDP Client Mode.
Server Ranges 1...4	Definition of up to 4 UDP Server Ranges as target(s) for sending the serial data. Each Server range needs to be defined by - Start IP address, - End IP address and - UDP port number.
Note: The behavior of data processing (Latency, Buffering, etc.) between Ethernet and serial interface and vice versa can be adapted via parameters 'Force TX Interval Time', 'Delimiter' and 'Flush Data Buffer After' in menu Serial Port Setting → Data Processing.	



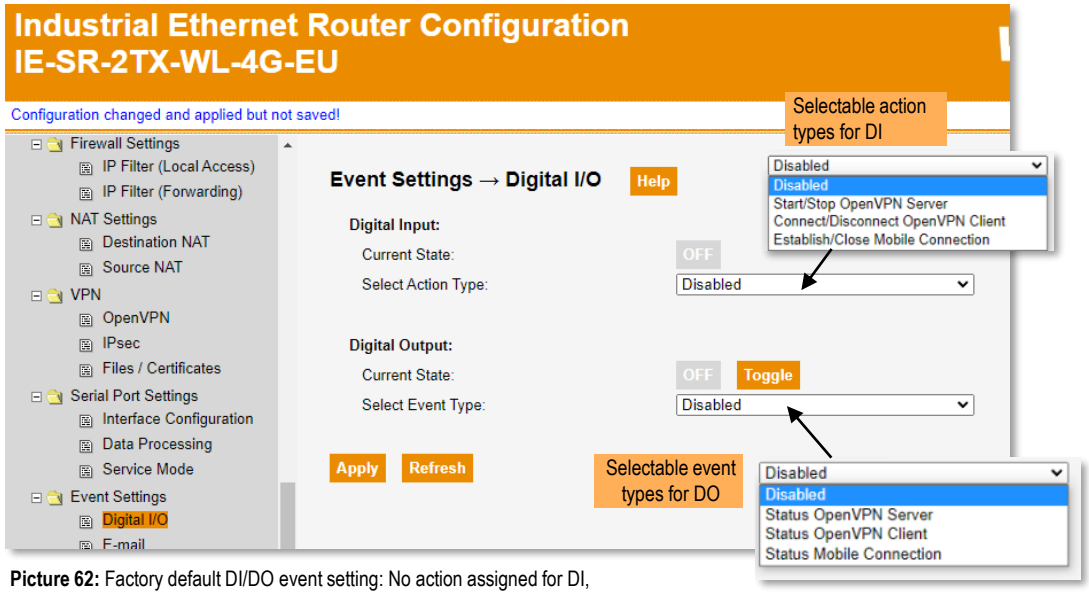
Picture 61: Service mode 'UDP Server/Client' selected.

4.34 Event Settings → Digital I/O (1 / 2)

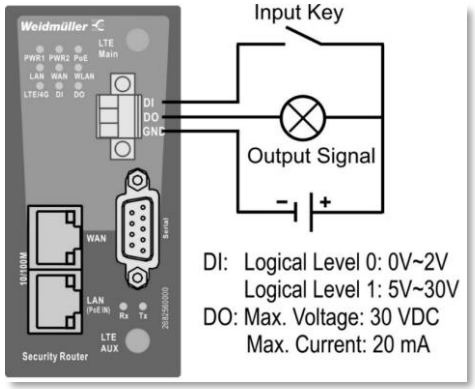
Via this webpage both device IOs 'Digital Input' and 'Digital Output' can be configured in terms of doing an action or an event-based signaling.

Digital Input → Status and Parameter settings	
Current State	Shows current input status. ON if digital input is powered from 5 to 30 VDC, OFF if not connected or for power input 0 to 2 VDC.
Select Action Type	Selection of one of following actions triggered by a DI signal change from OFF to ON or vice versa.
- Disabled	No action assigned to DI signal change
- Start / Stop OpenVPN Server	Starts or Stops the OpenVPN Server process if configured and enabled.
- Connect / Disconnect OpenVPN Client	Establishes or cancels a VPN connection to a remote OpenVPN server if the OpenVPN Client is configured and enabled.
Note: If for DI an action is selected, and a trigger event is assigned but the associated action type is neither configured nor enabled then a DI signal change does not have any effect.	

Digital Output → Status and Parameter settings	
Current State	Shows current output signal state.
Toggle (Button)	Can be used to toggle the digital output (OFF to ON and vice versa).
Select Event Type	Selection of one of following events triggering a DO signal change from OFF to ON or vice versa.
- Disabled	No event assigned to DO signal change.
- Status OpenVPN Server	Provides DO signaling when OpenVPN Server starts running or will be stopped.
- Status OpenVPN Client	Provides DO signaling when the configured OpenVPN Client either establishes or cancels a connection to a remote OpenVPN server.
- Status Mobile Connection	Provides DO signaling if the Mobile Interface establishes (Online) or cancels (Offline) the connection to the provider.
Note: If for DO an event is selected but the trigger event is neither configured nor enabled then a DO signal change never happens.	



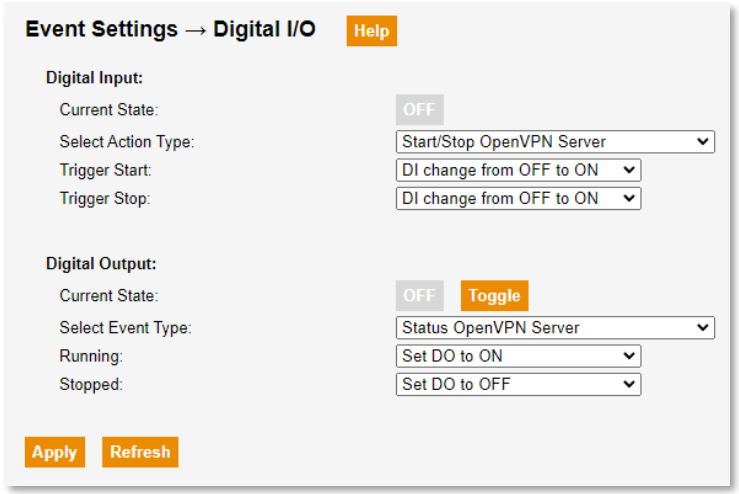
Picture 62: Factory default DI/DO event setting: No action assigned for DI, no state signaling associated to DO.



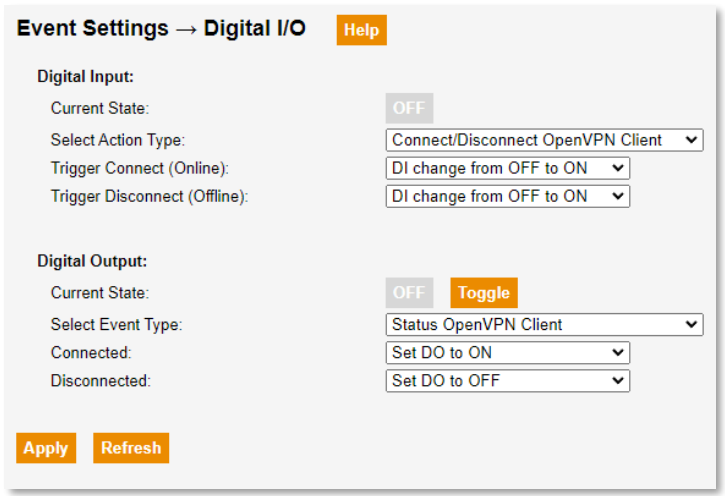
Picture 63: Wiring Digital Input and Output

4.34 Event Settings → Digital I/O (2 / 2)

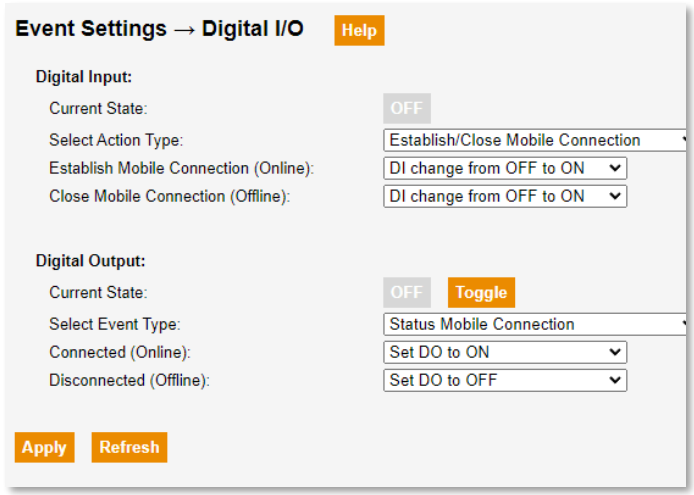
Screenshots of example configurations for DI and DO.



Picture 64: Example configuration 1
DI assigned to action type 'Start/Stop of OpenVPN Server instance'.
DO assigned to event type 'Status OpenVPN Server' (Running/Stopped).



Picture 65: Example configuration 2
DI assigned to action type 'Connect/Disconnect OpenVPN Client'.
DO assigned to event type 'Status OpenVPN Client' (Connected/disconnected).



Picture 66: Example configuration 3
DI assigned to action type 'Establish/cancel cellular connection' (Online/Offline).
DO assigned to event type 'Cellular connection status' (Online/Offline).

4.35 Event Settings → E-Mail

This web page provides the configuration of sending e-Mail alert messaged triggered by device events respectively status changes.

General Activation / Deactivation

e-Mail Event Warning — Enables or disables the mail event warning function generally.

Event Types

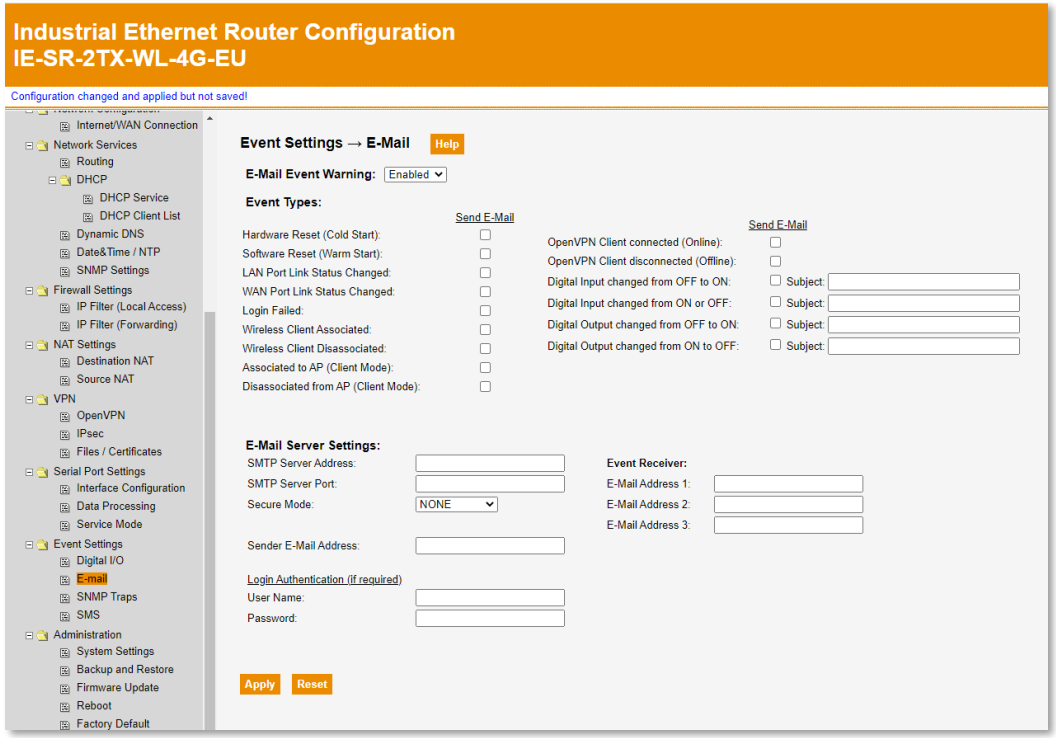
The Router supports following event types triggering a mail delivery to the defined mail receivers. The subject of an alert mail is same as the event naming except for DI/DO events, for which an individual subject can be configured.

List of event types:

- Hardware Reset (Cold Start)
- Software Reset (Warm Start)
- LAN Port Link Status Changed
- WAN Port Link Status Changed
- Login Failed
- Wireless Client Associated
- Wireless Client Disassociated
- Associated to AP (Client Mode)
- Disassociated from AP (Client Mode)
- Mobile Connection established (Online)
- Mobile Connection closed (Offline)
- OpenVPN Client connected (Online)
- OpenVPN Client disconnected (Offline)
- Digital Input changed from OFF to ON
- Digital Input changed from ON or OFF
- Digital Output changed from OFF to ON
- Digital Output changed from ON to OFF

e-Mail Server Settings

Configuration of the mail server, mail account and receivers for sending an event mail. Configure the parameters according to your used mail provider.



Picture 67: Factory Defaults of e-Mail event settings

Note: Due to security reasons nowadays a mail account on the mail (relaying) server is required using a secure access method (SSL/TLS). A simple mail relay via a server of a mail provider mostly is no longer allowed.

Hint when using a Google account (Gmail):

- Consider that some mail providers like Google requires further enhanced security settings. The result is that Gmail only allows access to their mail servers via secured mailers like the Gmail app but not for standard Linux-based mail programs.
- To nevertheless use a Gmail account for sending event mails from this device, it is possible to configure the Gmail account security for use of less-secure mailers. To do this - when logged in your Gmail account – you need to create an additional 16-digit 'app password' that gives a non-Google app or any device permission to access the Google account. Enter this special 'app password' into field 'password' instead of the normal Gmail password assigned to the used account.
- Please read published documentation from Google how to enable less secure apps for Gmail and to create the special 16-digit 'app password'.

4.36 Event Settings → SNMP Traps

Via this webpage some device status changes can be monitored triggering an SNMP trap as event.

General Activation / Deactivation

SNMP Traps — Enables or disables the warning function via SNMP trap generally.

Event Types

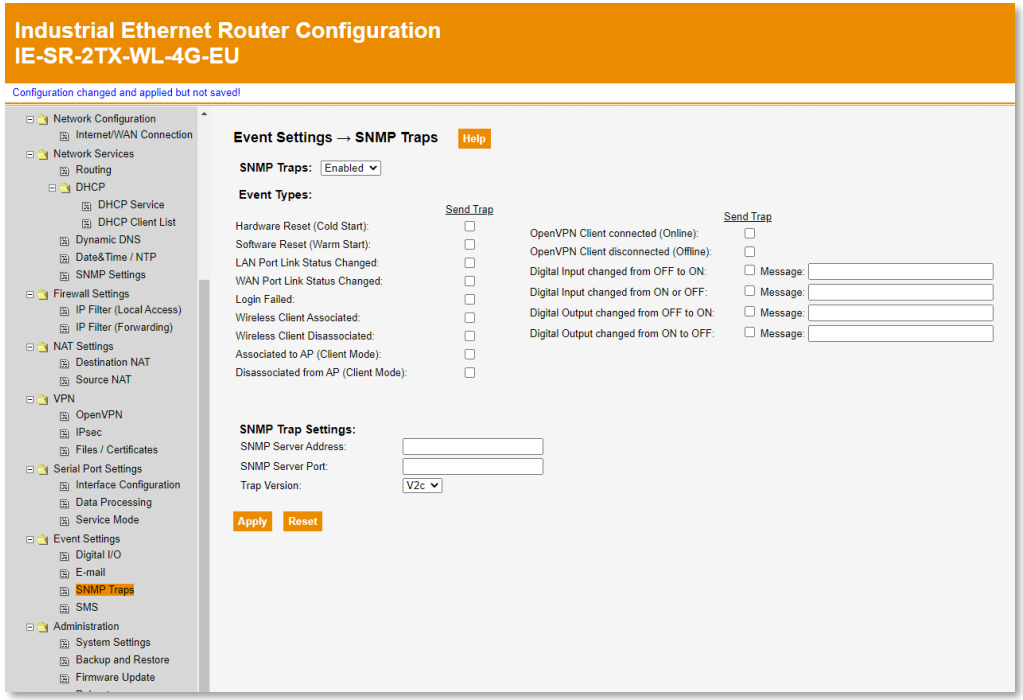
The Router supports below listed event types triggering an SNMP trap to the defined SNMP server. The trap message content is same as the event naming except for DI/DO events, for which an individual message can be configured.

List of Event Types:

- Hardware Reset (Cold Start)
- Software Reset (Warm Start)
- LAN Port Link Status Changed
- WAN Port Link Status Changed
- Login Failed
- Wireless Client Associated
- Wireless Client Disassociated
- Associated to AP (Client Mode)
- Disassociated from AP (Client Mode)
- Mobile Connection established (Online)
- Mobile Connection closed (Offline)
- OpenVPN Client connected (Online)
- OpenVPN Client disconnected (Offline)
- Digital Input changed from OFF to ON
- Digital Input changed from ON or OFF
- Digital Output changed from OFF to ON
- Digital Output changed from ON to OFF

SNMP Trap Settings (Receiver)

Configuration of the SNMP server address, port and the used version for SNMP traps.



Picture 68: Configuration window for SNMP traps.

Notes:

- Consider that for sending SNMP traps the SNMP agent also needs to be enabled (Webpage Network Services → SNMP Settings).
- Currently the Router supports only SNMP version v2c.

4.37 Event Settings → SMS (1 / 3)

This configuration page can be used for sending SMS alert messages and receiving SMS control messages triggering a defined action (only available for models equipped with LTE/4G modem).

General Activation / Deactivation

SMS Alert/Control Service: Enables or disables the SMS functionality generally.

SMS Alert and Control Numbers

Definition of up to 3 mobile numbers which will be used for both receiver for SMS messages and accepted (allowed) when receiving a SMS control message. The Router only communicates with defined mobile numbers in terms of SMS data exchange (Alert and Control).

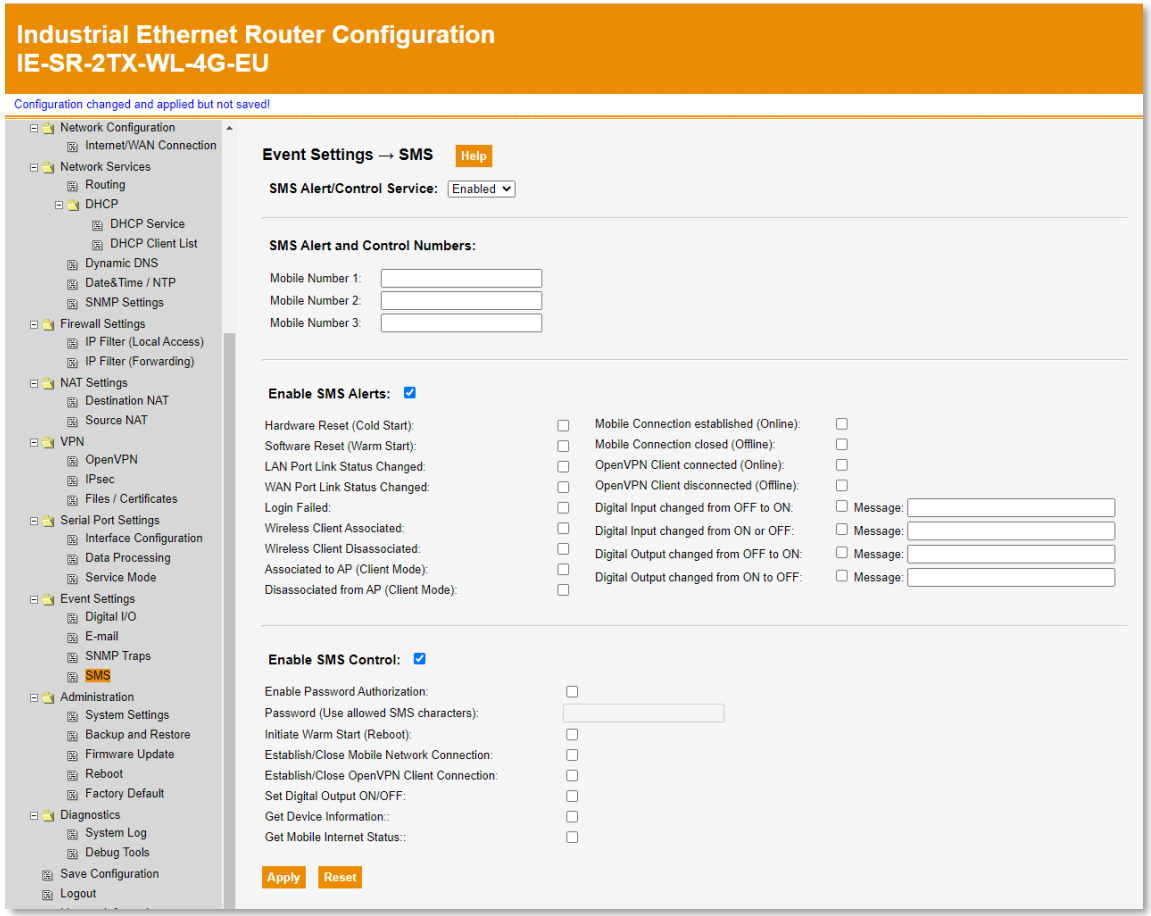
Section 'SMS Alerts'

The Router supports listed event types triggering a SMS message which will be sent to all defined mobile numbers. The SMS content is same as the event naming except for DI/DO events, for which an individual text can be configured.

Enable SMS Alerts: Enables or disables sending of SMS messages generally.

List of SMS Alerts:

- Hardware Reset (Cold Start)
- Software Reset (Warm Start)
- LAN Port Link Status Changed
- WAN Port Link Status Changed
- Login Failed
- Wireless Client Associated
- Wireless Client Disassociated
- Associated to AP (Client Mode)
- Disassociated from AP (Client Mode)
- Mobile Connection established (Online)
- Mobile Connection closed (Offline)
- OpenVPN Client connected (Online)
- OpenVPN Client disconnected (Offline)
- Digital Input changed from OFF to ON
- Digital Input changed from ON or OFF
- Digital Output changed from OFF to ON
- Digital Output changed from ON to OFF



Picture 69: Configuration window for SMS alerts and control messages.
This configuration page is only available for models with 4G/LTE modem.

4.37 Event Settings → SMS (2 / 3)

Section 'SMS Control'

The Router supports control messages for below listed actions. Depending on parameter setting "Enable Password Authorization" a control message needs to be sent with an additional password to enhance the access security.

Enable SMS Control: Enables or disables the reception of SMS messages triggering a defined action.

Enable Password Authorization: If checkbox is enabled, each SMS control message must be sent additionally with the defined password, otherwise it will not be accepted by the Router.

List of SMS Control Functions:

- Initiate Warm Start (Reboot)
- Establish/Close Mobile Network Connection
- Establish/Close OpenVPN Client Connection
- Set Digital Output ON/OFF
- Get Device Information
- Get Mobile Internet Status

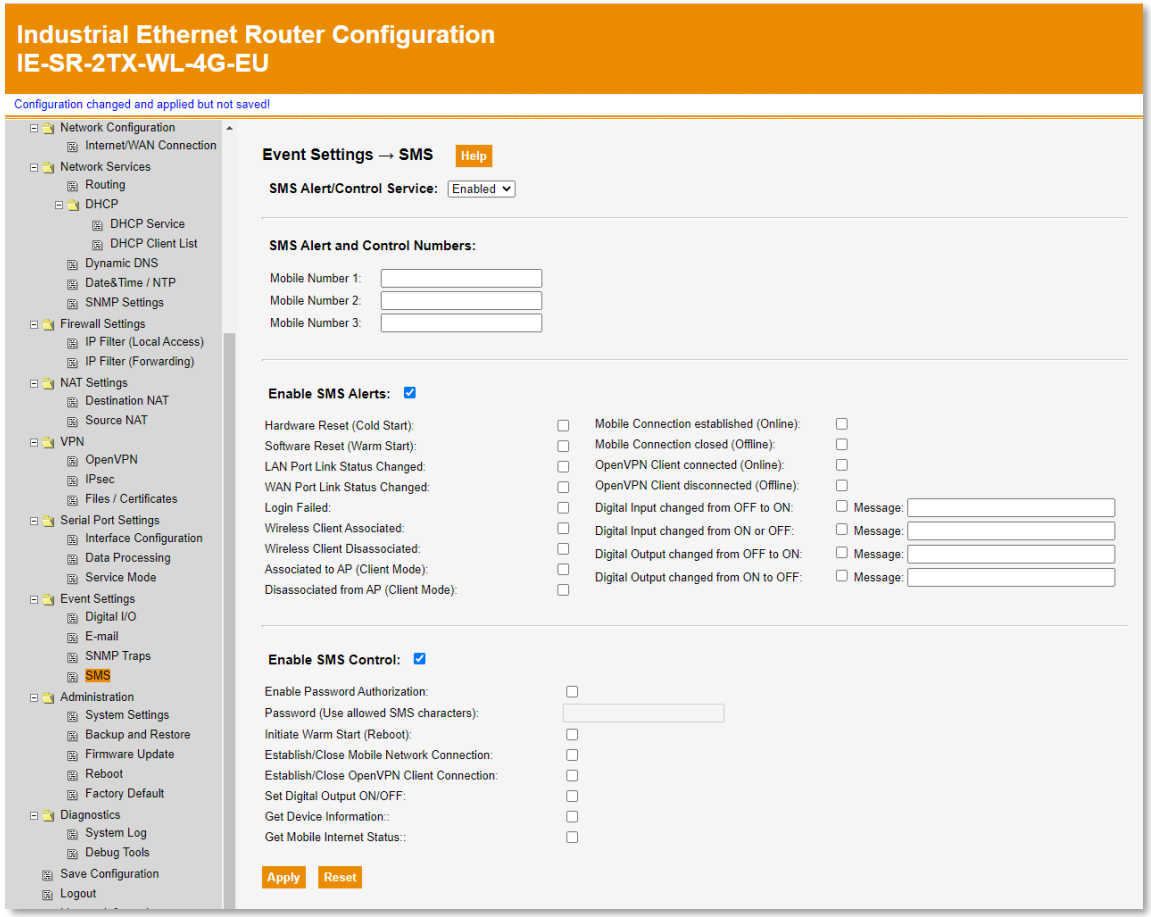
Process steps of an SMS control action:

1. Send SMS control message to Routers mobile number (if defined, with additional password).
2. Router checks received SMS for plausibility (format and security).

3a. If plausibility check is successful, Router sends back an acceptance message except for action types "Get Device Information" and "Get Mobile Internet Status". For these action types, the SMS response will be sent directly containing the required information. For the other ones, the Router starts to execute the action initiated by the SMS control message.

3b. If plausibility check fails, Router sends back an error message.

Refer to table **SMS Control commands** on next slide how to send an SMS control command.



Picture 70 (Same as picture 69)**:** Configuration window for SMS alerts and control messages.

Notes:

- For security reasons SMS control actions are applicable only for configured mobile numbers.
- If feedback about the actual implementation of an initiated action is necessary, then configure the appropriate SMS alert type for signalizing the result.

4.37 Event Settings → SMS (3 / 3)

Table SMS control commands

Control Function	Syntax SMS control message with password	Syntax SMS control message without password	SMS response if a plausibility error was detected. Will only be sent to defined mobile numbers.	SMS response if the required command was accepted (no plausibility error). Will only be sent to defined mobile numbers.
Initiate Warm Start (Reboot)	#password?reboot	?reboot	<System name>: Control message error: <Error message> Possible error messages: 1: Missing or wrong password 2: Mobile number not authorized (undefined) 3: Wrong syntax/format of command message 4: SMS Control not enabled 5: Required action not possible (improper device status or configuration).	<System name>: Command ? <command> accepted.
Establish Mobile Network Connection	#password?MobileConnection=on	?MobileConnection=on		
Close Mobile Network Connection	#password?MobileConnection=off	?MobileConnection=off		
Establish OpenVPN Client Connection	#password?VPNTunnel=on	?OpenVPNTunnel=on		
Close OpenVPN Client Connection	#password?VPNTunnel=off	?OpenVPNTunnel=off		
Set Digital Output to ON	#password?DO=on	?DO=on		
Set Digital Output to OFF	#password?DO=off	?DO=off		
Establish a predefined VPN Tunnel	#password?VPNTunnel=on	?OpenVPNTunnel=on		
Close an established VPN Tunnel	#password?VPNTunnel=off	?OpenVPNTunnel=off		
Get Device Information	#password?GetDeviceInfo	?GetDeviceInfo		<System name>: <Location>: <Device type>: <Serial number>: <Firmware version>
Get Mobile Internet Status	#password?GetMobileStatus	?GetMobileStatus		<System name>: <Connection state>: <Registration state>: <Network provider>: <Signal strength>
	Notes: 1. Control messages - except the password - are not case sensitive. 2. Replace ‚password' with the configured password.			

4.38 Administration → System Settings

This website is intended

- to define and describe application specific device information,
- to configure security settings regarding Router access,
- to change the password of user 'admin' for Router access and
- to configure some system logging related parameters.

Section System Data

Use parameters

- System Name,
- System Description,
- Location and
- Contact

for unique device identification. These input fields are freely editable.

Section Access Settings

This section defines the security settings in terms of device access for configuration. For device configuration the administrative user **'admin'** must be used generally.
In terms of the web-based configuration several access options (HTTP or HTTPS) and interfaces (LAN, WAN, WLAN, etc.) can be configured. By default, only a secured HTTPS web interface access via the LAN interface is allowed.
For users familiar with Linux respectively OpenWRT operating system, the Router can be released for low-level console access via SSH or Telnet by enabling the related checkboxes.
Use for access user 'root' and same password as set for user 'admin'.

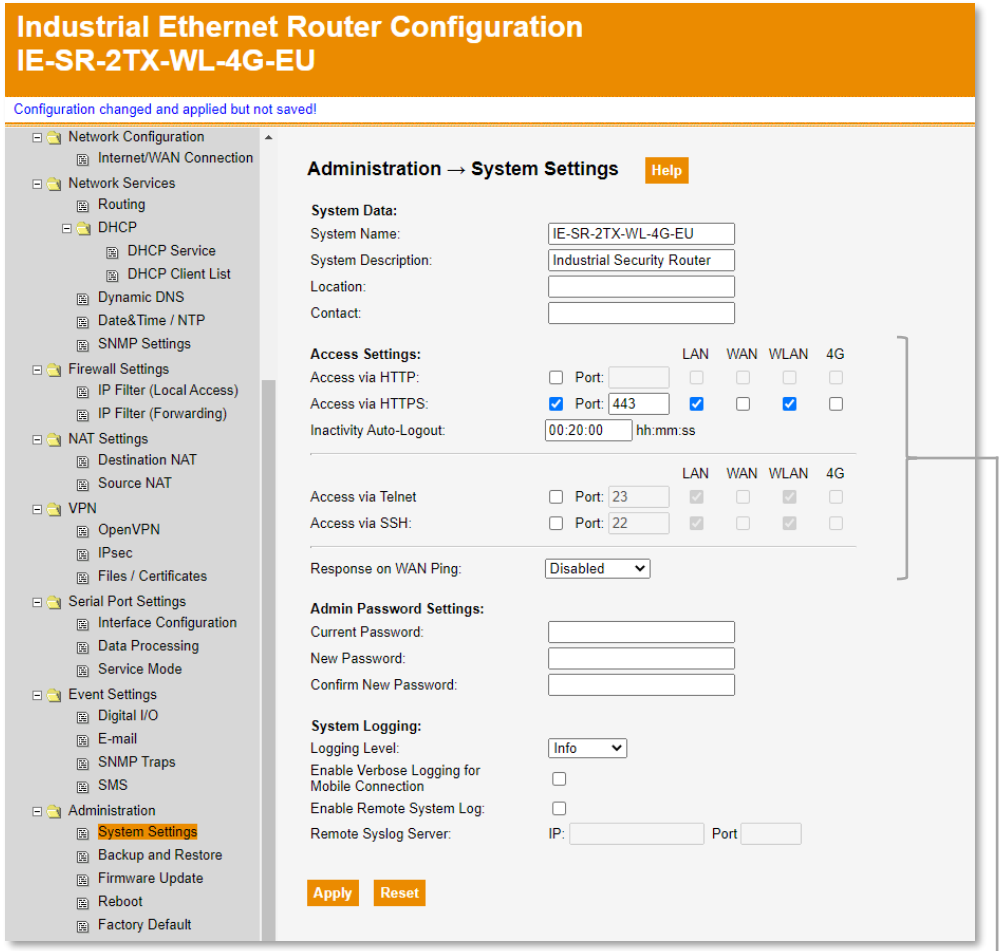
Attention: When doing a device access at root level of the Linux operating system, be aware that configuration changes can have a severe impact on the functionality of the running Router application (configured via the web interface). Any change is in the risk and responsibility of the user if the web-based Router application fails due to the intervention. For recovering the designed functionality based on the installed firmware reset the device to factory default settings (e.g., press external reset button larger 5 secs).

Section Admin Password Settings

Via this section a new password can be set for the administrative user account, currently being the only available user account. For password change you need to confirm the current password before setting a new one.

Section System Logging

This section defines the logging level of the 'System Log' for diagnostic purposes.
Additionally, the forwarding of system log data to a remote 'Syslog' server can be configured.



Picture 71: Factory defaults of 'System Settings'.

Note:

The checkboxes of section 'Access Settings' are related to specific firewall rules (IPtables Filter). If enabled, the corresponding rules allow the action, if disabled it will be rejected. These rules are independent of the settings of default filter policies 'Input LAN' and 'Input WAN' of configuration page 'Firewall Settings → IP Filter (Local Access)'. Means, if you allow a general access (Accept) via policies 'Input LAN' and 'Input WAN', for example you cannot access the Router as long the corresponding 'access' checkbox is not enabled.

4.39 Administration → Backup and Restore

This website is intended

- to save the Flash memory configuration to an external backup file
- and for restoring a configuration from a previously saved backup file.

Section Backup Configuration

By default, device model name with extension “cfg” is preset as backup file name. It is reasonable to adapt the file name having a unique reference to the device from which it will be exported. Pressing button ‘Export’ stores the backup file into the browsers download directory.

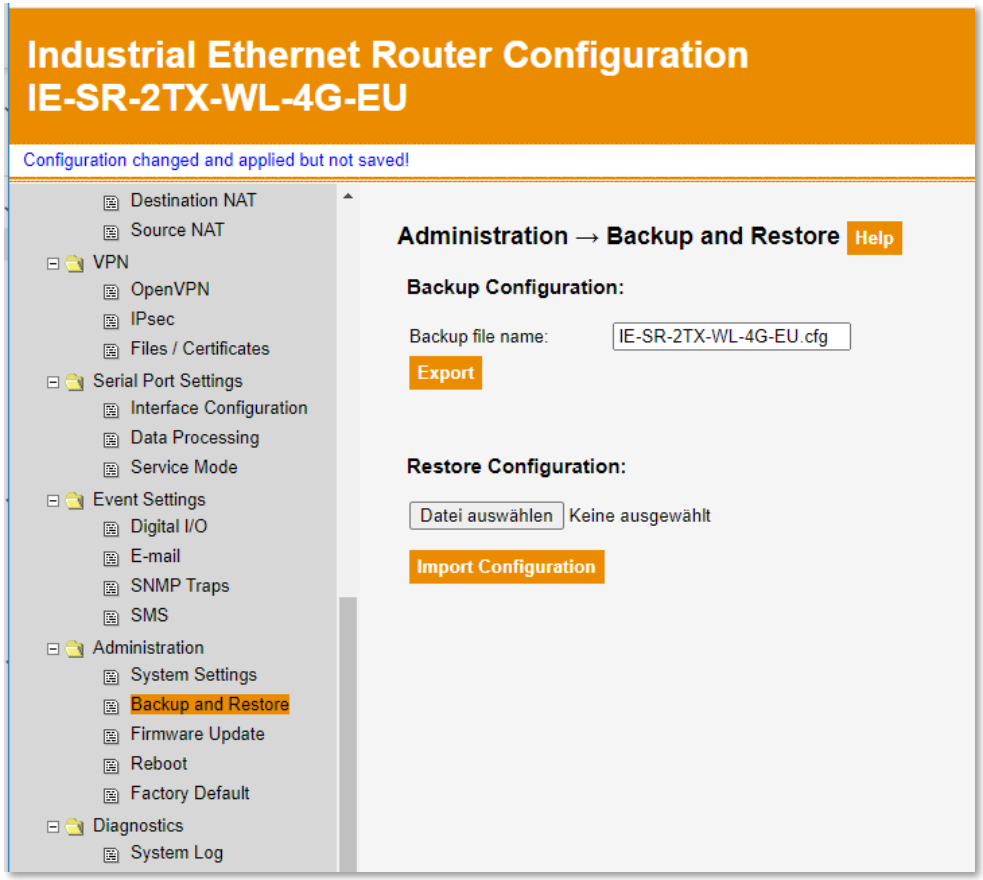
Note: The backup file is saved in a binary format which is not readable.

Section Restore Configuration

Select the file for import to restore the configuration which originally was exported as backup file.

After clicking button ‘Import Configuration’ the Router will be configured with content of selected import file followed by a system reboot.

Note: Be aware of possibly changed access credentials and/or IP addresses after system reboot. If so, you need to open a new browser window for web access using valid IP address and access credentials.



Picture 72: Application window for backup and restore of a configuration file.

4.40 Administration → Firmware Update

This menu is used for installing a new Router firmware by file update.

The Router is equipped with two firmware storage sections. One contains the running version the other section is used for firmware fallback if any error occurs during the upload and update process.

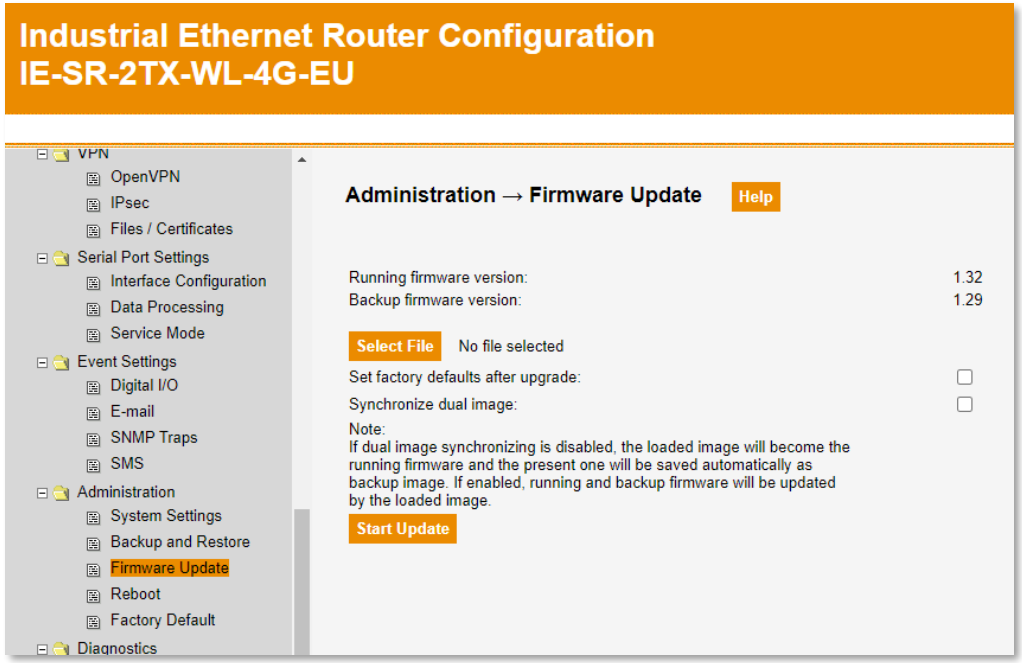
In normal operation the running firmware will be saved for backup and the uploaded firmware becomes the running one.

In case of any update problem then at reboot time the original version will be reactivated again as the running version.

Firmware Update Procedure

1. Select firmware file.
2. Enable checkbox 'Set Factory defaults after upgrade' if desired.
3. Enable checkbox 'Synchronize dual image' if both firmware images shall be updated to new firmware version.
4. Click button 'Start Update' to initiate the upload process of the firmware file.
5. After successful file upload the internal upgrade process starts **taking around 5 minutes** to finish.
6. The update process will be finished by a reboot before the device becomes ready again.

Note: If you have enabled checkbox 'Set factory defaults after upgrade', you need to open a new browser window with factory default IP for web access if IP address has been changed due to factory default settings..



Picture 73: Application window for file-based firmware update.

4.41 Administration → Reboot

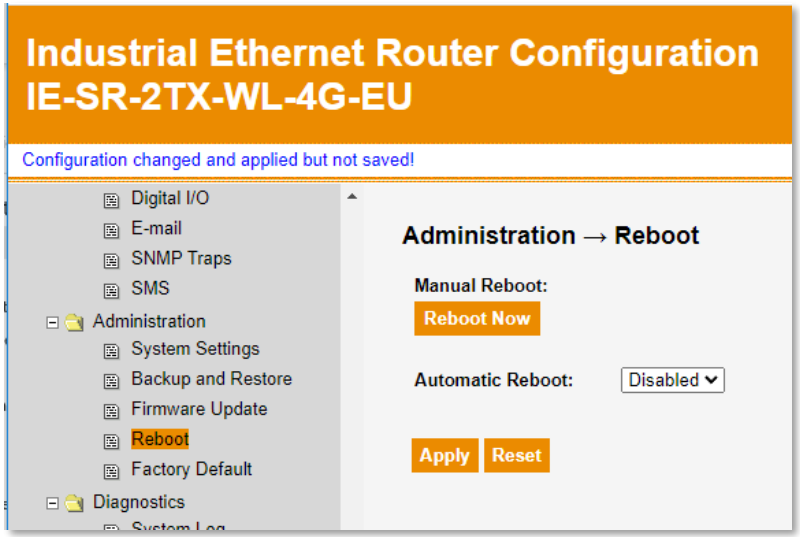
Via this website the device can be rebooted, either manually or automatically timed.

Manual Reboot

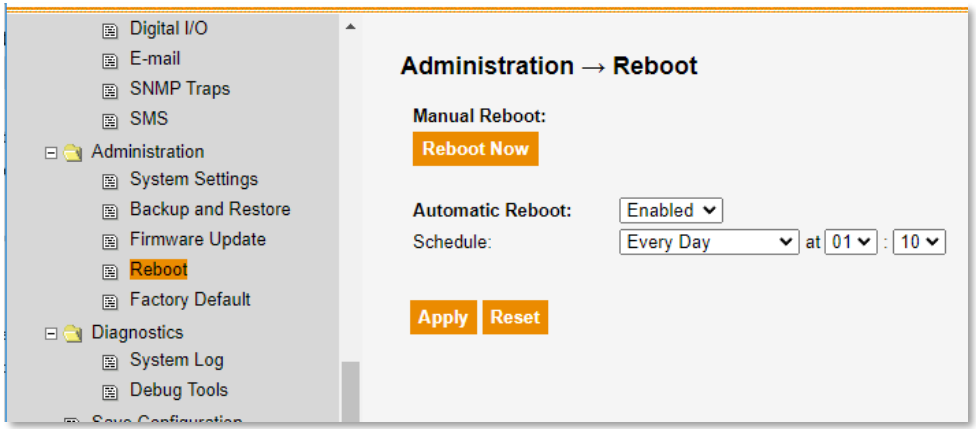
Pressing button 'Reboot Now' reboots the device immediately (Warm Start).

Automatic Reboot

An automatic reboot can be configured and scheduled
- either every day at a defined time or
- at a weekday at a defined time.



Picture 74: Factory settings of 'Reboot' window.



Picture 75: Example of a configured schedule for automatic reboot.

4.42 Administration → Factory Default

This website can be used to reset the Router to factory default settings.

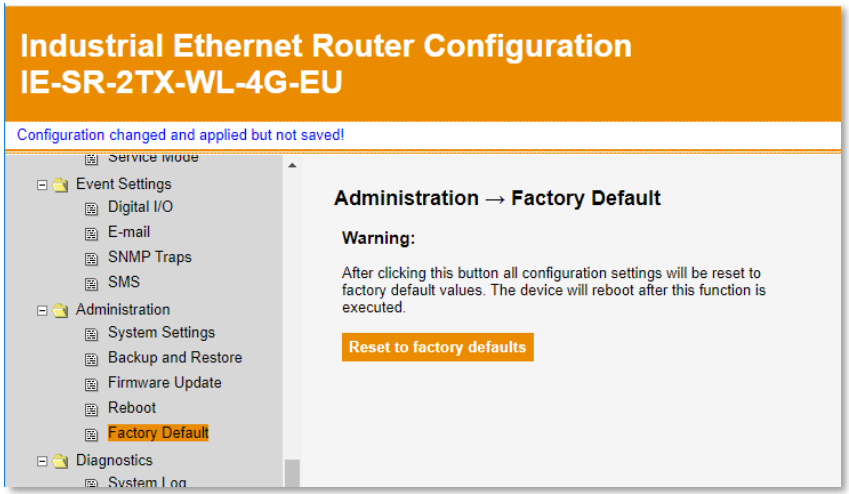
Click on button 'Reset to factory defaults' immediately initiates the reboot process of the device coming-up with factory default settings. The duration until the device is ready again is about 60 seconds.

Factory Default Settings:

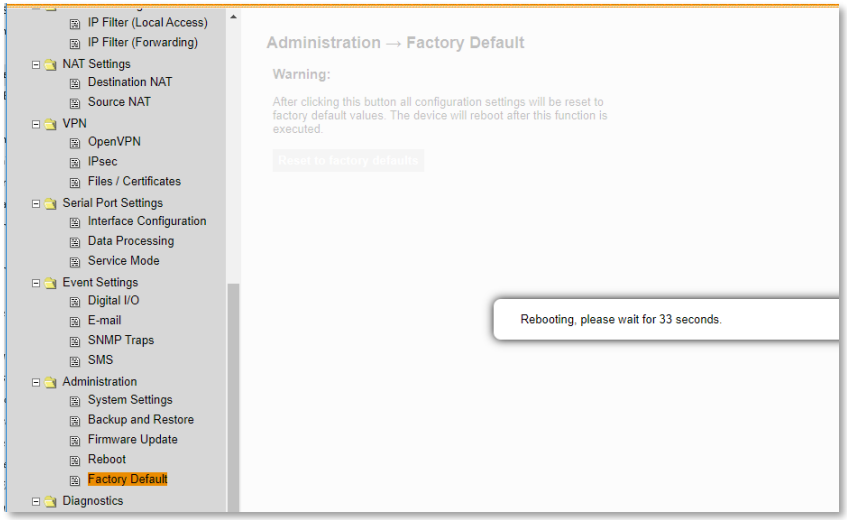
LAN port:	192.168.1.110 / 255.255.255.0 (static)
WAN port:	DHCP
Wireless LAN:	Disabled
Mobile Interface:	Disabled (only available for LTE/4G models)
Username:	admin
Password:	Weidmueller
Web Access:	HTTPS via LAN port

Consider: After setting to factory defaults, the Router only can be accessed by HTTPS-secured Web interface via the wired LAN Port. All other access modes (HTTP, Telnet, SSH) and any access from other interfaces are not allowed by default.

Note: Alternatively, the external reset button can be used for setting factory defaults.
Pressing < 5 seconds: Reboots the device (Warm Start) and sets IP of LAN port to factory default IP.
Pressing >= 5 seconds: Resets the device completely to factory default settings.



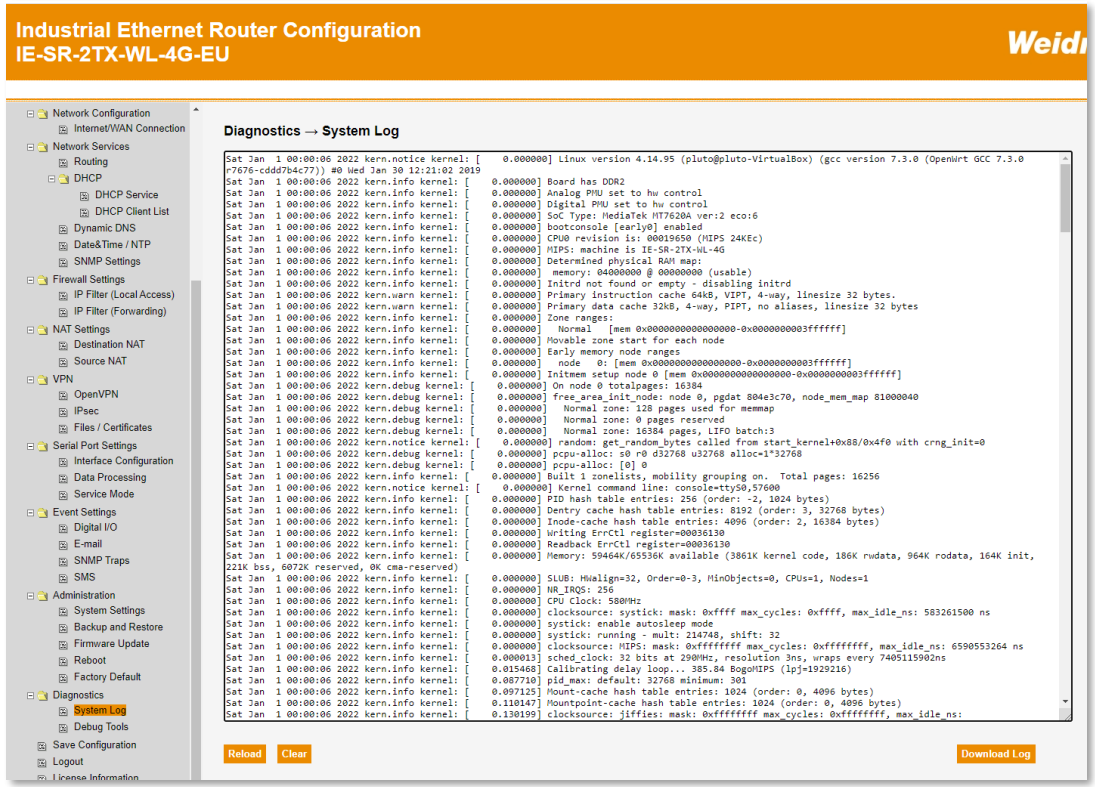
Picture 76: Application window for reset to factory default settings.



Picture 77: After initiation of the reset process a time counter is displayed counting from 60 to 0 seconds. Additionally, a beep signalizes that the reboot process almost has been finished and the device becomes ready again.

4.43 Diagnostics → System Log

This website displays the system log messages.



Picture 78: Screenshot of 'System Log'.

4.44 Diagnostics → Debug Tools

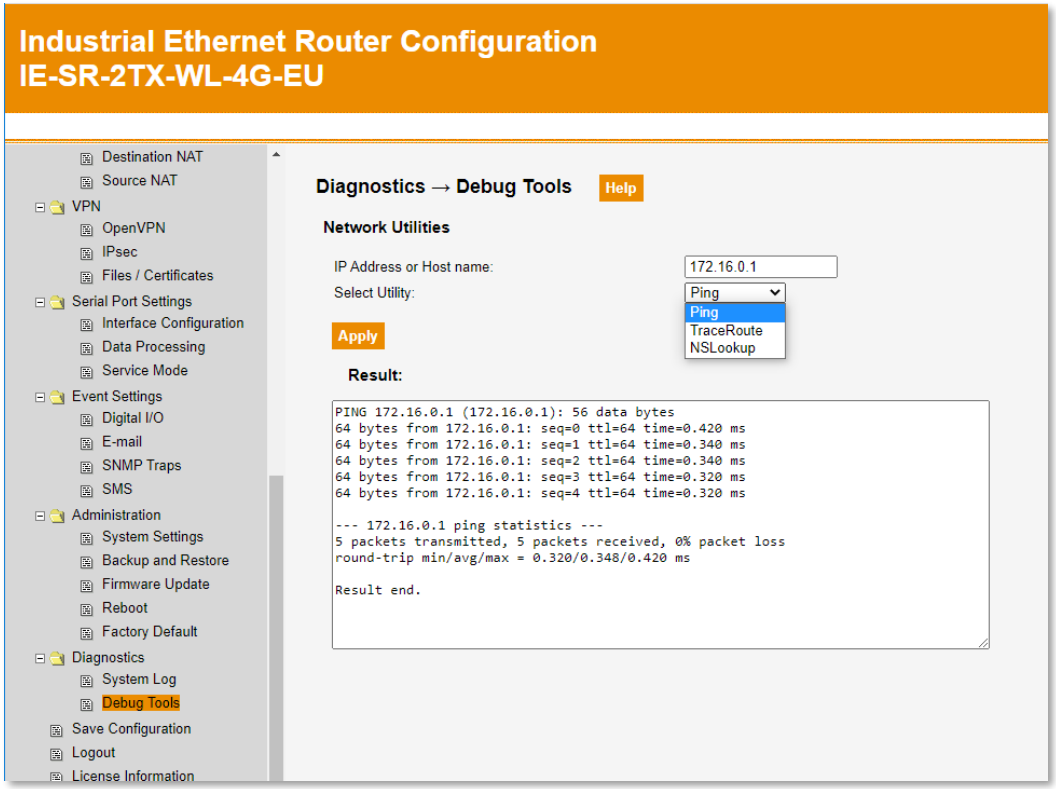
The Router supports network utilities

- Ping,
- TraceRoute and
- NSLookup

for diagnostic purposes.

For evaluation enter IP address or a DNS host name and select the desired network utility. After pressing 'Apply' button a window will be displayed showing the result.

Note: Some diagnostic tests like 'TraceRoute' can take a longer time and cannot be interrupted.



Picture 79: Example of network utility 'Ping'.

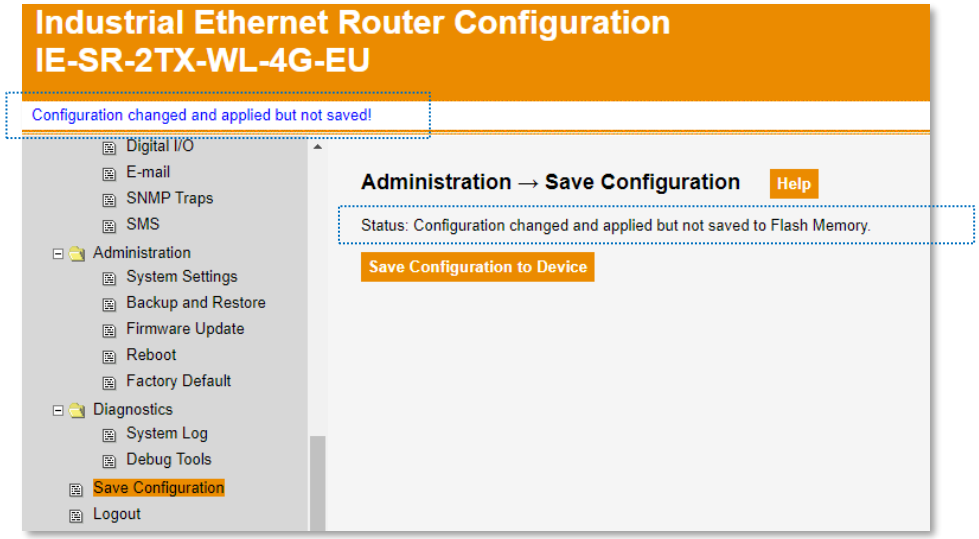
4.45 Save Configuration

Via this web page the running configuration will be saved to Flash memory.

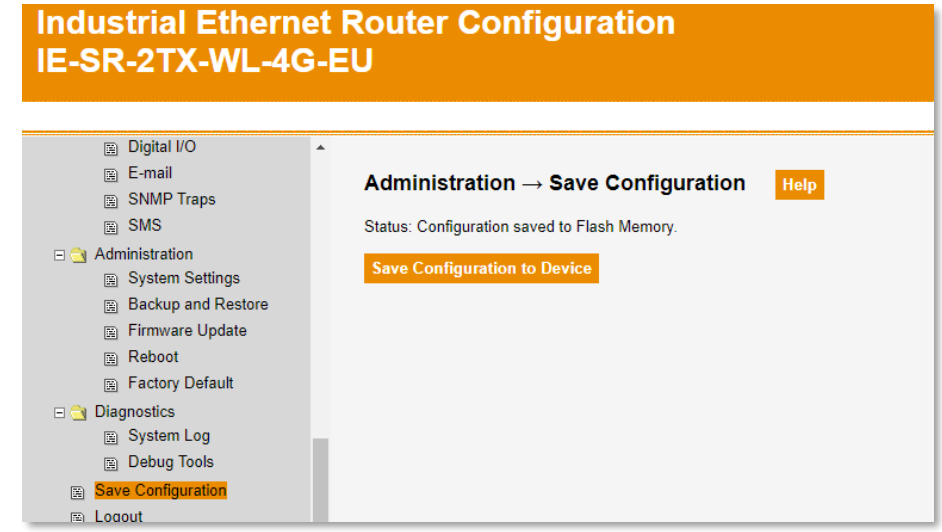
After applying of changed parameters on any configuration page the adaptions immediately becomes active, but they will not be saved automatically to Flash memory.

Applying any setting resulting in a difference between the running and the saved configuration triggers the display of blue-colored message 'Configuration changed and applied but not saved!' below the headline, signalizing that the running configuration still needs to be saved. The message disappears after clicking button 'Save Configuration to Device' indicating identical running and saved configurations.

Note: If the device will be rebooted or powered down and the message is still displayed, then all applied but not saved changes will be lost at next start-up.



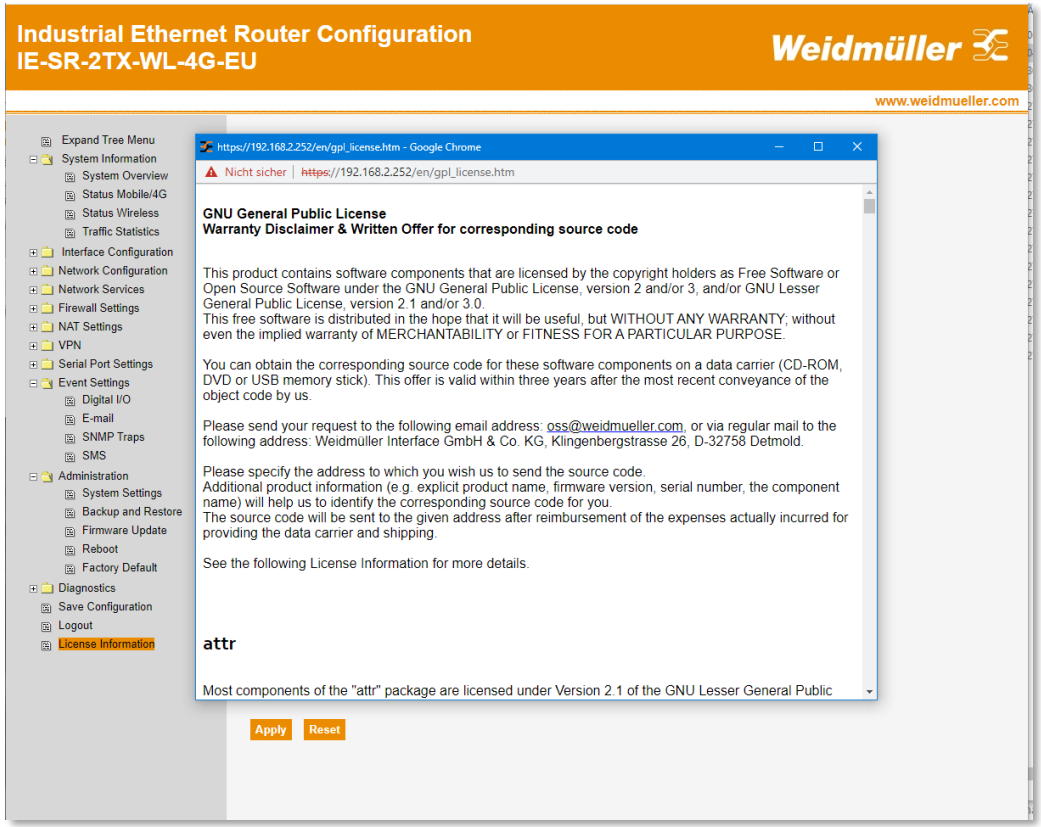
Picture 80: Example of notice display and status message that any change has been done and applied but not saved to Flash memory.



Picture 81: Status message after saving the configuration to Flash memory. The blue-colored notice is disappeared.

4.46 License Information

This web page provides information related to GNU General Public License and notes about warranty disclaimer and written offer for corresponding source code.



Picture 82: Screenshot showing window with license information.

A. Appendix

A1- **N**etwork **A**ddress **T**ranslation: Use cases and how to configure Source NAT and Destination NAT.

A1-1 Network Address Translation: Overview about NAT application types configurable by destination and source NAT rules (1 / 2)

NAT Type	Function	Use case / Application
1. Destination NAT **Protocol / Port** (DNAT)	An IP packet – typically **addressed to Routers (WAN) Interface IP** – will be forwarded to a local (LAN) device **dependent on protocol and destination port.**	Access to a **service** of a local device (LAN) via Router's "public" WAN interface IP. For example, access to a Modbus/TCP slave by forwarding protocol TCP and port 502.
2. Destination NAT **IP** (DNAT)	An IP packet - incoming at Routers WAN port and **addressed to a "virtual" IP** – will be forwarded to a local (LAN) device **based on protocol and destination port**. Each incoming IP packet (typically at WAN port) and having the configured virtual "public" IP as destination IP, will be forwarded to the configured target IP (real device at LAN side). Consider: The sending device only can send a packet to the "virtual" IP via the Router's interface, if either the Router's IP is the default gateway on the sending device, or if a route is configured on the sender device that the "virtual" IP can be reached via the Router's interface IP.	Hiding a local host (LAN) by a virtual "public" IP. Can be applied for a full host NAT (use of virtual IP for incoming and outgoing communication) in combination with NAT type "Source NAT IP/Port" (No. 6).
3. Destination NAT **Alias IP** (DNAT)	An IP packet - **addressed to an additionally created Router IP (WAN port Alias IP) -** will be forwarded to a local (LAN) device **based on protocol and destination port.** Typically, as 'Alias IP' a free (unused) IP of the WAN network will be configured which easily can be addressed from WAN devices resulting in accessing devices at Routers LAN port without having a route to the LAN network. Effectively, the Router can have multiple IP addresses, the configured WAN port IP and virtual 'Alias IPs' to be used as forwarding IPs to real LAN devices. The additional 'Alias IP' will be defined and created as part of the rule configuration.	Easy access from outside network (WAN) to a local LAN host without having any knowledge of the LAN network. No routing information is necessary for WAN devices because they are addressing devices which seem to be in their own IP subnet.
4. Destination NAT **IP Subnet** (NETMAP)	IP packets - incoming at Routers Interface and **addressed to a "virtual" IP range** – will be forwarded to an identical subnet of local (LAN) devices **based on used protocol (Any, TCP or UDP)**. The behavior of this function is similar as "Destination NAT IP (No. 2)" but with the difference that using this DNAT type multiple IP addresses (subnet) can be defined for forwarding instead of a single host IP.	Hiding a LAN subnet (private) by a virtual "public" IP range when accessed from outside network (WAN). Can be applied to setup a full "1:1 NAT" (use virtual public IPs for communication instead of real LAN IPs) in combination with NAT type "Source NAT IP Subnet" (No. 7) which replaces real source IP by the virtual "public" IP for outgoing traffic.
5. Destination NAT **Alias IP Subnet** (NETMAP)	IP packets - **addressed to additionally created Router IPs (Alias IPs on WAN port)** – will be forwarded to an identical subnet of local (LAN) devices **based on used protocol (Any, TCP or UDP).** The behavior of this function is similar as "Destination NAT Alias IP (No. 3)" but with the difference that using this DNAT type multiple IP addresses (subnet) can be created for forwarding instead of a single 'Alias IP' when using NAT type "Destination NAT Alias IP (No. 3)".	Easy access from the outside network (WAN) to a local LAN IP subnet (multiple devices) without having any knowledge of the LAN network (WAN devices do not need any routing information).

A1-1 Network address translation: Overview about NAT application types configurable by destination and source NAT rules (2 / 2)

NAT Type	Function	Use case / Application
6. Source NAT **IP / Port** (SNAT)	**Replacement of the source IP of a host** by a virtual "public" IP when the host device (typically a LAN member) initiates an outgoing communication via the Router. When a host packet passes the Router, the original source IP will be replaced by the configured IP of the SNAT rule when matching to defined criteria.	Hiding a private network device at LAN side by using the virtual "public" IP for outside communication initiated by the private host. Can be used for a **host 1:1 NAT** in combination with NAT type "Destination NAT IP" (No. 2). If both rules will be configured, the virtual IP is used as source IP for outgoing traffic initiated by the private LAN host as well as accessible destination IP if outside network devices initiate a connection to the private LAN host .
7. Source NAT **IP Subnet** (NETMAP)	**Replacement of the source IPs of a subnet** (multiple devices) by a defined virtual "public" IP range (subnet). For any host (device) of the defined subnet the host source IP will be replaced for outgoing communication passing the Router.	Hiding a private subnet at LAN side by a virtual "public" IP range for outside communication initiated by the private host (belonging to this subnet). Can be used for a **subnet 1:1 NAT** (both directions) in combination with NAT type "Destination NAT Subnet" (No. 5).

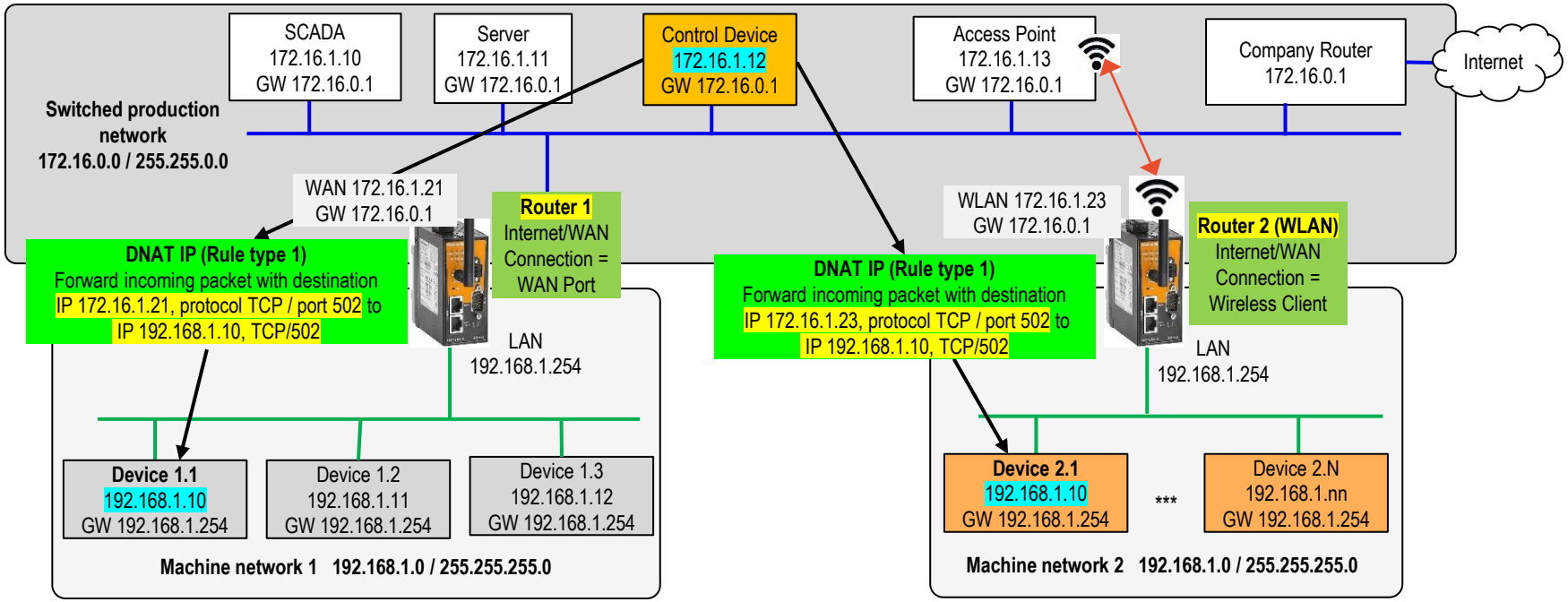
General note about applying of Source and Destination NAT:

- Source NAT replaces the source IP of an IP packet immediately before it will leave the Router outgoing on a defined or any interface. Any firewall rules applied to the IP packet have been done before to the original source IP if referred inside of a Firewall rule.

- Destination NAT replaces the destination IP of an IP packet immediately when it arrives at a defined or any Router interface. Any firewall rules applied to the IP packet when passing the Router will be done, if referred, to the new destination IP.

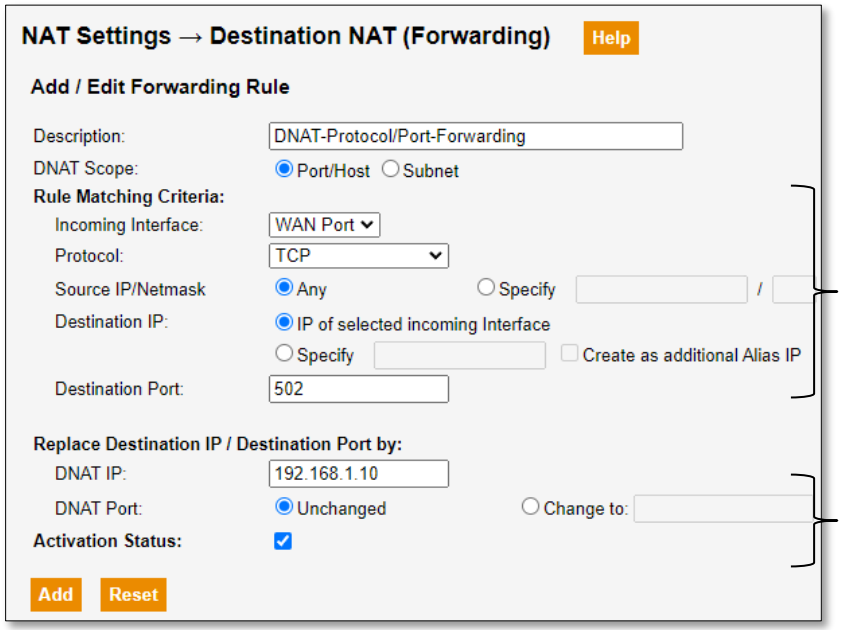
A1-2 Example of NAT type (1) 'DNAT Protocol/Port' → IP forwarding based on used protocol/port to a local (private) host via Router's interface IP (1 / 3)

Task	Condition	Solution
• Control device (Modbus/TCP Master using Protocol TCP / Port 502)) shall have access to Modbus/TCP slaves **Device 1.1 at machine network 1** and **Device 2.1 at machine network 2**.	• Gateway of control device is set to company router (172.16.0.1). • No routes can be configured on the control device to access Modbus Slave devices connected at Routers LAN side.	• Configure a DNAT rule on **Router 1** that each incoming IP packet with destination IP 172.16.1.21 (Router's WAN IP) and having protocol TCP / Port 502 will be forwarded to LAN IP 192.168.1.10. • Configure a DNAT rule on **Router 2 (WLAN)** that each incoming IP packet with destination IP 172.16.1.23 (Router's WLAN IP) and having protocol TCP / Port 502 will be forwarded to LAN IP 192.168.1.10.



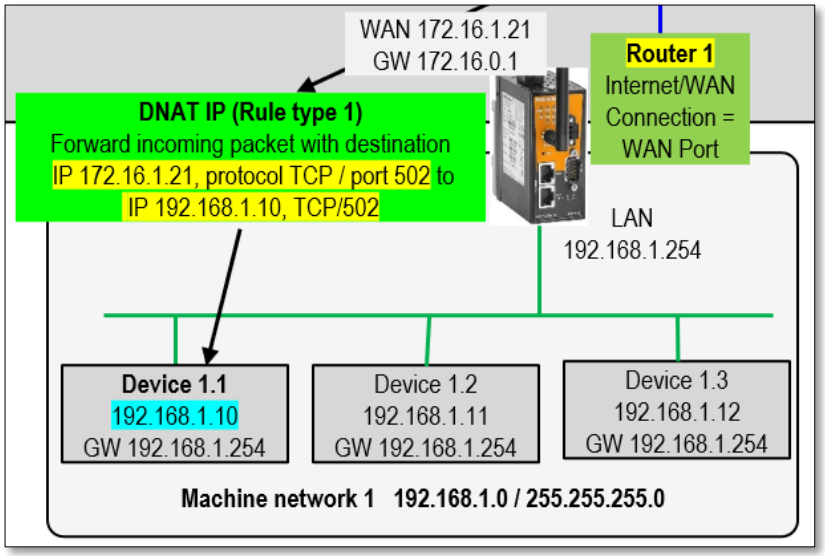
A1-2 Example of NAT type (1) 'DNAT Protocol/Port' → IP forwarding based on used protocol/port to a local (private) host via Router's interface IP (2 / 3)

Configuration of rule „DNAT Protocol/Port" on Router 1 according to illustrated application.



Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.



Active „DNAT Protocol/Port" forwarding rule after applying:

Active Forwarding Table:

#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT-Protocol/Port-Forwarding	WAN	TCP	Any	Interface IP	502	0	192.168.1.10	Unchanged	☑	Edit Delete

Apply Reset

Result: Modbus/TCP communication to Device 1.1 (real IP 192.168.1.10) can be established from WAN network via Router's IP 172.16.1.21.
Each IP packet incoming at **WAN** interface with (Router's) destination IP 172.16.1.21, protocol TCP and port number 502 will be forwarded to device with IP address 192.168.1.10.

A1-2 Example of NAT type (1) 'DNAT Protocol/Port' → IP forwarding based on used protocol/port to a local (private) host via Router's interface IP (3 / 3)

Configuration of DNAT Rule on Router 2 (WLAN) according to illustrated application.

NAT Settings → Destination NAT (Forwarding) Help

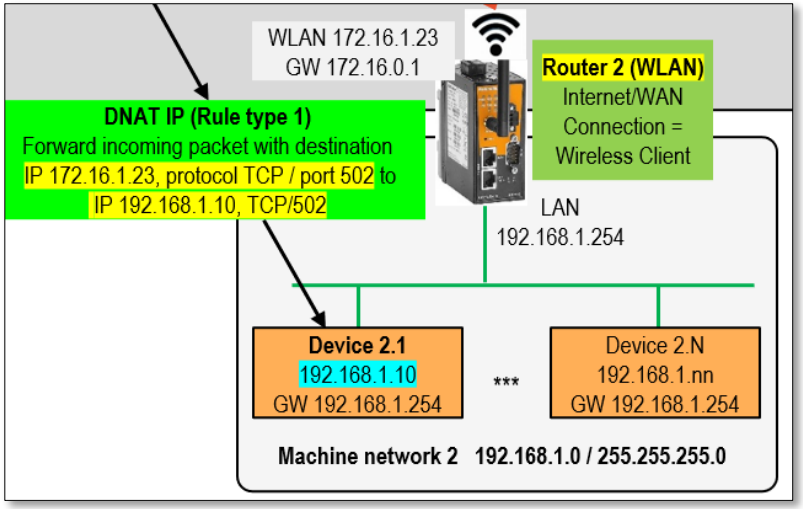
Add / Edit Forwarding Rule

Description:	DNAT-Protocol/Port-Forwarding
DNAT Scope:	(•) Port/Host ( ) Subnet
Rule Matching Criteria:	
Incoming Interface:	WLAN
Protocol:	TCP
Source IP/Netmask	(•) Any ( ) Specify /
Destination IP:	(•) IP of selected incoming Interface
	( ) Specify [ ] Create as additional Alias IP
Destination Port:	502
Replace Destination IP / Destination Port by:	
DNAT IP:	192.168.1.10
DNAT Port:	(•) Unchanged ( ) Change to:
Activation Status:	☑

Add Reset

Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.



Active „DNAT IP Forwarding" rule after applying:

Active Forwarding Table:

#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
*1	DNAT-Protocol/Port-Forwarding	WLAN	TCP	Any	Interface IP	502	0	192.168.1.10	Unchanged	☑	Edit Delete

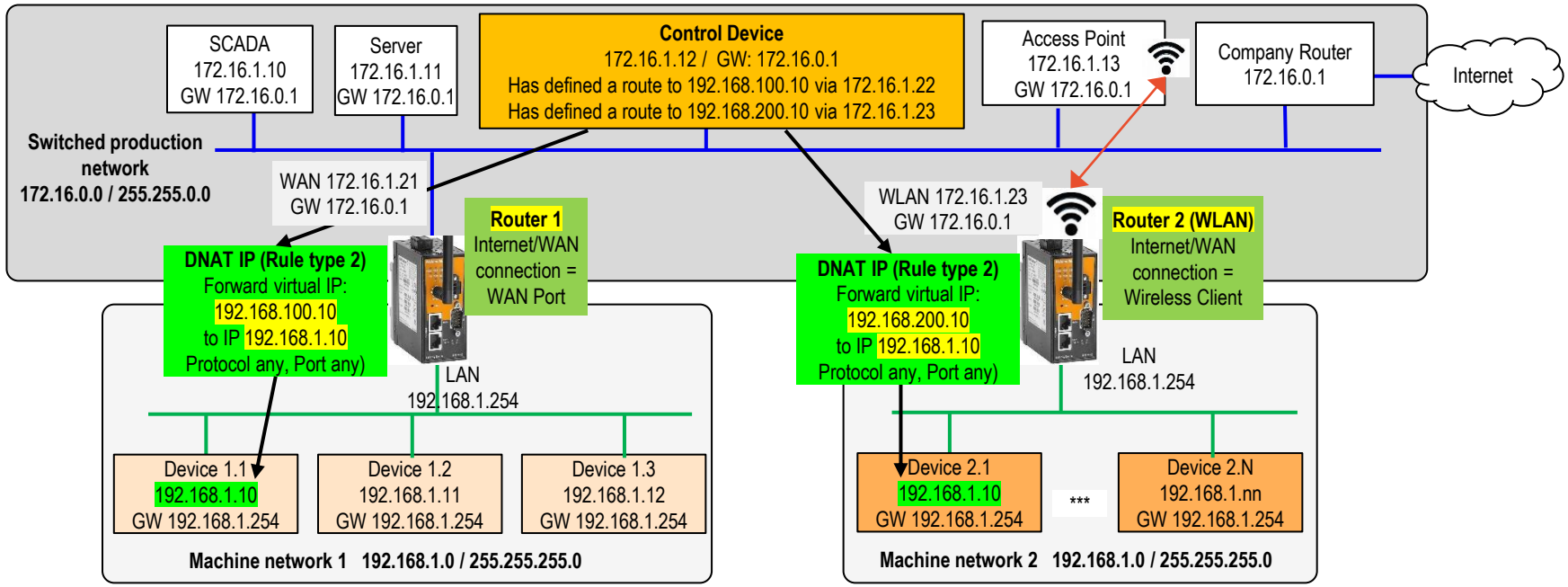
Apply Reset

Result: Modbus/TCP communication to Device 2.1 (real IP 192.168.1.10) can be established from WAN network via Router's IP 172.16.1.22.

Each IP packet incoming at **WLAN** interface with (Router's) destination IP 172.16.1.22, protocol TCP and port number 502 to will be forwarded to device with IP address 192.168.1.10.

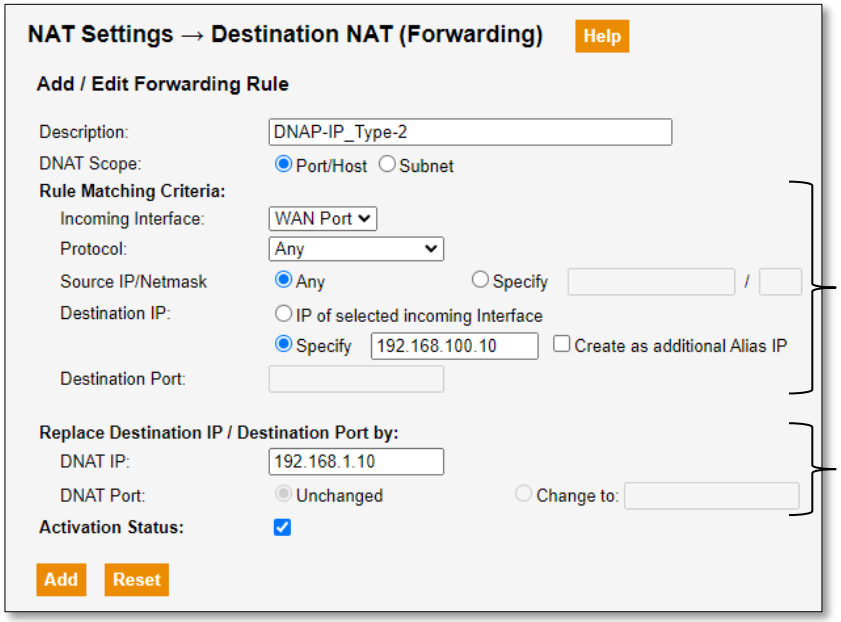
A1-3 Example of NAT type (2) 'DNAT IP' → IP forwarding (independent of used protocol/port) to a local (private) host via a virtual 'public' IP (1 / 3)

Task	Condition	Solution
• Control device shall have access to hidden (private) devices **Device 1.1** at machine network **1** and **Device 2.1** at machine network **2**.	• Devices 1.1 and 2.1, both having same IP address 192.168.1.10, must be accessible via unique IP addresses.	• Configure a DNAT rule on **Router 1** that each incoming packet with destination IP 192.168.100.10 (any free unused IP) and independent of used ‚Protocol' and ‚Destination port' will be forwarded to IP address 192.168.1.10 of the LAN network. • Configure a DNAT rule on **Router 2** that each incoming packet with destination IP 192.168.200.10 (any free unused IP) and independent of used ‚Protocol' and ‚Destination port' will be forwarded to IP address 192.168.1.10 of the LAN network. Note: This use case requires 2 routes configured on the control device or needs any other routing information that IP 192.168.100.10 is reachable via IP 172.16.1.21 and IP 192.168.200.10 accessible via IP 172.16.1.23.



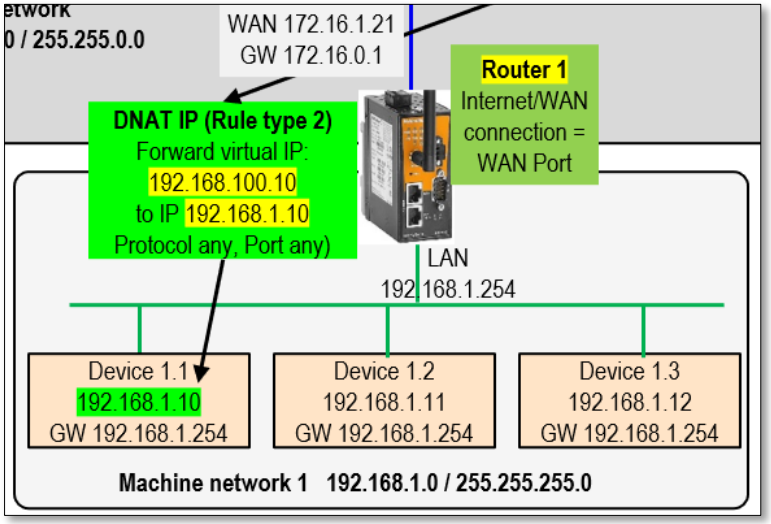
A1-3 Example of NAT type (2) 'DNAT IP' → IP forwarding (independent of used protocol/port) to a local (private) host via a virtual 'public' IP (2 / 3)

Configuration of rule „DNAT IP" on Router 1 according to illustrated application.

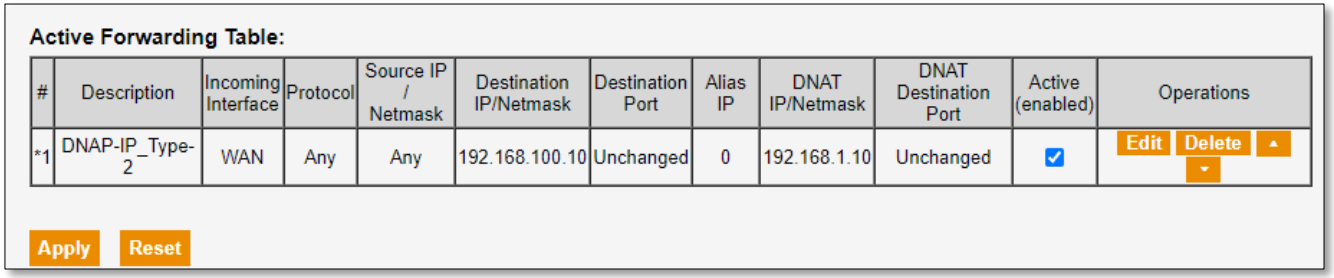


Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.



Active „DNAT IP" forwarding rule after applying:

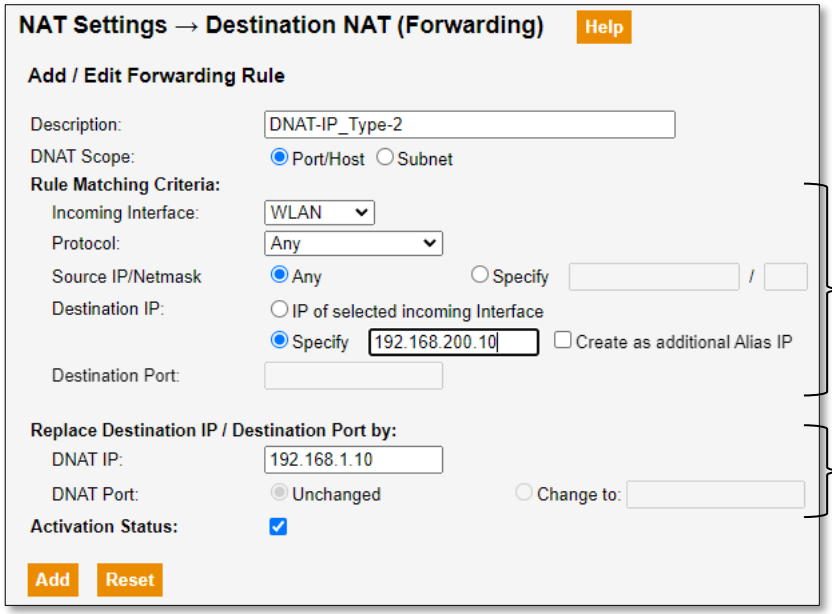


Result: Device 1.1 (real IP 192.168.1.10) can be accessed from WAN network via IP 192.168.100.10.

Each IP packet incoming at **WAN** interface with destination IP 192.168.100.10 will be forwarded independent of used protocol and port number to IP address 192.168.1.10.

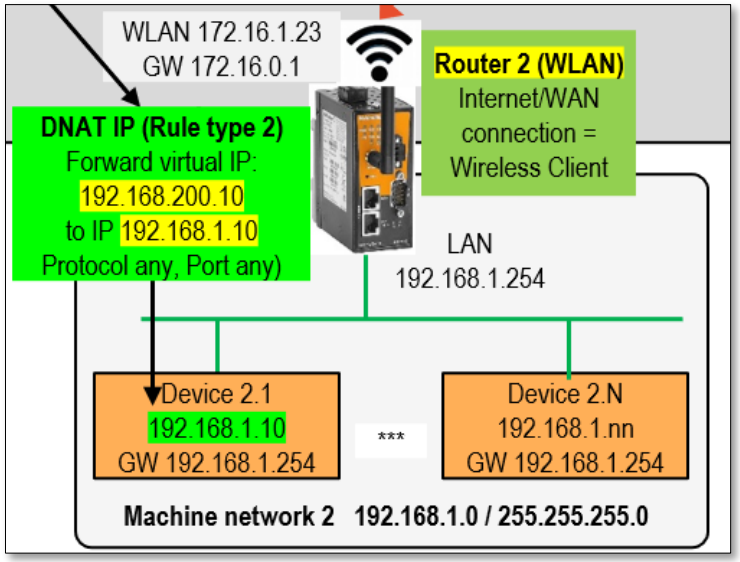
A1-3 Example of NAT type (2) 'DNAT IP' → IP forwarding (independent of used protocol/port) to a local (private) host via a virtual 'public' IP (3 / 3)

Configuration of rule „DNAT IP" on Router 2 (WLAN) according to illustrated application:

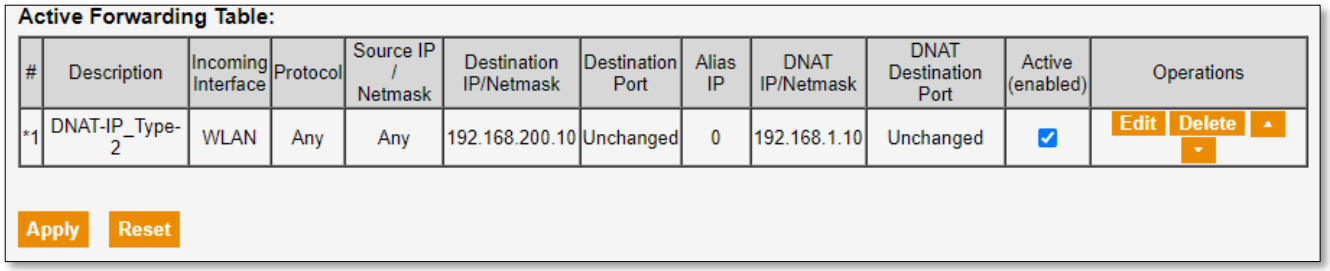


Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.



Active „DNAT IP" forwarding rule after applying:

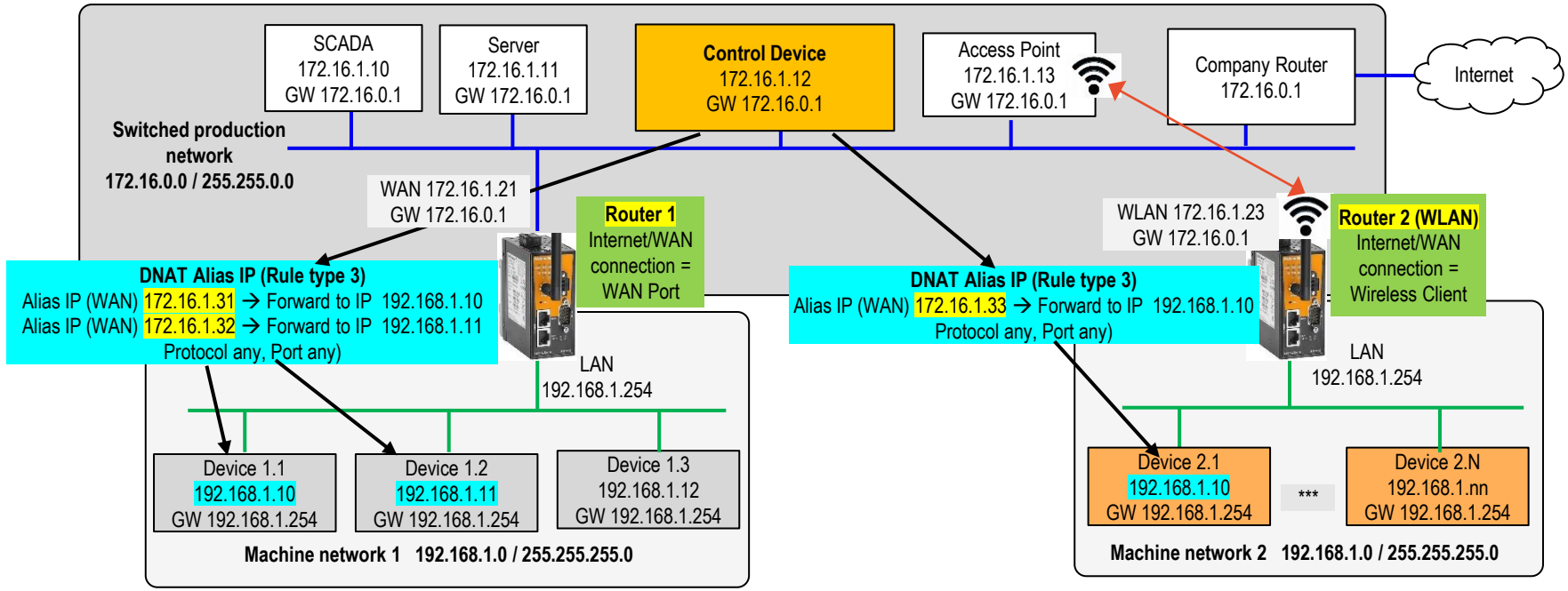


Result: Device 2.1 (real IP 192.168.1.10) can be accessed from WAN network via IP 192.168.200.10.

Each IP packet incoming at **WLAN** interface with destination IP 192.168.200.10 will be forwarded independent of used protocol and port number to IP address 192.168.1.10.

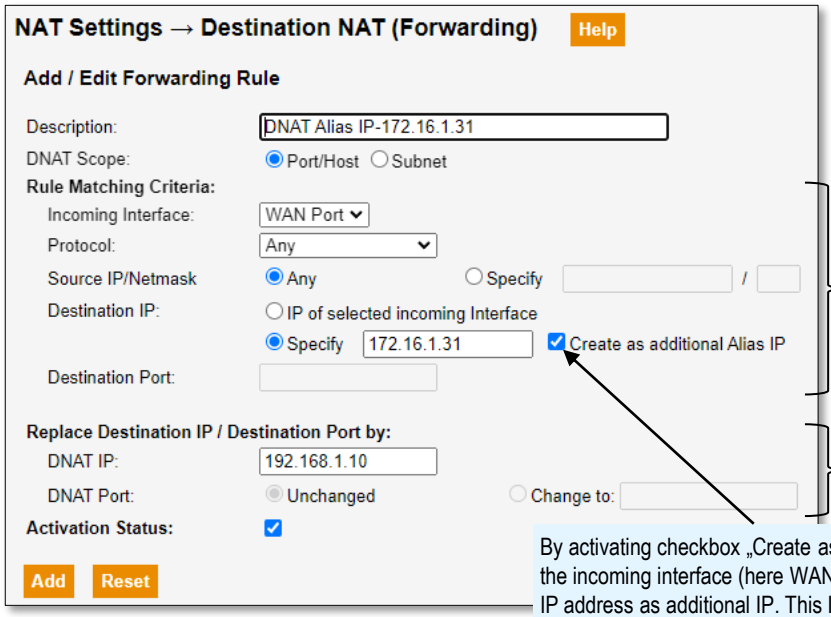
A1-4 Example of NAT type (3) 'DNAT Alias IP' → IP Forwarding to local (private) host based on additional Router IP (Alias IP) (1 / 3)

Task	Condition(s)	Solution
• Control device shall request data from hidden (private) devices ○ **Device 1.1**, **Device 1.2** at machine network **1** and ○ **Device 2.1** at machine network **2**.	• Gateway of control device is set to company router (172.16.0.1). • No routes can be configured on control device. • IP address range 172.16.1.30 to 40 is not used inside of class B production network 172.16.1.0 / 16.	• Configure first DNAT rule on **Router 1** including creation of an (additional) Alias IP 172.16.1.31 at WAN port that each incoming packet with destination IP 172.16.1.31 will be forwarded to LAN IP 192.168.1.10, independent of used protocol' and (destination) port. • Configure second DNAT rule on **Router 1** including creation of an (additional) Alias IP 172.16.1.32 at WAN port that each incoming packet with destination IP 172.16.1.32 will be forwarded to LAN IP 192.168.1.11, independent of used protocol' and (destination) port.. • Configure one DNAT rule on **Router 2** including creation of an (additional) IP 172.16.1.33 at WLAN interface that each incoming packet with destination IP 172.16.1.33 will be forwarded to LAN IP 192.168.1.10, independent of used protocol' and (destination) port.



A1-4 Example of NAT type (3) 'DNAT Alias IP' → IP Forwarding to local (private) host based on additional Router IP (Alias IP) (2 / 3)

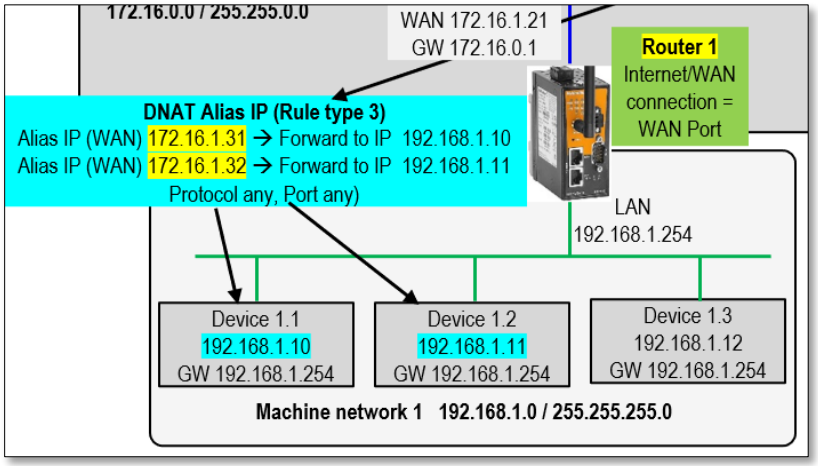
Configuration of first rule type „DNAT Alias IP" on Router 1 according to illustrated application:



Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.

By activating checkbox „Create as additional Alias IP" the incoming interface (here WAN Port) gets the defined IP address as additional IP. This IP address may not be used for any other network device to which the selected incoming interface is connected.



Active „DNAT Alias IP" rule after applying:

Active Forwarding Table:

#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT Alias IP-172.16.1.31	WAN	Any	Any	172.16.1.31	Unchanged	1	192.168.1.10	Unchanged	☑	Edit Delete
2	DNAT Alias IP-172.16.1.32	WAN	Any	Any	172.16.1.32	Unchanged	1	192.168.1.11	Unchanged	☑	Edit Delete

Apply Reset

Result: Device 1.1 (real IP 192.168.1.10) can be accessed from WAN network via additional Router IP 172.16.1.31.
Device 1.2 (real IP 192.168.1.11) can be accessed from WAN network via additional Router IP 172.16.1.32
No routing information is necessary for WAN devices because they can address these devices like being in their own IP subnet.

A1-4 Example of NAT type (3) 'DNAT Alias IP' → IP Forwarding to local (private) host based on additional Router IP (Alias IP) (3 / 3)

Configuration of rule type „DNAT Alias IP" on Router 2 (WLAN) according to illustrated application:

NAT Settings → Destination NAT (Forwarding) Help

Add / Edit Forwarding Rule

Description: DNAT Alias IP-172.16.1.33
DNAT Scope: (•) Port/Host ( ) Subnet
Rule Matching Criteria:
Incoming Interface: WLAN
Protocol: Any
Source IP/Netmask: (•) Any ( ) Specify /
Destination IP: ( ) IP of selected incoming Interface
(•) Specify 172.16.1.33 [x] Create as additional Alias IP
Destination Port:

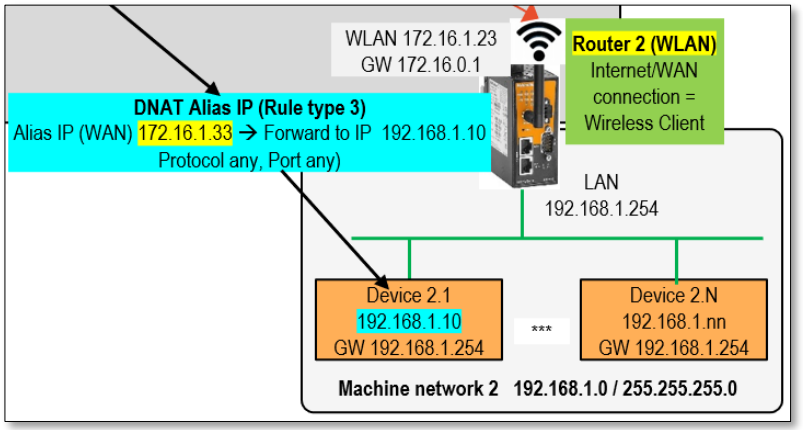
Replace Destination IP / Destination Port by:
DNAT IP: 192.168.1.10
DNAT Port: (•) Unchanged ( ) Change to:
Activation Status: [ ]

Edit Reset

Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target settings for packet redirection.

By activating checkbox „Create as additional Alias IP" the incoming interface (here WAN Port) gets the defined IP address as additional IP. This IP address may not be used for any other network device to which the selected incoming interface is connected.



Active „DNAT Alias IP" rule after applying:

Active Forwarding Table:

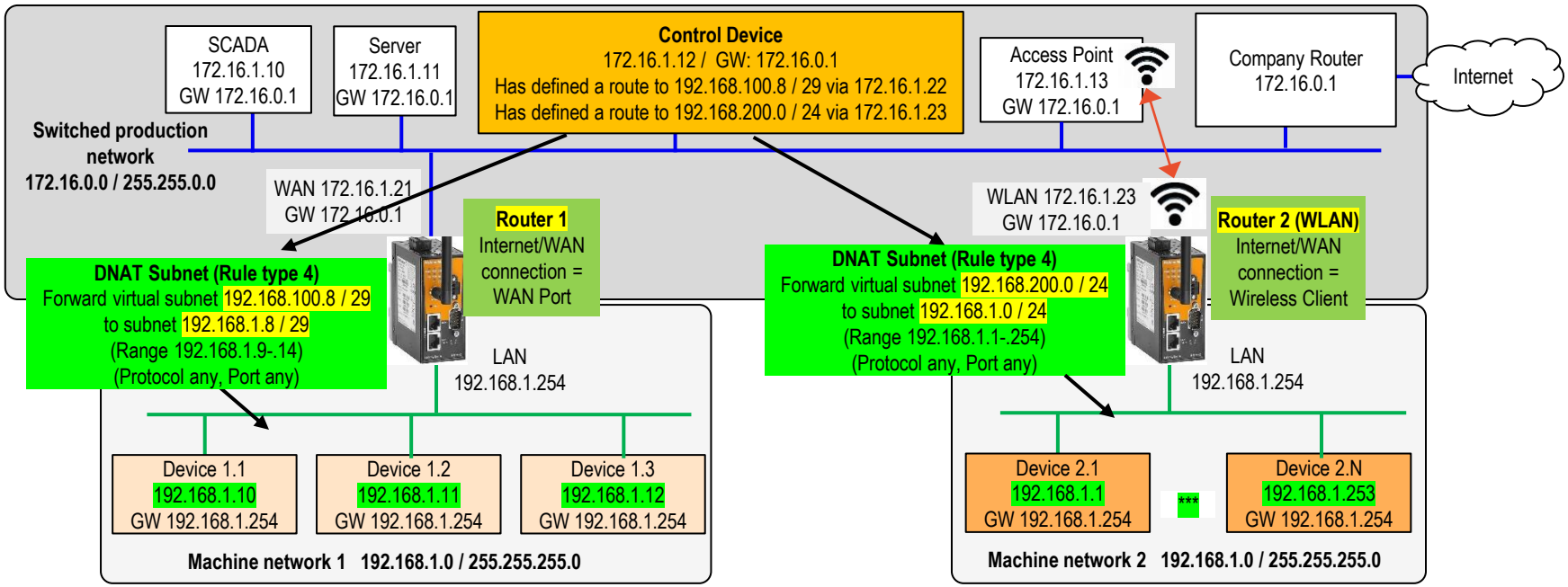
#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT Alias IP-172.16.1.33	WLAN	Any	Any	172.16.1.33	Unchanged	1	192.168.1.10	Unchanged	[ ]	Edit Delete ▲ ▼

Apply Reset

Result: Device 1.1 (real IP 192.168.1.10) can be accessed from WAN network via additional Router's Alias IP 172.16.1.33 (assigned to WLAN interface).
No routing information is necessary for WAN devices because this device can be addressed like being in their own IP subnet..

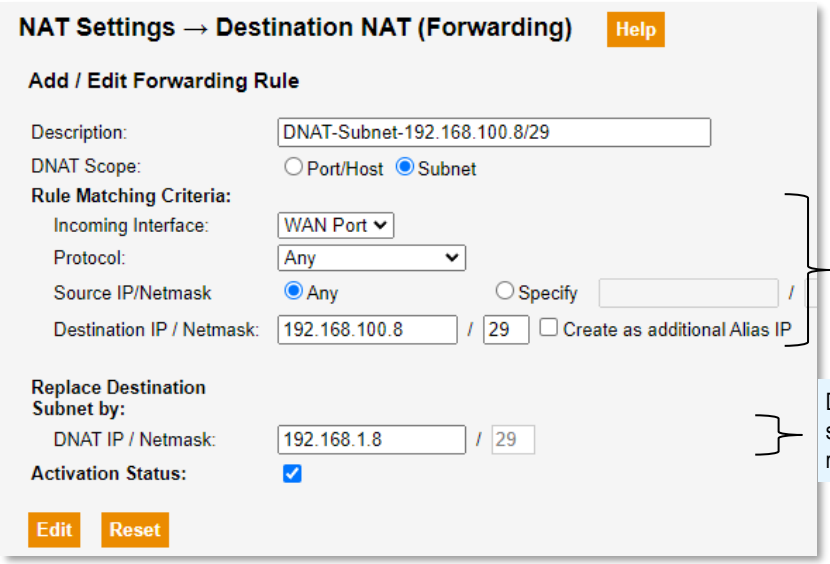
A1-5 Example of NAT type (4) 'DNAT IP Subnet' → IP subnet forwarding to a local (private) subnet via a virtual "public" IP range (1 / 3)

Task	Condition(s)	Solution
• Control device shall request data from hidden (private) devices – **Device 1.1** (192.168.1.10), **1.2** (192.168.1.11) **and 1.3** (192.168.1.12) of machine network **1** and – **all devices 2.1 to 2.N** (192.168.1.1 to 253) of machine network **2**.	• Devices of networks 1 and 2 - partly having same IP addresses - must be accessible via unique IP addresses.	• Create a DNAT rule on **Router 1** that each incoming packet with a destination IP of subnet 192.168.100.8 / 29 (Range 192.168.100.9 - .14) and based on used protocol (Any, TCP or UDP) will be forwarded to corresponding IP subnet 192.168.1.10 / 29 (IP addresses 192.168.1.9 - 14) of the LAN network. • Create a DNAT rule on **Router 2** that each incoming packet with destination IP subnet 192.168.200.0 / 24 (Range 192.168.200.1 to 254) and based on used protocol (Any, TCP or UDP) will be forwarded to corresponding IP range 192.168.1.0 / 24 (Range 192.168.1.1 to 254) of the LAN network . Note: This use case requires 2 routes configured on the control device or needs any other routing information that subnet 192.168.100.8 / 29 is reachable via WAN IP 172.16.1.21 and IP 192.168.200.0 / 24 is accessible via WAN IP 172.16.1.23.



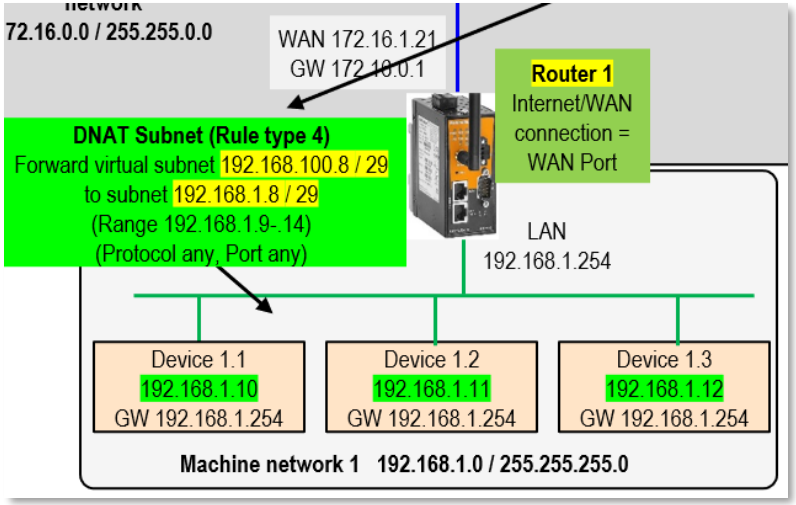
A1-5 Example of NAT type (4) 'DNAT IP Subnet' → IP subnet forwarding to a local (private) subnet via a virtual "public" IP range (2 / 3)

Configuration of rule type „DNAT IP Subnet" on Router 1 according to illustrated application:



Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target subnet for packet redirection.



Active „DNAT IP Subnet" rule after applying:

Active Forwarding Table:

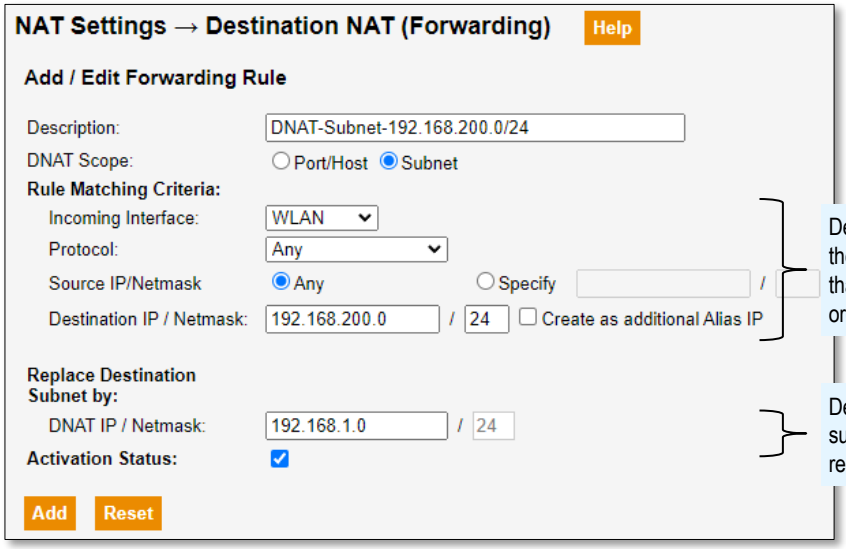
#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
*1	DNAT-Subnet-192.168.100.8/29	WAN	Any	Any	192.168.100.8/29	Unchanged	0	192.168.1.8/29	Unchanged	☑	Edit Delete

Apply Reset

Result: Device 1.1 (real IP 192.168.1.10) can be addressed from WAN network by virtual IP 192.168.100.10. Device 1.2 (real IP 192.168.1.11) can be addressed from WAN network by virtual IP 192.168.100.11.
Device 1.3 (real IP 192.168.1.12) can be addressed from WAN network by virtual IP 192.168.100.12.
Note: WAN devices need a route information that IP addresses 192.168.100.10/11/12 are accessible via Router's WAN IP 172.16.1.21.

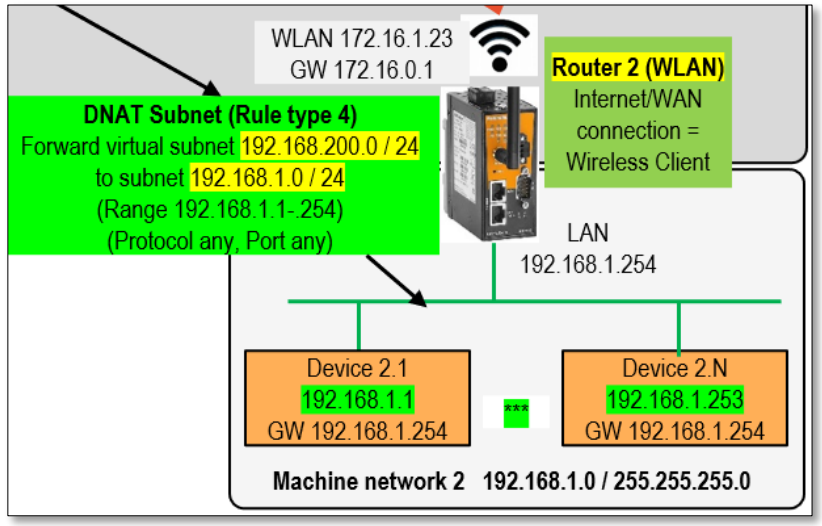
A1-5 Example of NAT type (4) 'DNAT IP Subnet' → IP subnet forwarding to a local (private) subnet via a virtual "public" IP range (3 / 3)

Configuration of rule type „DNAT IP Subnet" on Router 2 (WLAN) according to illustrated application:



Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target subnet for packet redirection.



Active „DNAT IP Subnet" rule after applying:

Active Forwarding Table:

#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT-Subnet-192.168.200.0/24	WLAN	Any	Any	192.168.200.0/24	Unchanged	0	192.168.1.0/24	Unchanged	☑	Edit Delete

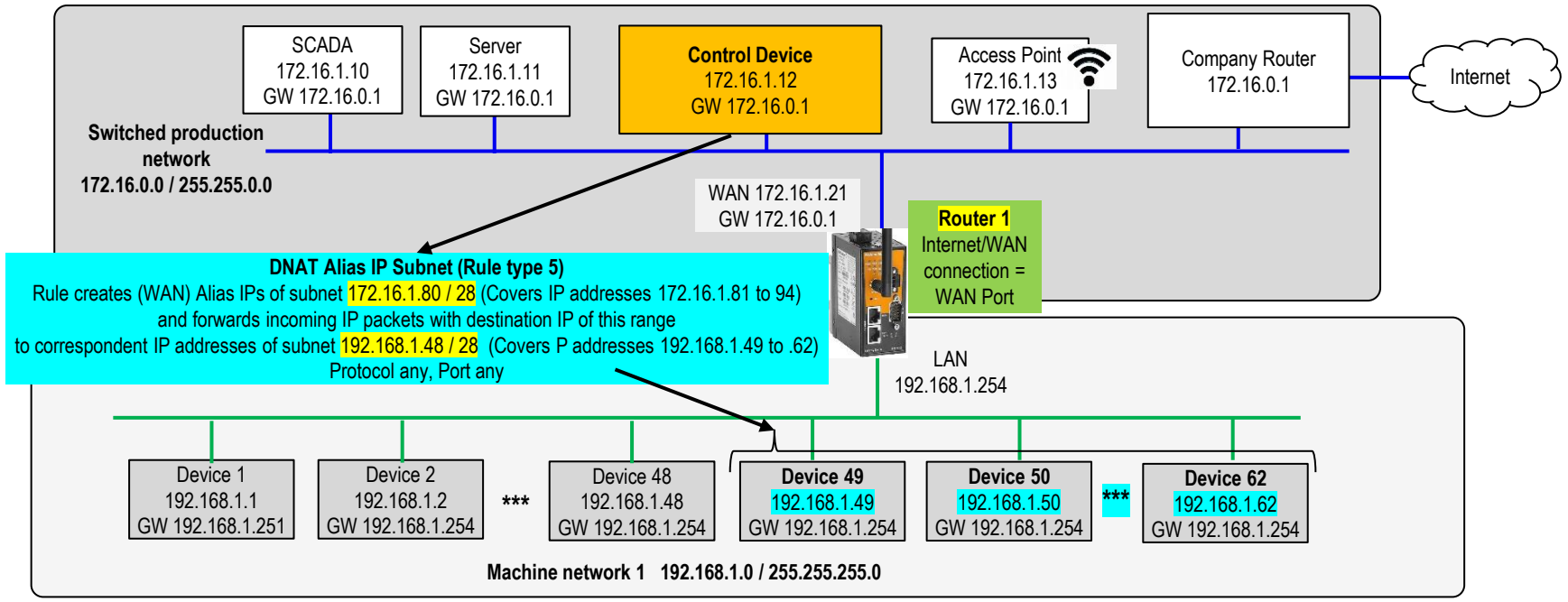
Apply Reset

Result: Each device of machine network 2 with real IP 192.168.1.xx can be accessed from WAN network via corresponding virtual IP 192.168.200.xx.

Note: WAN devices need a route information that IP subnet 192.168.200.0 is accessible via Router's WAN IP 172.16.1.23.

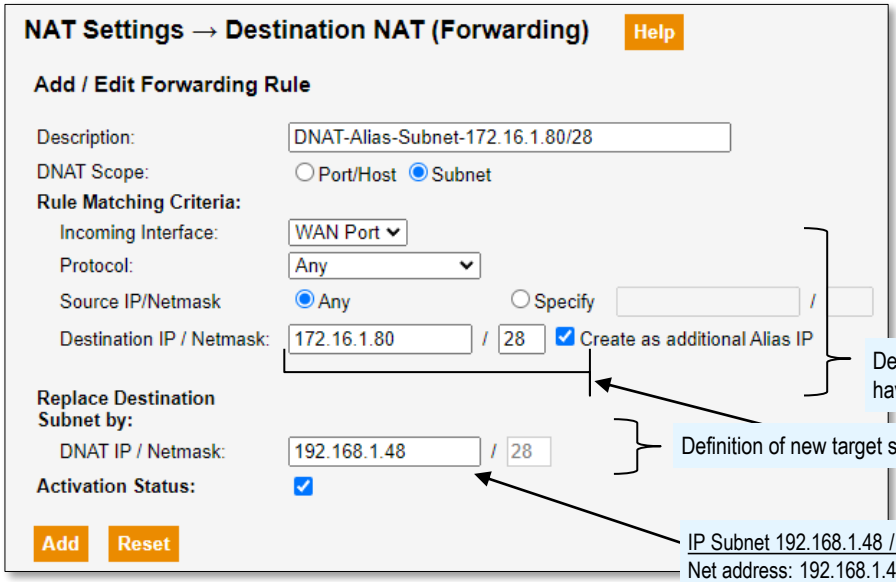
A1-6 Example of NAT type (5) 'DNAT Alias IP Subnet' → Forwarding of IP packets - addressed to virtual Router Alias IPs - to a real IP subnet (1 / 2)

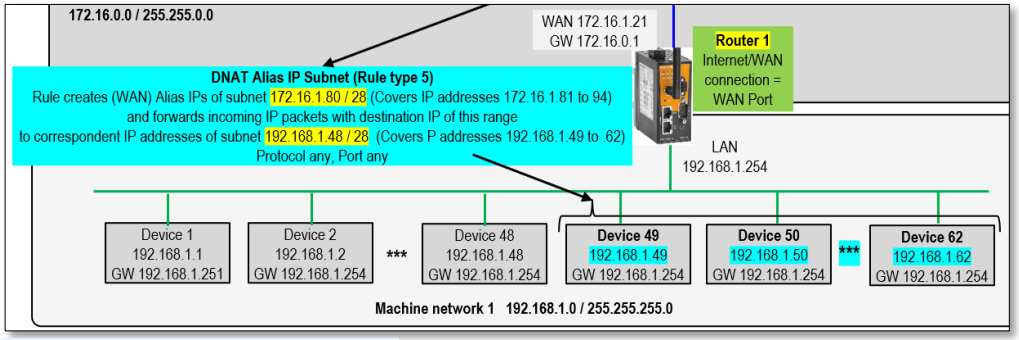
Task	Condition(s)	Solution
• Control device shall access units **Device 49** to **Device 62** of machine network **1**.	• Gateway of control device is set to company router (172.16.0.1). • No routes can be configured on the control device to access Router's LAN network devices. • IP address range 172.16.1.80 to 172.16.1.99 is not used inside of class B production network 172.16.1.0 / 16.	• Configure a DNAT rule on **Router 1** including creation of Alias IPs of subnet 172.16.1.80 / 28 (IP range 172.16.1.81 - 94) additional at WAN port that each incoming packet having a destination IP of this Alias IP subnet will be forwarded to the corresponding IP address of subnet 192.168.1.48 / 28 inside of the LAN network. Note: This example scenario forwards IP packets independent of used protocol (Any, TCP or UDP) but can be configured as additional criterion if necessary. .



A1-6 Example of NAT type (5) 'DNAT Alias IP Subnet' → Forwarding of IP packets - addressed to virtual Router Alias IPs - to a real IP subnet (2 / 2)

Configuration of rule type „DNAT Alias IP Subnet" on Router 1 according to illustrated application:





Definition of criteria for the incoming packet that have to match in order to be forwarded.

Definition of new target subnet for packet redirection.

IP Subnet 192.168.1.48 / 28:
Net address: 192.168.1.48
Host IP range : 192.168.1.49 to 62 (14 Hosts)
Broadcast address: 192.168.1.63

Alias IP Subnet 172.16.1.80 / 28:
Net address: 172.16.1.80
Host IP range : 172.16.1.81 to 94 (14 Hosts)
Broadcast address: 172.16.1.95

Active „DNAT Alias IP Subnet" rule after applying:

Active Forwarding Table:

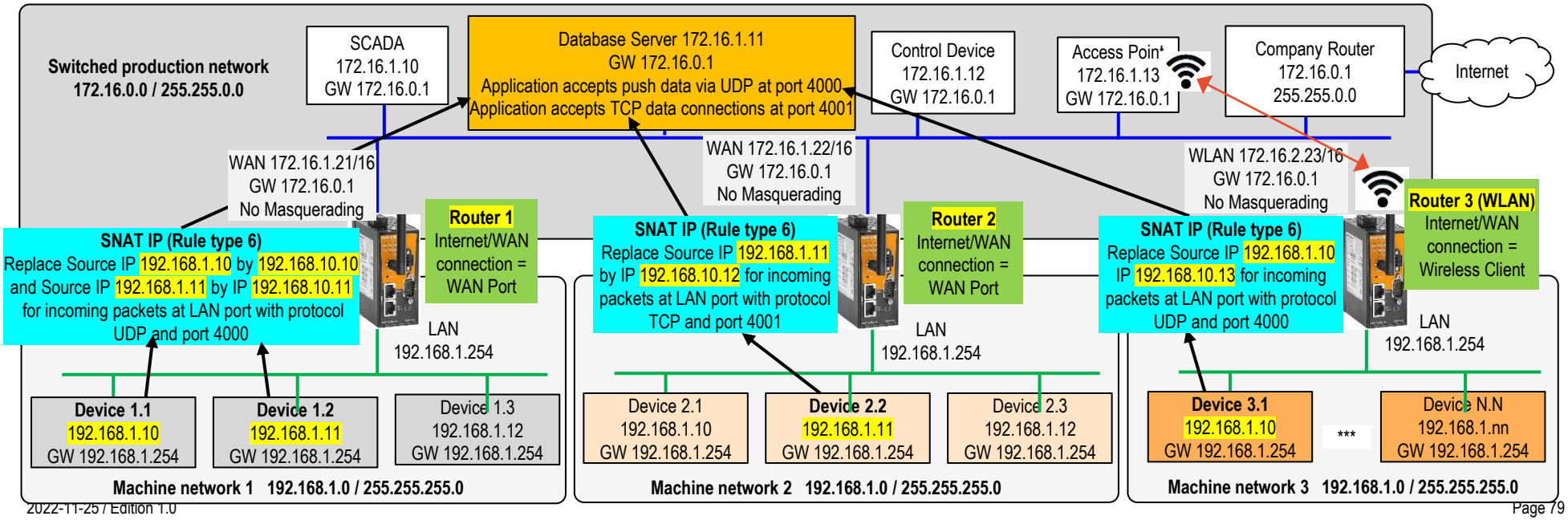
#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT-Alias-Subnet-172.16.1.80/28	WAN	Any	Any	172.16.1.80/28	Unchanged	1	192.168.1.48/28	Unchanged	☑	Edit Delete

Apply Reset

Result: Device 49 (real IP 192.168.1.49) can be accessed from WAN network via Router's Alias IP 172.16.1.81.
Device 50 (real IP 192.168.1.50) can be accessed from WAN network via Router's Alias IP 172.16.1.82.
…
Device 62 (real IP 192.168.1.62) can be accessed from WAN network via Router's Alias IP 172.16.1.94.

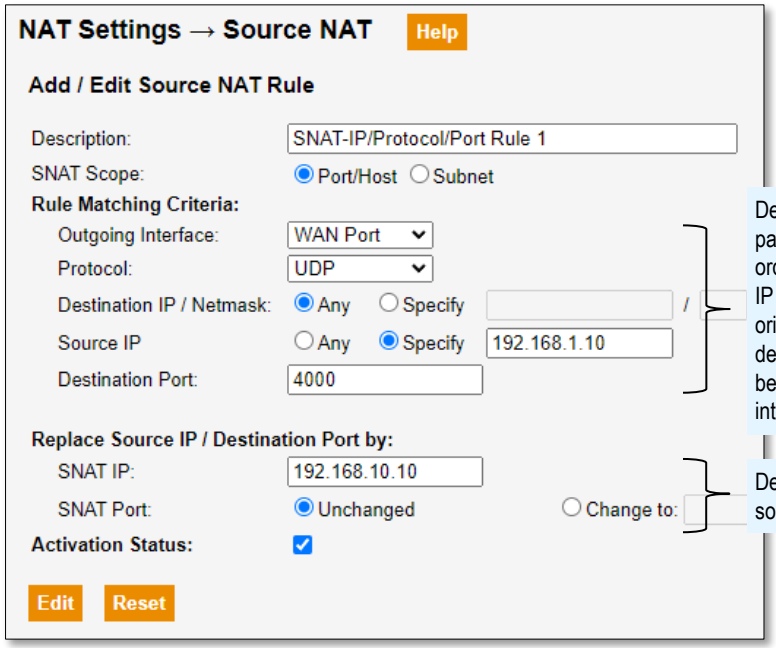
A1-7 Example of NAT type (6) 'SNAT IP Address' → Hiding a (local) host IP by a virtual 'public' IP for outgoing traffic (1 / 4)

Task	Condition(s)	Solution
• **Device 1.1**, **1.2**, **2.2** and **Device 3.1** located at **different** machine networks shall **push** any data to a database server located in the upper-level production network. • Devices 1.1, 1.2 and 3.1 push their data via protocol UDP / port 4000. • Device 2.2 establishes a TCP / 4001 socket and sends its data via this connection type.	• Due to network security reasons each device sending data to the database server shall be identified by a unique IP address (for example for evaluation by a Firewall in the communication path). • For this reason, masquerading at WAN port of the Routers may not be used.	• Create on **Router 1** two SNAT rules that replaces for each outgoing IP packet (at WAN port) - having source IP 192.168.1.10 respectively 192.168.1.11, protocol UDP and destination port 4000 - the source IP by 192.168.10.10 respectively IP 192.168.10.11 (any free unused IPs). New IPs 192.168.10.**10/11** will now become the „public" IPs for communication with the addressed database server. • Create on **Router 2** an SNAT rule that replaces for each outgoing IP packet (at WAN port) - having source IP 192.168.1.11, protocol TCP and destination port 4001 - the source IP by 192.168.10.12 (any free unused IP). If the TCP connection has been established, the replacement IP 192.168.10.12 becomes the „public" IP for the bidirectional communication between the devices. • Create on **Router 3** an SNAT rule that replaces for each outgoing IP packet (at WAN port) - having source IP 192.168.1.10, protocol UDP and destination port 4000 - the source IP by 192.168.10.13 (any free unused IP). If the TCP connection has been established, the replacement IP 192.168.10.13 becomes the „public" IP for the bidirectional communication between the devices. Note: These rules - **hiding private (local) IP addresses** by virtual public IP addresses - only can be applied for outgoing communication **initiated** by the LAN devices. If a local LAN device also shall be accessible via the configured virtual public IP - **initiated** from external devices - an IP DNAT rule (No. 2) needs to be configured additionally which forwards incoming IP packets addressed to the virtual public IP to the real device of the LAN network. Also consider that external devices need to have the routing information that virtual IPs are accessible via the Router's WAN interface IP.



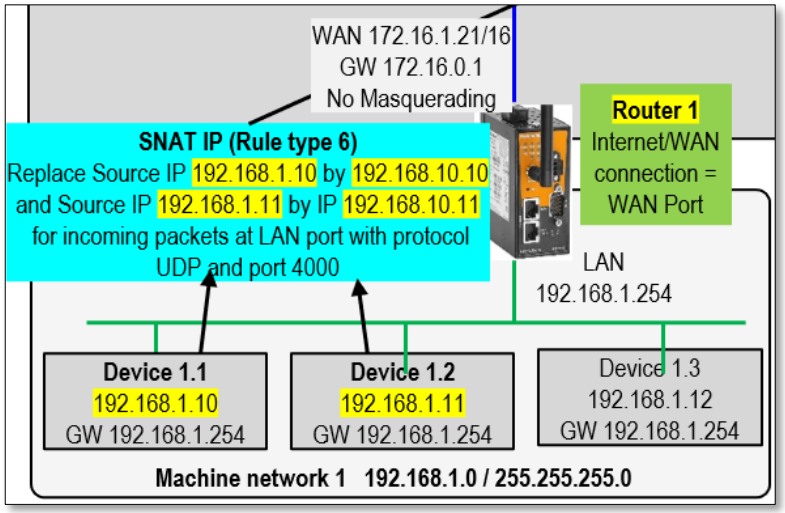
A1-7 Example of NAT type (6) 'SNAT IP Address' → Hiding a (local) host IP by a virtual 'public' IP for outgoing traffic (2 / 4)

Configuration of rule type „SNAT IP Address" at Router 1 according to illustrated application:



Definition of criteria for the packet that have to match in order to replace original source IP by defined SNAT IP and original destination port by defined SNAT port immediately before outgoing to defined interface.

Definition of replacements for source IP and destination port.



Active „SNAT IP Address" rules after applying:

Active SNAT Table :

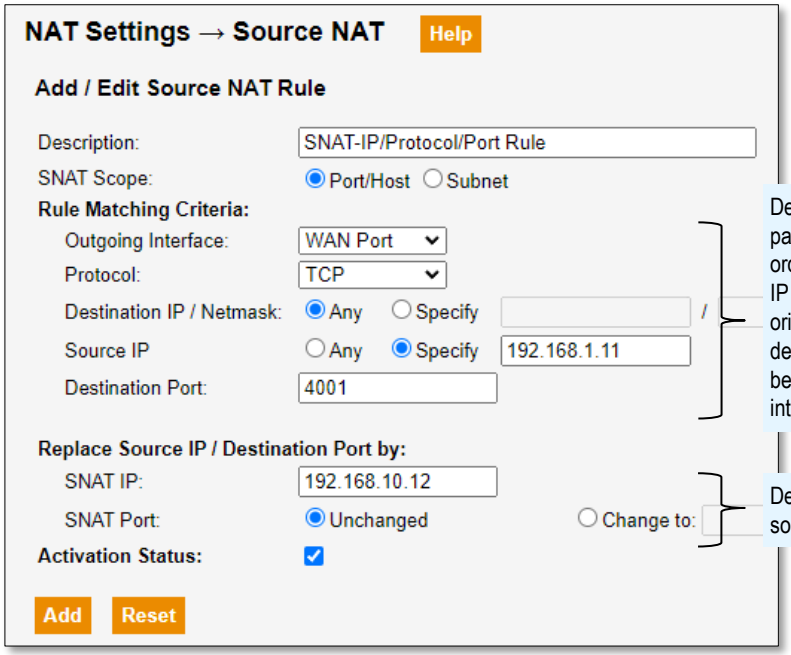
#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
*1	SNAT-IP/Protocol/Port Rule 1	WAN	UDP	Any	192.168.1.10	4000	192.168.10.10	Unchanged	☑	Edit Delete
*2	SNAT-IP/Protocol/Port Rule 2	WAN	UDP	Any	192.168.1.11	4000	192.168.10.11	Unchanged	☑	Edit Delete

Apply Reset

Result: When Device 1.1 (real IP 192.168.1.10) sends any data using protocol UDP and port 4000 it will be identified by the receiver via IP address 192.168.10.10.
When Device 1.2 (real IP 192.168.1.11) sends any data using protocol UDP and port 4000 it will be identified by the receiver via IP address 192.168.10.11.

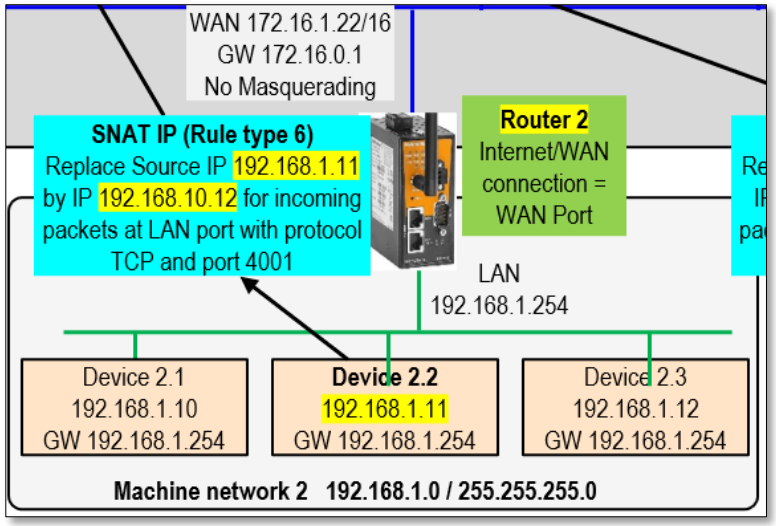
A1-7 Example of NAT type (6) 'SNAT IP Address' → Hiding a (local) host IP by a virtual 'public' IP for outgoing traffic (3 / 4)

Configuration of rule type „SNAT IP Address" at Router 2 according to illustrated application:



Definition of criteria for the packet that have to match in order to replace original source IP by defined SNAT IP and original destination port by defined SNAT port immediately before outgoing to defined interface.

Definition of replacements for source IP and destination port.



Active „SNAT IP Address" rule after applying:

Active SNAT Table :

#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
*1	SNAT-IP/Protocol/Port Rule	WAN	TCP	Any	192.168.1.11	4001	192.168.10.12	Unchanged	☑	Edit Delete

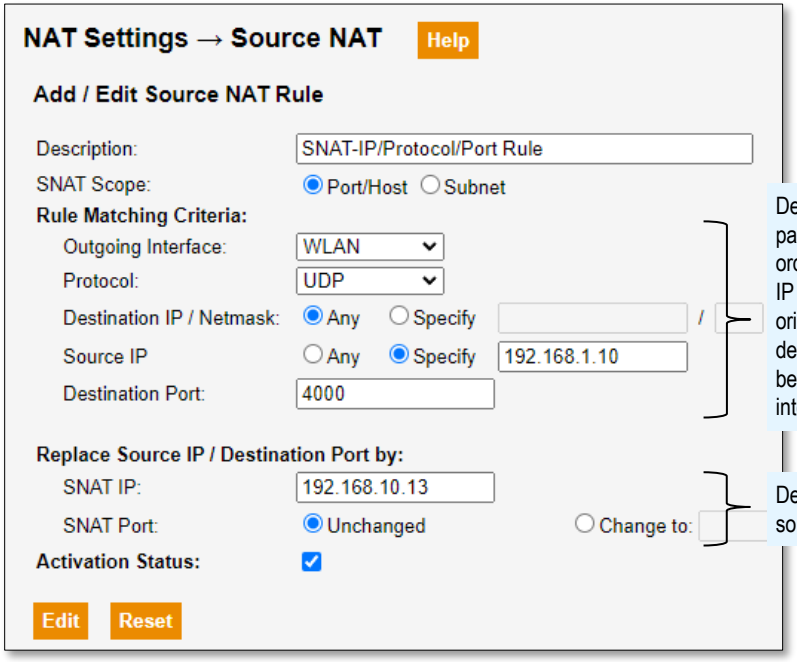
Apply Reset

Result: When Device 2.2 (real IP 192.168.1.11) initiates a TCP connection to any WAN device using port 4001 then it will be identified by the counterpart of the TCP socket by IP address 192.168.10.12 allowing a bidirectional socket data exchange.

Consider: An addressed WAN device needs a route information that a request from IP 192.168.10.12 has to be replied via Router's WAN IP 172.16.1.22.

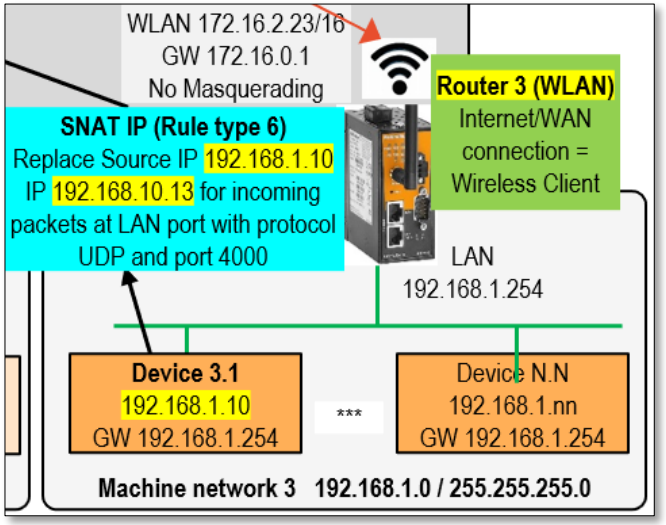
A1-7 Example of NAT type (6) 'SNAT IP Address' → Hiding a (local) host IP by a virtual 'public' IP for outgoing traffic (4 / 4)

Configuration of rule type „SNAT IP Address“ at Router 3 (WLAN) according to illustrated application:



Definition of criteria for the packet that have to match in order to replace original source IP by defined SNAT IP and original destination port by defined SNAT port immediately before outgoing to defined interface.

Definition of replacements for source IP and destination port.



Active „SNAT IP Address“ rule after applying:

Active SNAT Table :

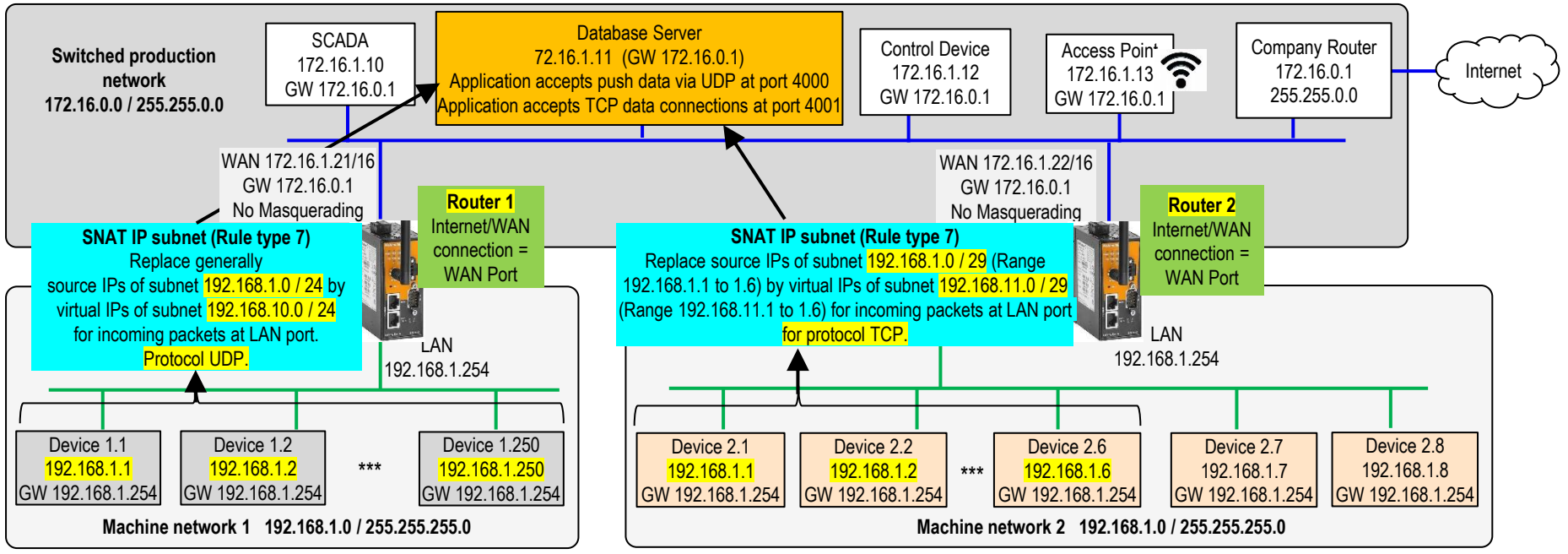
#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
*1	SNAT-IP/Protocol/Port Rule	WLAN	UDP	Any	192.168.1.10	4000	192.168.10.13	Unchanged	☑	Edit Delete

Apply Reset

Result: When Device 3.1 (real IP 192.168.1.10) sends any data using protocol UDP and port 4000 it will be identified by the receiver via IP address 192.168.10.13.

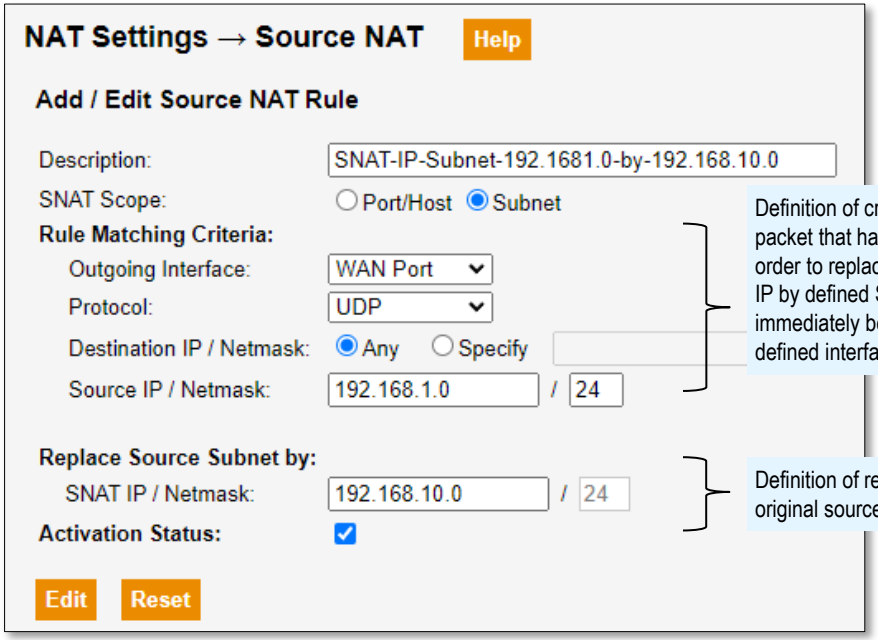
A1-8 Example of NAT type (7) 'SNAT IP Subnet' → Hiding a (local) IP subnet by a virtual "public" IP subnet for outgoing traffic (1 / 3)

Task	Condition(s)	Solution
• **All devices** of machine network **1** (Class C) shall push any data to the database server located in the upper-level production network via protocol UDP. • **Devices 2.2 to 2.6** of machine network **2** (Class C) shall send their data to the database server via connection type TCP.	• Due to network security reasons each device sending data to the database server shall be identified by a unique IP address (for example for evaluation by a Firewall in between of the communication path). • For this reason, masquerading (N:1 NAT) at WAN port of a Router may not be used.	• Configure an SNAT rule on **Router 1** that replaces for each incoming IP packet at LAN port - having a source IP of subnet 192.168.1.0/24 and protocol UDP - the source IP with corresponding IP of virtual public IP subnet 192.168.10.0 / 24. (any free unused IP range). Note: Subnet masks for replacing original source IPs to a new virtual IP range must be identical. • Configure an SNAT rule on **Router 2** that replaces for an incoming IP packet at LAN port - having a source IP of subnet 192.168.1.0 / 29 (IP range 192.168.1.1 to 1.6) and protocol TCP - the source IP with corresponding IP of subnet 192.168.11.0 / 29. ○ Consider: For establishing a TCP connection initiated from a device of machine network 2 to the database server using the SNAT rule, a route needs to be set on the database server that virtual IPs 192.168.11.1 to 192.168.11.6 are accessible via Router's WAN IP 172.16.1.22. Note: These rules - intended to hide private (local) IP addresses by virtual public IP addresses - only can be applied for an IP communication which is initated by a (local) LAN device. If an IP communication also shall be initiated from external devices by addressing a configured virtual public IP, then an IP DNAT rule (No. 2) needs to be configured additionally which forwards incoming IP packets - addressed to the virtual public IP - to the real device of the LAN network.



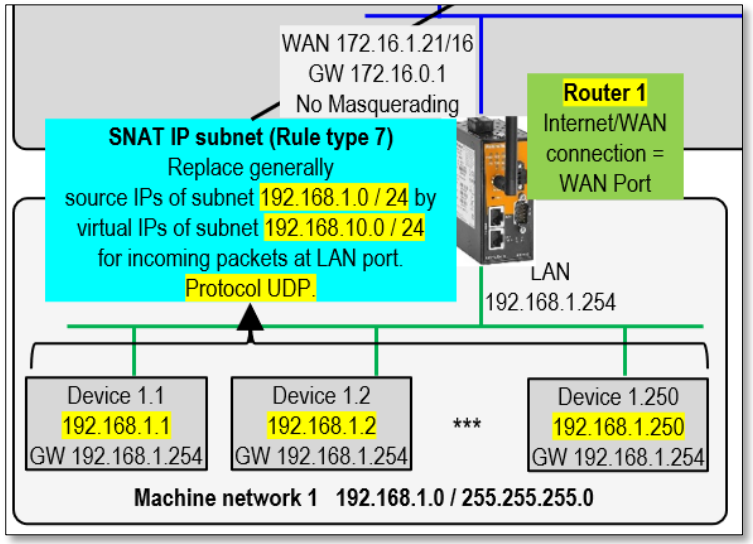
A1-8 Example of NAT type (7) 'SNAT IP Subnet' → Hiding a (local) IP subnet by a virtual "public" IP subnet for outgoing traffic (2 / 3)

Configuration of rule type „SNAT IP Subnet" at Router 1 according to illustrated application:



Definition of criteria for the packet that have to match in order to replace original source IP by defined SNAT IP immediately before outgoing to defined interface.

Definition of replacement IPs for original source IPs.



Active „ SNAT IP Subnet" rule after applying:

Active SNAT Table :

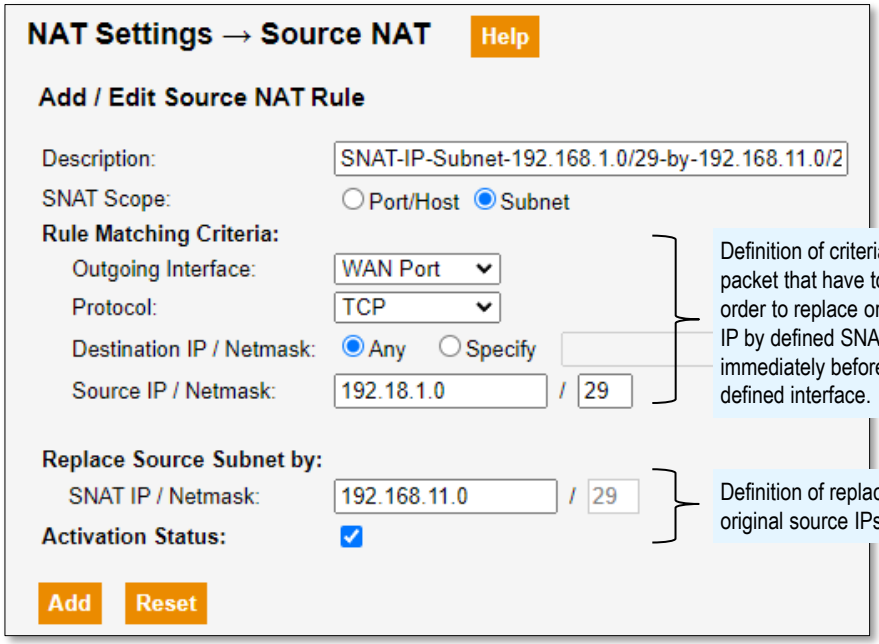
#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
1	SNAT-IP-Subnet-192.1681.0-by-192.168.10.0	WAN	Any	Any	192.168.1.0/24	Unchanged	192.168.10.0/24	Unchanged	☑	Edit Delete

Apply Reset

Result: For each device connected to LAN port the original source IP (any IP of subnet 192.168.1.0 / 24) will be replaced by the corresponding „virtual" IP of subnet 192.168.10.0 / 24 for outging IP packets sent by the LAN devices.

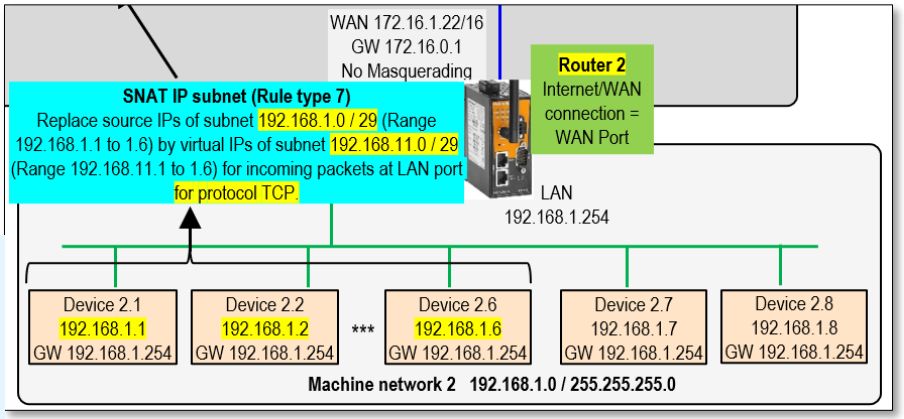
A1-8 Example of NAT type (7) 'SNAT IP Subnet' → Hiding a (local) IP subnet by a virtual "public" IP subnet for outgoing traffic (3 / 3)

Configuration of rule type „SNAT IP Subnet" at Router 2 according to illustrated application:



Definition of criteria for the packet that have to match in order to replace original source IP by defined SNAT IP immediately before outgoing to defined interface.

Definition of replacement IPs for original source IPs.



Active „ SNAT IP Subnet" rule after applying:

Active SNAT Table :

#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
*1	SNAT-IP-Subnet-192.168.1.0/29-by-192.168.11.0/29	WAN	TCP	Any	192.18.1.0/29	Unchanged	192.168.11.0/29	Unchanged	☑	Edit Delete

Apply Reset

Result: For outgoing IP packets sent by LAN devices of IP range 192.168.1.1 to 192.168.1.6 the original source IP will be replaced by the corresponding „virtual" IP of range 192.168.11.1 to 192.168.11.6.

Note: If one of these LAN devices initiates a TCP connection to an outside target device a route needs to be configured on the target device that requests coming from a virtual IP of range 192.168.11.1 to 192.168.11.6 can be replied via Router's WAN IP 172.16.1.22.

A1-9 Example of full 1:1 NAT applied for an IP subnet → Hiding a local IP subnet by a virtual 'public' IP subnet for any traffic with external devices (1 / 2)

Task

- Control device shall request data from (private) devices of machine network 1. The communication will be initiated by the control device, either via UDP or by establishing a TCP connection.
- The database server is acting as passive device and will be requested by machine network devices (communication initiators), either via UDP or by establishing a TCP connection.
- Due to future planned expansions – adding identical machines having same device IP addresses – virtual IP addresses shall be used for machine network devices for communication with the production network. This ensures, that after expansion realization each device can be accessed and identified by a unique „virtual" IP address.

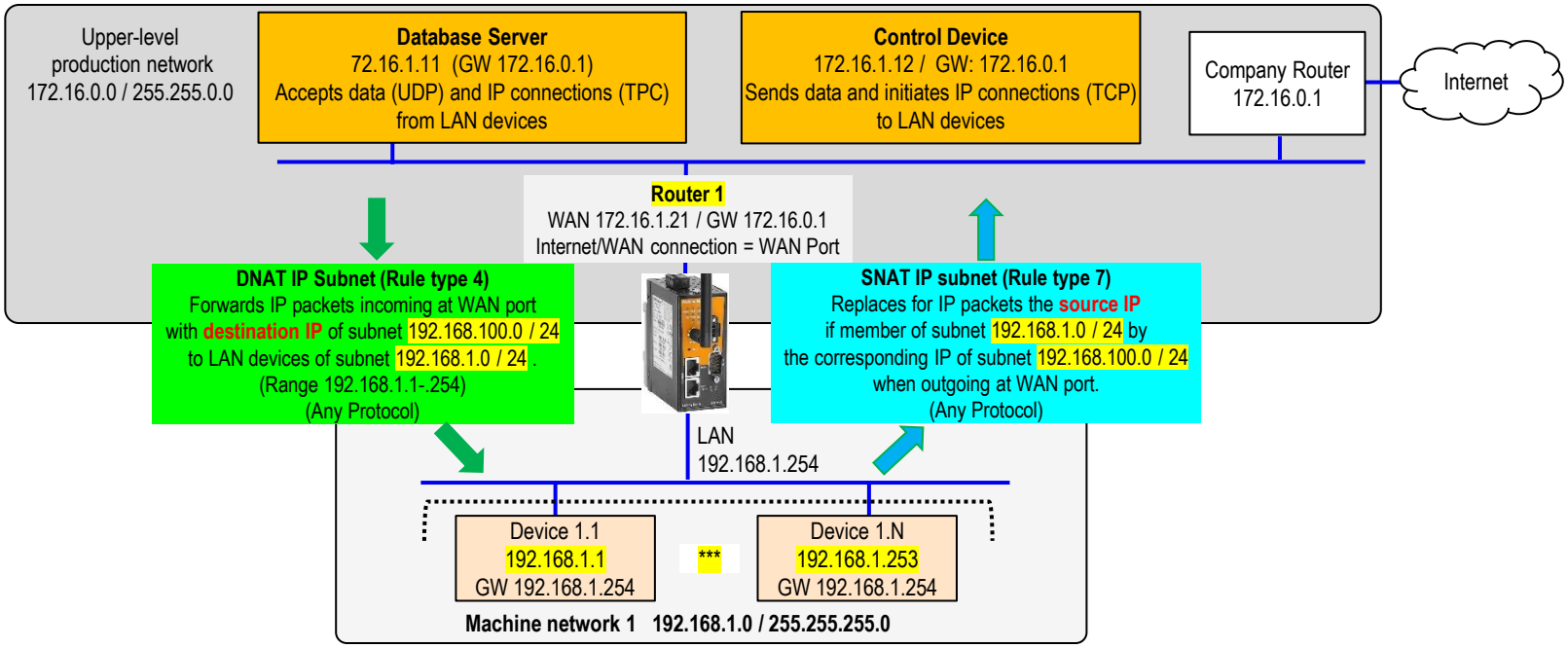
Solution

- Configure a DNAT rule on **Router 1** that each incoming packet at WAN port with destination IP of subnet 192.168.100.0 / 24 (Range 192.168.100.1 - 254) independent of used protocol and port will be forwarded to corresponding IP of range 192.168.1.0 / 24 (Range 192.168.1.1 - 254) of the LAN network.
- Configure an SNAT rule on **Router 1** that replaces for each incoming IP packet at LAN port - having a source IP of subnet 192.168.1.0 / 24 - the source IP with corresponding IP of virtual public IP subnet 192.168.100.0 / 24. (any free unused IP range). Note: Subnet masks for replacing original source IPs to a new virtual IP range must be identical.

Note: For addressing the machine network devices via their virtual (public) IP addresses the control device must have configured a route that subnet 192.168.100.0 / 24 is reachable via WAN IP 172.16.1.21.

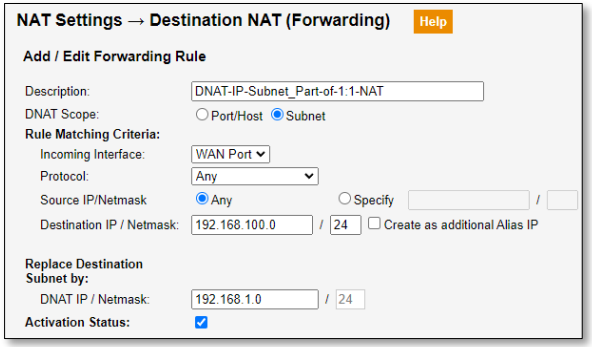
Result

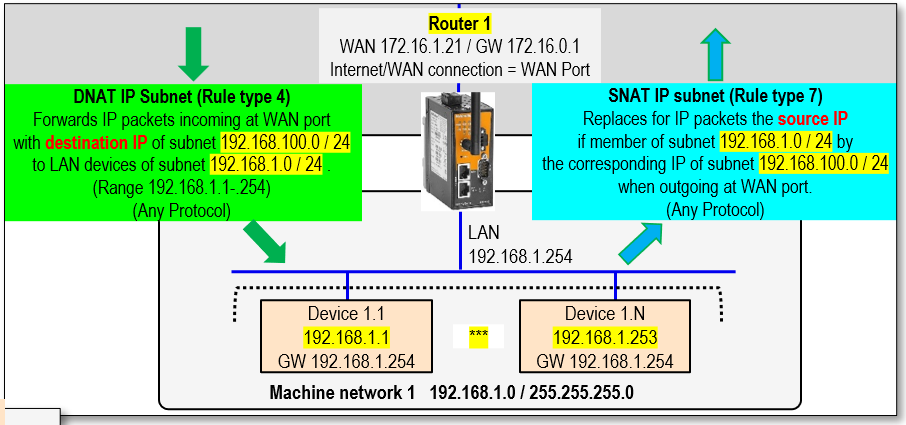
- Each device of the machine network is accessible by its virtual (public) IP address
- Each machine network device is identified by its virtual (public) IP for both communication directions.
- The use of the DNAT/SNAT rule combination allows the initiation of a communication from both sides, the local LAN and outside WAN network.



A1-9 Example of full 1:1 NAT applied for an IP subnet → Hiding a local IP subnet by a virtual 'public' IP subnet for any traffic with external devices (2 / 2)

Configuration of rule type „DNAT IP Subnet" at Router 1 according to illustrated application:



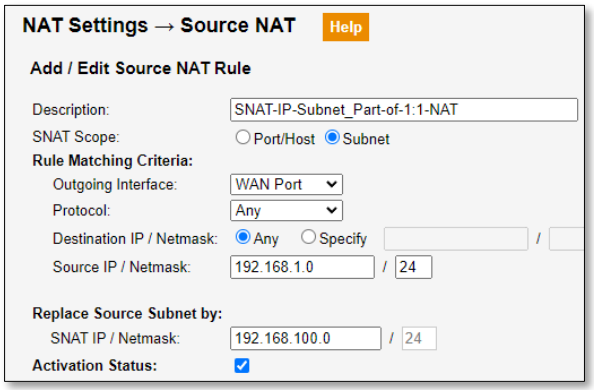


Active „ DNAT IP Subnet" rule after applying

Active Forwarding Table:

#	Description	Incoming Interface	Protocol	Source IP / Netmask	Destination IP/Netmask	Destination Port	Alias IP	DNAT IP/Netmask	DNAT Destination Port	Active (enabled)	Operations
1	DNAT-IP-Subnet_Part-of-1:1-NAT	WAN	Any	Any	192.168.100.0/24	Unchanged	0	192.168.1.0/24	Unchanged	☑	Edit Delete

Configuration of rule type „SNAT IP Subnet" at Router 1 according to illustrated application:



Active „ SNAT IP Subnet" rule after applying

Active SNAT Table :

#	Description	Outgoing Interface	Protocol	Destination IP / Netmask	Source IP/Netmask	Destination Port	SNAT IP/Netmask	SNAT Destination Port	Active (enabled)	Operations
1	SNAT-IP-Subnet_Part-of-1:1-NAT	WAN	Any	Any	192.168.1.0/24	Unchanged	192.168.100.0/24	Unchanged	☑	Edit Delete

Result: Each device of the machine network is accessible from outside by its virtual (public) IP address and is identified by its virtual (public) IP for communication initiated by the machine network device.

Note: If one of the LAN devices initiates a TCP connection to an outside target device a route needs to be configured on the target device that requests coming from an IP of subnet 192.168.100.0/24 can be replied via Router's WAN IP 172.16.1.21.