TURCK

Your Global Automation Partner

TBEN-L…-SE-M2
10-Port Ethernet Switch

Instructions for Use

Table of Contents

1 About these instructions

These instructions describe the setup, functions and use of the product and help you to operate the product according to its intended purpose. Read these instructions carefully before using the product. This will prevent the risk of personal injury and damage to property. Keep these instructions safe during the service life of the product. If the product is passed on, pass on these instructions as well.

1.1 Target groups

These instructions are written for specifically trained personnel and must be read carefully by anyone entrusted with the installation, commissioning, operation, maintenance, disassembly or disposal of the device.

When using the device in Ex areas, the user must also have knowledge of explosion protection (IEC/EN 60079-14 etc.).

1.2 Explanation of symbols

The following symbols are used in these instructions:

	**DANGER** DANGER indicates a hazardous situation with a high level of risk, which, if not avoided, will result in death or serious injury.
	**WARNING** WARNING indicates a hazardous situation with a medium level of risk, which, if not avoided, will result in death or serious injury.
	**CAUTION** CAUTION indicates a hazardous situation with a medium level of risk, which, if not avoided, will result in moderate or minor injury.
	**NOTICE** CAUTION indicates a situation which, if not avoided, may cause damage to property.
	**NOTE** NOTE indicates tips, recommendations and important information about special action steps and issues. The notes simplify your work and help you to avoid additional work.
▶	**MANDATORY ACTION** This symbol denotes actions that the user must carry out.
⇨	**RESULT OF ACTION** This symbol denotes the relevant results of an action.

1.3 Additional documents

The following additional documents are available online at **www.turck.com**

- Data sheet
- Declarations of conformity (current version)
- Notes on Use in Ex zone 2 and 22 (100022986)
- Approvals

1.4 Feedback about these instructions

We make every effort to ensure that these instructions are as informative and as clear as possible. If you have any suggestions for improving the design or if some information is missing in the document, please send your suggestions to **techdoc@turck.com**.

2 Notes on the product

2.1 Product identification

These instructions are valid for the following manageable IP67-Switches:

- TBEN-L4-SE-M2 (ID 100004426)
- TBEN-L5-SE-M2 (ID 100004425)
- TBEN-LL-SE-M2 (ID 100004427)

2.2 Open source software

The device contains open source software. All licenses used in the device are available on the device's web server under "Documentation" → "Licences".

2.3 Scope of delivery

The delivery consists of the following:

- TBEN switch
- Closing caps for M12 sockets
- Labelling clips

2.4 Turck service

Turck supports you in your projects – from the initial analysis right through to the commissioning of your application. The Turck product database at www.turck.com offers you several software tools for programming, configuring or commissioning, as well as data sheets and CAD files in many export formats.

For the contact details of our branches worldwide, please see page [▷ 150].

3 For your safety

The product is designed according to state of the art technology. Residual hazards, however, still exist. Observe the following safety instructions and warnings in order to prevent danger to persons and property. Turck accepts no liability for damage caused by failure to observe these safety instructions.

3.1 Intended use

The manageable switch manageable Switch TBEN-L…-SE-M2 is used within a machine or cell for decentralized connection of Industrial Ethernet devices to controllers. Line, star, ring and mixed topologies are supported. With its integrated firewall, NAT routing, the VLAN function and a second configurable Ethernet interface (designated as WAN), the device is used to network machine cells or to integrate machines into higher-level factory networks. The device is only suitable for use in Local Area Networks.

The switch can be integrated into an Ethernet network as a PROFINET or EtherNet/IP device or Modbus TCP server for network monitoring.

Installation directly in the field is possible thanks to degree of protection IP65, IP67 IP67K. Devices with the Ex marking are suitable for use in the Ex area in zone 2 and zone 22.

The device must only be used as described in these instructions. Any other use is not in accordance with the intended use. Turck accepts no liability for any resulting damage.

3.2 General safety instructions

- The device must only be fitted, installed, operated, parameterized and maintained by trained and qualified personnel.
- Only use the device in compliance with the applicable national and international regulations, standards and laws.
- The device meets the EMC requirements for the industrial areas. When used in residential areas, take measures to prevent radio frequency interference.
- Change the default password of the integrated web server after the first login. Turck recommends the use of a secure password.

3.3 Notes on UL approval

- Use UL certified PVVA or CYJV cables that are suitable for the current/voltage rating and have an insulation temperature of at least 80 °C.
- Only use the device in an area of not more than pollution degree 2.
- The TBEN-L…-SE-M2 is only suitable for use in LAN networks.

3.4 Notes on Ex protection

- When using the device in Ex areas, the user must have knowledge of explosion protection (IEC/EN 60079-14 etc.).
- Observe national and international regulations for explosion protection.
- Only use the device within the permissible operating and ambient conditions (see certification data and Ex approval specifications).
- The document "Notes on Use in Ex Zone 2 and 22" (ID 100022986) contains the approval data for using the device in hazardous areas. Observe the requirements in the document.

3.5 Requirements for Ex approval

- Only use the device in an area with no more than pollution degree 2.
- Only disconnect and connect circuits when there is no potentially explosive atmosphere or when the power supply is switched off
- Only operate the switches when there is no potentially explosive atmosphere or when the power supply is switched off.
- Connect the metal protective cover to the equipotential bonding in the Ex area (cable cross-section: 4 mm^2).
- Ensure impact resistance in accordance with EN IEC 60079-0 – alternative measures:
  - Install the device in the TB-SG-L protective housing (available in the set with Ultem window: ID 100014865) and replace the Lexan service window with the Ultem window.
  - Install the device in an area offering impact protection (e.g. in the robot arm) and attach a warning sign: "DANGER: Do not connect or disconnect circuits under live conditions. Do not actuate the switch under live conditions".
- Keep the service window of the devices closed during operation in order to comply with the IP protection.
- Do not install the device in areas critically exposed to UV light.
- Prevent risks caused by electrostatic charge.
- Provide unused male connectors with suitable sealing or blanking caps in order to ensure degree of protection IP65, IP67 or IP69K The tightening torque for the M4 screws is 0.5 Nm.

4 Product description

The devices are designed in a fully encapsulated housing with degree of protection IP65/IP67/IP69K.

Der TBEN-L…-SE-M2 is a 10-port Ethernet switch. The switch has two 8-pin, X coded M12 Gigabit Ethernet ports (XF9 and XF10) with a transmission speed of 10/100/1000 Mbps and eight 4-pin, D coded M12 Fast Ethernet ports (XF1…XF8) with a transmission speed of 10/100 Mbps.

For connecting the supply voltage, 4-pin (TBEN-L4) 7/8" connectors, 5-pin (TBEN-L5) 7/8" connectors or 5-pin M12 connectors (TBEN-LL) are available.

4.1 Device overview

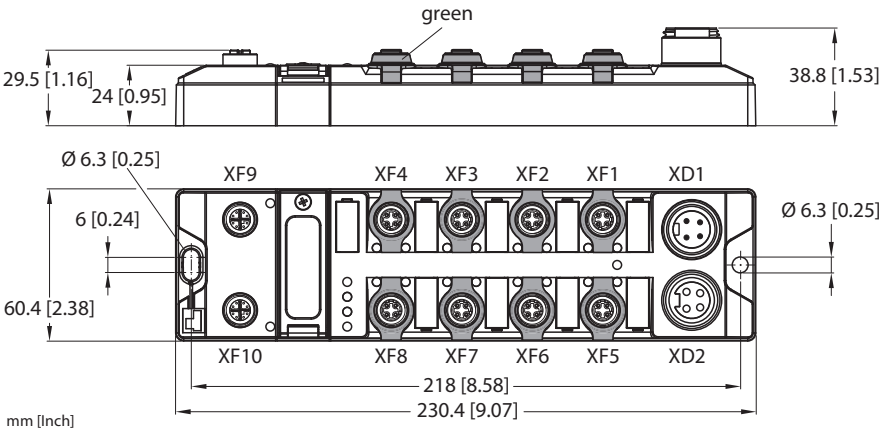

Fig. 1: Dimensions TBEN-L4-SE-M2

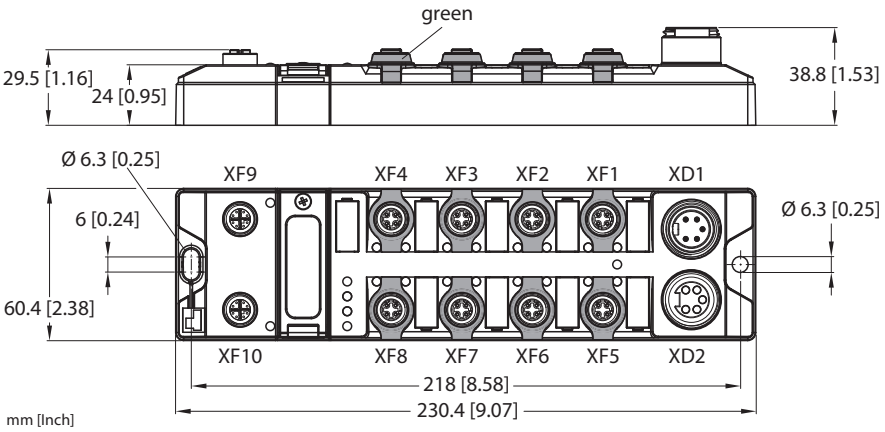

Fig. 2: Dimensions TBEN-L5-SE-M2

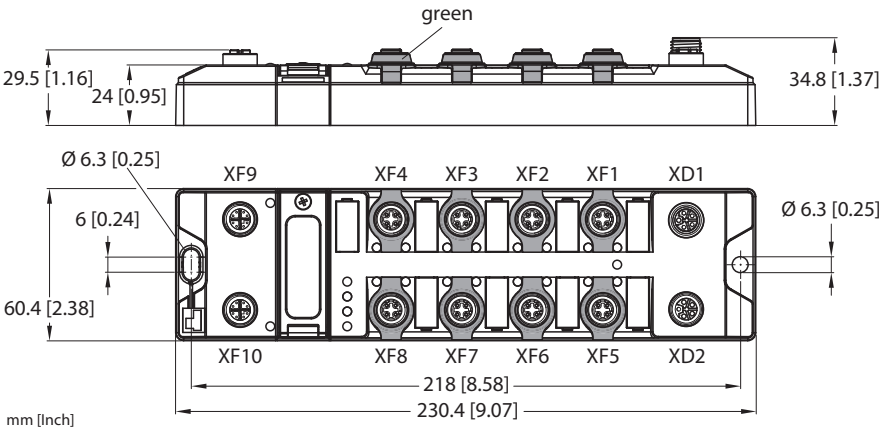

Fig. 3: Dimensions TBEN-LL-SE-M2

4.1.1 Operating elements

The devices are provided with the following operating elements:

- Rotary coding switches and DIP switch for setting the IP address
- SET button for executing USB Host functions

4.1.2 Display elements

The device is provided with the following LEDs:

- Power supply voltage
- Group and bus error
- Status
- Diagnostics

4.2 Properties and features

- Fiber-glass reinforced housing
- Shock and vibration tested
- Fully potted module electronics
- Degree of protection IP65/IP67/IP69K
- UV-resistant according to DIN EN ISO 4892-2
- Metal connectors
- Ethernet ports:
  - 2 × M12, X coded, 10/ 10/100 Mbps
  - 8 × M12, D coded, 10/100 Mbps
- Web based management
- Configurable LAN and WAN zones
- Configurable Layer 3 features
- Field bus integration from FW version 2.0 (PROFINET device, EtherNet/IP device, Modbus server)

4.3 Operating principle

The TBEN-L…-SE-M2 is used to build industrial Ethernet networks according to IEEE 802.3. and connects up to ten network segments. The switch controls the data traffic within a network domain and forwards data telegrams specifically to connected devices. A switch can send and receive messages simultaneously.

The switch can manage two different network zones (LAN and WAN). All Ethernet ports that are assigned to one of the two zones are switched with each other.

In the delivery state, the device behaves as a layer 2 switch. Layer 3 functions can be activated optionally.

As a participant in PROFINET, EtherNet/IP or Modbus TCP networks (LAN zone only), the device sends network diagnostics to a higher-level controller.

4.4 Functions and operating modes

4.4.1 Fieldbus integration: Multiprotocol technology

The device can be used in the following Ethernet protocols:

- PROFINET
- EtherNet/IP
- Modbus TCP

The required Ethernet protocol can be detected automatically or determined manually.

Automatic protocol detection

A multiprotocol device can be operated without intervention of the user (which means, without changes in the parameterization) in all of the three Ethernet protocols mentioned.

During the system start-up phase (snooping phase), the module detects which Ethernet protocol requests a connection to be established and adjusts itself to the corresponding protocol. After this an access to the device from other protocols is read-only.

Manual protocol selection

The user can also define the protocol manually. In this case, the snooping phase is skipped and the device is fixed to the selected protocol. With the other protocols, the device can only be accessed read-only.

Protocol dependent functions

The device supports the following Ethernet profile-specific functions:

PROFINET

- Topology detection
- Address allocation with LLDP
- S2 redundancy
- DHC (Data Hold Counter)
- MRP Client (Media Redundancy Protocol)

EtherNet/IP

- DLR participant (Device Level Ring)

Ethernet ports used

Port	Protocol
00022	SFTP
00053	DNS TCP
00067	DHCP
00080	HTTP
00093	PROFINET DCP
00502	Modbus TCP
58554	Turck Services

4.4.2 SNMP agent

The switch supports SNMP (Simple Network Management Protocol) V1, V2c and V3. SNMP V3 is only supported in the LAN and with deactivated fieldbus control. The SNMP function of the device can be configured via the web server.

Implemented MIBs

- System MIB
- ifTable MIB

Implemented traps

- Link up
- Link down
- Reboot

4.4.3 Neighborhood detection via LLDP (Link Layer Discovery Protocol)

The switch uses the LLDP protocol for neighborhood detection. Like all LLDP-capable network devices, the switch sends information about itself and stores information received from its neighbors. This information is queried by a network management system via the Simple Network Management Protocol (SNMP) and used for topology detection.

4.4.4 Prioritization/classification of data packets via QoS

The function QoS (Quality of Service) enables the prioritization (via PCP) or classification (via DSCP) of data telegrams.

- PCP (Priority Code Point)
  This function prevents time-critical data traffic from being disrupted by less time-critical data traffic in heavily loaded networks. By assigning high priorities for time-critical data and low priorities for less time-critical data, an optimal data flow for high-priority data is achieved. Frames to be transmitted are divided into priority classes from 0 to 7. 0 is used for frames that are not assigned a specific priority.
- DSCP (Differentiated Services Codepoint)
  DDSCPs are used to classify data packets. A DSCP (0…63) specifies a forwarding behavior for a data packet, i.e. it determines how a packet is handled.

4.4.5 DHCP

The switch supports the following DHCP options:

- DHCP server
- DHCP client
- DHCP server option 82, port-based IP address assignment

4.4.6 Network redundancy

The switch supports network redundancy via RSTP and MSTP as well as fieldbus-specific redundancy protocols such as MRP (PROFINET) [▶ 43] and DLR (EtherNet/IP) [▶ 52].

Network redundancy via RSTP (Rapid Spanning Tree Protocol)

RSTP is a further development of the STP with shorter switching times of 1 to 10 seconds. With RSTP on network participant acts as root. Unnecessary ports of network participants that lead to network loops and thus to unnecessary data traffic are deactivated and only activated in the event of an error to form a backup path.

Network redundancy via MSTP (Multiple Spanning Tree Protocol)

MSTP is an extension of the RSTP. MSTP enables different instances of the Spanning Tree in conjunction with Virtual Local Area Networks (VLANs). For a VLAN or a group of VLANs, independent STP instances can be formed that use their own spanning trees within a LAN.

4.4.7 Routing

Routing is used to forward data packets between networks with different IP address ranges. Several routing rules can be defined in the switch for data transfer between the configurable LAN and WAN network zones.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

4.4.8 Firewall

The switch firewall offers the possibility to set up rules for incoming and outgoing data packets as well as forwarding rules for data packets. The rules can be defined network-wide or IP-address-based and apply to all data packets or only to UDP-based or TCP-based packets.

4.4.9 NAT (Network Address Translation)

If IP forwarding (forwarding of data packets between networks with different IP address ranges) is activated, IP addresses of one network are translated into IP addresses of another network. Example: IP addresses of network participants of an internal network are assigned to IP addresses of an external network.

4.4.10 PAT (Port Address Translation)

PAT (Port Address Translation) is a variant of Network Address Translation (NAT). IP addresses from an internal network (e.g. plant network) are replaced by a single IP address from an external network (e.g. factory network). The port numbers of the participants in the internal network are also replaced by the port number of the router. The router bundles the data packets of all senders of the internal network and is the sender of all sent data packets for the external network.

4.4.11 Mirroring – mirroring switch ports

With the Mirroring function, data present on one port of the switch can be mirrored to another port. Only incoming, only outgoing or both types of data packets can be mirrored.

4.4.12 IGMP (Internet Group Management Protocol)

IGMP is the protocol for IP multicast applications in TCP/IP networks and is used to organize multicast groups. The switch can log on or off by sending IGMP messages to a router to receive multicast telegrams.

5 Installing

5.1 Installing a device in zone 2 and zone 22

The devices can be used in combination with the TB-SG-L (ID 100014865) protective housing set in zone 2 and zone 22.

DANGER
Potentially explosive atmosphere
Risk of explosion due to spark ignition
Operation in zone 2 or zone 22:
- ▶ Only install the device if there is no potentially explosive atmosphere present.
- ▶ Observe the requirements for Ex approval.

- ▶ Screw on the housing. Use a Torx T8 screwdriver.
- ▶ Replace the service window with the supplied Ultem window.
- ▶ Place the device on the base plate of the protective housing fasten both together on the mounting plate, see [▷ 16].
- ▶ Connect the device, see [▷ 18].
- ▶ Fit the housing cover and screw on as shown in the following figure. The tightening torque for the Torx T8 screw is 0.5 Nm.

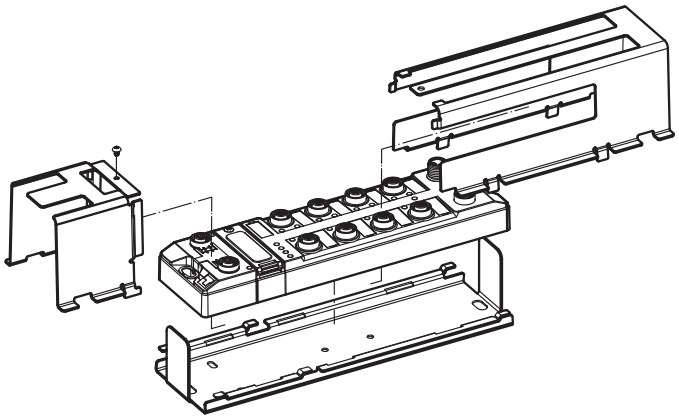

Fig. 4: Installing the device in the TB-SG-L protective housing

5.2 Mounting onto a mounting plate

NOTICE
Mounting on uneven surfaces
Device damage due to stresses in the housing
- ▶ Attach the device to the mounting plate with two M6 screws.

- ▶ Attach the module to the mounting surface with two M6 screws. The maximum tightening torque for the screws is 1.5 Nm.
- ▶ Optional: Ground the device.

5.3 Outdoor device installation

The device is UV resistant in accordance with DIN EN ISO 4892-2. Direct sunlight may cause material wear and changes in color. The mechanical and electrical properties of the device are not impaired.

- ▶ To prevent material wear and color changes: Protect the device from direct sunlight with protective panels.

5.4 Grounding the device

5.4.1 Equivalent wiring diagram and shielding concept

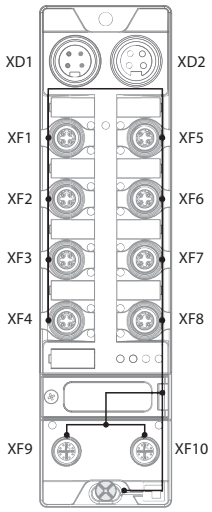

Fig. 5: TBEN-L4-SE-M2 – equivalent wiring diagram and shielding concept

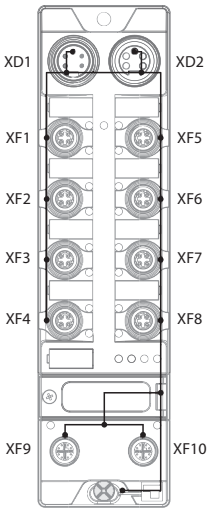

Fig. 6: TBEN-L5-SE-M2 – equivalent wiring diagram and shielding concept

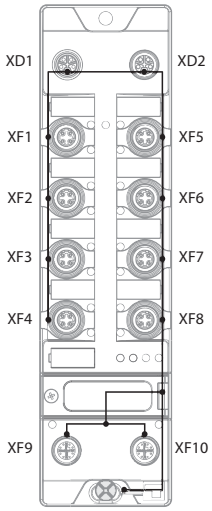

Fig. 7: TBEN-LL-SE-M2 – equivalent wiring diagram and shielding concept

5.4.2 Shielding the Ethernet ports

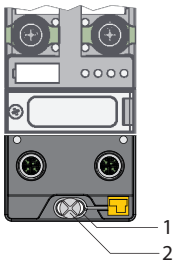

Fig. 8: Grounding ring (1) and mounting screw (2)

The grounding ring (1) is the module grounding. The shielding of the Ethernet ports is permanently connected to the module grounding. The module grounding is only connected to the reference potential of the installation when the module is mounted.

In the device variants TBEN-L5-SE-M2 and TBEN-LL-SE-M2, the earthing can also be connected via pin 5 of the connector for the supply voltage.

5.4.3 Grounding the device – mounting on a mounting plate

- ▶ For mounting onto a mounting plate: Fix the module with an M6 metal screw through the lower mounting hole.
- ⇨ The shielding of the M12 flanges for the I/O level is connected to the reference potential of the installation via the M6 metal screw.

6 Connecting

NOTICE
Penetration of liquids or foreign objects due to leaking connections
Loss of degree of protection IP65/IP67/IP69K possible

- Tighten M12 male connectors with a tightening torque of 0.6 Nm.
- Tighten 7/8″ male connectors with a tightening torque of 0.8 Nm.
- Only use accessories that guarantee the protection class.
- Provide unused male connectors with suitable sealing or blanking caps. The tightening torque for the M4 screws is 0.5 Nm.

6.1 Connecting a device in zone 2 and zone 22

DANGER
Explosive atmosphere
Explosion due to ignitable sparks
For use in Zone 2 and Zone 22:

- Only disconnect and connect circuits when there is no potentially explosive atmosphere or when the power supply is switched off
- Only use connecting cables that are approved for use in potentially explosive atmospheres.
- Use all connectors or seal them with screw caps or blind caps. The tightening torque for the screw caps is 0.5 Nm.
- Observe requirements for Ex approval.

6.2 Connecting network segments

To connect the Ethernet network segments, the device has two 8-pin , X coded M12 Gigabit Ethernet connectors and eight 4-pin, d coded M12 Fast Ethernet connectors. The maximum tightening torque is 0.6 Nm.

Gigabit ports (10/100/100 Mbps)

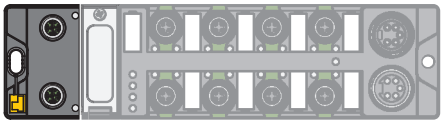

Fig. 9: M12 Gigabit Ethernet connector

- ▶ Connect the device to Ethernet according to the pin assignment below.

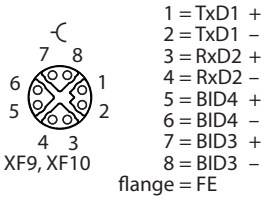

Fig. 10: M12 Gigabit Ethernet connector

Fast Ethernet ports (10/100 Mbps)

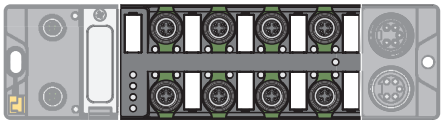

Fig. 11: M12 Fast Ethernet connector

- ▶ Connect the device to Ethernet according to the pin assignment below.

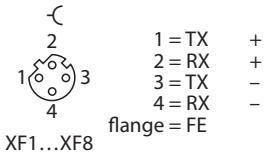

Fig. 12: M12 Fast Ethernet connector

6.3 Connecting the power supply

TBEN-L4-SE-M2/TBEN-L5-SE-M2

For the connection to the power supply, the device has two 5-pin 7/8" connectors. The power supply connectors are designed as 4-pin (TBEN-L4) or 5-pin (TBEN-L5) 7/8" connectors. V1 and V2 are galvanically isolated. The maximum tightening torque is 0.8 Nm.

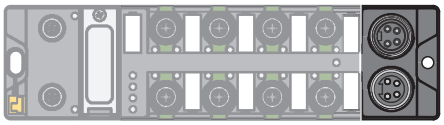

Fig. 13: TBEN-L4-SE-M2 – 7/8" for connecting the supply voltage

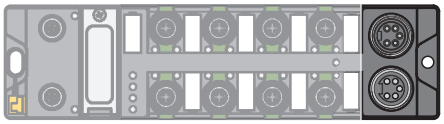

Fig. 14: TBEN-L5-SE-M2 – 7/8" for connecting the supply voltage

▶ Connect the device to the power supply according to the pin assignment shown below.

Connector	Function
X1	Power feed
X2	Continuation of the power to the next node

Voltage	Function
V1	System voltage: power supply 1 (incl. supply of electronics)
V2	Load voltage: power supply 2, fed through, not used in device

TBEN-LL-SE-M2

For the connection to the supply voltage, the device has two 5-pin, L coded M12 connectors. V1 and V2 are galvanically isolated. The maximum tightening torque is 0.6 Nm.

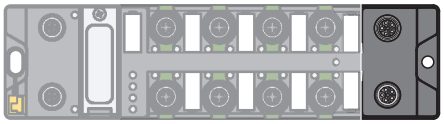

Fig. 15: M12 connector for connecting the supply voltage

- ▶ Connect the device to the power supply according to the pin assignment shown below.
- ▶ Provide unused male connectors with suitable sealing or blanking caps. The tightening torque for the M4 screws is 0.5 Nm.

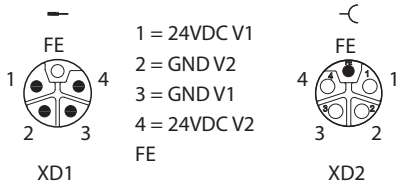

Fig. 16: Pin assignment power supply connectors

Connector	Function
XD1	Power feed
XD2	Continuation of the power to the next node

Voltage	Function
V1	System voltage: power supply 1 (incl. supply of electronics)
V2	Load voltage: power supply 2, fed through, not used in device

6.3.1 Supply concept

The device is supplied via V1. All Ethernet ports are galvanically isolated. V2 is fed through.

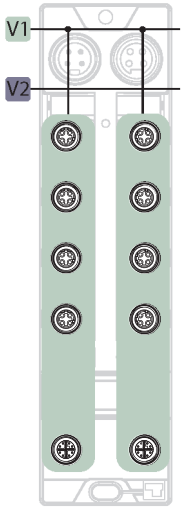

Fig. 17: Supply TBEN-L4-SE-M2

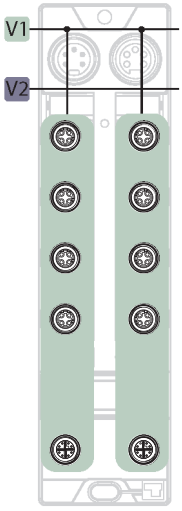

Fig. 18: Supply TBEN-L5-SE-M2

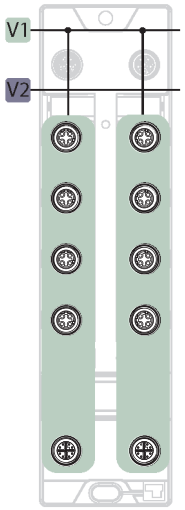

Fig. 19: Supply TBEN-LL-SE-M2

7 Commissioning

7.1 Device web server

The web server can be opened from a web browser or from the Turck Automation Suite (TAS). Accessing the web server via TAS is described in the section entitled "Adjusting network settings."

7.1.1 Web server login

- Open the web server.
- Log on to the device as administrator. The default user for the web server is "admin", the default password is "password".
- Enter user name and password in the login field on the start page of the web server.
- Click **Login**.

NOTE
The password is transmitted in plain text for HTTP connections. The password is only encrypted if access to the web server is established via an HTTPS connection.

7.1.2 Securing device access with password

NOTICE
Inadequately secured devices
Unauthorized access to sensitive data
- Change password after first login. Turck recommends using a secure password.
- Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

7.2 Adjusting network settings

The network settings for the LAN network zone of the switch can be set via two decimal rotary coding switches and DIP switches on the device, via the web server or via TAS (Turck Automation Suite).

The network settings for the WAN network zone on the switch can only be set via the device's web server.

7.2.1 Adjusting network settings via switches on the device

The network settings can be adjusted via two decimal rotary coding switches and the DIP switch [Mode] on the device. The switches are located under a service window together with the USB ports and the SET button.

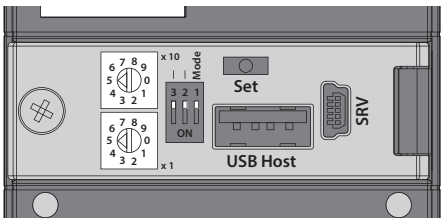

Fig. 20: Switches for setting the IP address

- Open the service window.
- Set the rotary coding switch to the desired position according to the table below.
- Set the DIP switch [Mode] to the desired position according to the table below.
- Execute a power cycle.
- NOTICE! IP67 or IP69K protection is not guaranteed when the cover over the rotary coding switches is opened. Device damage through penetrating foreign objects or liquids is possible. Tightly close the service window.

Switch positions

The network settings of the device depend on the selected mode. Changes to the settings become active after a voltage reset.

Switch position			
DIP switch [MODE]	**Rotary coding switches**	**Setting option**	**Description**
0	00	Network reset	The Network reset resets the following the network settings to the default values: IP address: 192.168.1.100 Subnet mask: 255.255.255.0 Gateway: 192.168.1.1
0	1…99	Rotary	In rotary mode (static rotary), the last byte of the IP address can be set manually at the gateway. The other network settings are stored in the non-volatile memory of the gateway and cannot be changed in rotary mode. Addresses from 1…99 can be set.
1	40	DHCP	In DHCP mode, the network settings are automatically assigned by a DHCP server in the network. The subnet mask assigned by the DHCP server and the default gateway address are stored non-volatile in the memory of the gateway, DHCP supports three mechanisms for IP address allocation: ■ Automatic address assignment: The DHCP server assigns a permanent IP address to the client. ■ Dynamic address assignment: The IP address assigned by the server is only reserved for a certain period of time. After this time has elapsed or after the explicit release by a client, the IP address is reassigned. ■ Manual address assignment: A network administrator assigns an IP address to the client. In this case, DHCP is only used to transmit the assigned IP address to the client. ■ Default IP address: 192.168.1.254
1	50	PGM	In PGM mode, the complete network settings can be assigned manually via TAS, the Turck Service Tool, FDT/DTM or a web server. The settings are stored in the device in non-volatile memory. ■ Default IP address: 192.168.1.254
1	60	PGM-DHCP	In PGM-DHCP mode, the device is initially a DHCP client and sends DHCP requests until it is assigned a fixed IP address. The DHCP client is automatically deactivated as soon as the device has received an IP address via the DTM or the web server. The settings are stored in the device in non-volatile memory. ■ Default IP address: 192.168.1.254
1	90	Factory Reset:	The factory(F_Reset) all settings to the default values: ■ Network setting (IP address, subnet mask, gateway) ■ Device parameters
1	00	Restore	Restore only resets the IP address of the device. ■ IP address: 192.168.1.254

7.2.2 Adjusting network settings via the web server

NOTE
To be able to adjust the network settings via the web server, the device must be in PGM mode.

- Open the web server.
- Log-in to the device as administrator. The default user for the web server is "admin", the default password is "password".
- **Click Configuration → IP .**
- Change the IP address and if necessary also the subnet mask and default gateway for **Zone LAN**, **Zone WAN** and/or for **Zone VLAN** (If defined [▶ 98]). Zone LAN is only displayed if at least one of the switch's interfaces has been assigned to the VLAN [▶ 96].
- Write the new IP address, the subnet mask and the default gateway to the device via **Set Addresses.**

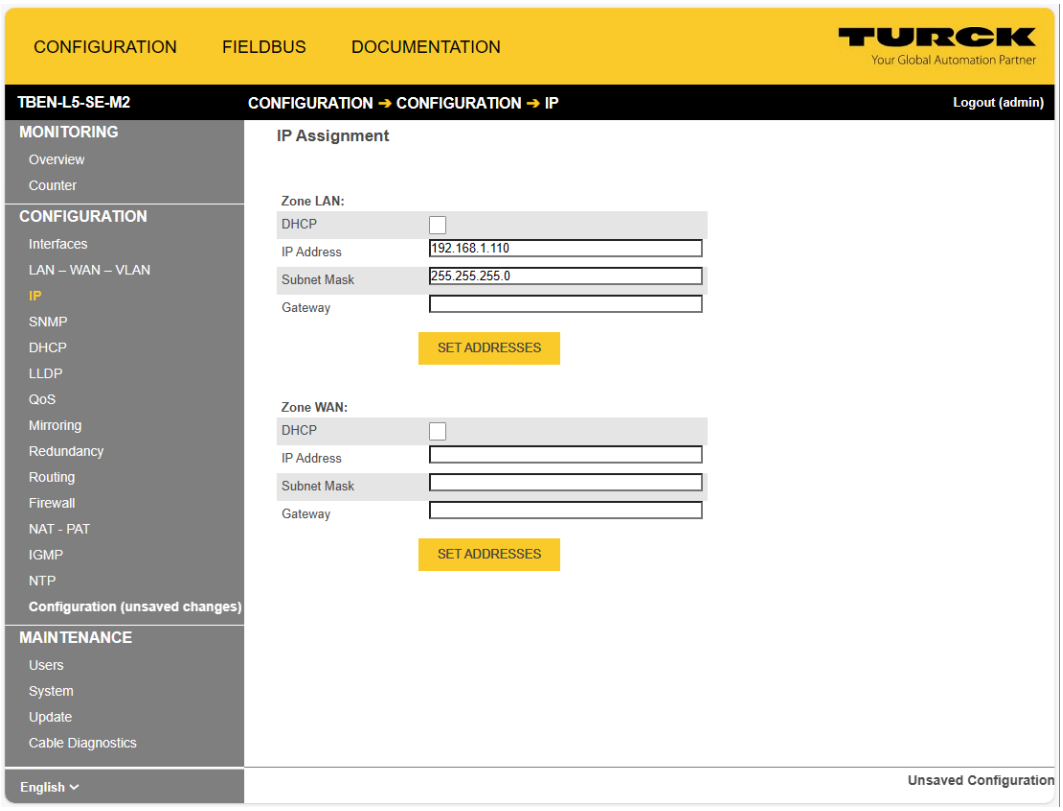

Fig. 21: Adjusting network settings via the web server

7.3 User management and rights assignment

Users are created in the web server under **Maintenance → Users**.

Security in the web server

In the web server, a default-password is assigned in Turck-module for the administrator login.

NOTICE
Inadequately secured devices
Unauthorized access to sensitive data

- ▶ Change password after first login. Turck recommends using a secure password.
- ▶ Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

The password is transmitted in plain text for HTTP connections. The password is only encrypted if access to the web server is established via an HTTPS connection.

In the delivery state or after a factory reset, the default settings are as follows:

- User: admin
- Password: password

7.3.1 Authorization levels

The following table lists the authorization levels and the associated user rights.

Authorization level	Meaning	Rights
0	Admin	The user has full access to all functions of the device: ■ Configuration of the general switch functions (interfaces, VLAN, IP addresses, SNMP, DHCP, …) ■ Accept and reset the changed configuration, upload and download a configuration ■ User administration ■ Firmware update
1	Configuration	The user has access to the configuration of the general switch functions (interfaces, VLAN, IP addresses, SNMP, DHCP, …).
2	Read access	The user has read-only access.

7.3.2 Adding a user

✓ The logged in user is a user with admin rights (area permission level 0).

▶ Assign a user name and an initial password for the new user under **Maintenance → Users.**

▶ Select the authorization level and create the new user via **Add user.**

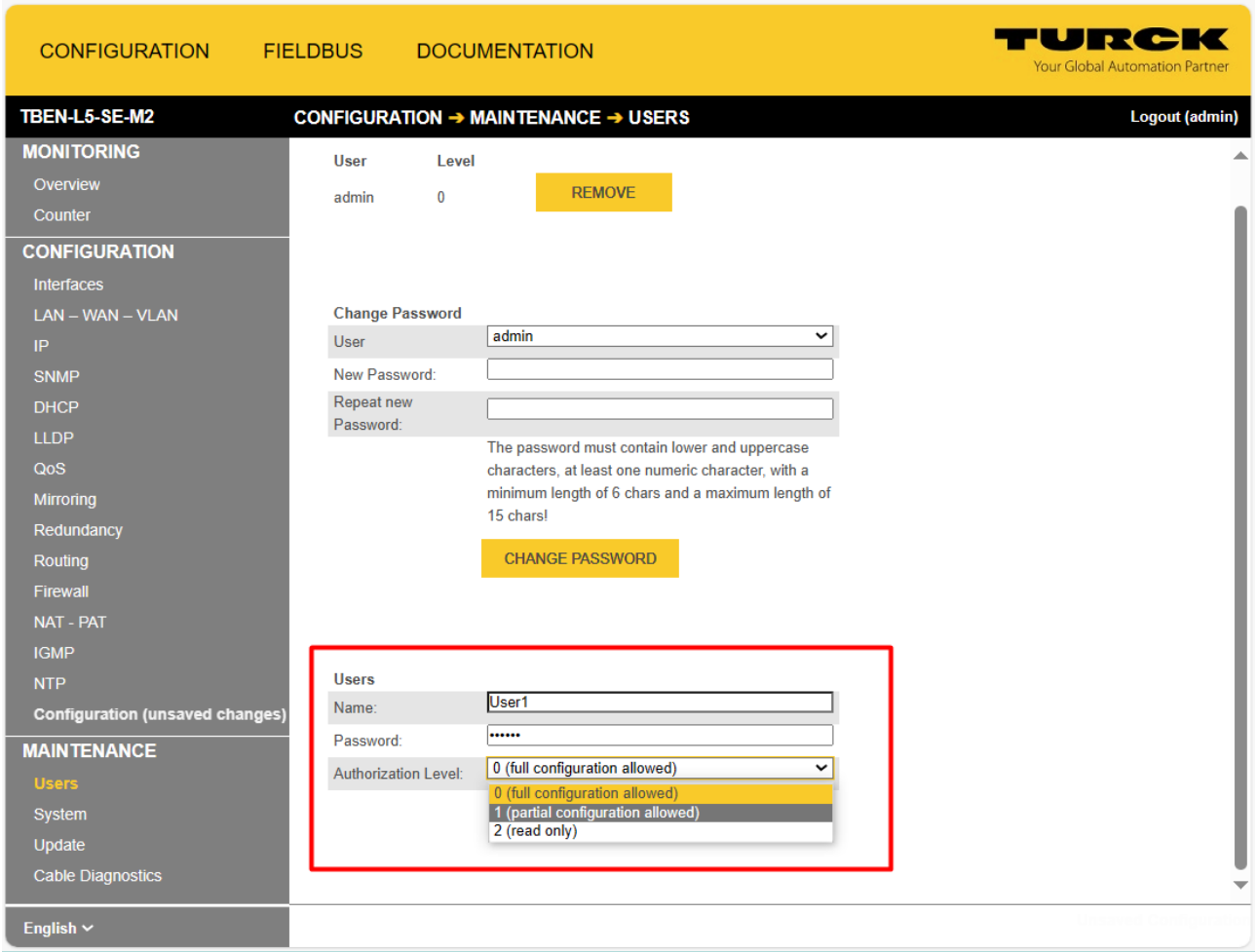

Fig. 22: Creating a new user

NOTICE

Inadequately secured devices

Unauthorized access to sensitive data

▶ Change password after first login. Turck recommends using a secure password.

▶ Adapt the password to the requirements of the network security concept of the system in which the devices are installed.

7.4 Fieldbus control of the device

In order to integrate the switch into an Ethernet network as a PROFINET device, EtherNet/IP device or Modbus server, fieldbus control must be activated. The fieldbus control is deactivated per default.

The fieldbus control can be activated or deactivated in the engineering tool or in the web server (example web server: **Configuration → Maintenance → System → Enable fieldbus**).

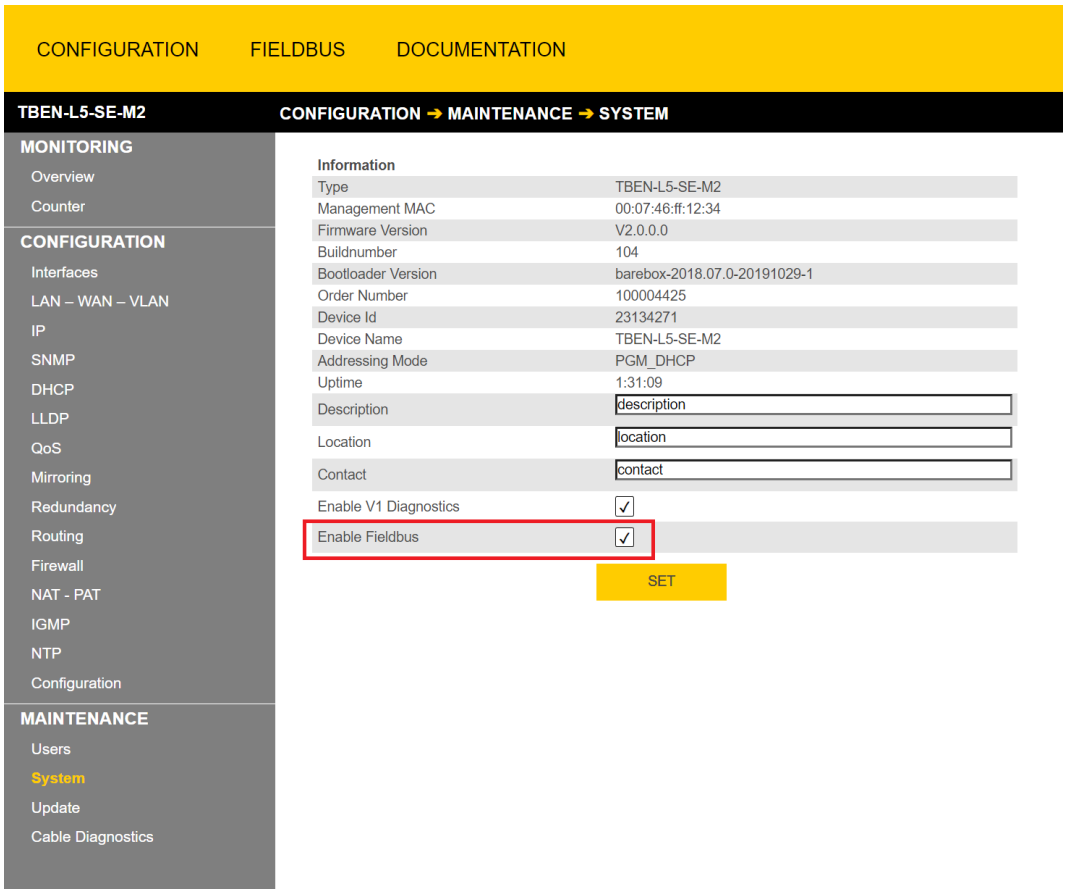

Fig. 23: Fieldbus control activated for the device

NOTE
If the fieldbus control is deactivated in the engineering tool, the device can only be accessed via the web server.

If fieldbus control is activated, the fieldbus functionality is activated by default for all switch ports and all ports are automatically assigned to the LAN.

Limiting the number of ports with fieldbus functionality

The number of ports that are controlled via the fieldbus can be limited in the web server or engineering tool via GSDML, EDS, etc. using the parameters "Enable fieldbus control" (EN FB CTRL) and "Last port with fieldbus functionality (FBUS LAST PORT)" [▷ 126]. The ports for which no fieldbus control is configured are automatically assigned to the WAN.

Example:

- Activate the parameter **Enable fieldbus control** via **Fieldbus** → **Local I/O** → **Parameters** → **Fieldbus control** and limit the ports with fieldbus functionality (here in the example to 5).

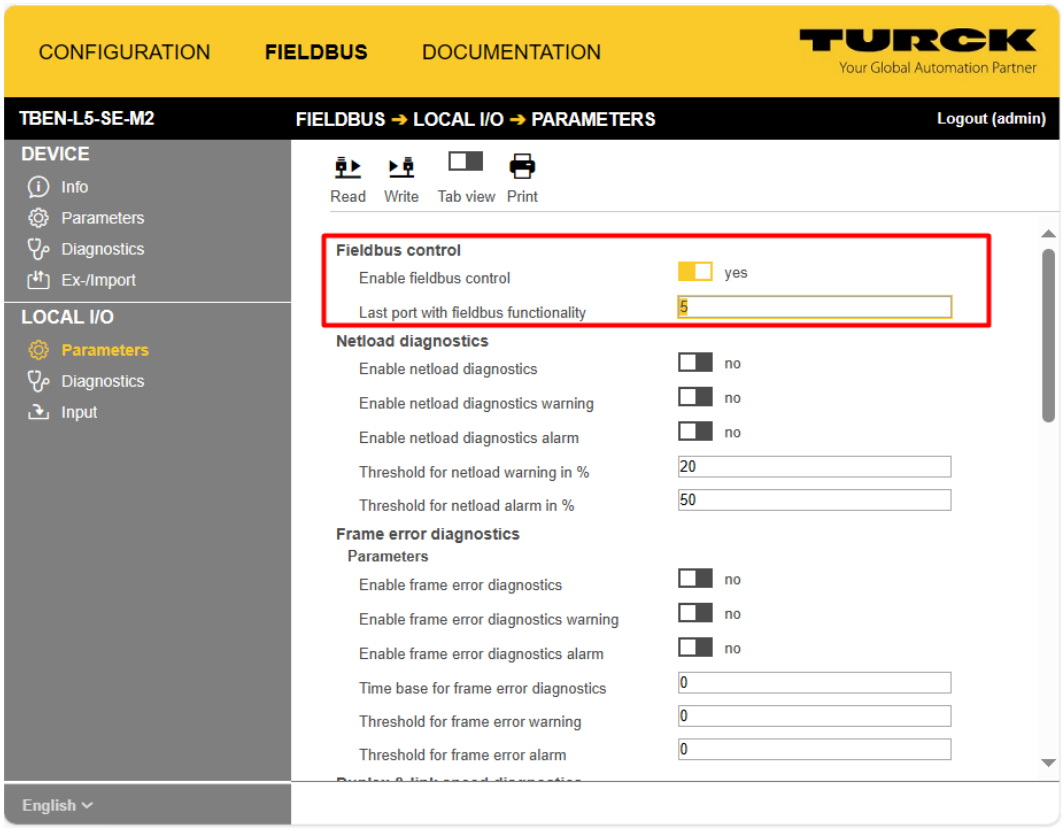

Fig. 24: Limited ports with fieldbus functionality

⇨ The fieldbus control is now only activated for the switch ports XF1…XF5. Ports XF6… XF10 no longer support field bus control. Ports XF1…XF5 are assigned to the LAN, ports XF6…XF10 automatically belong to the WAN.

7.5 Commissioning the devices in PROFINET

7.5.1 Device model TBEN-L…-SE-M2, slots and sub slots

The TBEN-L…-SE-M2 have eight virtual slots for various device functions (fieldbus control, port de-/ activation…), network diagnostics (netload diagnostics, Frame Error diagnostics, …) and status information (module status).

Besides Slot 0 (DAP) all other slots of the device contain only one sub slot. For this reason slots and sub slots are described as synonyms in the following.

Slot no.	Slot name	Description
0	TBEN-L…-SE-M2	Device interface to PROFINET IO, Device Access Point
1	Fieldbus control	Enabling or disabling the fieldbus control and definition of the switch ports with fieldbus functionality Sub module: ■ Fieldbus control
2	Diagnostics netload	Enabling or disabling of netload diagnostics, warnings and alarms and configuration of the thresholds for notifications. Possible sub modules: ■ Netload diagnostics Basic ■ Netload diagnostics Advanced ■ Netload diagnostics Full
3	Diagnostics frame errors	Enabling or disabling of frame error diagnostics, warnings and alarms and configuration of the thresholds for notifications. Possible sub modules: ■ Frame error diagnostics Basic ■ Frame error diagnostics Advanced ■ Frame error diagnostics Full
4	Diagnostics duplex/ link speed	Enabling or disabling of half duplex and link speed diagnostics and alarms. Sub module: ■ Duplex and link speed diagnostics
5	Port control	Enabling or disabling port control and port-by-port enabling and disabling of ports XF1…XF10. Sub module: ■ Port control
6	PN DHC	Enabling or disabling of diagnostics for PROFINET DHC (Data Hold Counter) Sub module: ■ PROFINET DHC
7	RSTP	Enabling or disabling of RSTP for the LAN network. Sub module: ■ RSTP
8	Module status	See status and control word [▶ 134]

Sub module "Fieldbus control"

The sub module "Fieldbus control" can be plugged into slot 1.

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Fieldbus control				
EN FB CTRL Enable fieldbus control	0	0x0	No	The number of ports for which fieldbus control is activated cannot be limited.
	1	**0x1**	**Yes**	The number of ports for which fieldbus control is activated can be limited via the "Last port with fieldbus functionality" (FBUS LAST PORT) parameter.
FBUS LAST PORT Last port with fieldbus functionality	01…**10**	0x01… **0x0A**		The parameter can only be set if the parameter "Enable fieldbus control" (EN FB CTRL) is activated. The number of ports (port 1 to port…) for which fieldbus control is to be activated is limited (default: 0x0A = fieldbus control activated for all ports). Example: FBUS LAST PORT = 8 → fieldbus control activated for ports XF1…XF8. **Note:** The PLC must be connected to one of the defined ports. If the parameter is changed independently of the PLC program in the web server or similar (e.g. restriction of the ports with fieldbus control in the above example to FBUS LAST PORT = 6), the PLC will no longer have access to the device.

- **Process input data** [▶ 130]

Process value	Offset	Data type
Last port with fieldbus functionality	%IB0	USINT

Sub module "Netload diagnostics Basic, Advanced, Full"

The sub module "Netload diagnostics Basic, Advanced, Full" can be plugged into slot 2.

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Netload diagnostics				
EN NL DIAG Enable netload diagnostics	0	0x0	No	Netload diagnostics deactivated
	1	**0x1**	**Yes**	Netload diagnostics activated Input data, warnings or alarms about netload will be sent.
EN NL WARN Enable warnings for netload diagnostics	0	0x0	No	Sending of warnings for netload deactivated
	1	**0x1**	**Yes**	Sending of warnings for netload activated.
EN NL ALARM Enable alarms for netload diagnostics	**0**	**0x0**	**No**	Sending of alarms for netload deactivated
	1	0x1	Yes	Sending of alarms for netload activated
TH NL WARN Threshold for netload warnings in %	0…100, **30**	0x0000…0x0064, **0x001E**		If the threshold defined here is exceeded, warnings are issued for network load diagnostics. The parameters "Enable netload diagnostics (EN NL DIAG)" and "Enable warnings for netload diagnostics" (EN NL WARN) have to be activated.
TH NL ALARM Threshold for netload alarms in %	0…100, **80**	0x0000…0x0064, 0x0050		If the threshold defined here is exceeded, alarms are issued for network load diagnostics. The parameters "Enable netload diagnostics (EN NL DIAG)" and "Enable warnings for netload diagnostics" (EN NL ALARM) have to be activated.

- **Process input data "Netload diagnostics Basic"** [▶ 130]

Process value	Offset	Data type
Netload diagnostics	%IB0	USINT
Netload warning	%IX0.0	BOOL
Netload alarm	%IX0.1	BOOL

- **Process input data "Netload diagnostics Advanced"** [▶ 130]

Process value	Offset	Data type
Netload diagnostics	%IB0	USINT
Netload warning	%IX0.0	BOOL
Netload alarm	%IX0.1	BOOL
Reserved	%IB1	USINT
Max. current netload (%)	%IB2	USINT
reserved	%IB3	USINT

- **Process input data "Netload diagnostics Full"** [▶ 130]

Process value	Offset	Data type
Netload diagnostics	%IB0	USINT
■ Netload warning	%IX0.0	BOOL
■ Netload alarm	%IX0.1	BOOL
reserved	%IB1	USINT
Max. current netload (%)	%IB2	USINT
reserved	%IB3	USINT
Max. netload peak (since last PLC connection) [%]	%IB4	USINT
reserved	%IB5	USINT
Netload diagnostics	%IB6	USINT
■ RX netload warning XF1	%IX6.0	BOOL
■ RX netload warning XF2	%IX6.1	BOOL
■ RX netload warning XF3	%IX6.2	BOOL
■ RX netload warning XF4	%IX6.3	BOOL
■ RX netload warning XF5	%IX6.4	BOOL
■ RX netload warning XF6	%IX6.5	BOOL
■ RX netload warning XF7	%IX6.6	BOOL
■ RX netload warning XF8	%IX6.7	BOOL
Netload diagnostics	%IB7	USINT
■ RX netload warning XF9	%IX7.0	BOOL
■ RX netload warning XF10	%IX7.1	BOOL
Netload diagnostics	%IB8	USINT
■ TX netload warning XF1	%IX8.0	BOOL
■ TX netload warning XF2	%IX8.1	BOOL
■ TX netload warning XF3	%IX8.2	BOOL
■ TX netload warning XF4	%IX8.3	BOOL
■ TX netload warning XF5	%IX8.4	BOOL
■ TX netload warning XF6	%IX8.5	BOOL
■ TX netload warning XF7	%IX8.6	BOOL
■ TX netload warning XF8	%IX8.7	BOOL
Netload diagnostics	%IB9	USINT
■ TX netload warning XF9	%IX9.0	BOOL
■ TX netload warning XF10	%IX9.1	BOOL
Netload diagnostics	%IB10	USINT
■ RX netload alarm XF1	%IX10.0	BOOL
■ RX netload alarm XF2	%IX10.1	BOOL
■ RX netload alarm XF3	%IX10.2	BOOL
■ RX netload alarm XF4	%IX10.3	BOOL
■ RX netload alarm XF5	%IX10.4	BOOL
■ RX netload alarm XF6	%IX10.5	BOOL
■ RX netload alarm XF7	%IX10.6	BOOL
■ RX netload alarm XF8	%IX10.7	BOOL

Process value	Offset	Data type
Netload diagnostics	%IB11	USINT
■ RX netload alarm XF9	%IX11.0	BOOL
■ RX netload alarm XF10	%IX11.1	BOOL
Netload diagnostics	%IB12	USINT
■ TX netload alarm XF1	%IX12.0	BOOL
■ TX netload alarm XF2	%IX12.1	BOOL
■ TX netload alarm XF3	%IX12.2	BOOL
■ TX netload alarm XF4	%IX12.3	BOOL
■ TX netload alarm XF5	%IX12.4	BOOL
■ TX netload alarm XF6	%IX12.5	BOOL
■ TX netload alarm XF7	%IX12.6	BOOL
■ TX netload alarm XF8	%IX12.7	BOOL
Netload diagnostics	%IB13	USINT
■ TX netload alarm XF9	%IX13.0	BOOL
■ TX netload alarm XF10	%IX13.1	BOOL

Sub module "Frame error diagnostics Basic, Advanced, Full"

The sub module "Frame error diagnostics" can be plugged into slot 3.

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Frame error diagnostics				
EN FRM DIAG Enable frame error diagnostics	0	0x0	**No**	Frame error diagnostics deactivated
	1	**0x1**	Yes	Frame error diagnostics activated Input data, warnings or alarms for frame errors will be sent.
EN FRM WARN Enable warnings for frame error diagnostics	0	0x0	**No**	Sending of warnings for frame errors deactivated
	1	**0x1**	Yes	Sending of warnings for frame errors activated
EN FRM ALARM Enable alarms for frame error diagnostics	**0**	**0x0**	**No**	Sending of alarms for frame errors deactivated
	1	0x1	Yes	Sending of alarms for frame errors activated
FRM TB Time base for frame error diagnostics	0…65535, **60**	0x0… 0xFFFF, **0x3C**		Period of time in s in which the number of frame errors is calculated and returned
TH FRM WARN Threshold for frame error warnings	0… 4294967295, **100**	0x0… 0xFFFFFFFF, **0x64**		If the threshold defined here is exceeded, warnings are issued for frame error diagnostics. The parameters "Enable frame error diagnostics (EN FRM DIAG)" and "Enable warnings for frame error diagnostics" (EN FRM WARN) have to be activated.
TH FRM ALARM threshold for frame error alarms	0… 4294967295, **1000**	0x0… 0xFFFFFFFF, **0x03E8**		If the threshold defined here is exceeded, alarms are issued for frame error diagnostics. The parameters "Enable frame error diagnostics (EN FRM DIAG)" and "Enable warnings for frame error diagnostics" (EN FRM ALARM) have to be activated.

- **Process input data "Frame error diagnostics Basic"** [▶ 130]

Process value	Offset	Data type
Diagnostics	%IB0	USINT
■ Frame error warning	%IX0.0	BOOL
■ Frame error alarm	%IX0.1	BOOL
reserved	%IB1	USINT

Process input data "Frame error diagnostics Advanced" [▶ 130]

Process value	Offset	Data type
	%ID0	
Diagnostics	%IB0	USINT
■ Frame error warning	%IX0.0	BOOL
■ Frame error alarm	%IX0.1	BOOL
Reserved	%IB1	USINT
Max. current frame errors (%)	%ID1	UDINT

Process input data "Frame error diagnostics Full" [▶ 130]

Process value	Offset	Data type
	%ID0	
Diagnostics	%IB0	USINT
■ Frame error warning	%IX0.0	BOOL
■ Frame error alarm	%IX0.1	BOOL
reserved	%IB1	USINT
Max. current frame errors	%ID1	UDINT
Max. number frame errors (peak) since last PLC connection	%ID2	UDINT
Port based alarms and warnings at port	%IB12	USINT
■ Frame error warning XF1	%IX12.0	BOOL
■ Frame error warning XF2	%IX12.1	BOOL
■ Frame error warning XF3	%IX12.2	BOOL
■ Frame error warning XF4	%IX12.3	BOOL
■ Frame error warning XF5	%IX12.4	BOOL
■ Frame error warning XF6	%IX12.5	BOOL
■ Frame error warning XF7	%IX12.6	BOOL
■ Frame error warning XF8	%IX12.7	BOOL
Netload diagnostics	%IB13	USINT
■ Frame error warning XF9	%IX13.0	BOOL
■ Frame error warning XF10	%IX13.1	BOOL
Netload diagnostics	%IB14	USINT
■ Frame error alarm XF1	%IX14.0	BOOL
■ Frame error alarm XF2	%IX14.1	BOOL
■ Frame error alarm XF3	%IX14.2	BOOL
■ Frame error alarm XF4	%IX14.3	BOOL
■ Frame error alarm XF5	%IX14.4	BOOL
■ Frame error alarm XF6	%IX14.5	BOOL
■ Frame error alarm XF7	%IX14.6	BOOL
■ Frame error alarm XF8	%IX14.7	BOOL
Netload diagnostics	%IB15	USINT
■ Frame error alarm XF9	%IX15.0	BOOL
■ Frame error alarm XF10	%IX15.1	BOOL

Sub module "Duplex and link speed diagnostics"

The sub module "Duplex and link speed diagnostics" can be plugged into slot 4.

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Duplex and link speed diagnostics				
EN DUP DIAG Enable full duplex diagnostics	**0**	**0x0**	**No**	Half duplex diagnostics deactivated
	1	0x1	Yes	Half duplex diagnostics activated Input data, warnings or alarms for half duplex diagnostics will be sent.
EN DUP ALARM Enable half duplex diagnostics	**0**	**0x0**	**No**	Sending of alarms for half duplex diagnostics deactivated
	1	0x1	Yes	Sending of alarms for half duplex diagnostics activated
EN LS DIAG Enable half duplex diagnostics	**0**	**0x0**	**No**	Link speed diagnostics deactivated
	1	0x1	Yes	Link speed diagnostics activated Input data, warnings or alarms for link speed diagnostics will be sent.
EN LS ALARM Enable link speed diagnostics	**0**	**0x0**	**No**	Sending of alarms for link speed diagnostics deactivated
	1	0x1	Yes	Sending of alarms for link speed diagnostics activated

- **Process input data** [▶ 130]

Process value	Offset	Data type
Duplex and link speed diagnostics	%IB0	USINT
■ Half duplex detected at XF1	%IX0.0	BOOL
■ Half duplex detected at XF2	%IX0.1	BOOL
■ Half duplex detected at XF3	%IX0.2	BOOL
■ Half duplex detected at XF4	%IX0.3	BOOL
■ Half duplex detected at XF5	%IX0.4	BOOL
■ Half duplex detected at XF6	%IX0.5	BOOL
■ Half duplex detected at XF7	%IX0.6	BOOL
■ Half duplex detected at XF8	%IX0.7	BOOL
Duplex and link speed diagnostics	%IB1	USINT
■ Half duplex detected at XF9	%IX1.0	BOOL
■ Half duplex detected at XF10	%IX1.1	BOOL
Duplex and link speed diagnostics	%IB2	USINT
■ 10 Mbps detected at XF1	%IX2.0	BOOL
■ 10 Mbps detected at XF2	%IX2.1	BOOL
■ 10 Mbps detected at XF3	%IX2.2	BOOL
■ 10 Mbps detected at XF4	%IX2.3	BOOL
■ 10 Mbps detected at XF5	%IX2.4	BOOL
■ 10 Mbps detected at XF6	%IX2.5	BOOL
■ 10 Mbps detected at XF7	%IX2.6	BOOL

Process value	Offset	Data type
■ 10 Mbps detected at XF8	%IX2.7	BOOL
Duplex and link speed diagnostics	%IB3	USINT
■ 10 Mbps detected at XF9	%IX3.0	BOOL
■ 10 Mbps detected at XF10	%IX3.1	BOOL

Sub module "Port control"

The sub module "Port control" can be plugged into slot 5.

■ **Parameters** [▶ 126]

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Port control				
EN PORTCTL Enable port control	0	0x0	No	Port control enabled The ports cannot be switched on or off via the fieldbus.
	1	**0x1**	**Yes**	Port control activated The ports can be enabled or disabled via the parameter "Activate XF…" (XF… STATE) parameter.
XF… activated Activate XF1… activate XF10	0	0x0	No	Port XF… deactivated
	1	**0x1**	**Yes**	Port XF… activated

■ **Process input data** [▶ 130]

Process value	Offset	Data type
XF activated	%IB0	USINT
■ XF1 activated	%IX0.0	BOOL
■ XF2 activated	%IX0.1	BOOL
■ XF3 activated	%IX0.2	BOOL
■ XF4 activated	%IX0.3	BOOL
■ XF5 activated	%IX0.4	BOOL
■ XF6 activated	%IX0.5	BOOL
■ XF7 activated	%IX0.6	BOOL
■ XF8 activated	%IX0.7	BOOL
XF activated	%IB1	USINT
■ XF9 activated	%IX1.0	BOOL
■ XF10 activated	%IX1.1	BOOL

Sub module "PROFINET DHC (PN DHC)"

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
PROFINET DHC (PROFINET only)				
EN DHC DIAG Enable PN DHC diagnostics	**0**	**0x0**	**No**	Diagnostics for PROFINET DHC (Data Hold Counter) deactivated
	1	0x1	Yes	Diagnostics for PROFINET DHC (Data Hold Counter) activated Input data, warnings or alarms for PROFINET DHC diagnostics will be sent.
EN DHC WARN Enable warnings for netload diagnostics	**0**	**0x0**	**No**	Sending of warnings for PROFINET DHC diagnostics deactivated
	1	0x1	Yes	Sending of warnings for PROFINET DHC diagnostics activated
EN DHC ALARM Enable alarms for PROFINET DHC diagnostics	**0**	**0x0**	**No**	Sending of alarms for PROFINET DHC diagnostics deactivated
	1	0x1	Yes	Sending of alarms for PROFINET DHC diagnostics activated
TH DHC WARN Threshold for PN DHC warnings	**2**…255	**0x02**…0xFF		If the threshold defined here is exceeded, warnings are issued for PROFINET DHC diagnostics. The parameters "Enable PROFINET DHC diagnostics (EN DHC DIAG)" and "Enable warnings for PROFINET DHC diagnostics" (EN DHC WARN) have to be activated.
TH DHC ALARM Threshold for PN DHC alarms	2…255, **3**	0x02… 0xFF, **0x03**		If the threshold defined here is exceeded, alarms are issued for PROFINET DHC diagnostics. The parameters "Enable PROFINET DHC diagnostics (EN DHC DIAG)" and "Enable alarms for PROFINET DHC diagnostics" (EN DHC ALARM) have to be activated.

- **Process input data** [▶ 130]

Process value	Offset	Data type
Max. number of successively lost PN RT frames since last PLC connection	%IB0	USINT
Reserved	%IB1	USINT
Max. number of successively lost PN RT frames since 10 minutes	%IB2	USINT
Reserved	%IB3	USINT

Sub module "RSTP"

The sub module "RSTP" can be plugged into slot 7.

- **Parameters** [▶ 126]

  Default values are **shown in bold.**

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
RSTP				
FB RSTP Enable RSTP	**0**	**0x0**	**No**	RSTP for LAN deactivated
	1	0x1	Yes	RSTP for LAN activated

Sub module "Module status"

The sub module "Module status" can be plugged into slot 8.

- **Process input data** [▶ 130]

Process value	Offset	Data type
Module status	%IB0	USINT
Undervoltage V1	%IX0.1	BOOL
Internal error	%IX0.2	BOOL
I/O-ASSISTANT Force Mode active	%IX0.6	BOOL
Module status	%IB1	USINT
Module diagnostics pending	%IX1.0	BOOL

7.5.2 Address setting in PROFINET

In IP-based communication, the field devices are addressed by means of an IP address. PROFINET uses the Discovery and Configuration Protocol (DCP) for IP assignment.

NOTE
DCP is a standard protocol and can also be used outside PROFINET, e.g. in IPC operating systems (Windows, Linux). DCP is available in tool packages such as WinPcap, Npcap, Wireshark etc.

When delivered, each field device has, among other things, a MAC address. The MAC address is sufficient to give the respective field device a unique name.

The address is assigned in two steps:

- Assignment of a unique plant specific name to the respective field device
- Assignment of the IP address from the IO-Controller before the system start-up based on the plant-specific (unique) name

PROFINET naming convention

The names are assigned via DCP. The device name is checked for correct spelling during input. The following rules apply to the use of the device name in accordance with PROFINET specification V2.3.

- All device names must be unique.
- Maximum name size: 240 characters
  Allowed:
  - Lower case letters a…z
  - Numbers 0…9
  - Hyphen and dot
- The name may consist of several components separated by a period. A name component, i.e. a string between two dots, may be a maximum of 63 characters long.
- The device name must not start or end with a hyphen.
- The name must not begin with or "port-xyz" (y…z = 0…9).
- The name must not have the form of an IP address (n.n.n.n, n = 0…999).
- Do not use special characters.
- Do not use capital letters.

7.5.3 MRP (Media Redundancy Protocol)

The device supports MRP. MRP is a standardized protocol according to IEC 62439. It describes a mechanism for media redundancy in ring topologies. With MRP, a defective ring topology with up to 50 nodes is detected and reconfigured in the event of an error. With MRP a trouble-free switch-over is not possible.

A Media Redundancy Manager (MRM) checks the ring topology of a PROFINET network defined by the network configuration for functionality. All other network nodes are Media Redundancy Clients (MRC). In the error-free state, the MRM blocks normal network traffic on one of its ring ports, with the exception of the test telegrams. The physical ring structure thus becomes a line structure again at the logical level for normal network traffic. If a test telegram fails to appear, a network error has occurred. In this case, the MRM opens its blocked port and establishes a new functioning connection between all remaining devices in the form of a linear network topology.

The time between ring interruption and recovery of a redundant path is called reconfiguration time. For MRP, this is a maximum of 200 ms. Therefore, an application must be able to compensate for the 200 ms interruption. The reconfiguration time always depends on the Media Redundancy Manager (e.g. the PROFINET PLC) and the I/O cycle and watchdog times set here. For PROFINET, the response monitoring time must be selected accordingly > 200 ms.

It is not possible to use Fast Start-Up in an MRP network.

NOTE
The TBEN-L…-SE-M2 is a media redundancy client (1-ring topologies). The two Ethernet ports used for MRP are freely selectable (XF1…XF10). The fieldbus control [▶ 29] has to be activated for both ports.

MRP is activated in the PROFINET engineering tool.

7.5.4 User data for acyclic services

The acyclic data exchange is by using via Record Data CRs (Communication Relation). Via these Record Data CRs the reading and writing of the following services is realized:

- Writing of AR data (AR = Application Relation)
- Writing of configuration data
- Reading and writing of device data
- Reading of diagnostic data
- Reading of I/O data
- Reading of Identification Data Objects (I&M functions)

Acyclic device user data

Index		Name	Data type	Access	Comment
Dec.	Hex.				
1	0x01	Module parameters	WORD	read/ write	Parameter data of the module (slot 0)
2	0x02	Module designation	STRING	read	Designation assigned to the module (slot 0)
3	0x03	Module revision	STRING	read	Firmware revision of the module
4	0x04	Vendor ID	WORD	read	Vendor ID for Turck
5	0x05	Module name	STRING	read	The device name assigned to the module
6	0x06	Module type	STRING	read	Device type of the module
7	0x07	Device ID	WORD	read	Device ID of the module
8…23	0x08… 0x17	reserved	-	-	-
24	0x18	Module diagnostics	WORD	read	Diagnostic data of the module (slot 0).
25…31	0x19… 0x1F	reserved	-	-	-
32	0x20	Input list	ARRAY of BYTE	read	List of all module input channels
33	0x21	Output list	ARRAY of BYTE	read	List of all module output channels
34	0x22	Diag. list	ARRAY of BYTE	read	List of all I/O-channel diagnostics
35	0x23	Parameter list	ARRAY of BYTE	read	List of all I/O-channel parameters
36… 28671	0x24… 0x6FFF	reserved	-	-	-
28672	0x7000	Module parameters	WORD	read/ write	Activate fieldbus protocol
28673… 45039	0x7001 … 0xAFEF	reserved	-	-	-
45040	0xAFF0	I&M0-functions		read	Identification & Maintaining
45041	0xAFF1	I&M1-functions	STRING[54]	read/ write	I&M Tag function and location

Index		Name	Data type	Access	Comment
45042	0xAFF2	I&M2-functions	STRING[16]	read/ write	I&M Installation Date
45043	0xAFF3	I&M3-functions	STRING[54]	read/ write	I&M Description Text
45044	0xAFF4	I&M4-functions	STRING[54]	read/ write	I&M Signature
45045… 45055	0xAFF5 … 0xAFFF	I&M5 to I&M15-functions		-	Not supported

7.6 Connecting the devices to a PROFINET controller with TIA Portal

Used hardware

The following hardware components are used in this example:

- Siemens PLC S7-1500
- TBEN-LL-SE-M2

Used software

The following software tools are used in this example:

- Totally Integrated Automation Portal (TIA Portal), SIMATIC STEP7 Professional V17
- GSDM file for TBEN-L…-SE-M2 (downloadable free of charge under www.turck.com)

Prerequisites

- The software is started.
- A new project has been created.
- The controller has been added to the project.

7.6.1 Installing the GSDML-file

The GSDML file is available for free at www.turck.com.

▶ Adding the GSDML file: Click **Options** → **Manage general station description files (GSD)**.

▶ Installing the GSDML file: Define the source path for the GSDML-file and click **Install**.

⇨ The device is added to the hardware catalog.

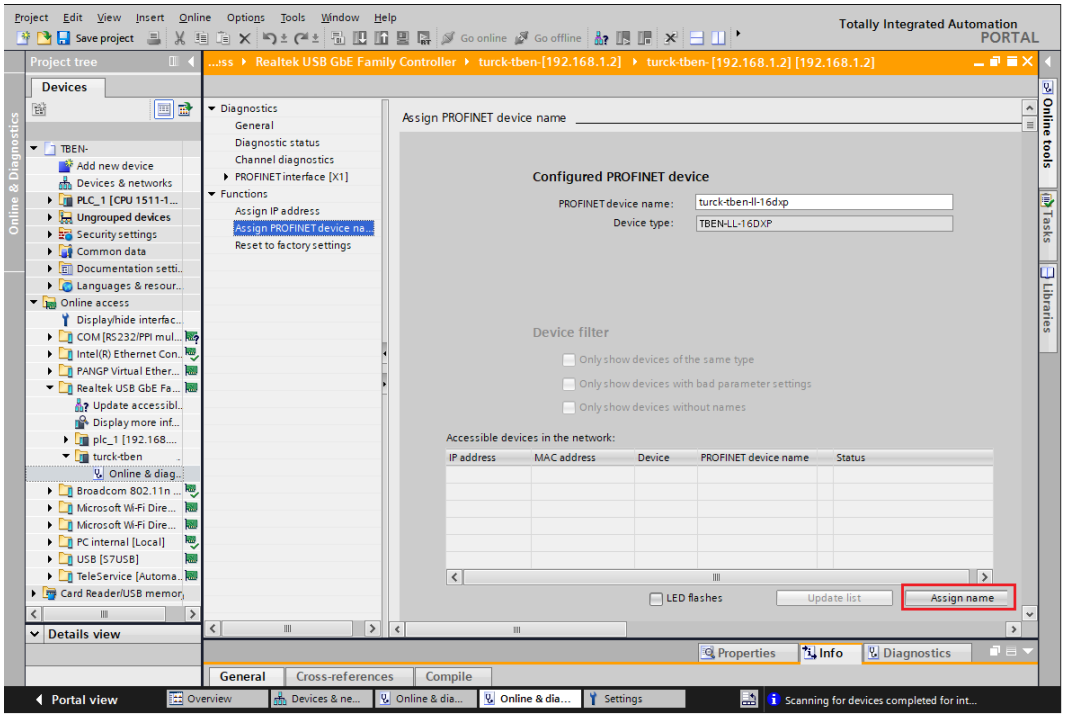

Fig. 25: Installing the GSDML file in TIA Portal

7.6.2 Connecting the device to the PLC

- Select the TBEN device from the Hardware catalog and drag it into the hardware window.
- Connect the devices to the PLC in the **Devices & networks** editor.

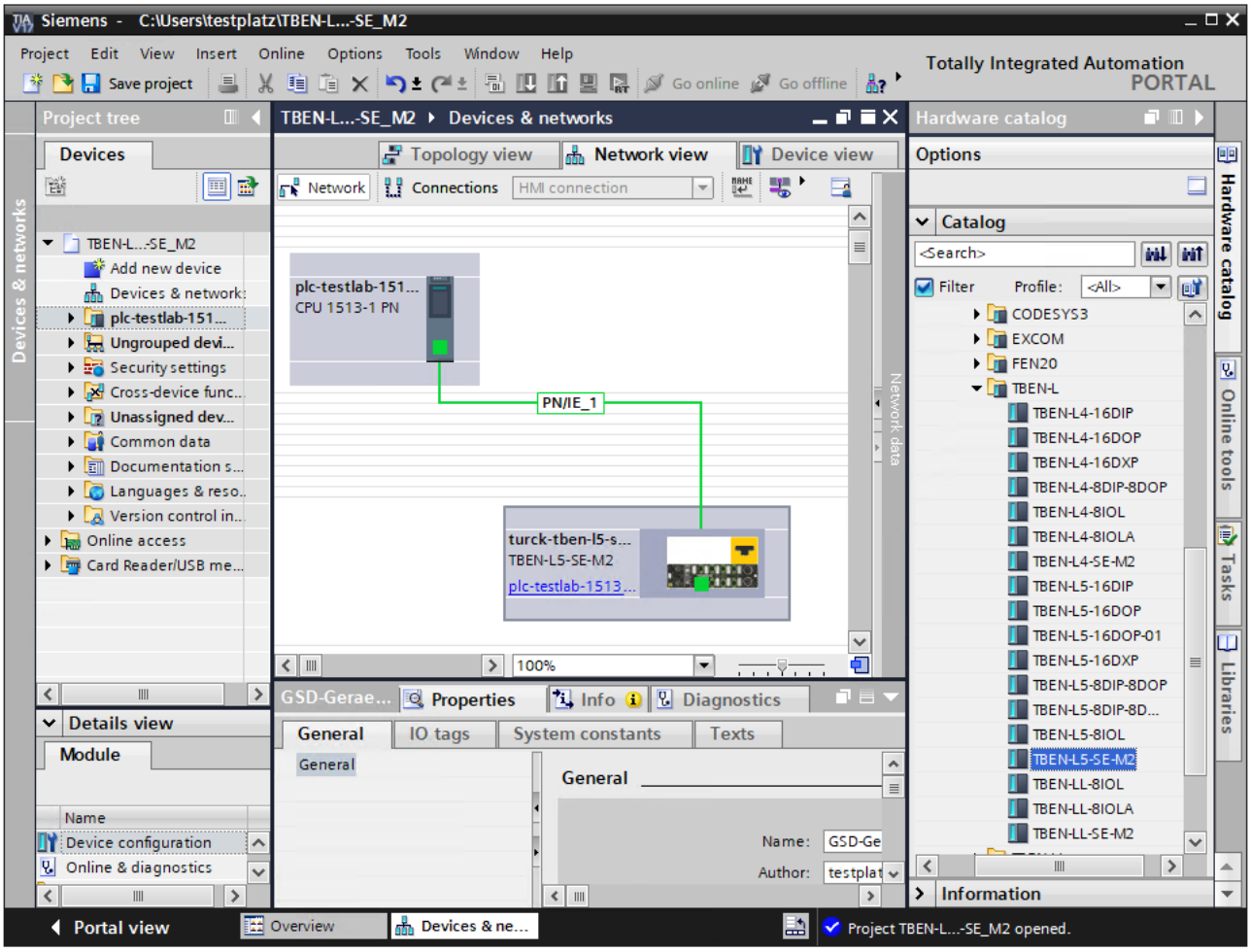

Fig. 26: Connecting the device to the PLC in TIA Portal

7.6.3 Setting the IP address in TIA Portal

- **Select Device view** → register **Properties** → **Ethernet addresses.**
- Assign the desired IP address.

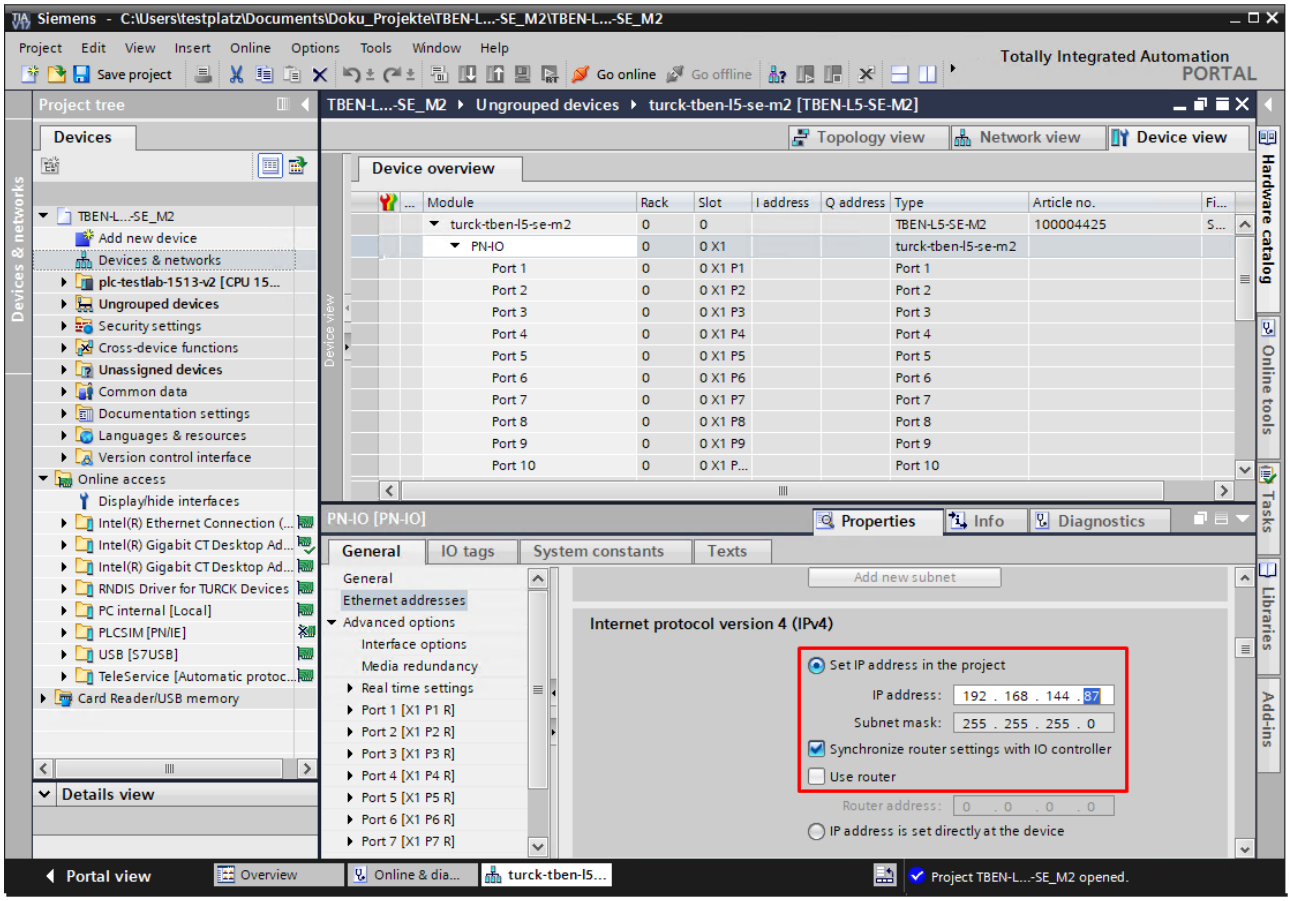

Fig. 27: Setting the IP address in TIA Portal

7.6.4 Configuring Device Functions

The TBEN-L…-SE-M2 appears as a modular slave with eight empty virtual slots. Slot 0 is already configured.

The function of the empty slots is defined in the GSDML file. The slots can only be used for a specific purpose.

Slot	Meaning
0	Main module tben-l…se-m2 (default name) Parameterization of functions, which are valid for the whole module
X1	Parameterization of PROFINET functions (IP address MRP, etc.)
X1 port 0…port 10	Parameterization of the Ethernet port properties (topology, connection options etc.).
Fieldbus control	Enabling or disabling fieldbus control or restricting the switch ports with fieldbus functionality [▷ 29]
Diagnostics netload	Enabling or disabling of netload diagnostics, warnings and alarms and configuration of the thresholds for notifications.
Diagnostics frame errors	Enabling or disabling of frame error diagnostics, warnings and alarms and configuration of the thresholds for notifications.
Diagnostics duplex/ link speed	Enabling or disabling of half duplex and link speed diagnostics and alarms.
Port control	Enabling or disabling port control and port-by-port enabling and disabling of ports XF1…XF10.
PN DHC	Enabling or disabling of diagnostics, warnings and alarms for PROFINET DHC (Data Hold Counter) and configuration of the thresholds for notifications
RSTP	Enabling or disabling of RSTP for the LAN network.
Module status	Optional mapping of the module status into the masters process image.

- **Select Device view → Device overview.**
- Select the switch functions from the hardware catalog and add them to the device slots via drag&drop.

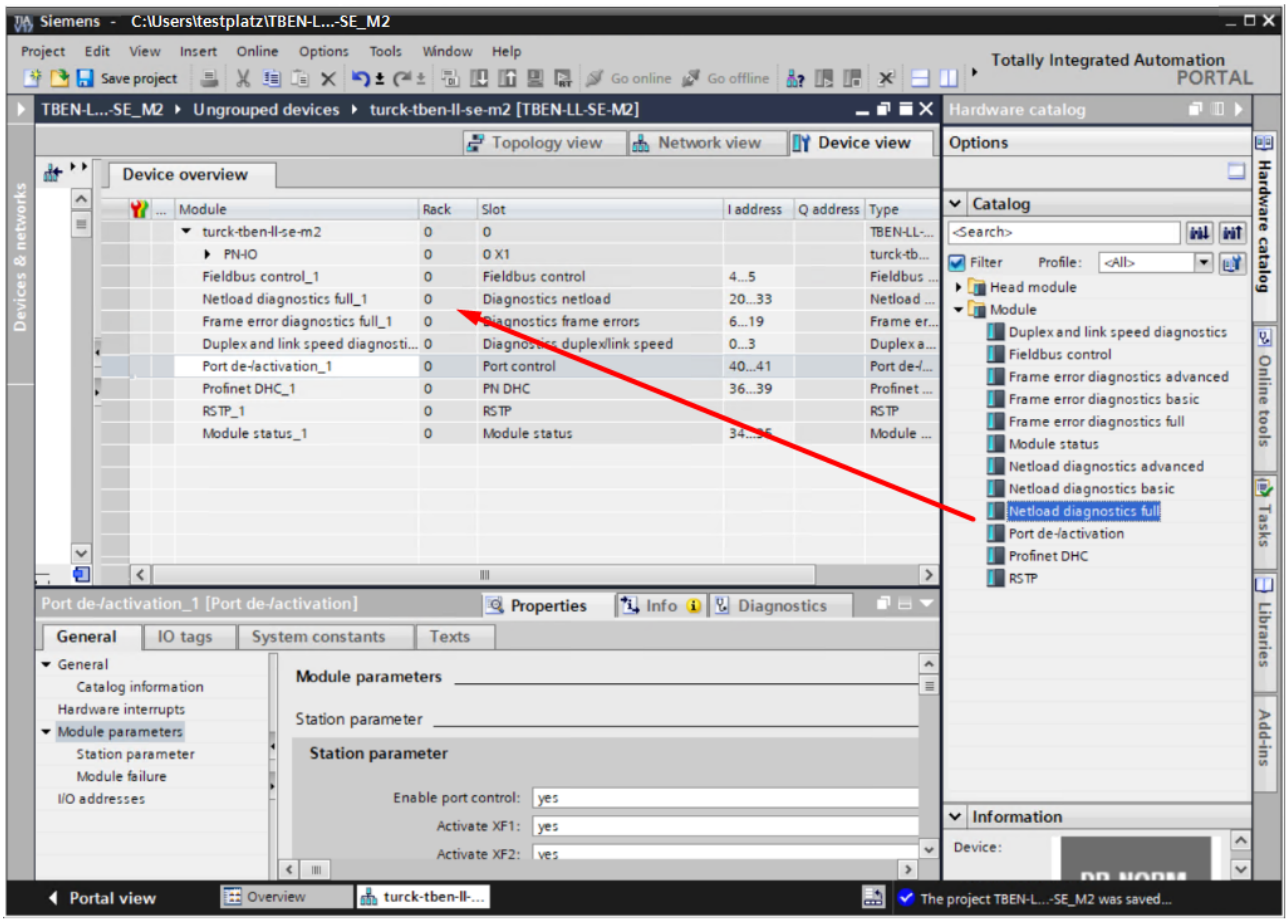

Fig. 28: Configuring the device slots in TIA Portal

7.6.5 Connecting the device online with the controller

- ▶ Start the online mode (Go online).
- ⇨ The device has been successfully connected to the PLC.

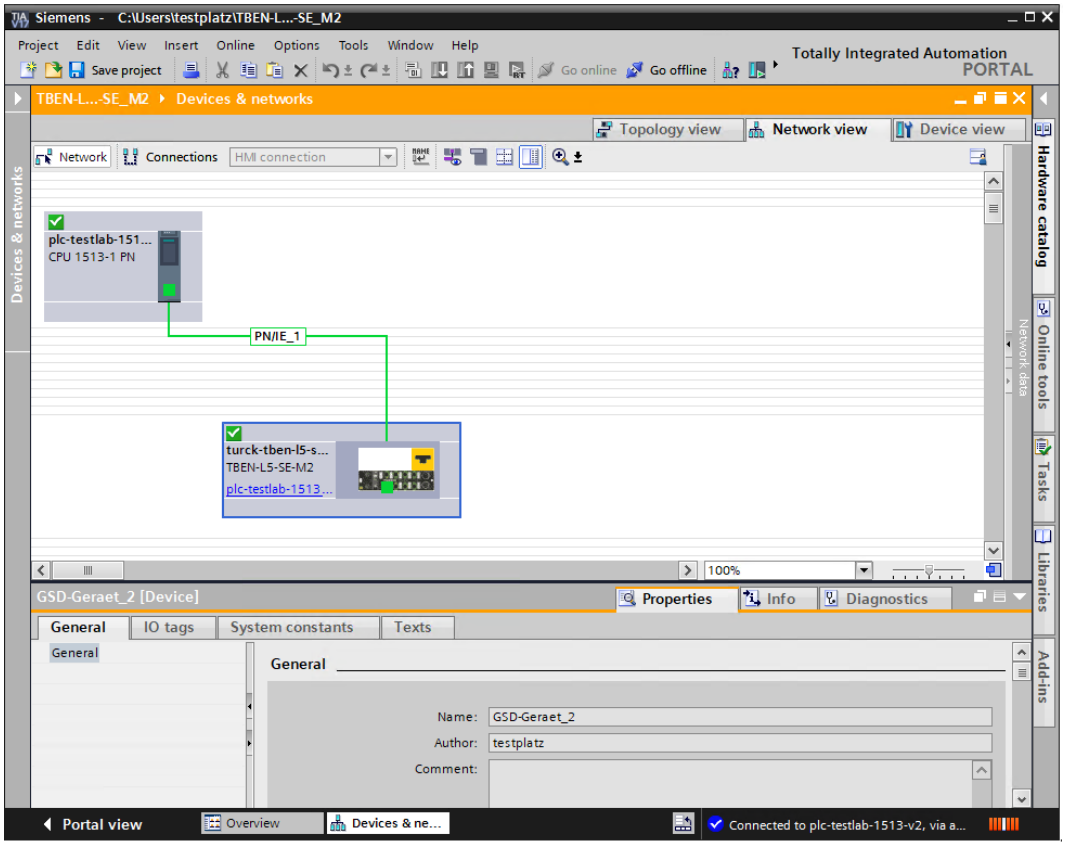

Fig. 29: Online mode in TIA Portal

7.7 Commissioning the devices in EtherNet/IP

7.7.1 EDS files and catalog files

The EDS and catalog files can be downloaded free of charge from www.turck.com.

7.7.2 Device Level Ring (DLR)

The devices support DLR (Device Level Ring). The DLR redundancy protocol is used to increase the stability of EtherNet/IP networks.

DLR-enabled devices have an integrated switch and can thus be integrated into a ring topology. The DLR protocol is used to detect an interruption in the ring. If the data line is interrupted, data are sent through an alternative network section, so that the network can be reconfigured as soon as possible.

DLR-capable network nodes (DLR supervisor) are provided with extended diagnostic functions which enable the devices to localize errors and thus decrease the time for error search and maintenance. Normally, the controller (i.e. the controller/PLC) assumes the supervisor function, all other network nodes are DLR participants. The supervisor blocks one of its two ports for normal Ethernet traffic, so that a line topology is created for normal Ethernet telegrams. DLR messages can continue to use the ring in both directions and thus continuously check the function of the ring.

NOTE
The TBEN-L…-SE-M2 is a DLR participant (1-ring topologies). The two Ethernet ports used for DLR are freely selectable (XF1…XF10) and are set in the device's web server. The fieldbus control [▶ 29] has to be activated for both ports.

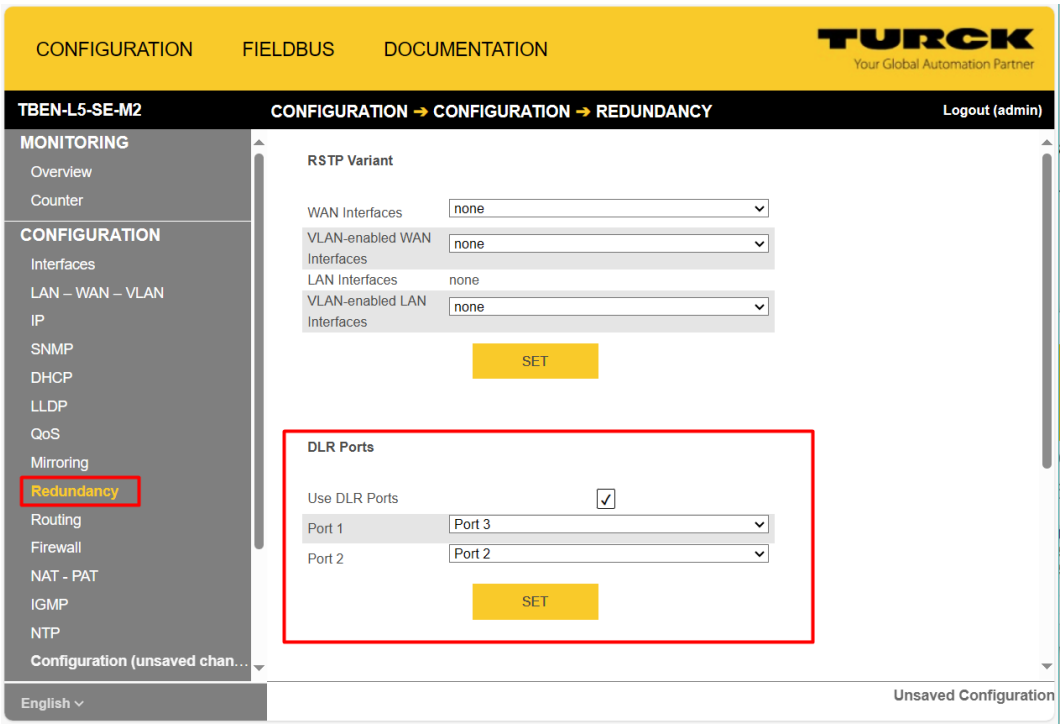

Fig. 30: Setting the switch ports for DLR in the web server

7.7.3 EtherNet/IP standard classes

The modules support the following EtherNet/IP Standard Classes in accordance with the CIP specification.

Class Code		Object name
Dec.	Hex.	
01	0x01	Identity Object [▶ 53]
04	0x04	Assembly Object [▶ 55]
06	0x06	Connection Manager Object [▶ 58]
245	0xF5	TCP/IP Interface Object [▶ 59]
246	0xF6	Ethernet Link Object [▶ 62]

Identity Object (0x01)

The following description of the Ethernet Link Object is taken from the CIP specification, Vol. 2, Rev. 2.1 by ODVA & ControlNet International Ltd. and adapted to the Turck products.

Instance attributes

Attr. no.		Attribute name	Get/Set	Type	Value
Dec.	Hex.				
1	0x01	Vendor	G	UINT	Contains the manufacturer ID. Turck = 0x30
2	0x02	Product type	G	UINT	Shows the general product type. Communications Adapter 12_{dez} = 0x0C
3	0x03	Product code	G	UINT	Identifies a special product in a device type. default: 27247_{dec} = 0x6A6F
4	0x04	Revision ■ Major ■ Minor	G	STRUCT OF: ■ USINT ■ USINT	Revision of the device which is represented by the Indentity Object ■ 0x01 ■ 0x06
5	0x05	Device status	G	WORD	WORD
6	0x06	Serial number	G	UDINT	Contains the last 3 bytes of the MAC ID.
7	0x07	Product name	G	STRUCT OF: USINT STRING [13]	i. e.: TBEN-LL-SE-M2

Device Status

Bit	Name	Definition
0…1	Reserved	Default = 0
2	Configured	TRUE = 1: The application in the device has been configured (default setting).
3	Reserved	Default = 0

Bit	Name	Definition
4…7	Extended Device Status	0011 = no I/O connection established 0110 = at least one I/O connection is in RUN mode 0111 = at least one I/O connection established, all in IDLE mode All other settings = reserved
8	Minor recoverable fault	Recoverable fault, e.g.: ■ Undervoltage ■ Force mode of DTM active ■ Diagnostics at I/O channel active
9…10	Reserved	
11	Diag	Common error bit
12…15	Reserved	Default = 0

Common services

Service code		Class	Instance	Service name
Dec.	Hex.			
1	0x01	Yes	Yes	Get_Attribute_All Returns a predefined list of object attributes.
5	0x05	No	Yes	Reset Starts the reset service for the device.
14	0x0E	Yes	Yes	Get_Attribute_Single Returns the content of a specified attribute.
16	0x10	No	No	Set_Attribute_Single Modifies a single attribute.

Assembly Object (0x04)

Assembly Objects bind attributes of multiple objects. to allow data to or from each object to be sent or received over a single connection.

The following description of the Ethernet Link Object is taken from the CIP specification, Vol. 2, Rev. 2.1 by ODVA & ControlNet International Ltd. and adapted to the Turck products.

Class attributes

Attr. no.		Attribute name	Get/set	Type	Value
Dec.	Hex.				
1	0x01	Revision	G	UINT	2
2	0x02	Max. object instance	G	UINT	104

Instance Attributes

Attr. no.		Attribute name	Get/set	Type	Value
Dec.	Hex.				
3	0x03	Data	S	ARRAY OF BYTE	Identifies a special product in a device type. default: $27247_{dec.}$ = 0x6A6F
4	0x04	Size	G	UINT	Number of bytes in attribute 3: 256 or variable

Common services

Service code		Class	Instance	Service name
Dec.	Hex.			
1	0x01	Yes	Yes	Get_Attribute_All Returns a predefined list of object attributes.
14	0x0E	Yes	Yes	Get_Attribute_Single Returns the content of a specified attribute.

Configuration Assembly (Instance 106)

The modules support Configuration Assembly.

The Configuration Assembly contains:

10 bytes module configuration data (EtherNet/IP specific)

+ x Byte (parameter data, depending on device type)

- Configuration Assembly

Byte no.		Bit no.							
Dec.	**Hex.**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0…9	0x00…0x09	-	-	-	-	-	-	-	-
Parameter data									
10	0x0A	-	-	-	-	-	-	-	EN FB CTRL
11	0x0B	FBUS LAST PORT							
12	0x0C	-	-	-	-	-	-	-	EN NL DIAG
13	0x0D	-	-	-	-	-	-	-	EN NL WARN
14	0x0E	-	-	-	-	-	-	-	EN NL ALARM
15	0x0F	TH NL WARN							
16	0x10	TH NL ALARM							
17	0x11	-							
18	0x12	-	-	-	-	-	-	-	EN FRM DIAG
19	0x13	-	-	-	-	-	-	-	EN FRM WARN
20	0x14	-	-	-	-	-	-	-	EN FRM ALARM
21	0x15	-							
22	0x16	FRM TB							
23	0x17								
24	0x18	TH FRM WARN							
25	0x19								
26	0x1A								
27	0x1B								
28	0x1C	TH FRM ALARM							
29	0x1D								
30	0x1E								
31	0x1F								
32	0x20	-	-	-	-	-	-	-	EN DUP DIAG
33	0x21	-	-	-	-	-	-	-	EN DUP ALARM
34	0x22	-	-	-	-	-	-	-	EN LS DIAG
35	0x23	-	-	-	-	-	-	-	EN LS ALARM
36	0x24	-	-	-	-	-	-	-	EN PORT CTRL
37	0x25	-	-	-	-	-	-	-	XF1 activated
…	…	-	-	-	-	-	-	-	…
46	0x2E	-	-	-	-	-	-	-	XF10 activated
47	0x2F	-							
48	0x30	-	-	-	-	-	-	-	EN RSTP

Meaning of parameter bits [▶ 126]

Process data instances

Instance 103 and Instance 104

- Input Assembly Instance 103:
  38 byte
- Output Assembly Instance 104:
  2 bytes Control word (no function)

Process data mapping

NOTE
Activating or deactivating the status and control Word in EtherNet/IP changes the process data mapping.

▶ Observe the offset in the device's process data mapping.

- **Input data**
  Status word + 18 words

Word no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Status																
0x0000	-	FCE	-	-	-	COM	V1	-	-	-	-	-	-	-	-	DIAG
IN																
0x0001	-	-	-	-	-	-	-	-	FBUS LAST PORT							
0x0002	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0x0003	-	-	-	-	-	-	-	-	NL MAX							
0x0004	-	-	-	-	-	-	-	-	NL MAX PLC							
0x0005	-	-	-	-	-	-	NL WARN RX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN RX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0x0006	-	-	-	-	-	-	NL WARN TX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN TX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0x0007	-	-	-	-	-	-	NL ALARM RX XF10	NL ALARM RX XF9	NL ALARM RX XF8	NL ALARM RX XF7	NL ALARM RX XF6	NL ALARM RX XF5	NL ALARM RX XF4	NL ALARM RX XF3	NL ALARM RX XF2	NL ALARM RX XF1
0x0008	-	-	-	-	-	-	NL ALARM TX XF10	NL ALARM TX XF9	NL ALARM TX XF8	NL ALARM TX XF7	NL ALARM TX XF6	NL ALARM TX XF5	NL ALARM TX XF4	NL ALARM TX XF3	NL ALARM TX XF2	NL ALARM TX XF1
0x0009	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0x000A	FE MAX															
0x000B																
0x000C	FE MAX PLC															
0x000D																
0x000E	-	-	-	-	-	-	FE WARN XF10	FE WARN XF9	FE WARN XF8	FE WARN XF7	FE WARN XF6	FE WARN XF5	FE WARN XF4	FE WARN XF3	FE WARN XF2	FE WARN XF1

Word no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0x000F	-	-	-	-	-	-	FE ALARM XF10	FE ALARM XF9	FE ALARM XF8	FE ALARM XF7	FE ALARM XF6	FE ALARM XF5	FE ALARM XF4	FE ALARM XF3	FE ALARM XF2	FE ALARM XF1
0x0010	-	-	-	-	-	-	DUP XF10	DUP XF9	DUP XF8	DUP XF7	DUP XF6	DUP XF5	DUP XF4	DUP XF3	DUP XF2	DUP XF1
0x0011	-	-	-	-	-	-	LS XF10	LS XF9	LS XF8	LS XF7	LS XF6	LS XF5	LS XF4	LS XF3	LS XF2	LS XF1
0x0012	-	-	-	-	-	-	PS XF10	PS XF9	PS XF8	PS XF7	PS XF6	PS F5	PS XF4	PS XF3	PS XF2	PS XF1

Meaning of the process data bits [▶ 130]

- **Output data**
  Control word (no function)

Word no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Control																
0x0000	reserved															

Connection Manager Object (0x06)

This object is used for connection and connectionless communications, including establishing connections across multiple subnets.

The following description of the Ethernet Link Object is taken from the CIP specification, Vol. 2, Rev. 2.1 by ODVA & ControlNet International Ltd. and adapted to the Turck products.

Common services

Service code		Class	Instance	Meaning
Dec.	Hex.			
84	0x54	No	Yes	FWD_OPEN_CMD (opens a connection)
78	0x4E	No	Yes	FWD_CLOSE_CMD (closes a connection)
82	0x52	No	Yes	UNCONNECTED_SEND_CMD

TCP/IP Interface Object (0xF5)

The following description of the Ethernet Link Object is taken from the CIP specification, Vol. 2, Rev. 1.1 by ODVA & ControlNet International Ltd. and adapted to the Turck products.

Class attributes

Attr. no.		Designation	Get/Set	Type	Value
Dec.	Hex.				
1	0x01	Revision	G	UINT	1
2	0x02	Max. object instance	G	UINT	1
3	0x03	Number of instances	G	UINT	1
6	0x06	Max. class identifier	G	UINT	7
7	0x07	Max. instance attribute	G	UINT	6

Instance Attributes

Attr. no.		Designation	Get/Set	Type	Value
Dec.	Hex.				
1	0x01	Status	G	DWORD	Interface status
2	0x02	Configuration capability	G	DWORD	Interface capability flag
3	0x03	Configuration control	G/S	DWORD	Interface control flag
4	0x04	Physical link object	G	STRUCT	
		Path size		UINT	Number of 16 bit words: 0x02
		Path		Padded EPATH	0x20, 0xF6, 0x24, 0x01
5	0x05	Interface configuration	G	Structure of:	TCP/IP network interface configuration
		IP address	G	UDINT	Actual IP address
		Network mask	G	UDINT	Actual network mask
		Gateway addr.	G	UDINT	Actual default gateway
		Name server	G	UDINT	0 = no server address configured
		Name server 2	G	UDINT	0 = no secondary server address configured
		Domain name	G	UDINT	0 = no Domain Name configured
6	0x06	Host name	G	STRING	0 = no host name configured
12	0x0C	QuickConnect	G/S	BOOL	0 = deactivate 1 = activate

Common services

Service code		Class	Instance	Meaning
Dec.	Hex.			
1	0x01	Yes	Yes	Get_Attribute_All
2	0x02	No	No	Set_Attribute_All
14	0x0E	Yes	Yes	Get_Attribute_Single
16	0x10	No	Yes	Set_Attribute_Single

Interface Status

The Status attribute indicates the status of the TCP/IP network interface.

Bit	Designation	Meaning
0…3	Interface configuration status	Indicates the status of the Interface Configuration attribute: 0 = The Interface Configuration attribute has not been configured 1 = The Interface Configuration attribute contains valid configuration. 2…15 = reserved
4…31	Reserved	

Configuration Capability

The Configuration Capability indicates the device's support for optional network configuration capability.

Bit	Designation	Meaning	Value
0	BOOTP client	The device is capable of obtaining its network configuration via BOOTP.	1
1	DNS client	The device is capable of resolving host names by querying a DNS server.	0
2	DHCP client	The device is capable of obtaining its network configuration via DHCP.	1

Configuration control

The Configuration Control attribute is used to control network configuration options.

Bit	Designation	Meaning
0…3	Startup configuration	Determines how the device shall obtain its initial configuration. 0 = The device shall use the interface configuration values previously stored (for example, in non-volatile memory or via hardware switches, etc). 1…3 = reserved
4	DNS Enable	Always 0
5…31	Reserved	Set to 0

Interface Configuration

This attribute contains the configuration parameters required to operate a TCP/IP device.

To change this attribute, proceed as follows:

- ▶ Read out the attribute.
- ▶ Change the parameters.
- ▶ Set the attribute.
- ⇨ The TCP/IP Interface Object applies the new configuration upon completion of the Set service. If the value of the Startup Configuration bits (Configuration Control attribute) is 0, the new configuration is stored in non-volatile memory.

The device does not reply to the set service until the values are safely stored to non-volatile memory.

An attempt to set any of the components of the Interface Configuration attribute to invalid values results in an error (status code 0x09) returned from the Set service. If initial configuration is obtained via BOOTP or DHCP, the Interface Configuration attribute components are all 0 until the BOOTP or DHCP reply is received. Upon receipt of the BOOTP or DHCP reply, the Interface Configuration attribute shows the configuration obtained via BOOTP/DHCP.

Host name

This attribute contains the device's host name. The host name attribute is used when the device supports the DHCP-DNS Update capability and has been configured to use DHCP upon start up. The mechanism allows the DHCP client to transmit its host name to the DHCP server. The DHCP server then updates the DNS records on behalf of the client.

Ethernet Link Object (0xF6)

The following description of the Ethernet Link Object is taken from the CIP specification, Vol. 2, Rev. 1.1 by ODVA & ControlNet International Ltd. and adapted to the Turck products.

Class attributes

Attr.-no.		Designation	Get/Set	Type	Value
Dec.	Hex.				
1	0x01	Revision	G	UINT	1
2	0x02	Max. object instance	G	UINT	1
3	0x03	Number of instances	G	UINT	1
6	0x06	Max. class identifier	G	UINT	7
7	0x07	Max. instance attribute	G	UINT	6

Instance attributes

Attr.-no.		Designation	Get/Set	Type	Value
Dec.	Hex.				
1	0x01	Interface speed	G	UDINT	Speed in megabit per second (e.g. 10, 100, 1000 etc.)
2	0x02	Interface flags	G	DWORD	Interface capability flag
3	0x03	Physical address	G	ARRAY OF USINT	Contains the interface's MAC address (Turck: 00:07:46:xx:xx:xx)
6	0x06	Interface control	G	2 WORD	Allows port-wise changes of the Ethernet-settings
7	0x07	Interface type	G		
10	0x0A	Interface label	G		

Interface flags

Bit	Designation	Meaning	Default value
0	Link status	Indicates whether or not the Ethernet communications interface is connected to an active network. 0 = inactive link 1 = active link	Depends on application
1	Half/full duplex	0 = Half duplex 1 = Full duplex If the Link Status flag is 0, the value of the Half/Full Duplex flag is indeterminate.	Depends on application
2…4	Negotiation status	Indicates the status of the automatic autonegotiation 0 = autonegotiation in progress 1 = autonegotiation and speed detection failed, using default values for speed and duplex (10 Mbps/half duplex). 2 = auto-negotiation failed but detected speed (default: half duplex). 3 = successfully negotiated speed and duplex 4 = autonegotiation not started, yet. Forced speed and duplex.	Depends on application

Bit	Designation	Meaning	Default value
5	Manual setting requires reset	0 = interface can activate changes to link parameters (auto-negotiate, duplex mode, interface speed) automatically 1 = device requires a Reset service to be issued to its Identity Object in order to adapt the changes.	0
6	Local Hardware Fault	0 = interface detects no local hardware fault 1 = local hardware error detected	0

Common services

Service code		Class	Instance	Meaning
Dec.	Hex.			
1	0x01	Yes	Yes	Get_Attribute_All
14	0x0E	Yes	Yes	Get_Attribute_Single
76	0x4C	No	Yes	Enetlink_Get_and_Clear

7.7.4 Vendor Specific Classes (VSC)

In addition to supporting the above named CIP Standard Classes, the device support the vendor specific classes (VSCs) described in the following.

Class Code		Name	Description
Dec.	Hex.		
100	0x64	Gateway	Data and parameters for the field bus specific part of the device.
190	0xBE	Fieldbus control	
191	0xBF	Diagnostics netload	
192	0xC0	Diagnostics frame errors	
193	0xC1	Duplex & Link speed	
194	0xC2	Port control	
196	0xC4	RSTP	Enabling/disabling of RSTP

Gateway Class (VSC 100)

This class contains all information concerning the whole device.

Object Instance 2, Gateway Instance

Attr. no.		Designation	Get/Set	Type	Meaning
Dec.	Hex.				
109	0x6D	Device Status	G	STRUCT	Contains the device status.
138	0x8A	GW status register	G/S	DWORD	Activates or deactivates the mapping of the status word into the device's input data. Activating or deactivating of the status word is only possible in Assembly Instance 103.
139	0x8B	GW Control Register	G/S	DWORD	Activates or deactivates the mapping of the control word into the device's output data. Activating or deactivating of the control word is only possible in Assembly Instance 104.

Fieldbus control (VSC 190)

Attr. no.		Designation	Get/ Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Enable fieldbus control	G/S	USINT	0: no 1: yes
2	0x02	Last port with fieldbus functionality	G/S	USINT	0x01…0x0A, Default: 0x0A
Process data					
3	0x03	Last port with fieldbus functionality	G	USINT	

Diagnostics netload (VSC 191)

Attr. no.		Designation	Get/Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Enable netload diagnostics	G/S	USINT	0 = no 1: yes (default)
2	0x02	Enable warnings for netload diagnostics	G/S	USINT	0: no 1: yes (default)
3	0x03	Enable alarms for netload diagnostics	G/S	USINT	0: no (default) 1: yes
4	0x04	Threshold for netload warnings in %	G/S	USINT	0x0000…0x0064, Default: 0x001E
5	0x05	Threshold for netload alarms in %	G/S	USINT	0x0000…0x0064, Default: 0x0050
Diagnostics					
6	0x06	Netload warning	G	USINT	0: inactive 1: active
7	0x07	Netload alarm	G	USINT	0: inactive 1: active
8	0x08	RX netload warning XF	G	WORD	Bit 0: Netload diagnostics 1 (XF1) Bit 1: Netload diagnostics 2 (XF2) Bit 2: Netload diagnostics 3 (XF3) … Bit 8: Netload diagnostics 9 (XF9) Bit 9: Netload diagnostics 10 (XF10)
9	0x09	TX netload warning XF	G	WORD	Bit 0: Netload diagnostics 1 (XF1) Bit 1: Netload diagnostics 2 (XF2) Bit 2: Netload diagnostics 3 (XF3) … Bit 8: Netload diagnostics 9 (XF9) Bit 9: Netload diagnostics 10 (XF10)

Attr. no.		Designation	Get/Set	Type	Meaning
Dec.	Hex.				
10	0x0A	RX netload alarm XF	G	WORD	Bit 0: Netload diagnostics 1 (XF1) Bit 1: Netload diagnostics 2 (XF2) Bit 2: Netload diagnostics 3 (XF3) … Bit 8: Netload diagnostics 9 (XF9) Bit 9: Netload diagnostics 10 (XF10)
11	0x0B	RX netload alarm XF	G	WORD	Bit 0: Netload diagnostics 1 (XF1) Bit 1: Netload diagnostics 2 (XF2) Bit 2: Netload diagnostics 3 (XF3) … Bit 8: Netload diagnostics 9 (XF9) Bit 9: Netload diagnostics 10 (XF10)
Process data					
12	0x0C	Netload warning	G	USINT	0: inactive 1: active
13	0x0D	Netload alarm	G	USINT	0: inactive 1: active
14	0x0E	Max. current netload (%)	G	USINT	
15	0x0F	Max. netload (peak) since last PLC connection (%)	G	USINT	
16	0x10	RX netload warning XF1	G	USINT	0: inactive 1: active
…	…	…			
25	0x12	RX netload warning XF10	G	USINT	0: inactive 1: active
26	0x1A	TX netload warning XF1	G	USINT	0: inactive 1: active
…	…	…	G	USINT	
35	0x23	TX netload warning XF10	G	USINT	0: inactive 1: active
36	0x24	RX netload alarm XF1	G	USINT	0: inactive 1: active
…	…	…			
45	0x2D	RX netload alarm XF10	G	USINT	0: inactive 1: active
46	0x2E	TX netload alarm XF1	G	USINT	0: inactive 1: active
…	…	…			
55	0x37	TX netload alarm XF10	G	USINT	0: inactive 1: active

Diagnostics frame errors (VSC 192)

Attr. no.		Designation	Get/Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Enable frame error diagnostics	G/S	USINT	0: no 1: yes (default)
2	0x02	Enable warnings for frame error diagnostics	G/S	USINT	0: no 1: yes (default)
3	0x03	Enable alarms for frame error diagnostics	G/S	USINT	0: no (default) 1: yes
4	0x04	Time base for frame error diagnostics	G/S	USINT	0x0000…0xFFFF, Default: 0x3C
5	0x05	Threshold for frame error warnings	G/S	USINT	0x00000000…0xFFFFFFFF, Default: 0x64
6	0x06	Threshold for frame error alarms	G	USINT	0x00000000…0xFFFFFFFF, Default: 0x03E8
Diagnostics					
7	0x07	Frame error warning	G	USINT	0: inactive 1: active
8	0x08	Frame error alarm	G	USINT	0: inactive 1: active
9	0x09	Frame error alarm	G	WORD	Bit 0: Frame error diagnostics 1 (XF1) Bit 1: Frame error diagnostics 2 (XF2) Bit 2: Frame error diagnostics 3 (XF3) … Bit 8: Frame error diagnostics 9 (XF9) Bit 9: Frame error diagnostics 10 (XF10)
10	0x0A	Frame error warning XF	G	WORD	Bit 0: Frame error diagnostics 1 (XF1) Bit 1: Frame error diagnostics 2 (XF2) Bit 2: Frame error diagnostics 3 (XF3) … Bit 8: Frame error diagnostics 9 (XF9) Bit 9: Frame error diagnostics 10 (XF10)
Process data					
11	0x0B	Frame error warning XF1	G	USINT	0: inactive 1: active
…	…	…			
24	0x18	Frame error warning XF10	G	USINT	0: inactive 1: active
25	0x19	Frame error alarm XF1	G	USINT	0: inactive 1: active
…	…	…	G	USINT	
34	0x22	Frame error alarm XF10	G	USINT	0: inactive 1: active

Duplex & Link speed (VSC 193)

Attr. no.		Designation	Get/Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Enable half duplex diagnostics	G/S	USINT	0: no (default) 1: yes
2	0x02	Enable half duplex alarms	G/S	USINT	0: no (default) 1: yes
3	0x03	Enable link speed diagnostics	G/S	USINT	0: no (default) 1: yes
4	0x04	Enable link speed alarms	G/S	USINT	0: no (default) 1: yes
Diagnostics					
5	0x05	Half duplex detected at XF…	G	WORD	Bit 0: Duplex and link speed diagnostics 1 (XF1) Bit 1: Duplex and link speed diagnostics 2 (XF2) Bit 2: Duplex and link speed diagnostics 3 (XF3) … Bit 8: Duplex and link speed diagnostics 9 (XF9) Bit 9: Duplex and link speed diagnostics 10 (XF10)
6	0x06	10 Mbps detected at XF…	G	WORD USINT	Bit 0: Duplex and link speed diagnostics 1 (XF1) Bit 1: Duplex and link speed diagnostics 2 (XF2) Bit 2: Duplex and link speed diagnostics 3 (XF3) … Bit 8: Duplex and link speed diagnostics 9 (XF9) Bit 9: Duplex and link speed diagnostics 10 (XF10)
Process data					
7	0x07	Half duplex detected at XF…	G	WORD	Bit 0: Duplex and link speed diagnostics 1 (XF1) Bit 1: Duplex and link speed diagnostics 2 (XF2) Bit 2: Duplex and link speed diagnostics 3 (XF3) … Bit 8: Duplex and link speed diagnostics 9 (XF9) Bit 9: Duplex and link speed diagnostics 10 (XF10)
8	0x08	10 Mbps detected at XF…	G	WORD	Bit 0: Duplex and link speed diagnostics 1 (XF1) Bit 1: Duplex and link speed diagnostics 2 (XF2) Bit 2: Duplex and link speed diagnostics 3 (XF3) … Bit 8: Duplex and link speed diagnostics 9 (XF9) Bit 9: Duplex and link speed diagnostics 10 (XF10)

Port control (VSC 194)

Attr. no.		Designation	Get/ Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Port control	G/S	USINT	0: no 1: yes (default)
2	0x02	Activate XF…	G/S	WORD	Bit 0: Port de-/activation 1 (XF1) Bit 1: Port de-/activation 2 (XF2) Bit 2: Port de-/activation 3 (XF3) Bit 3: Port de-/activation 4 (XF4) Bit 4: Port de-/activation 5 (XF5) Bit 5: Port de-/activation 6 (XF6) Bit 6: Port de-/activation 7 (XF7) Bit 7: Port de-/activation 8 (XF8) Bit 8: Port de-/activation 9 (XF9) Bit 9: Port de-/activation 10 (XF10)
Process data					
3	0x03	XF active	G	WORD	Bit 0: Port de-/activation 1 (XF1) Bit 1: Port de-/activation 2 (XF2) Bit 2: Port de-/activation 3 (XF3) Bit 3: Port de-/activation 4 (XF4) Bit 4: Port de-/activation 5 (XF5) Bit 5: Port de-/activation 6 (XF6) Bit 6: Port de-/activation 7 (XF7) Bit 7: Port de-/activation 8 (XF8) Bit 8: Port de-/activation 9 (XF9) Bit 9: Port de-/activation 10 (XF10)

RSTP (VSC 196)

Attr. no.		Designation	Get/ Set	Type	Meaning
Dec.	Hex.				
Parameters					
1	0x01	Enable RSTP…	G/S	USINT	0: no 1: yes (default)

7.8 Connecting the devices to an EtherNet/IP scanner with Studio 5000

Used hardware

The following hardware components are used in this example:

- Rockwell PLC ControlLogix 1756-L72, Logix 5572
- Rockwell Scanner 1756-EN2TR
- TBEN-LL-SE-M2

Used software

The following software tools are used in this example:

- Rockwell Studio 5000
- Catalog file for TBEN-L…-SE-M (downloadable free of charge together with EDS files under **www.turck.com**)

Prerequisites

- An instance of the software with the catalog files is opened.
- A new project has been created in a second instance of Studio 5000.
- The PLC and the scanner mentioned above have been added to the project in the second instance of Studio 5000.

7.8.1 Adding the devices from the Catalog files to the new project

▶ Right-click the device entry and use **Copy**.

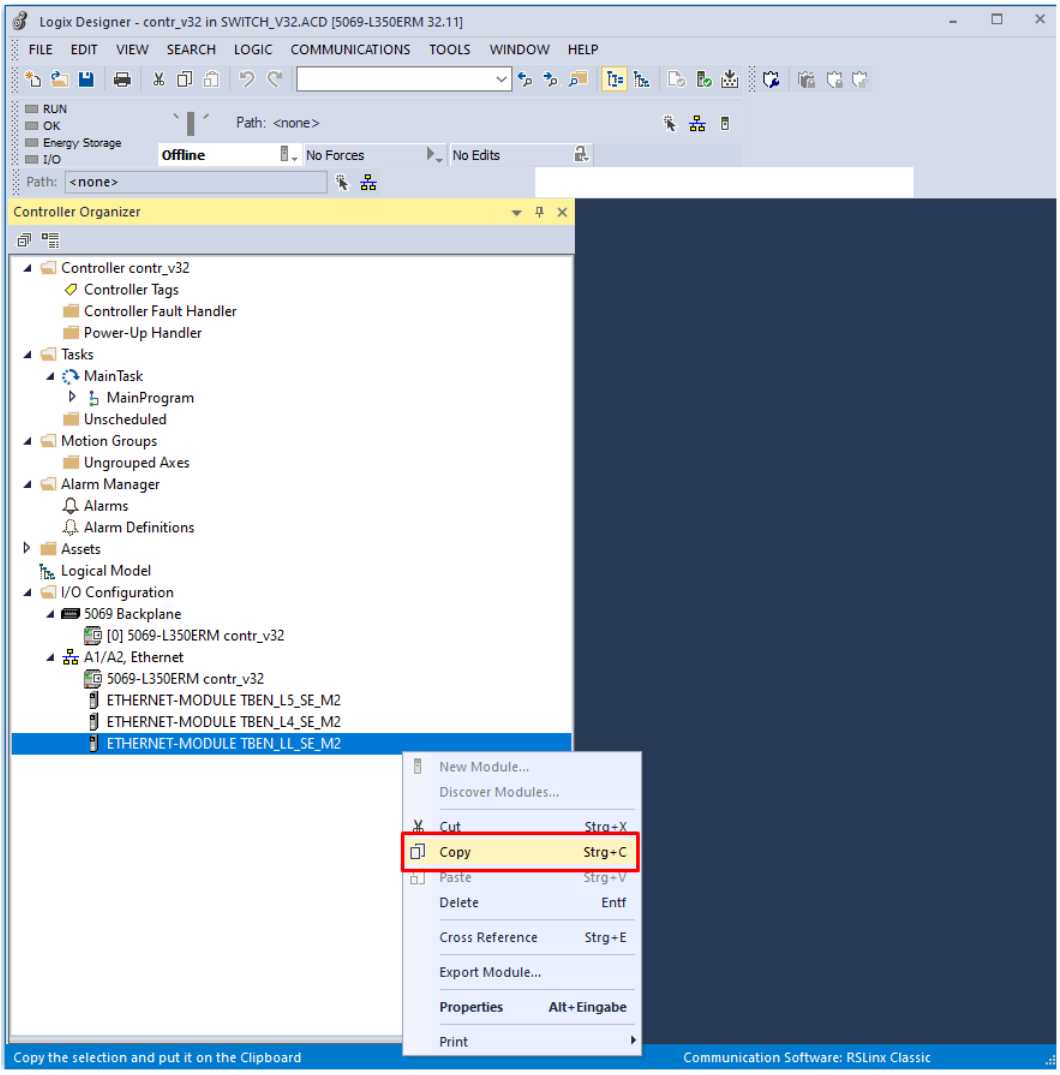

Fig. 31: Copying the device from catalog file in Logix Designer

▶ Right-click the EtherNet/IP Scanner in the 2nd instance of Logix Designer and add the device to the project via **Paste**.

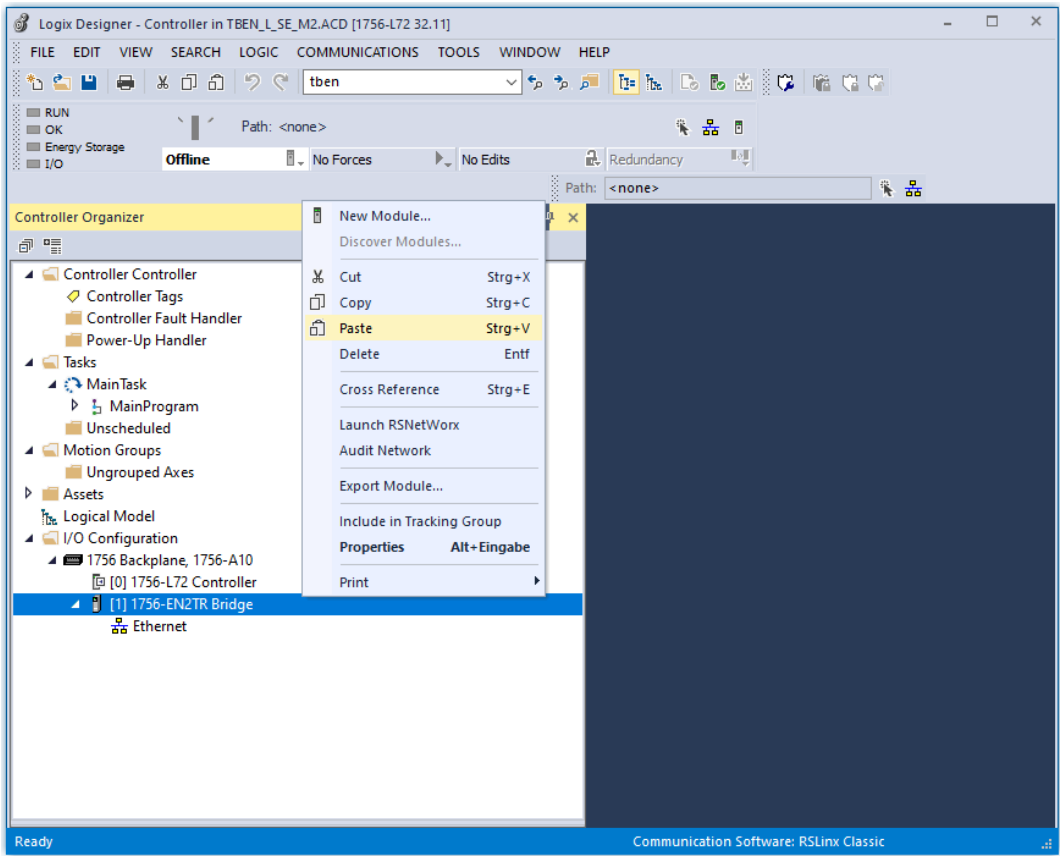

Fig. 32: Adding the device to the project in Logix Designer

7.8.2 Configuring the device in Logix Designer

- Open the device entry by double-clicking.
- Assign a module name.
- Set the IP address of the device (example: 192.168.145.181).

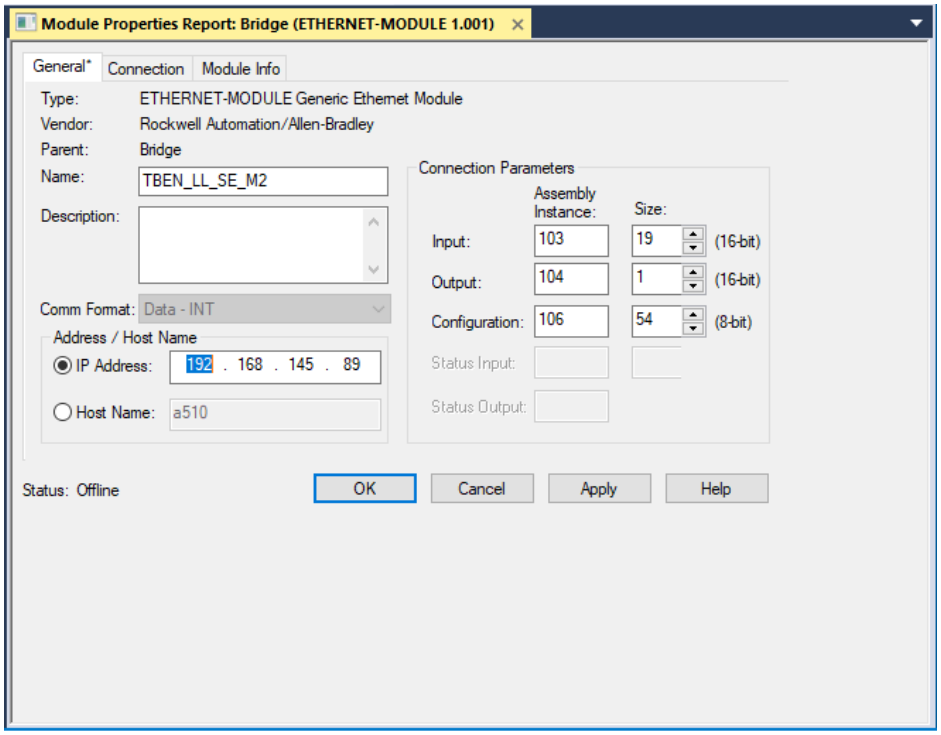

Fig. 33: Assigning device name and IP address

- Optional: Set the connection parameters.

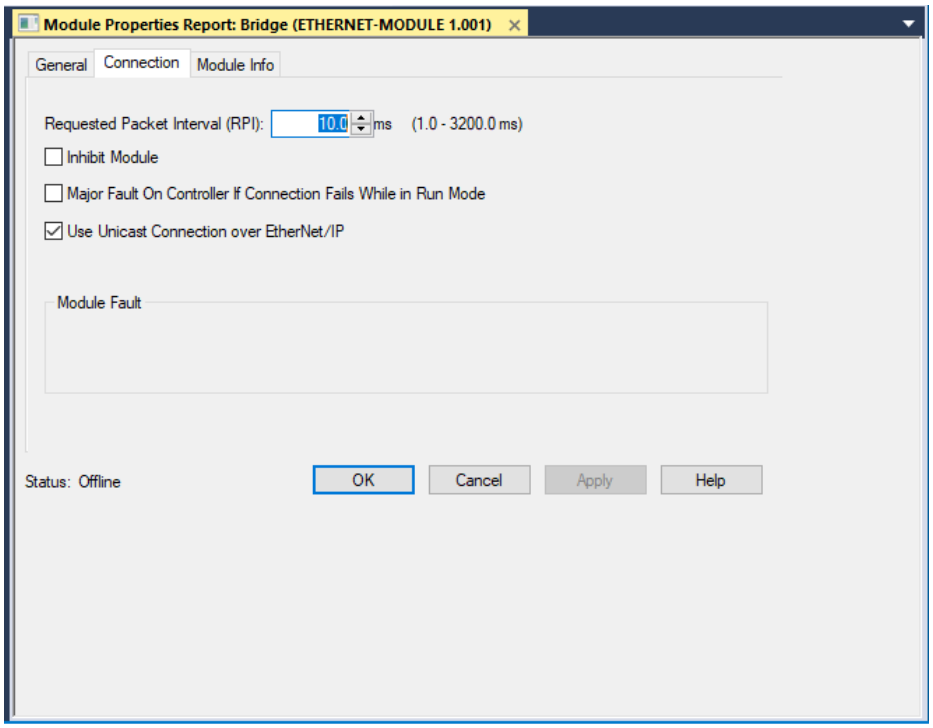

Fig. 34: Setting the connection parameters

7.8.3 Parameterizing the device

- Open the Controller Tags of the device.
- Parameterize the device via the Controller Tags **TBEN-LL-SE-M2:C**.

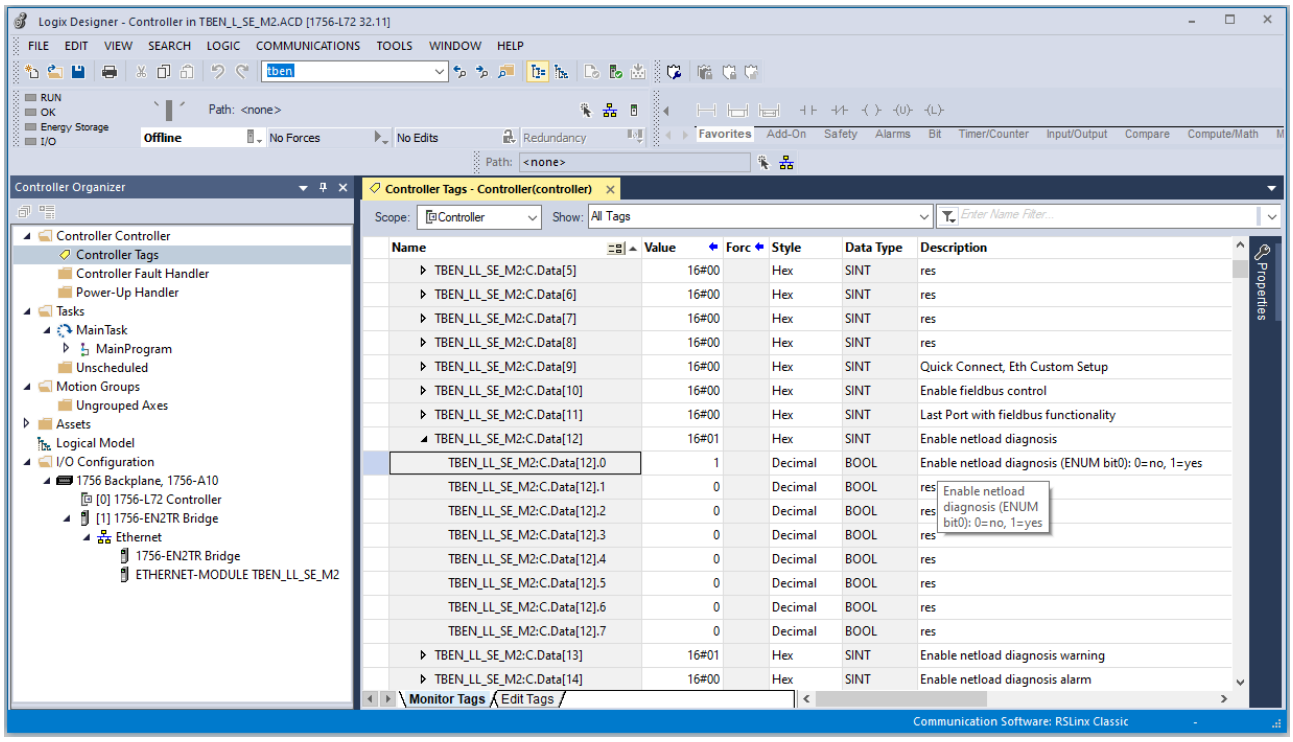

Fig. 35: Parameterizing the device

7.8.4 Going online with the PLC

- ▶ Search the network via the **Who Active** button.
- ▶ Select the PLC.
- ▶ Set the communication path via **Set Project Path**.
- ⇨ The communication path is set.

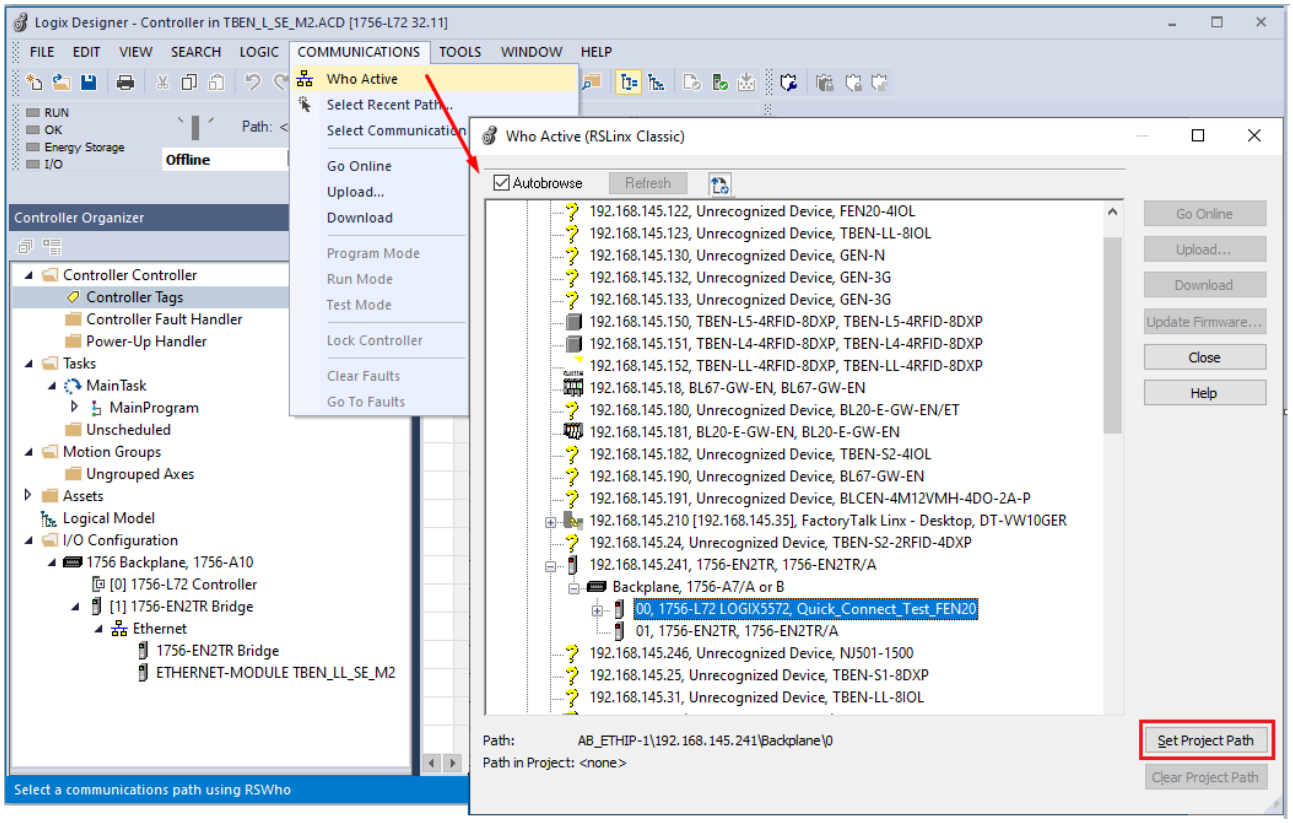

Fig. 36: Setting the communication path

- ▶ Select the PLC.
- ▶ Click **Go online**.

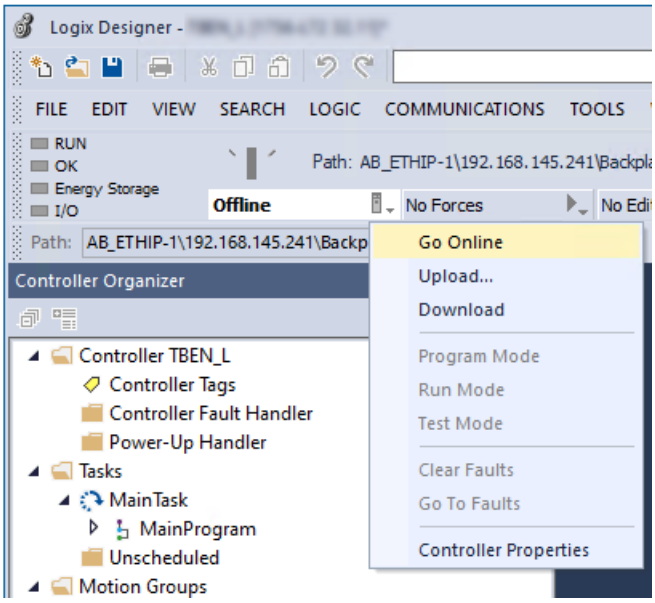

Fig. 37: Going online with the device

- ▶ Click **Download** in the following dialog (Connect To Go Online).
- ▶ Confirm all following messages.
- ⇨ The program is downloaded to the PLC. The online connection is established.

7.8.5 Reading process data

- ▶ Open the Controller Tags in the project tree by double-clicking the entry.
- ⇨ The access to the input data (**TBEN-LL-SE-M2:I**) and output data (**TBEN-LL-SE-M2:O**) is possible.

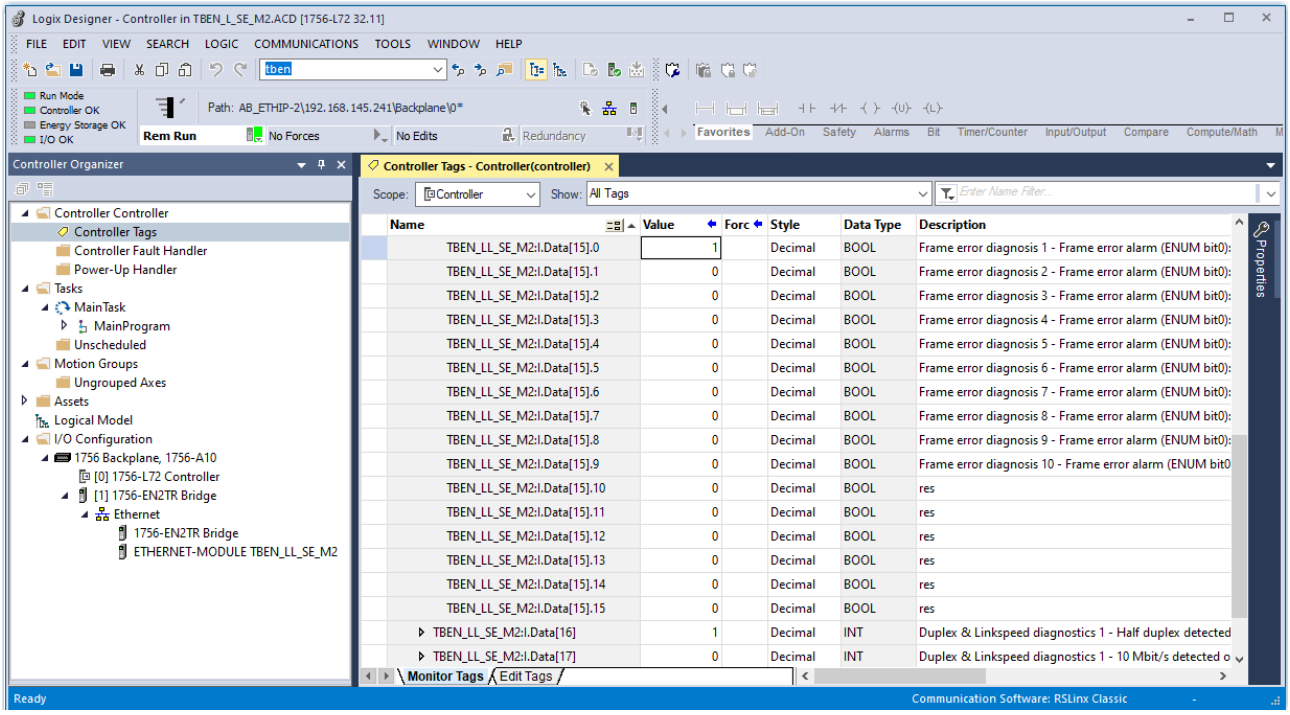

Fig. 38: Controller Tags in the project tree of the Logix Designer

7.9 Commissioning the device in Modbus TCP

7.9.1 Implemented Modbus functions

The devices support the following functions for accessing process data, parameters, diagnostics and other services.

Function Code	
3	Read Holding Registers – reading multiple output registers
4	Read Input Registers – reading multiple input registers
6	Write Single Register – writing single output register
16	Write Multiple Registers – writing multiple output
23	Read/Write Multiple Registers – reading and writing multiple registers

7.9.2 Modbus registers

Address	Access	Meaning
0x0000…0x01FF	read only	Process data of the inputs (identical to registers 0x8000… 0x8FFF)
0x1000…0x100B	read only	Module identifier, contains the first 24 characters of the device type
0x100C	read only	Module status
0x1017	read only	Register mapping revision (always 2, if not, mapping is incompatible with this description)
0x1020	read only	Watchdog, actual time in ms
0x1120	read/write	Watchdog, predefined time in ms (default: 500 ms
0x1130	read/write	Modbus connection mode register
0x1131	read/write	Modbus connection timeout in s. (default: 0 = never)
0x113C…0x113D	read/write	Modbus parameter restore (reset of parameters to default values)
0x113E…0x113F	read/write	Modbus parameter save (permanent storing of parameters)
0x1140	read/write	Deactivate protocol Deactivates explicitly the selected Ethernet protocol: ■ Bit 0 = deactivate EtherNet/IP ■ Bit 1 = deactivate Modbus TCP ■ Bit 2 = deactivate PROFINET ■ Bit 15 = deactivate web server
0x1141	read/write	Active protocol ■ Bit 0 = EtherNet/IP active ■ Bit 1 = Modbus TCP active ■ Bit 2 = PROFINET active ■ Bit 15 = web server active
0x2400	read only	V1 in mV: 0 at undervoltage
0x8000…0x8400	read only	Process data of the inputs (identical to registers 0x0000… 0x01FF)
0xA000…0xA400F	read only	Diagnostics
0xB000…0xB400	read/write	Parameters

The following table shows the register mapping for the different Modbus addressing methods:

Description	Hex	Decimal	5 digit	Modicon
Inputs	0x0000…0x01FF	0…511	40001…40512	400001…400512
Module identifier	0x1000…0x1006	4096…4102	44097…44103	404097…404103
Module status	0x100C	4108	44109	404109
Watchdog, actual time	0x1020	4128	44129	404129
Watchdog, predefined time	0x1120	4384	44385	404385
Modbus connection mode register	0x1130	4400	44401	404401
Modbus connection timeout in s.	0x1131	4401	44402	404402
Modbus parameter restore	0x113C…0x113D	4412…4413	44413…44414	404413…404414
Modbus parameter save	0x113E…0x113F	4414…4415	44415…44416	404415…404416
Deactivate protocol	0x1140	4416	44417	404417
Active protocol	0x1141	4417	44418	404418
V1 in mV	0x2400	9216	49217	409217
Process data inputs	0x8000, 0x8001	32768, 32769	-	432769, 432770
Diagnostics	0xA000, 0xA001	40960, 40961	-	440961, 440962
Parameters	0xB000, 0xB001	45056, 45057	-	445057, 445058

Register 0x1130: Modbus connection mode

This register defines the behavior of the Modbus connections.

Bit	Designation	Value	Meaning
0	MB_OnlyOneWrite Permission	**0**	All Modbus connections receive the write authorization.
		1	Only one Modbus connection can receive the write permission. A write permission is opened until a disconnect. After the disconnect the next connection which requests a write access receives the write authorization.
1	MB_ImmediateWrite Permission	**0**	With the first write access, a write authorization for the respective Modbus connection is requested. If this request fails, an exception response with exception-code 0x01 is generated. If the request is accepted, the write access is executed and the write authorization remains active until the connection is closed.
		1	The write authorization for the respective Modbus connection is already opened during the connection establishment. The first Modbus connection thus receives the write authorization, all following connections don't (only if bit 0 = 1).
2…15	Reserved	-	-

Register 0x1131: Modbus connection timeout

This register defines after which time of inactivity a Modbus connection is closed through a disconnect.

Value range: 0…65535 s

default: 0 s = never (Modbus connection will never be closed)

Behavior of the BUS LED

If Modbus is the active protocol in case of a connection timeout and no further Modbus connections exist, the BUS LED behaves as follows:

Connection timeout	BUS LED
Timeout	Green flashing

Register 0x113C and 0x113D: Restore Modbus connection parameters

Registers 0x113C and 0x113D serve for resetting the parameter-register 0x1120 and 0x1130 to 0x113B to the default settings. The service resets the parameters without saving them.

Procedure:

- ▶ Write 0x6C6F to register 0×113C.
- ▶ To activate the reset of the registers, write 0x6164 (”load”) within 30 seconds in register 0x113D. Both registers can also be written with one single request using the function codes FC16 and FC23.
- ⇨ The parameters are reset tot default values.
- ▶ Save changes via a subsequent Save service.

Register 0x113E and 0x113F: Save Modbus connection parameters

Registers 0x113E and 0x113F are used for the non-volatile saving of parameters in registers 0x1120 and 0x1130 to 0x113B.

Procedure:

- ▶ Write 0x7361 to register 0×113E.
- ▶ Write 0x7665 (”save”) within 30 seconds in register 0x113F to activate the reset of the registers. Both registers can also be written with one single request using the function codes FC16 and FC23.
- ⇨ The parameters are saved.

7.9.3 Data width of the devices

The following table shows the data width of the TBEN-L… modules within the Modbus register area and the type of data alignment.

Module	Process input	Process output	Alignment
TBEN-L…-SE-M2	16 bit	-	Bit by bit

7.9.4 Register mapping of the devices

Input registers

Register no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Fieldbus control																
0x0000	-	-	-	-	-	-	-	-	FBUS LAST PORT							
Netload diagnostics, Basic																
0x0001	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
Netload diagnostics, Advanced																
0x0001	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0x0002	-	-	-	-	-	-	-	-	NL MAX							
0x0003	-	-	-	-	-	-	-	-	NL MAX PLC							
Netload diagnostics, Full																
0x0001	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0x0002	-	-	-	-	-	-	-	-	NL MAX							
0x0003	-	-	-	-	-	-	-	-	NL MAX PLC							
0x0004	-	-	-	-	-	-	NL WARN RX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN RX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0x0005	-	-	-	-	-	-	NL WARN TX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN TX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0x0006	-	-	-	-	-	-	NL ALARM RX XF10	NL ALARM RX XF9	NL ALARM RX XF8	NL ALARM RX XF7	NL ALARM RX XF6	NL ALARM RX XF5	NL ALARM RX XF4	NL ALARM RX XF3	NL ALARM RX XF2	NL ALARM RX XF1
0x0007	-	-	-	-	-	-	NL ALARM TX XF10	NL ALARM TX XF9	NL ALARM TX XF8	NL ALARM TX XF7	NL ALARM TX XF6	NL ALARM TX XF5	NL ALARM TX XF4	NL ALARM TX XF3	NL ALARM TX XF2	NL ALARM TX XF1
Frame error diagnostics, Basic																
0x0008	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
Frame error diagnostics, Advanced																
0x0008	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0x0009	FE MAX															
0x000A																
Frame error diagnostics, Full																
0x0008	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0x0009	FE MAX															
0x000A																

Register no.	Bit no.															
	15	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0x000B	FE MAX PLC															
0x000C																
0x000D	-	-	-	-	-	-	FE WARN XF10	FE WARN XF9	FE WARN XF8	FE WARN XF7	FE WARN XF6	FE WARN XF5	FE WARN XF4	FE WARN XF3	FE WARN XF2	FE WARN XF1
0x000E	-	-	-	-	-	-	FE ALARM XF10	FE ALARM XF9	FE ALARM XF8	FE ALARM XF7	FE ALARM XF6	FE ALARM XF5	FE ALARM XF4	FE ALARM XF3	FE ALARM XF2	FE ALARM XF1
Duplex diagnostics																
0x000F	-	-	-	-	-	-	DUP XF10	DUP XF9	DUP XF8	DUP XF7	DUP XF6	DUP XF5	DUP XF4	DUP XF3	DUP XF2	DUP XF1
Link speed diagnostics																
0x0010	-	-	-	-	-	-	LS XF10	LS XF9	LS XF8	LS XF7	LS XF6	LS XF5	LS XF4	LS XF3	LS XF2	LS XF1
Port status																
0x0011	-	-	-	-	-	-	PS XF10	PS XF9	PS XF8	PS XF7	PS XF6	PS XF5	PS XF4	PS XF3	PS XF2	PS XF1
Counter for lost PROFINET RT frames (only for PROFINET)																
0x0012	-	-	-	-	-	-	-	-	MAX PN RT FRAMES PLC							
0x0013	-	-	-	-	-	-	-	-	MAX PN RT FRAMES							
Module status																
0x0014	-	-	-	-	-	-	-	DIAG	-	FCE	-	-	-	COM	V1	-

Meaning of the process data bits [▶ 130]

Diagnostic registers

Register no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Netload diagnostics																
0xA000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0xA001	-	-	-	-	-	-	NL WARN RX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN RX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0xA002	-	-	-	-	-	-	NL WARN TX XF10	NL WARN TX XF9	NL WARN TX XF8	NL WARN TX XF7	NL WARN TX XF6	NL WARN TX XF5	NL WARN TX XF4	NL WARN TX XF3	NL WARN TX XF2	NL WARN TX XF1
0xA003	-	-	-	-	-	-	NL ALARM RX XF10	NL ALARM RX XF9	NL ALARM RX XF8	NL ALARM RX XF7	NL ALARM RX XF6	NL ALARM RX XF5	NL ALARM RX XF4	NL ALARM RX XF3	NL ALARM RX XF2	NL ALARM RX XF1
0xA004	-	-	-	-	-	-	NL ALARM TX XF10	NL ALARM TX XF9	NL ALARM TX XF8	NL ALARM TX XF7	NL ALARM TX XF6	NL ALARM TX XF5	NL ALARM TX XF4	NL ALARM TX XF3	NL ALARM TX XF2	NL ALARM TX XF1
Frame error diagnostics																
0xA005	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0xA006	-	-	-	-	-	-	FE WARN XF10	FE WARN XF9	FE WARN XF8	FE WARN XF7	FE WARN XF6	FE WARN XF5	FE WARN XF4	FE WARN XF3	FE WARN XF2	FE WARN XF1
0xA007	-	-	-	-	-	-	FE ALARM XF10	FE ALARM XF9	FE ALARM XF8	FE ALARM XF7	FE ALARM XF6	FE ALARM XF5	FE ALARM XF4	FE ALARM XF3	FE ALARM XF2	FE ALARM XF1
Duplex diagnostics																
0xA008	-	-	-	-	-	-	DUP XF10	DUP XF9	DUP XF8	DUP XF7	DUP XF6	DUP XF5	DUP XF4	DUP XF3	DUP XF2	DUP XF1
Link speed diagnostics																
0xA009	-	-	-	-	-	-	LS XF10	LS XF9	LS XF8	LS XF7	LS XF6	LS XF5	LS XF4	LS XF3	LS XF2	LS XF1
PROFINET DHC error diagnostics (PROFINET only)																
0xA00A	-	-	-	-	-	-	DHC ALARM AR2	DHC ALARM AR1	-	-	-	-	-	-	DHC WARN AR2	DHC WARN AR1

Meaning of diagnostic bits [▶ 135]

Parameter registers

Register no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Fieldbus control																
0xB000	FBUS LAST PORT									-	-	-	-	-	-	EN FB CTRL
Netload diagnostics																
0xB001	-	-	-	-	-	-	-	-	-	-	-	-	-	EN NL ALARM	EN NL WARN	EN NL DIAG
0xB002	-	-	-	-	-	-	-	-	TH NL WARN							
0xB003	-	-	-	-	-	-	-	-	TH NL ALARM							
Frame error diagnostics																
0xB004	-	-	-	-	-	-	-	-	-	-	-	-	-	EN FRM ALARM	EN FRM WARN	EN FRM DIAG
0xB005	FRM TB															
0xB006	TH FRM WARN															
0xB007																
0xB008	TH FRM ALARM															
0xB009																
Duplex and link speed diagnostics																
0xB00A	-	-	-	-	-	-	EN LS ALARM	EN LS DIAG	-	-	-	-	-	-	EN DUP ALARM	EN DUP DIAG
Port control																
0xB00B	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	EN PORT CTRL
0xB00C	-	-	-	-	-	-	XF10 activ-ated	XF9 activ-ated	XF8 activ-ated	XF7 activ-ated	XF6 activ-ated	XF5 activ-ated	XF4 activ-ated	XF3 activ-ated	XF2 activ-ated	XF1 activ-ated
PROFINET DHC (PROFINET only)																
0xB00D	-	-	-	-	-	-	-	-	-	-	-	-	-	EN DHC ALARM	EN DHC WARN	EN DHC DIAG
0xB00E	TH DHC WARN															
0xB00F	TH DHC ALARM															
RSTP																
0xB010	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	EN RSTP

Meaning of parameter bits [▶ 126]

7.10 Connecting devices to a Modbus Client with CODESYS

Naming convention

Turck uses the terms "Modbus client" and "Modbus server" according to Modbus Organization. The following description uses the terms "Modbus TCP Master" and "Modbus TCP Slave" only because of the naming in CODESYS.

Used hardware

The following hardware components are used in this example:

- TX715-P3CV01 (IP address: 192.168.145.72)
- Block module TBEN-L…- (IP address: 192.168.145.200)

Used software

The following software tools are used in this example:

- CODESYS 3.5.18.2 (can be downloaded for free at www.turck.com).

Prerequisites

- The software is started.
- A new project has been created.
- The controller has been added to the project.

7.10.1 Connecting the device to the PLC

The following components have to be added to CODESYS first, in order to connect the device to the PLC.

- Ethernet adapter
- Modbus TCP client (in CODESYS: Modbus TCP Master)
- Modbus TCP server (in CODESYS: Modbus TCP Slave)

Adding the Ethernet Adapter

- ▶ Right-click **Device** in the project tree **TX715-P3CV01**.
- ▶ Select **Add Device**.
- ▶ Select **Ethernet Adapter**.
- ▶ Click **Insert device.**
- ⇨ The Ethernet Adapter is added to the project tree as **Ethernet (Ethernet)**.

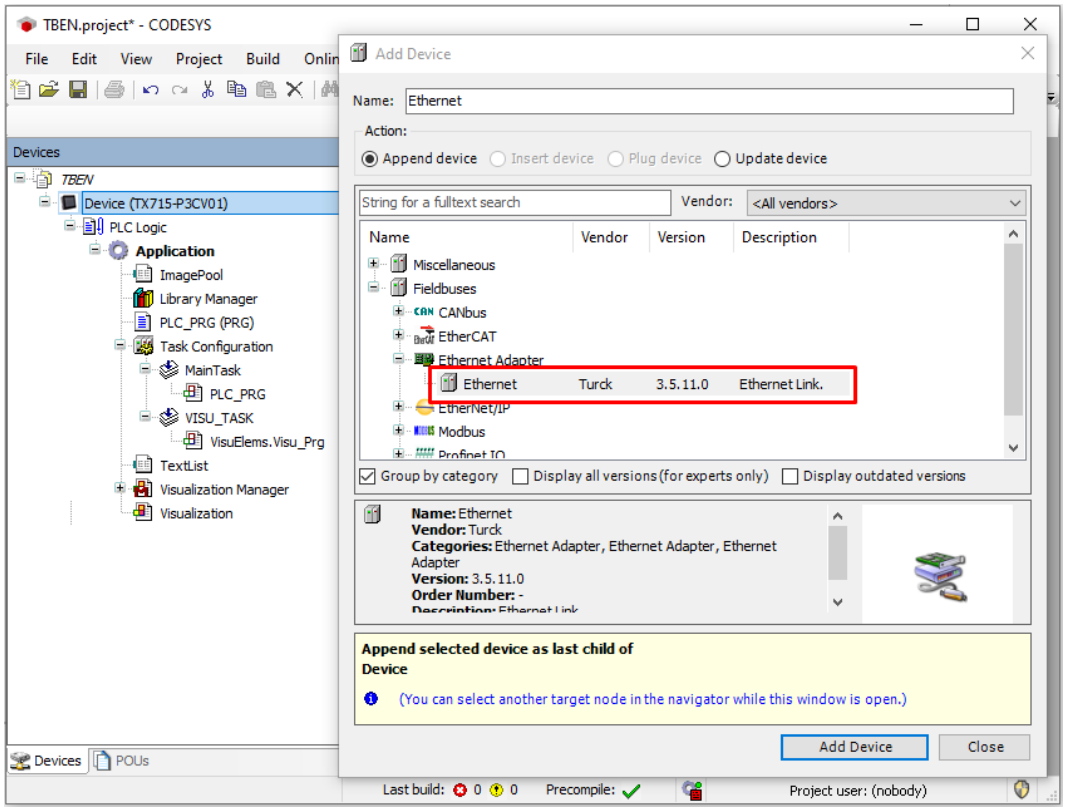

Fig. 39: Adding the Ethernet Adapter

Adding the Modbus TCP Master

- ▶ Right-click the **Ethernet (Ethernet)** in the project tree.
- ▶ Select **Add Device**.
- ▶ Double-click **Modbus TCP Master**.
- ⇨ The **Modbus_TCP_Master** is added to the project tree.

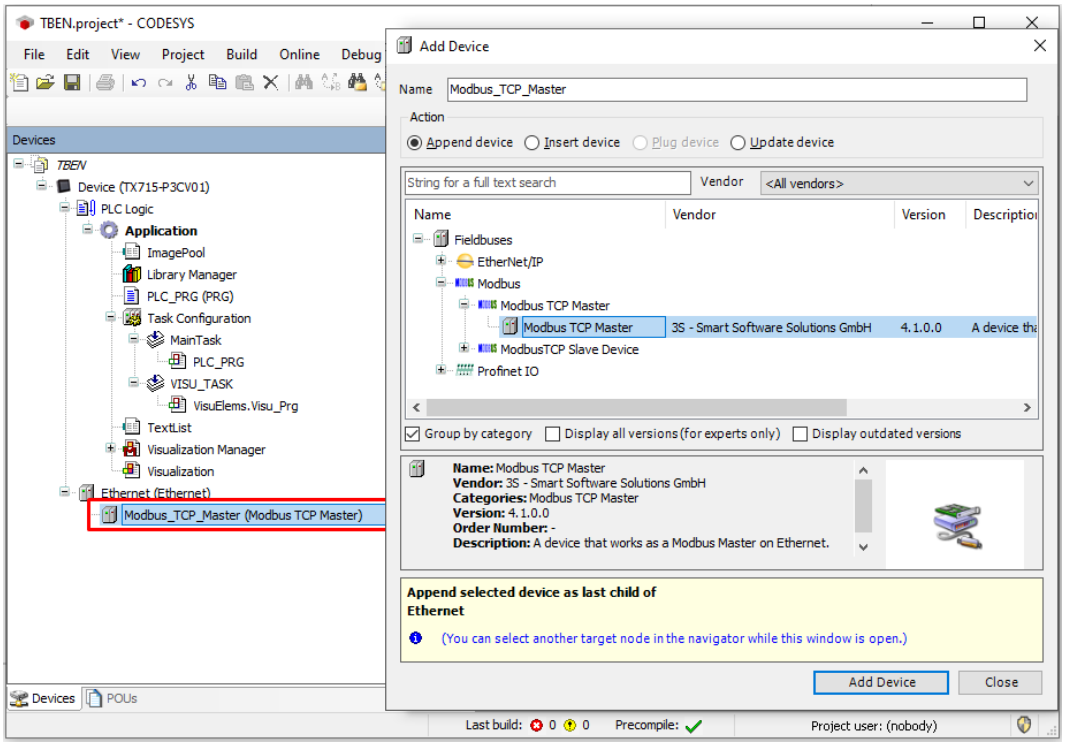

Fig. 40: Adding the Modbus TCP Master

Adding the Modbus TCP Server (Slave)

- ▶ Right-click the **Modbus TCP Master** in the project tree.
- ▶ Select **Add Device**.
- ▶ Double-click **Modbus TCP Slave**.
- ⇨ The **Modbus_TCP_Slave** is added to the project tree.

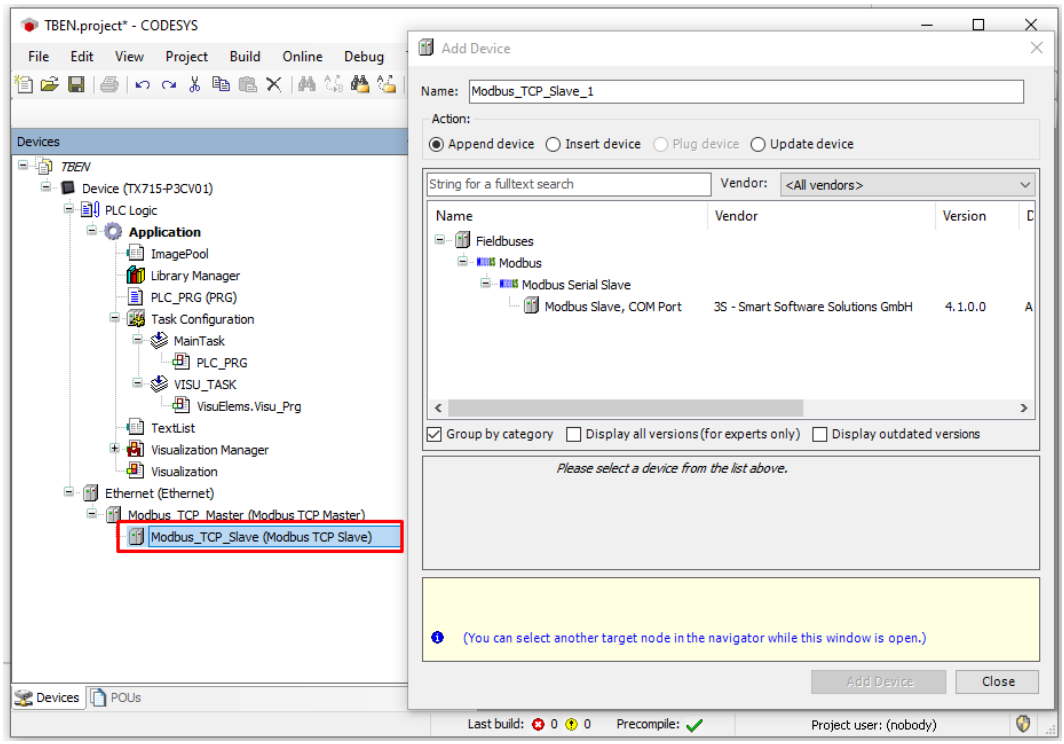

Fig. 41: Adding the Modbus TCP Slave

7.10.2 Configuring the Network Interface

- Click **Device → Scan network**.
- Select Modbus TCP Master (here: TX715-P3CV01) and confirm with OK.

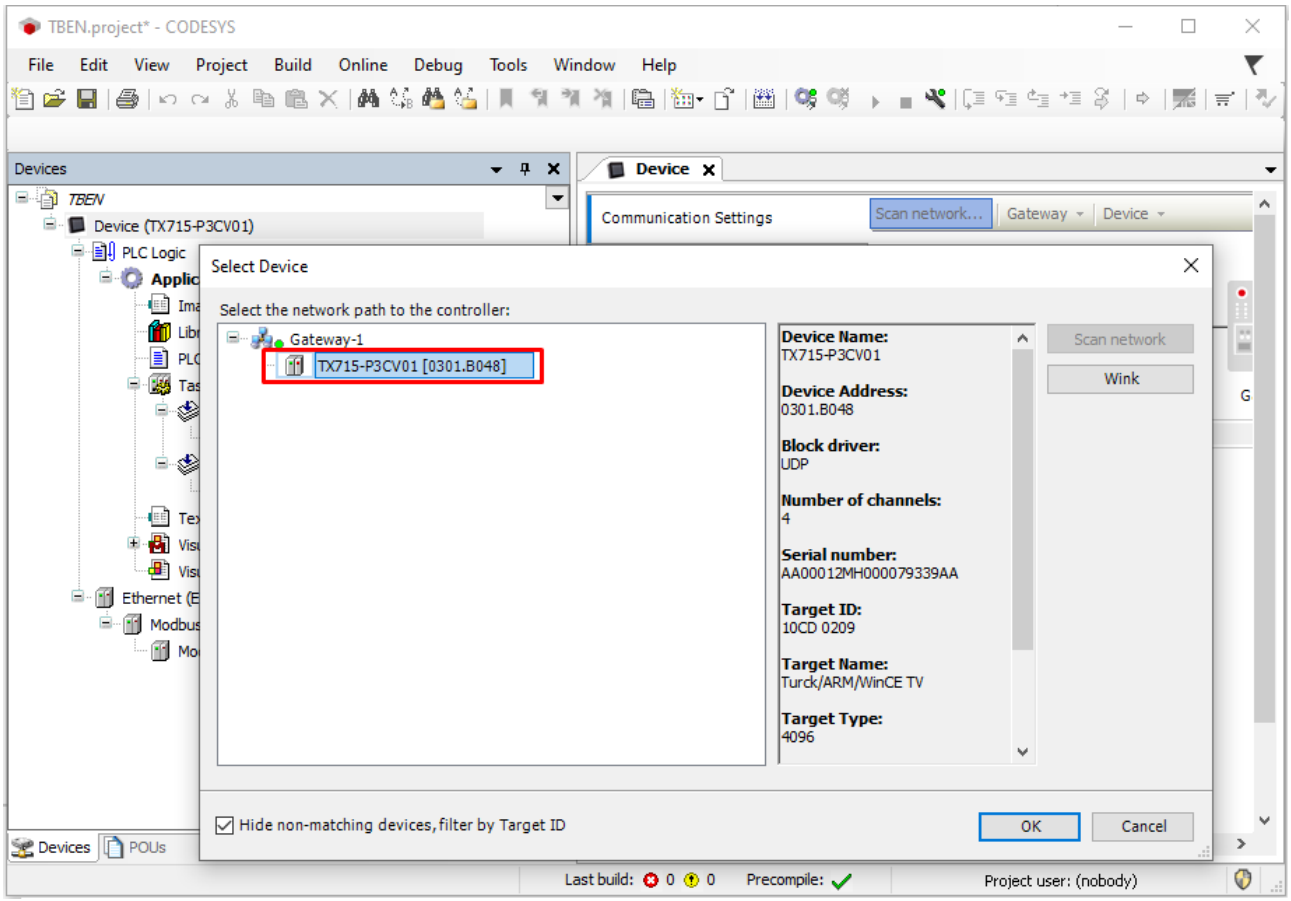

Fig. 42: Configuring the network interface

- Double-click **Ethernet**.
- Open the dialog box **Network Adapter** by clicking the **Browse…** button in the register tab **General**.
- Select the interface TX715-P3CV01 (here: 192.168.145.72)

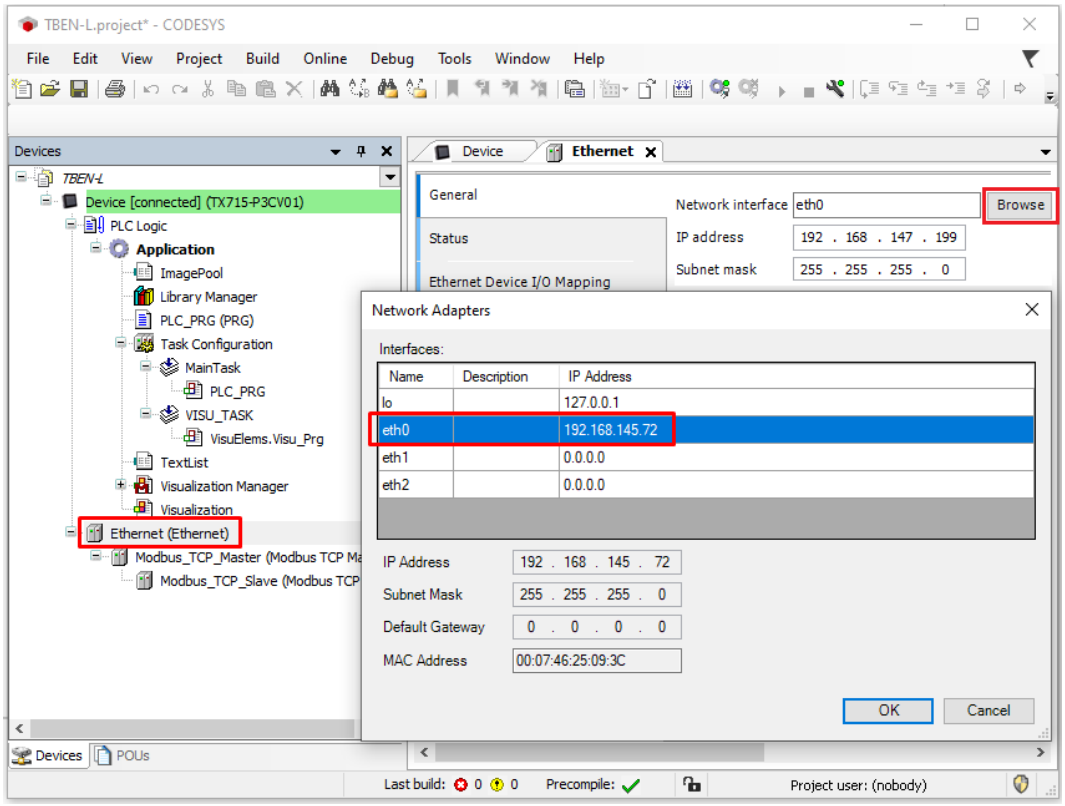

Fig. 43: Selecting the interface

7.10.3 Modbus TCP Server (Slave): setting the IP address

- Double click **Modbus TCP Server (Slave)**.
- Enter the **slave IP address** in the **General** register tab (here: 192.168.145.200).

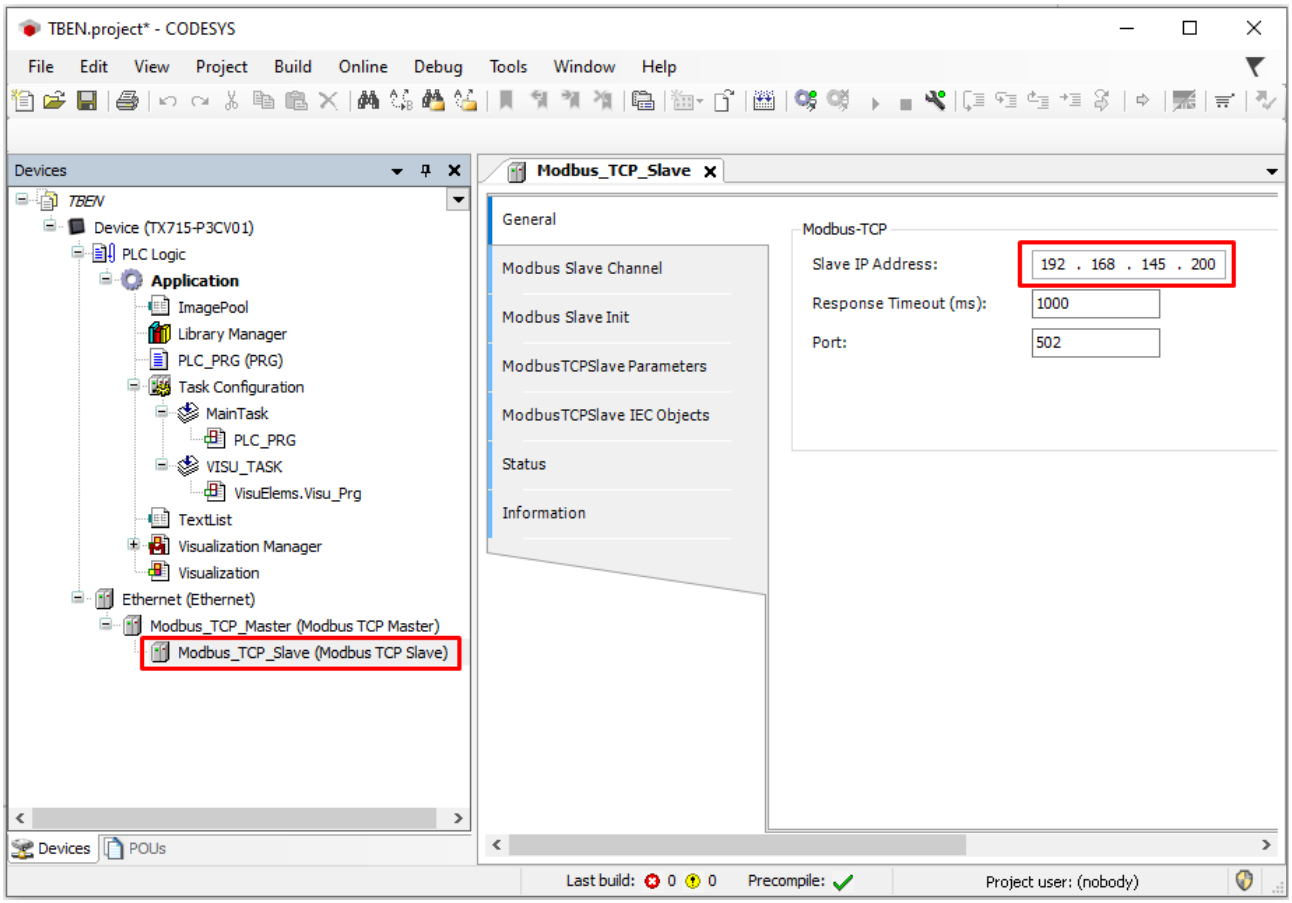

Fig. 44: Modbus TCP Slave: Setting the IP address

7.10.4 Defining modbus channels

Example: Defining channel 0 (input data)

- Double-click **Modbus TCP Slave** .
- Select **Modbus slave channel** → **Add channel**.
- Enter the following values:
  Channel name
  Access type: Read Input Registers
  Offset: 0x0000
  Length: 1 register
- Confirm with OK.

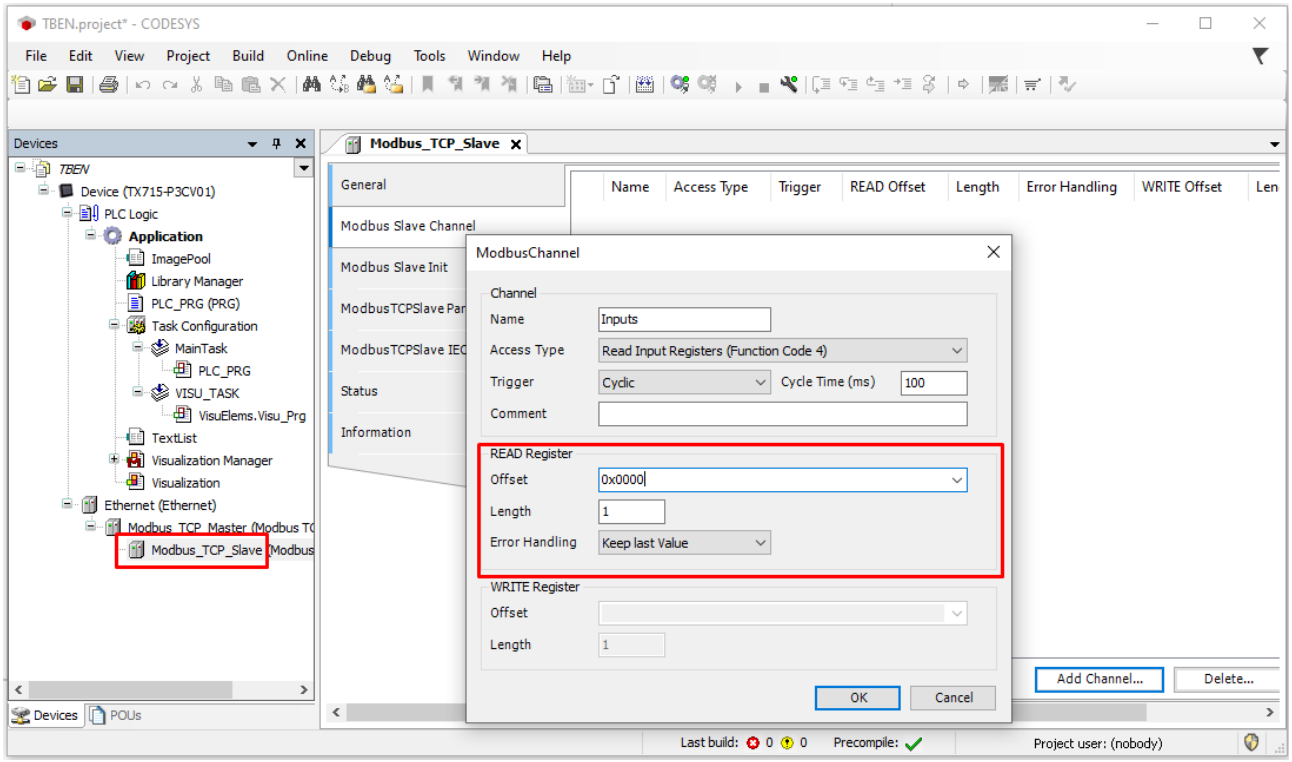

Fig. 45: Defining the input register

7.10.5 Going online with the PLC

- Select the device.
- Click **Online → Login**.

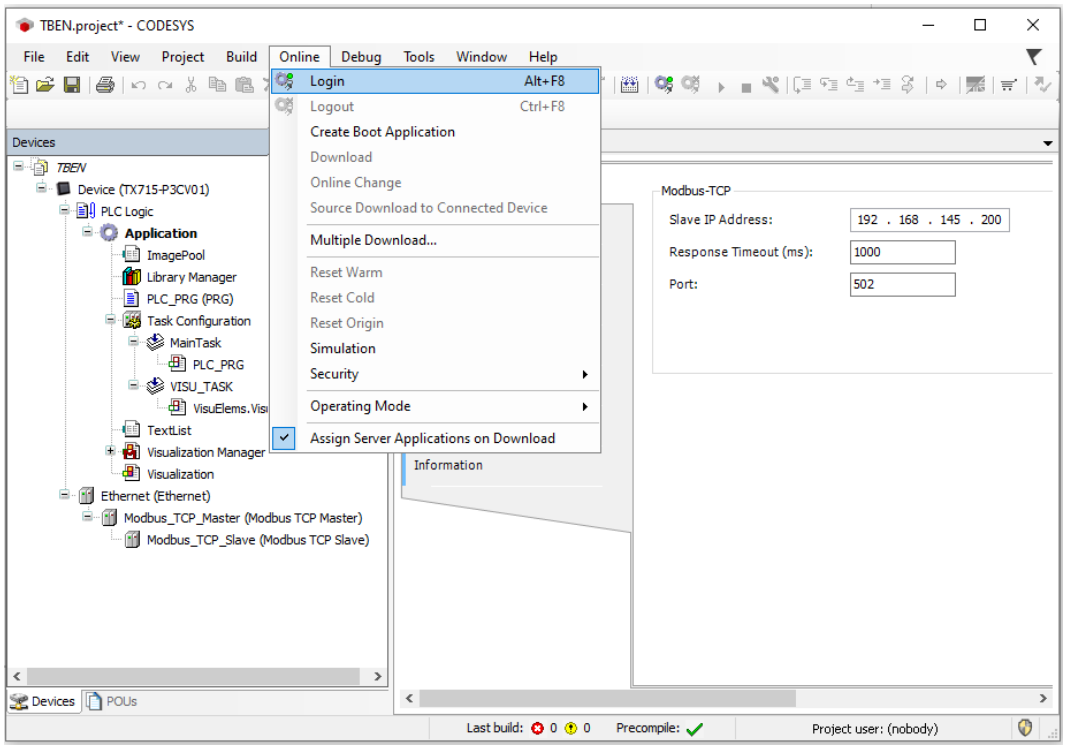

Fig. 46: Login

▶ Download the application to the PLC and start it via **Debug** → **Start**.

⇨ The Modbus TCP communication is setup.

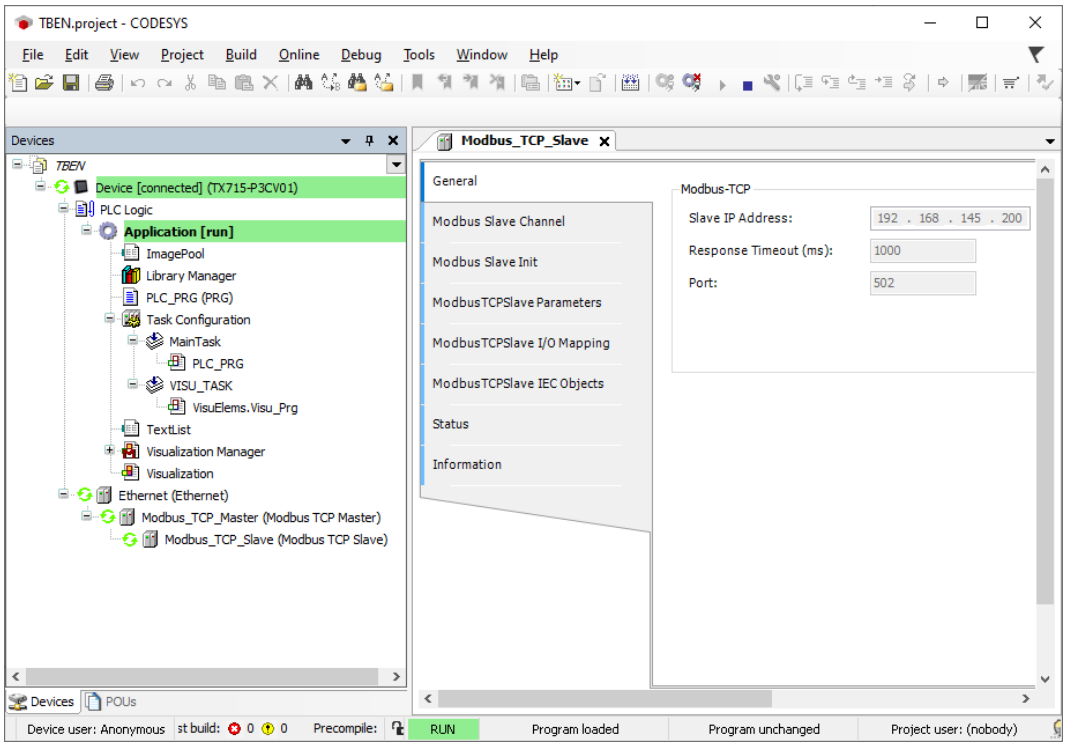

Fig. 47: Modbus TCP communication

7.10.6 Reading process data

The process data can be interpreted by means of the mapping ([▶ 81]) if the device is connected to the PLC.

- ▶ Double click **Modbus TCP Slave**.
- ▶ Click onto register tab **Modbus TCP Slave I/O Mapping**.
- ▶ Set the function **Always update variables** to **Enabled 1 (…)**.
- ⇨ The process data are displayed.

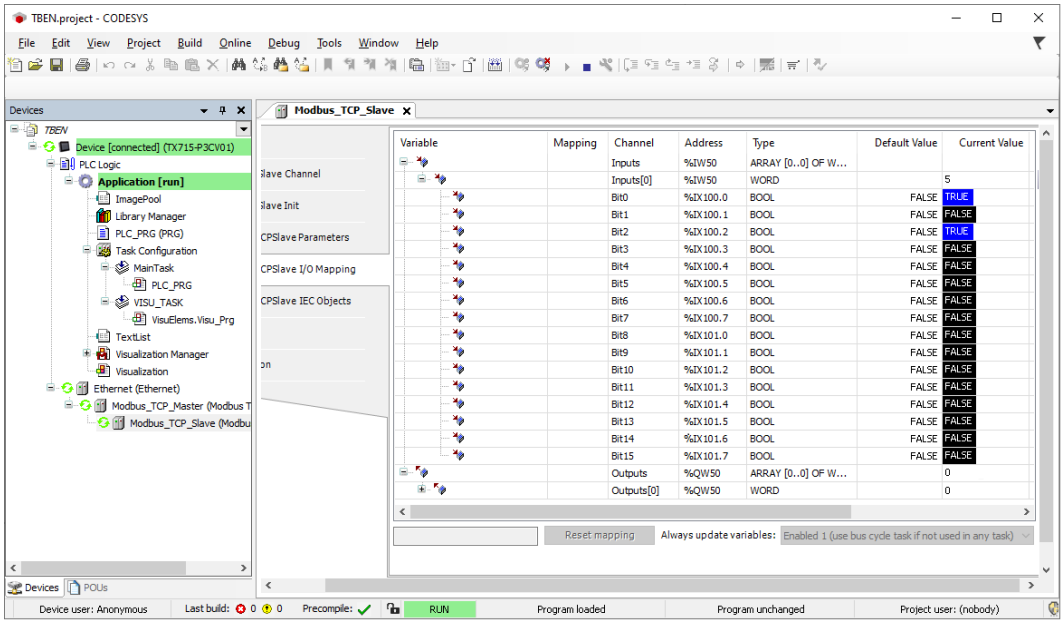

Fig. 48: Process data

8 Parameterizing and configuring

8.1 Configuring device functions with the web server

NOTE
Changes to the configuration of the device are stored non-fail-safe in the device. Unsaved configuration changes are displayed via the **Nonpersistant Configuration** addition on the web server interface. In order to store a changed configuration fail-safe, it must be saved via **Configuration (changed)** → **Make current configuration persistent** [▶ 123].

8.1.1 Configuring the Ethernet interfaces (Interfaces)

Interfaces is used to configure the Ethernet ports of the device.

Interface Settings

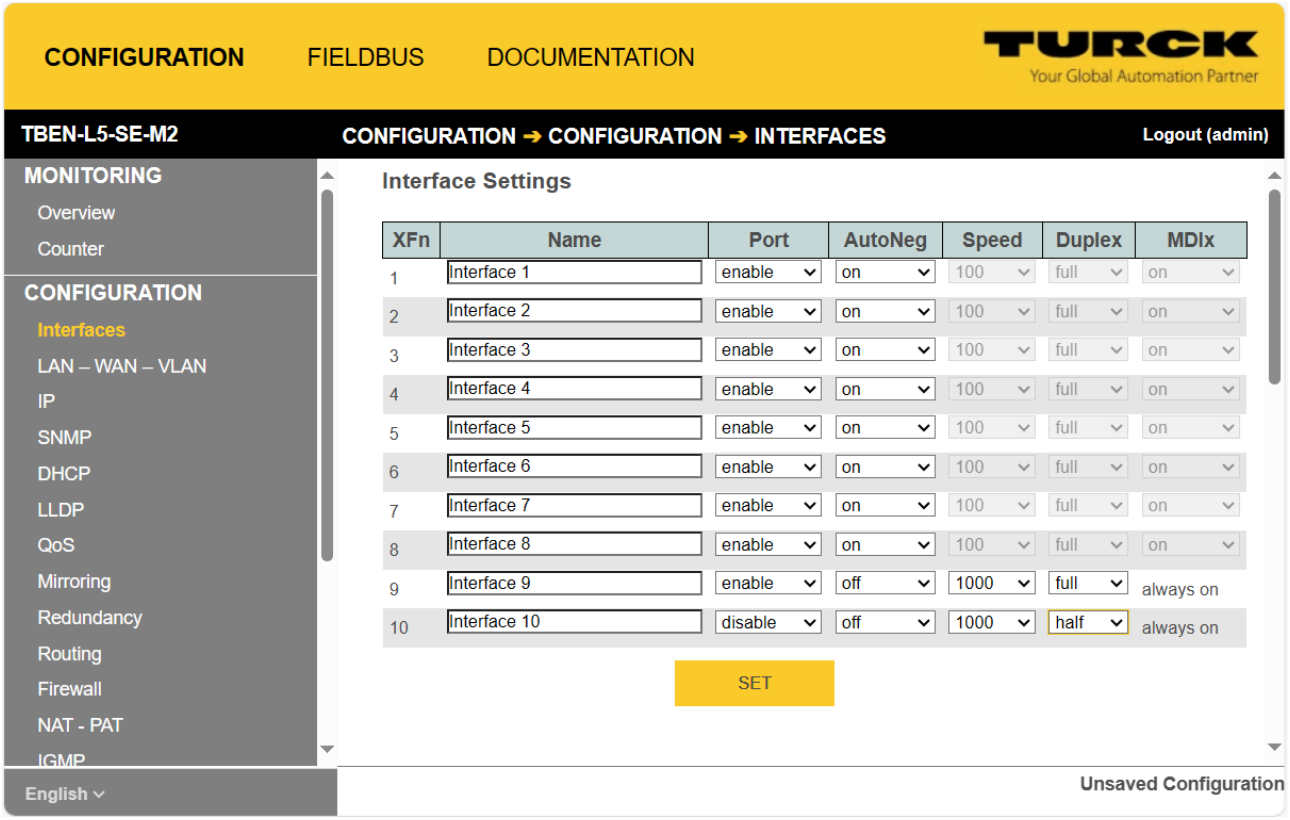

Fig. 49: Configuring the Ethernet ports in the web server

▶ Configure settings on ports XF1…XF10 and accept changes with **SET** .

Setting	Value	Meaning	
XFn	1…10	Number of the Ethernet port	
Name		Freely selectable name	
Port	Enable	Port activated	
	Disable	Port deactivated	
AutoNeg	On	Autonegotiation activated	
	Off	Autonegotiation deactivated	
Speed	10	Setting the transmission rate of the Ethernet ports	
	100		
	1000		(only XF9 and XF10)
Duplex	Full	Setting the transmission rate	
	Half		
MDIx	On	Auto MDIx activated	(only XF1…XF8)
	Off	Auto MDIx deactivated	

Switching

Function	Meaning	
Broadcast Storm Protection		Reduces the forwarding of broadcast messages. The function should only be activated if problems occur due to broadcast storms. In PROFINET applications, relevant PROFINET frames may be suppressed if Broadcast Storm Protection is activated.
Flood unknown Multicasts/ Unicasts	On	Activates the forwarding of multicast or unicast telegrams to all ports. The function must be activated for PROFINET applications.
	Off	Deactivates the forwarding of multicast or unicast telegrams.
	IGMP only	Activates the reception of IGMP telegrams, other multicast or unicast telegrams are not received.

▶ Configure settings and accept changes with **SET** .

Interface Status and Interface MAC Addresses

Interface Status and **Interface MAC Addresses** show status information (activity, transmission speed, MAC addresses, etc.) for the Ethernet ports.

8.1.2 Assigning the IP address (IP)

On the **IP Assignment** page, the IP addresses for the LAN, WAN and VLAN (if defined) network zones are assigned [▶ 98]). The assignment of the IP address via the web server is described in the chapter "Commissioning" [▶ 26].

NOTE
The IP addresses of the different networks (LAN, WAN, VLAN) must be assigned to different networks.

8.1.3 Configuring network zones and VLAN (LAN – WAN – VLAN)

Zones

Under **Zones**, the Ethernet ports of the switch are assigned to the LAN (e.g. plant network) or WAN (e.g. factory network) network zones. If ports are assigned to the WAN, an IP address for the WAN must be assigned under **IP**.

- ▶ Assign the zones and write them to the device via **SET ZONES**.

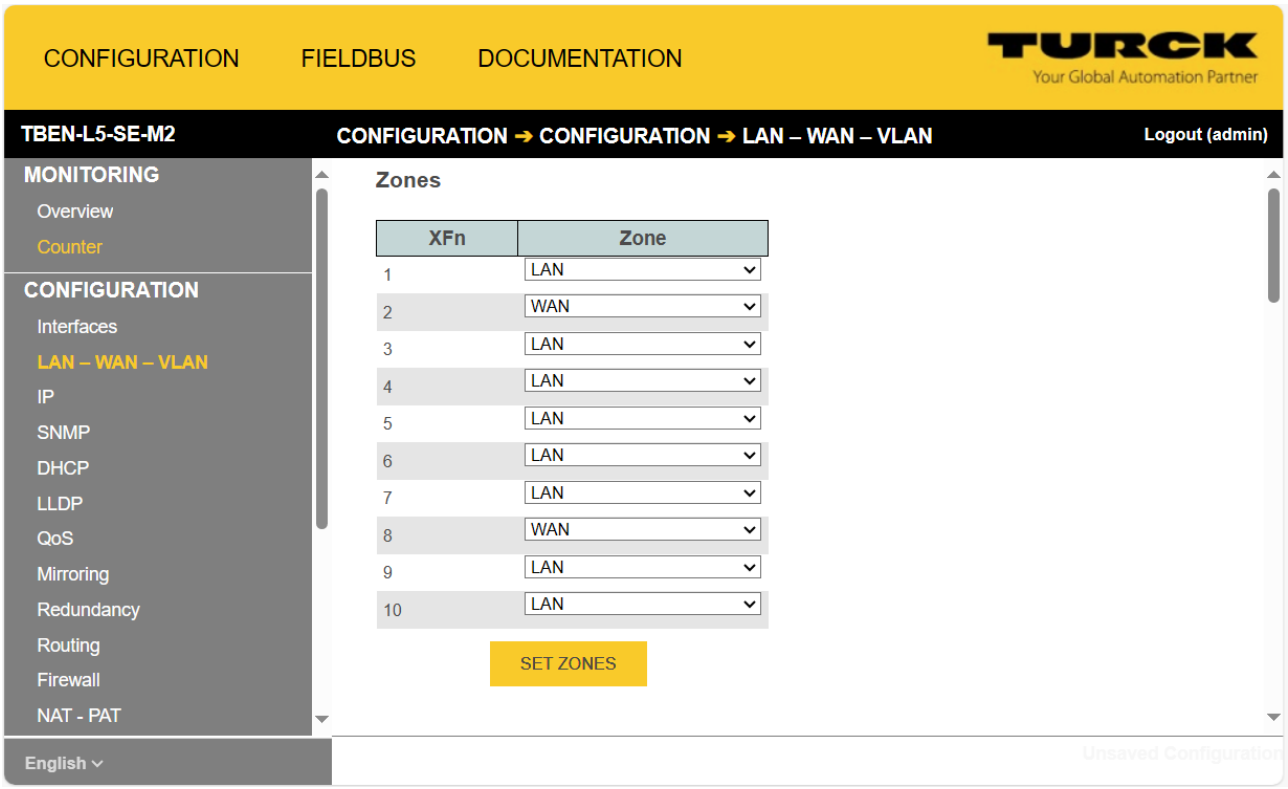

Fig. 50: Assigning zones

- ▶ Set the IP address for the WAN as described under "Setting the IP Address via the web server" [▶ 26].

VLAN Interface Settings

Under **VLAN Interface Settings**, the Ethernet ports are assigned to the previously defined VLANs.

- Assign the VLAN ID and name if necessary and create them via **ADD ID**.
- Set the VLAN tag at the Ethernet port to **enabled** and assign the port to a VLAN by selecting the **Default VLAN ID**.

NOTE
The switch ports can be participants in several VLANs at the same time. The default VLAN ID defines which of the VLAN IDs the port's data packets are tagged with during forwarding.

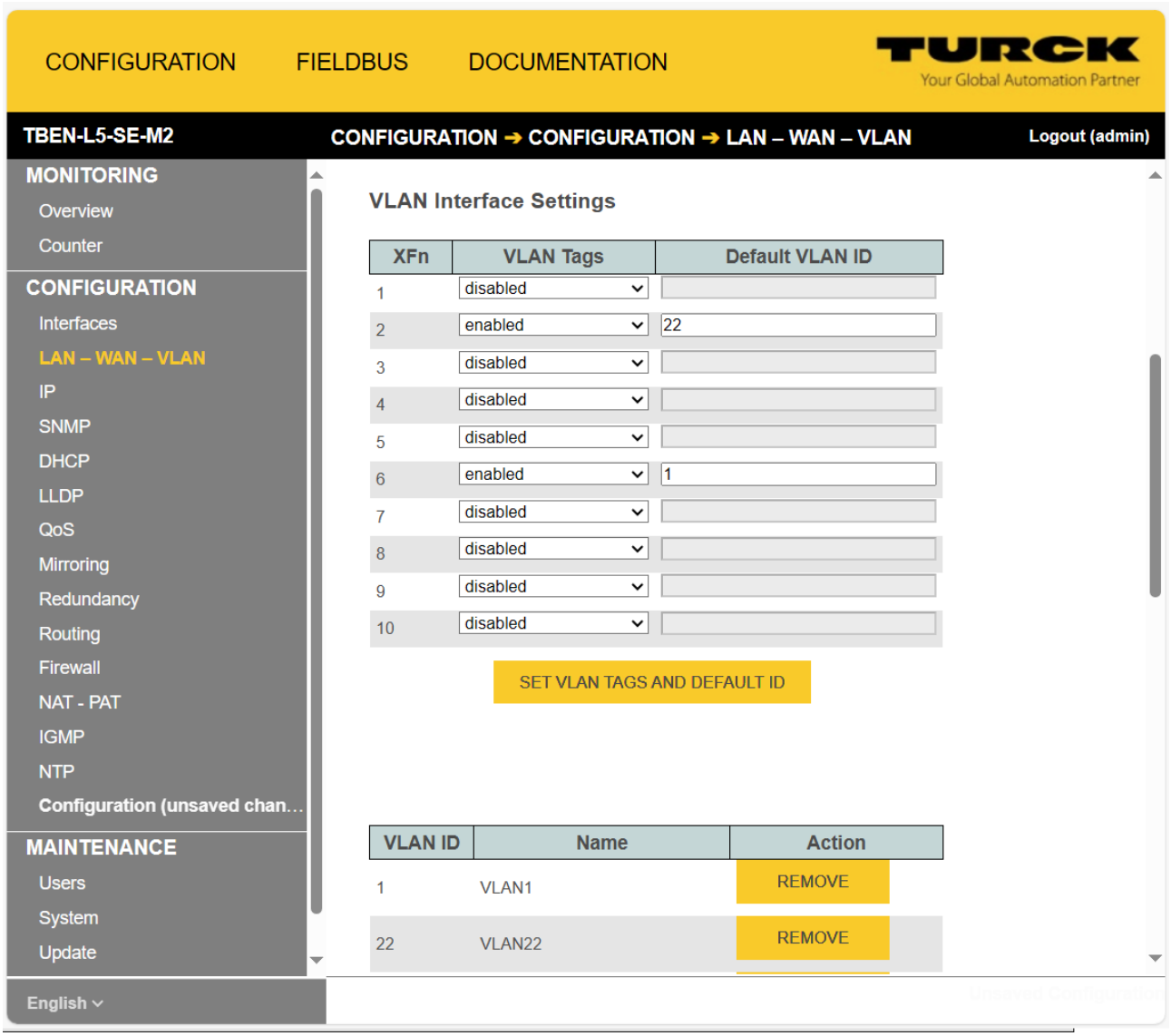

Fig. 51: Defining VLAN IDs and assigning Ethernet ports

▶ Under **VLAN ID/Interface Mapping**, define how the switch port is handled in the VLAN.

Option	Description
Not a member	The switch port is not a member of this VLAN.
Untagged	The port is an untagged member of the VLAN. The VLAN is port-based, which means one VLAN can be set per switch port. The port accepts all (tagged and untagged) packets and then forwards them tagged with the **Default VLAN ID**.
Tagged	The Ethernet port is a tagged member of the VLAN and only receives data packets tagged for it. All packets forwarded by the interface are tagged. The packets contain VLAN information. Tagged VLANs allow multiple VLANs to be used on one switch port.

8.1.4 SNMP: setting up SNMP

SNMP configuration

SNMP Configuration is used to configure the supported SNMP versions as well as the read and write communities for authentication with SNMP V1 and SNMP V2c are.

- ▶ Configure and transfer settings to the device with **SET** .

SNMP User

SNMP User contains a list of all users created under **Add User** for SNMP version 3.

REMOVE is used to delete created SNMP users.

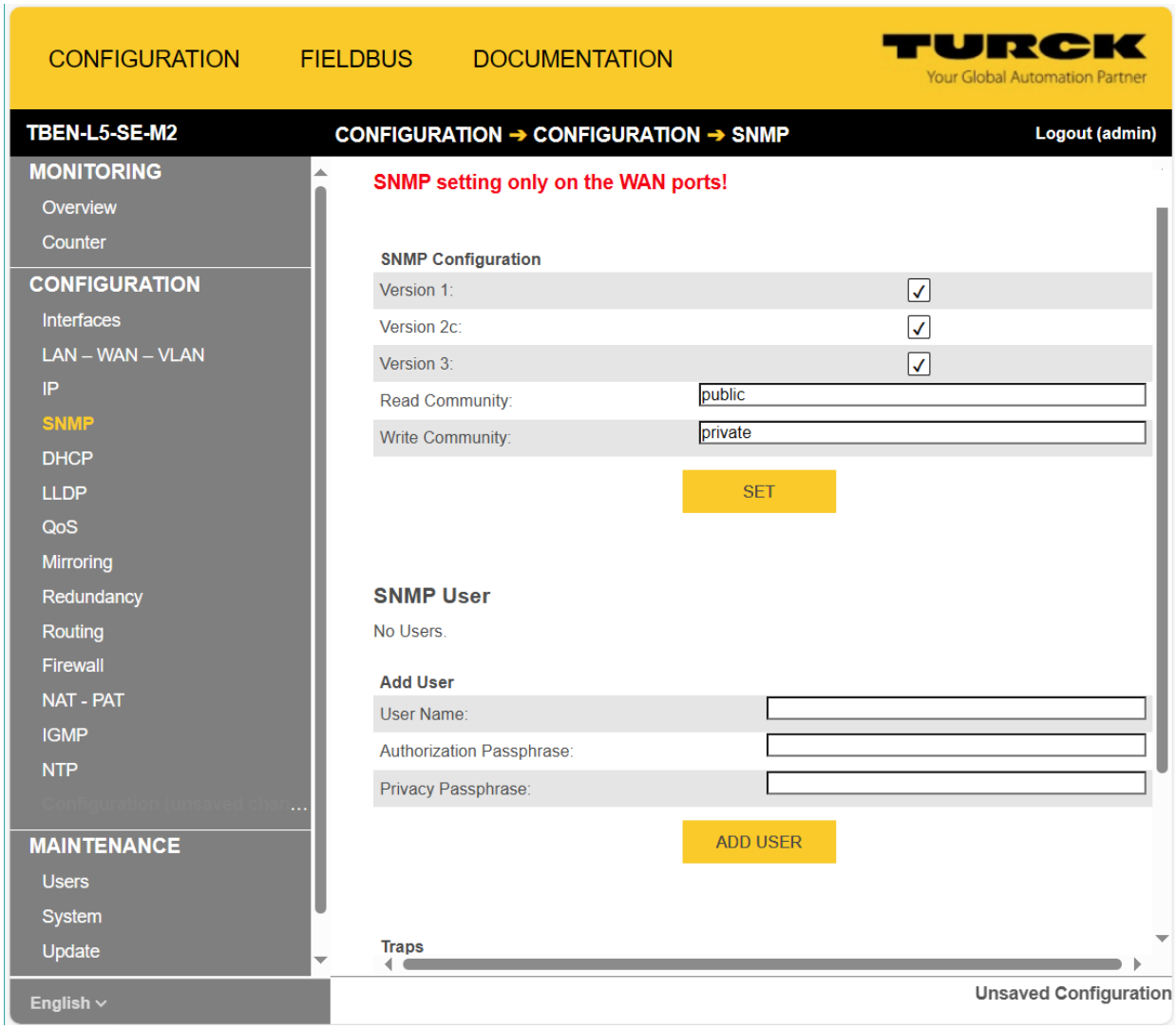

Fig. 52: Configuring SNMP

Add User

Under **Add User** SNMP users are created for the authentication of devices with SNMP V3.

- ▶ Assign user name (User Name) and passwords.
- ▶ Add the user via **Add User** .

Traps

SNMP traps are a standard for error and change notifications in network management. If a device detects an error or change, it sends a notification to one or more trap recipients, a trap community.

The switch sends traps on the following events:

Trap	Description
Link up	A new connection is established, a device is connected to one of the ports.
Link down	The connection to a connected device is interrupted.
Reboot	The switch is restarted.

- ▶ Under **Destination** , specify the IP address of the device on the network that is to receive the traps.
- ▶ Under **Community** , enter the community to which the traps are to be sent.
- ▶ Write the configuration to the device via **SET** .

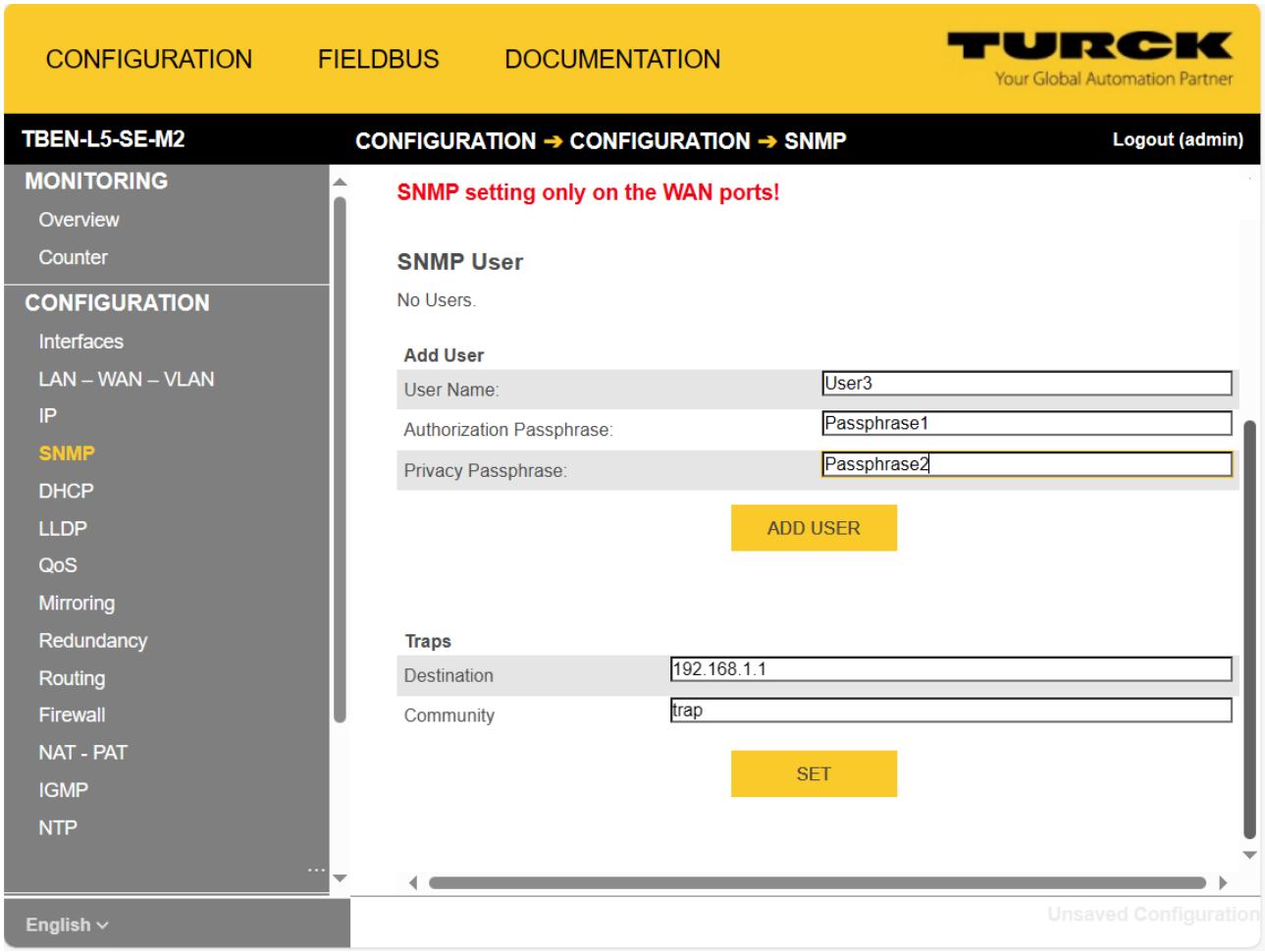

Fig. 53: Adding users and configuring traps

8.1.5 DHCP: setting up a DHCP server

DHCP Server Configuration

DHCP Server Configuration Is used to configure the DHCP server in the device.

- Activate the DHCP server via **Enable** .
- Use **Pool Start** and **Pool End** to define the IP address range from which the switch assigns addresses to other network participants.
- Define other settings (subnet mask, gateway, lease time, etc.).
- Under **Zones** , select the network zone (LAN or WAN) in which the switch is to function as a DHCP server. The WAN network zone only appears if Ethernet ports have been assigned to the WAN [▶ 98] and if an IP address has been set for the WAN zone under [▶ 26] .
- If necessary, define one or more DNS servers. By default, the Google DNS server (8.8.8.8) is used.
- Write the configuration to the device via **SET** .

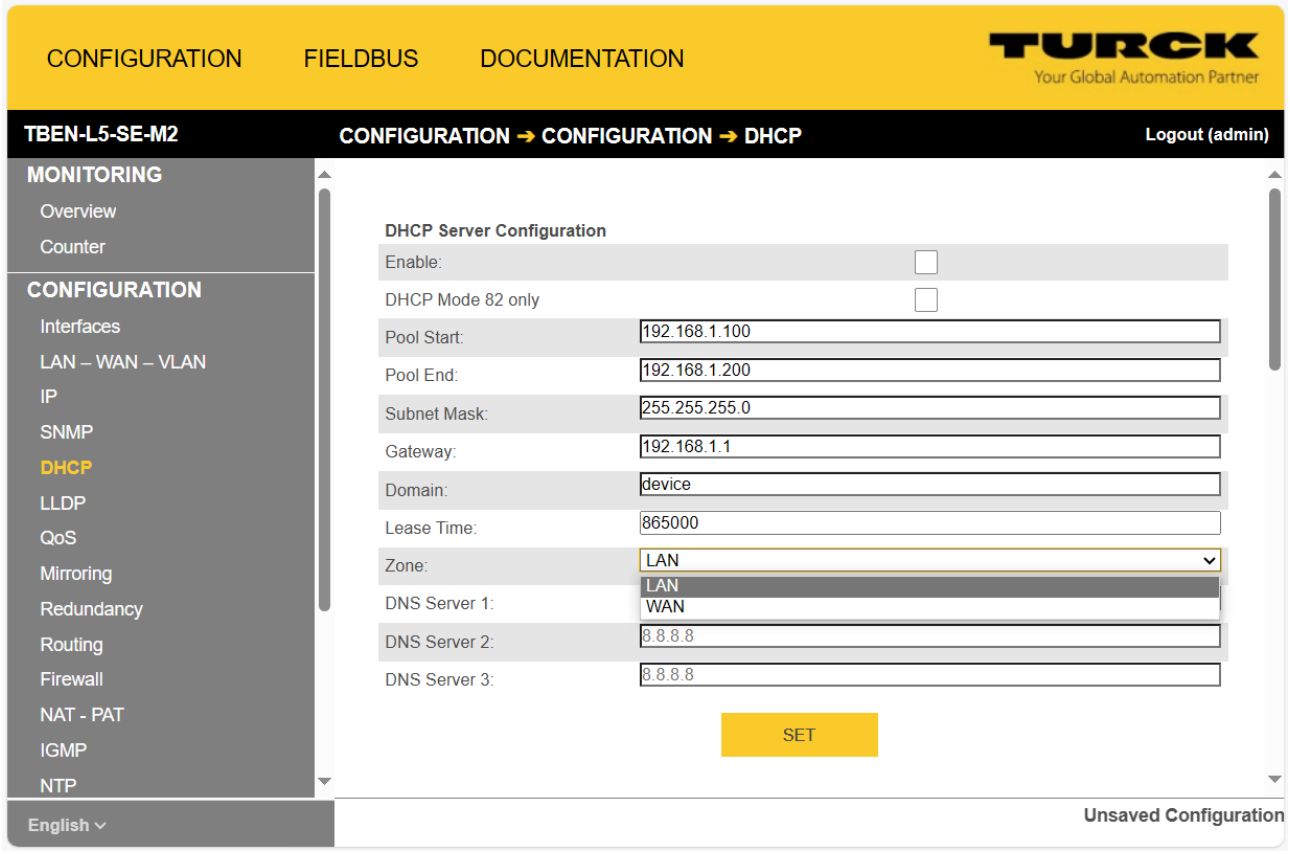

Fig. 54: Configuring the DHCP server

DHCP Mode 82 only

In DHCP mode 82, fixed IP addresses are assigned to the switch ports. The IP address is also assigned independently of the connected device in the event of a device exchange. The fixed IP addresses are defined under **Interface-based IP Assigment** . The DHCP Mode 82 is only suitable for applications with one single device per switch port.

Static Leases

In the section Static Leases, devices can be defined for which a static IP address is to be assigned independently of the lease time. Static addresses are permanently stored. They are not deleted after the Aging Time has expired or when the switch is restarted.

- Enter the IP address that is to be permanently assigned. This IP address must be beyondthe previously defined IP address range.
- Enter the MAC address of the device that will be permanently assigned this IP address.

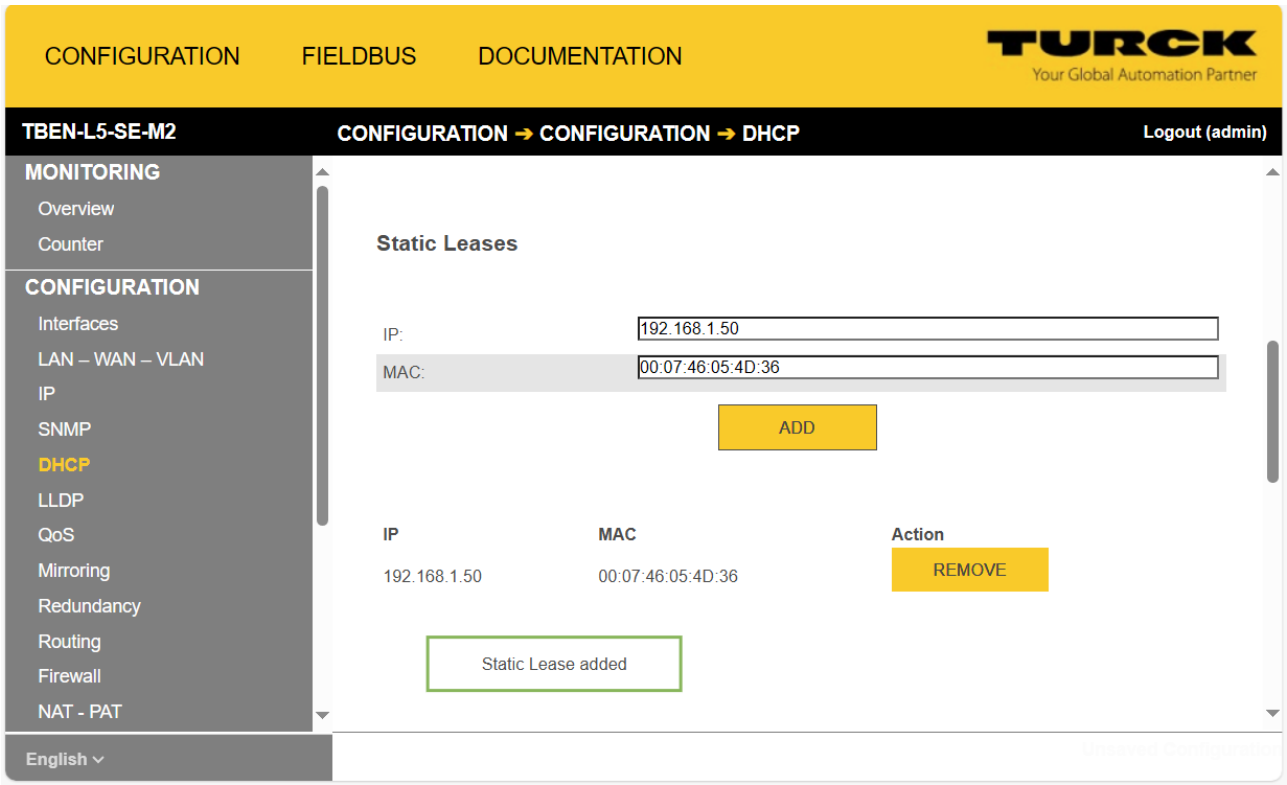

Fig. 55: Assigning static IP addresses

Interface-based IP assignment

Under **Interface-based IP assignment** , Ethernet port-dependent IP addresses can be assigned. The IP addresses are assigned independently of the device for the first connected device that sends a DHCP request. If further devices are connected to the port, these devices receive an IP address from the DHCP address pool.

- ▶ Enter IP addresses at the respective port.
- ▶ Write the configuration to the device via **SET** .

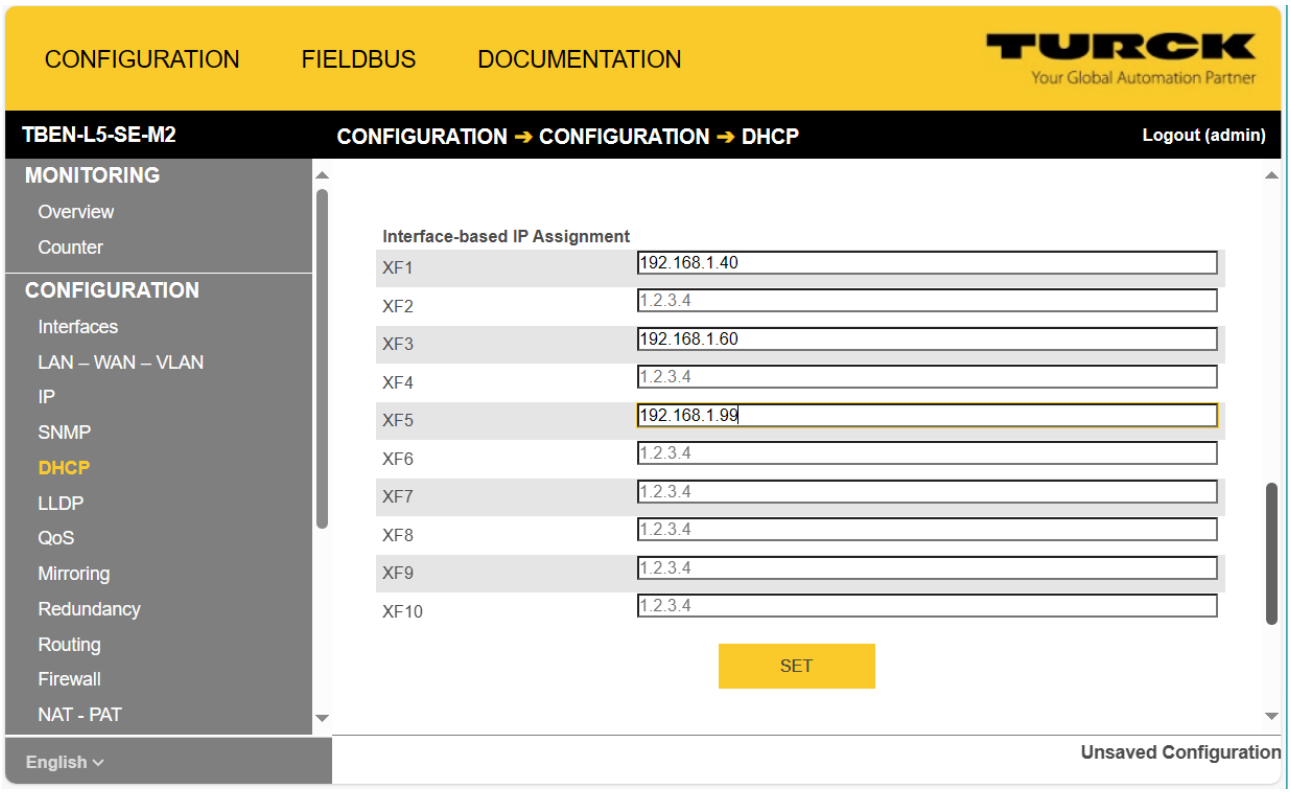

Fig. 56: Assigning Ethernet port-dependent IP addresses

Active Leases

Active Leases contains a list of devices that have already been assigned an IP address via DHCP.

8.1.6 LLDP: configuring neighborhood detection

- ▶ Set up LLDP port by port for incoming (Receive) or for incoming and outgoing (Receive & Transmit).
- ▶ Transfer settings to the device with **SET** .

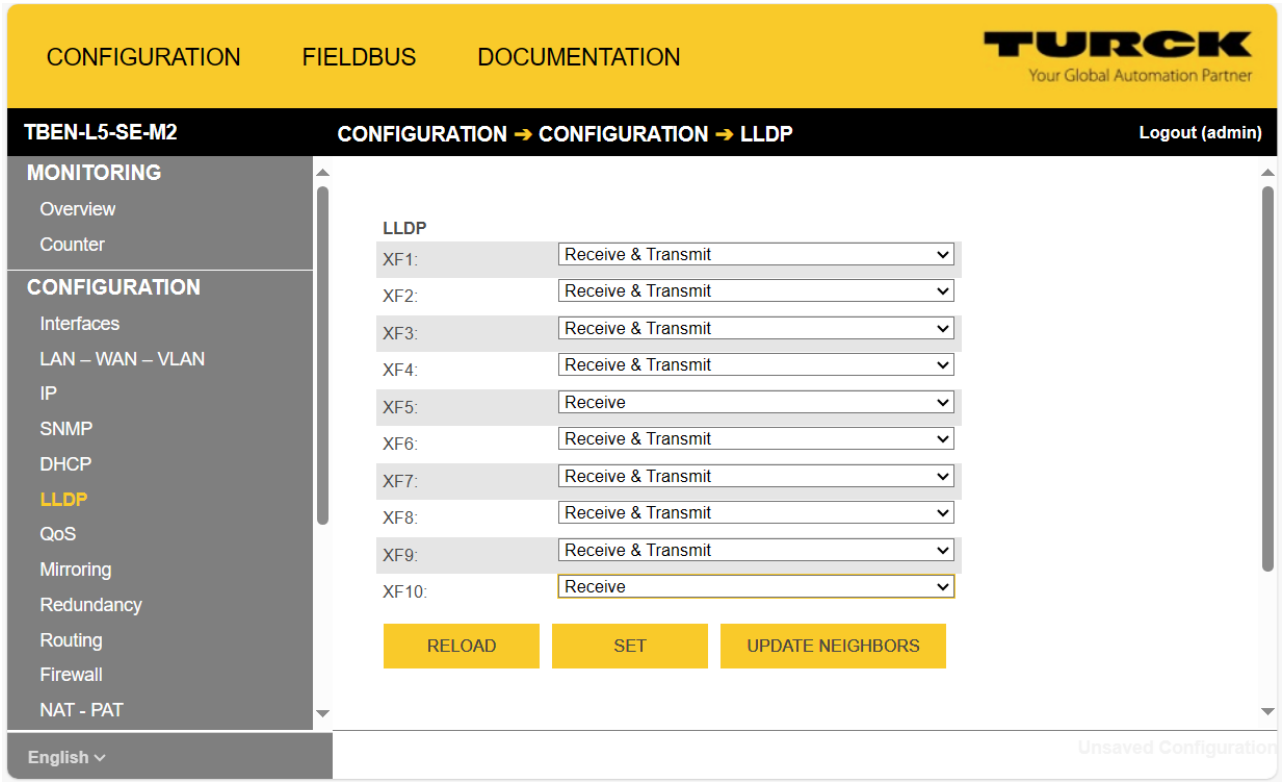

Fig. 57: Configuring LLDP

➪ The table below shows a list of all neighboring devices.

Device							Port		
Port	DeviceName	Age	Type	Value	Desc	Mgmt-IP	Type	Value	Desc
XF4	DT-XXX	0 day, 04:47:48	local	dt-xxx	Hewlett-Packard HP ProBook 650 G1,A3009DD10303,5CG43501GH	192.168.1.131	local	port-001	
XF4	00:13:3b:a0:14:c6	0 day, 04:45:20	mac	00:13:3b:a0:14:c6		-	mac	00:13:3b:a0:14:c6	
XF6	turck-tben-s2-4iol	0 day, 04:45:30	local	turck-tben-s2-4iol	Turck, TBEN-S2-4IOL, 6814024, HW: 1, SW: V1.6.6.0	192.168.1.125	local	port-001	Turck TBEN-Sx port-001

Fig. 58: LLDP, neighboring devices

RELOAD restores the original configuration of the LLDP settings.

UPDATE NEIGHBORS updates the list of adjacent devices.

8.1.7 QoS: prioritizing or classifying data packets

Interface Settings

Interface Settings allows the port by port setting of prioritization or classification of data packets.

The default settings are **shown in bold** .

Function	Value	Meaning
XFn	1…10	
Prio Choice	**Default**	Telegrams are processed according to default prioritization.
	PCP > default	Telegrams that have been prioritized via PCP are always processed first.
	DSCP > default	Telegrams that have been prioritized via DSCP are always processed first.
	PCP > DSCP > default	Telegrams that have been prioritized via PCP are always processed first. This is followed by the processing of telegrams that have been classified via DSCP. All other telegrams are then processed
Default Queue	Q0 (weighted, 1×)	Queue 0: the data is processed with a weighting of 1.
	Q1 (weighted, 2×)	Queue 1: the data is processed with a weighting of 2.
	Q2 (weighted, 3×)	Queue 2: the data is processed with a weighting of 3.
	Q3 (weighted, 6×)	Queue 3: the data is processed with a weighting of 6.
	Q4 (weighted, 12×)	Queue 4: the data is processed with a weighting of 12.
	Q5 (3rd, strict)	Queue 5: Strict priority (3)
	Q6 (2nd, strict)	Queue 6: Strict priority (2)
	Q7 (1st, strict)	Queue 7: Strict priority (1)
Default PCP	Prioritization level according to IEEE 802.1, the prioritization according to PCPs is part of the VLAN tagging.	
	0	Lowest priority, for background processes the process
	1	Best effort
	2	Excellent effort
	3	Critical applications
	4	Video, < 100 ms delay
	5	Voice, < 10 ms delay
	6	Internetwork control
	7	Highest priority, network control

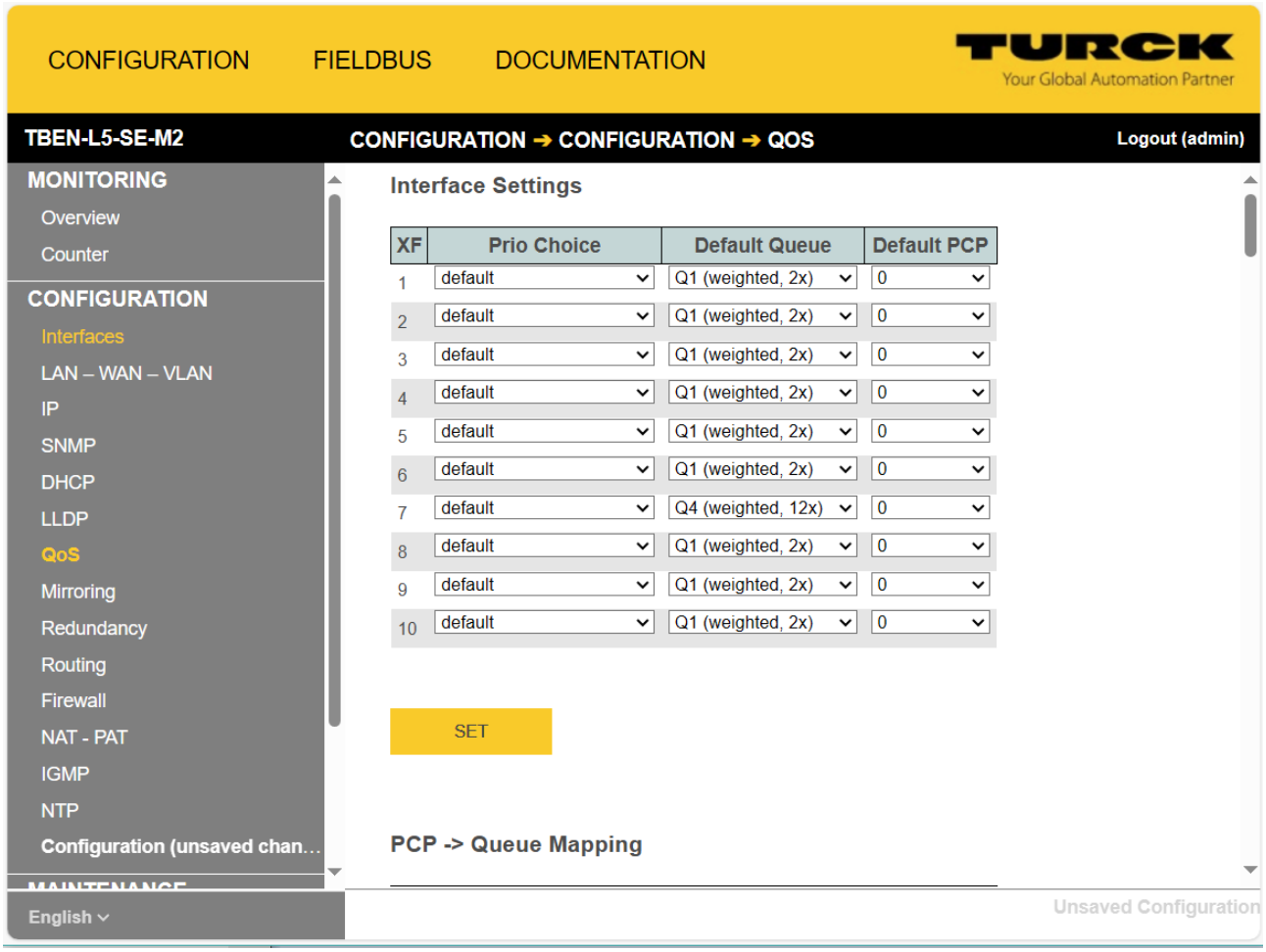

Fig. 59: QoS, port-wise prioritization of telegrams

- ▶ Set the prioritization for Ethernet ports.
- ▶ Accept the changes via **SET** .

PCP → Queue Mapping

PCP → Queue Mapping Is used to define to which output queues telegrams are assigned based on their PCP priorities.

Default settings:

PCP Value	Transmit Queue	PCP Value	Transmit Queue
0	Q1 (weighted, 2×)	4	Q4 (weighted, 12×)
1	Q0 (weighted, 1×)	5	Q5 (3rd, strict)
2	Q2 (weighted, 3×)	6	Q6 (2nd, strict)
3	Q3 (weighted, 6×)	7	Q7 (1st, strict)

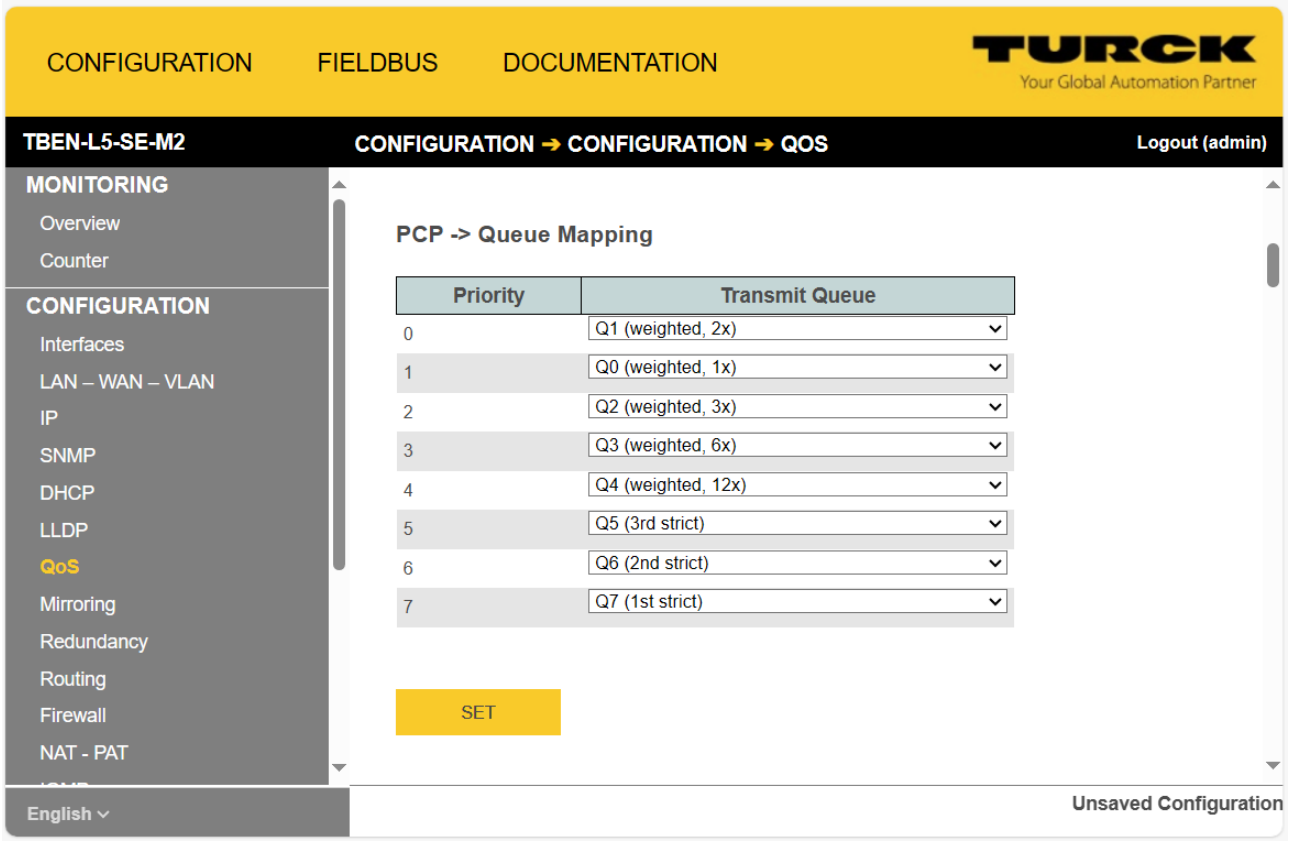

Fig. 60: QoS, configuring PCP Queue Mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET** .

DSCP → queue mapping

DSCP → Queue Mapping Is used to define to which output queues telegrams are assigned based on their DSCP values.

Default settings:

DSCP Value	Transmit Queue	DSCP Value	Transmit Queue
0…7	Q0 (weighted, 1×)	32…39	Q4 (weighted, 12×)
8…15	Q1 (weighted, 2×)	40…47	Q5 (3rd, strict)
16…23	Q2 (weighted, 3×)	48…55	Q6 (2nd, strict)
24…31	Q3 (weighted, 6×)	56…63	Q7 (1st, strict)

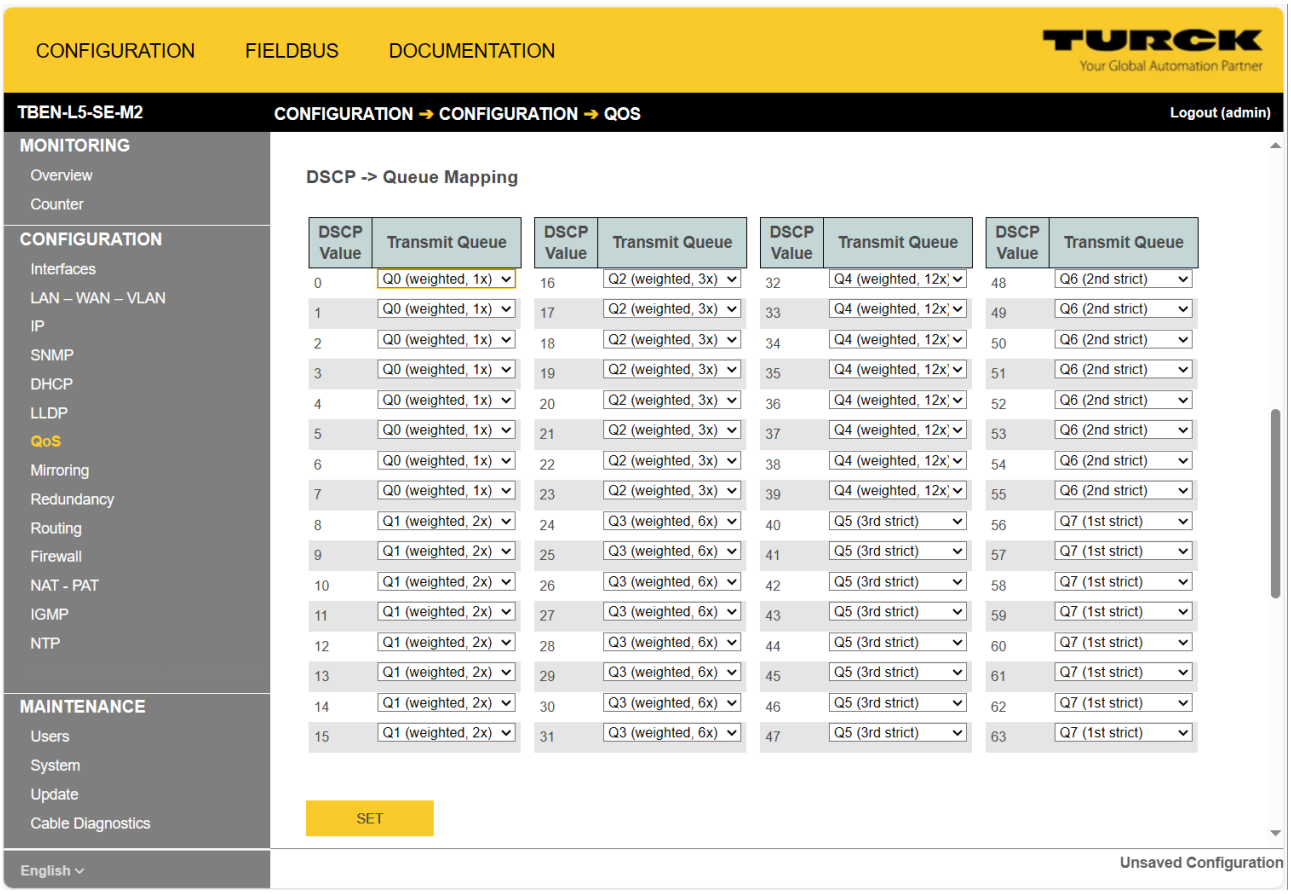

Fig. 61: QoS, configuring DSCP queue mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET** .

DSCP → PCP Mapping

Under **DSCP → PCP Mapping** , the DSCP entries are assigned to PCP priorities. In the following example, telegrams that were classified via a DSCP of 5 received the highest priority (7).

Default settings:

DSCP Value	Transmit Queue	DSCP Value	Transmit Queue
0…7	0	21…39	4
8…15	1	40…47	5
16…23	2	48…55	6
24…31	3	56…63	7

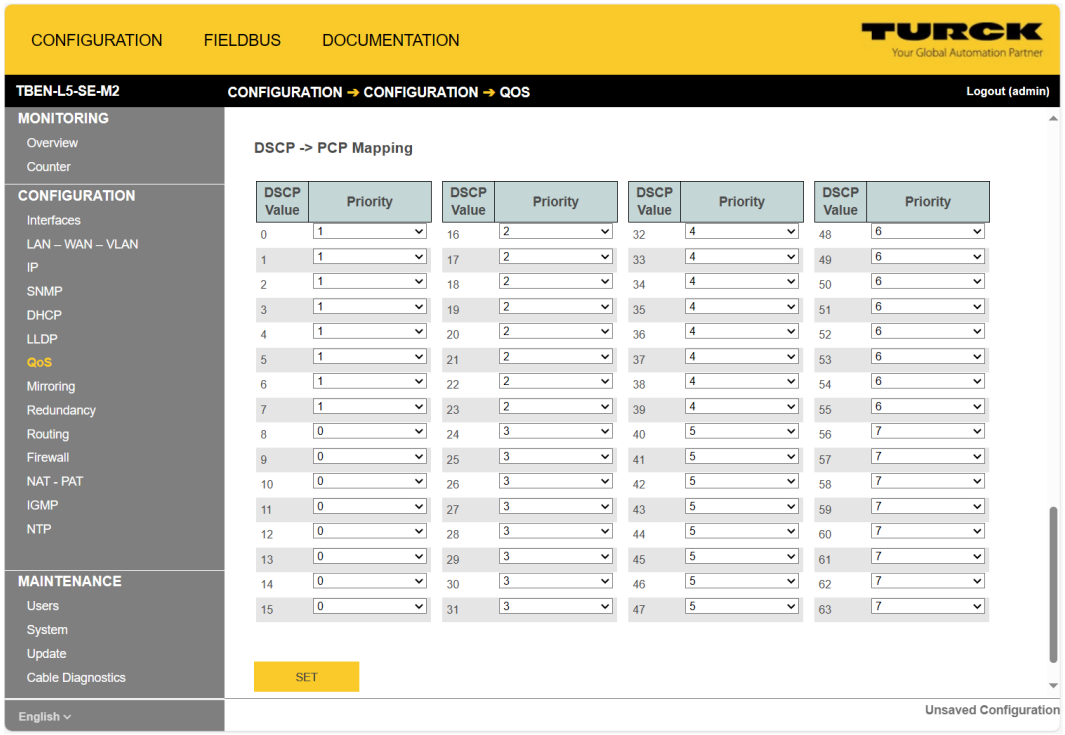

Fig. 62: QoS, configuring DSCP → PCP queue mapping

- ▶ Set the queue mapping.
- ▶ Accept the changes via **SET** .

8.1.8 Mirroring: configuring the mirroring of switch ports

Use **Mirroring** To configure the mirroring of one or more switch ports to another port. Only the incoming telegrams (mirror receive only), the outgoing telegrams (mirror transmit only) or both directions (mirror receive and transmit) can be mirrored.

- Under **Destination** → **Destination Interface** , define the port to which the port(s) to be mirrored are to be mirrored.
- Activate the desired mirroring at the switch ports XF1…XF10.
- Transfer settings to the device via **SET** .

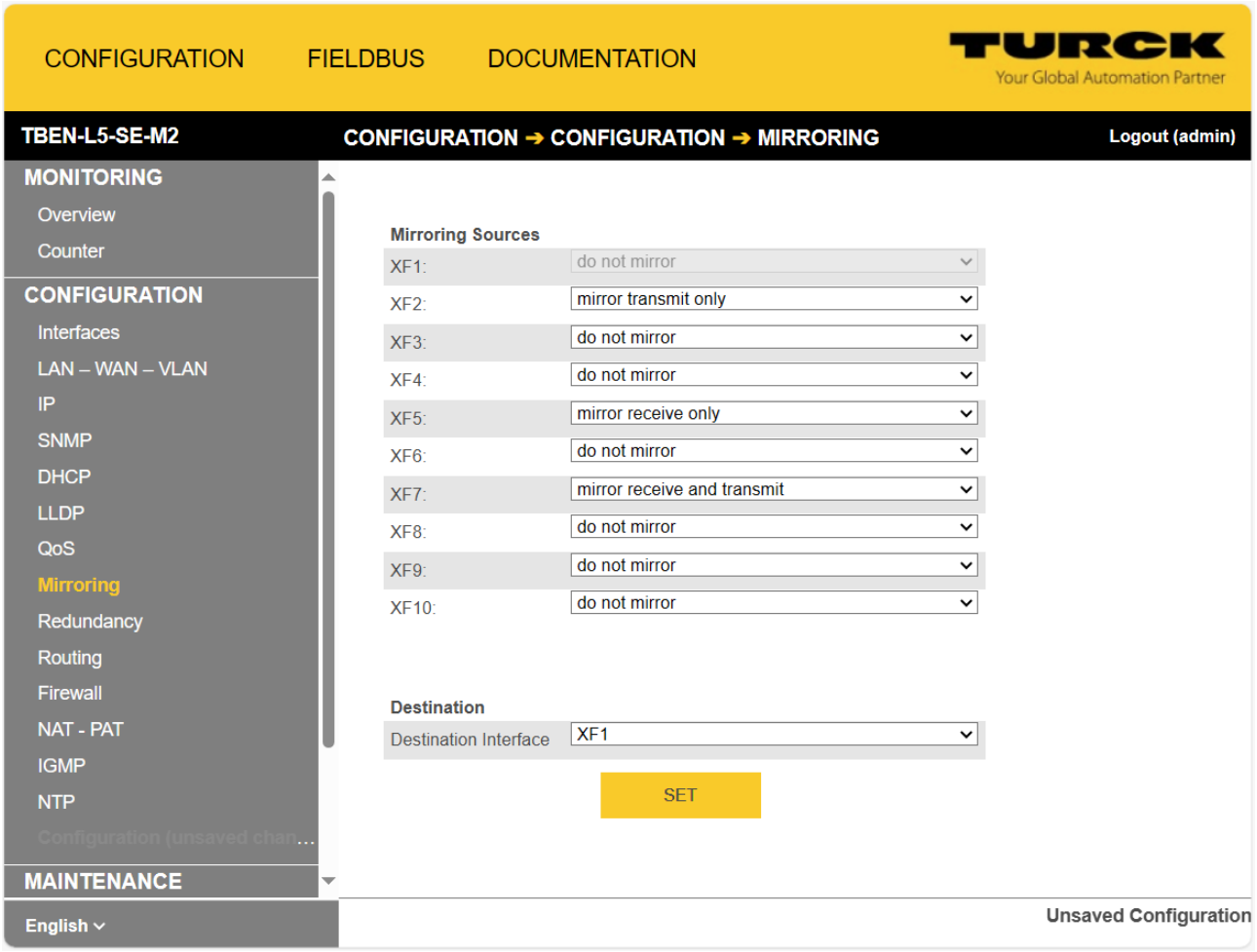

Fig. 63: Configuring the mirroring

8.1.9 Redundancy – configuring network redundancy

RSTP Variant

The section **RSTP Variant** defines which network redundancy protocol [▶ 14] is used in the network zones LAN, WAN, LAN-VLAN and WAN-VLAN.

- ▶ Select the network redundancy protocol.
- ▶ Send the configuration to the device via **SET**.

NOTE
If fieldbus control is active, the redundancy protocol can only be selected fieldbus-specifically (MRP or DLR) via the respective engineering software.

DLR-Ports is used to define the switch ports for the rings redundancy.

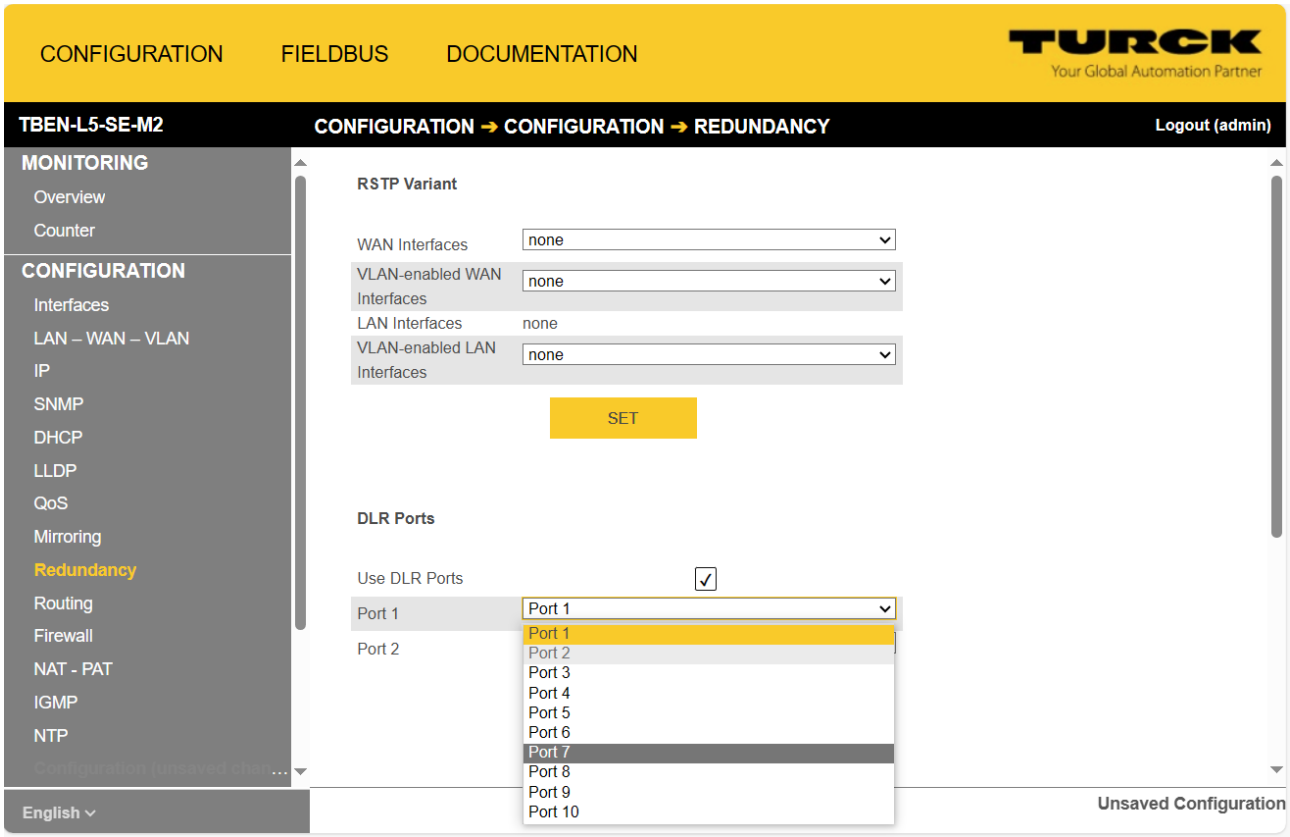

Fig. 64: Configuring redundancy in the web server

8.1.10 Routing: configuring rules (routes)

Routing defines forwarding rules (routes) for data transmission between the configurable LAN and WAN network zones.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

Add Route

Example:

Telegrams from network node 1 at port 2 of the switch will be forwarded to network node 2 of another network.

Network node 1	Network node 2
IP address: 10.17.2.12	IP address: 192.168.1.100
WAN zone: IP address: 10.17.2.0	LAN zone: IP address: 192.168.1.0
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0

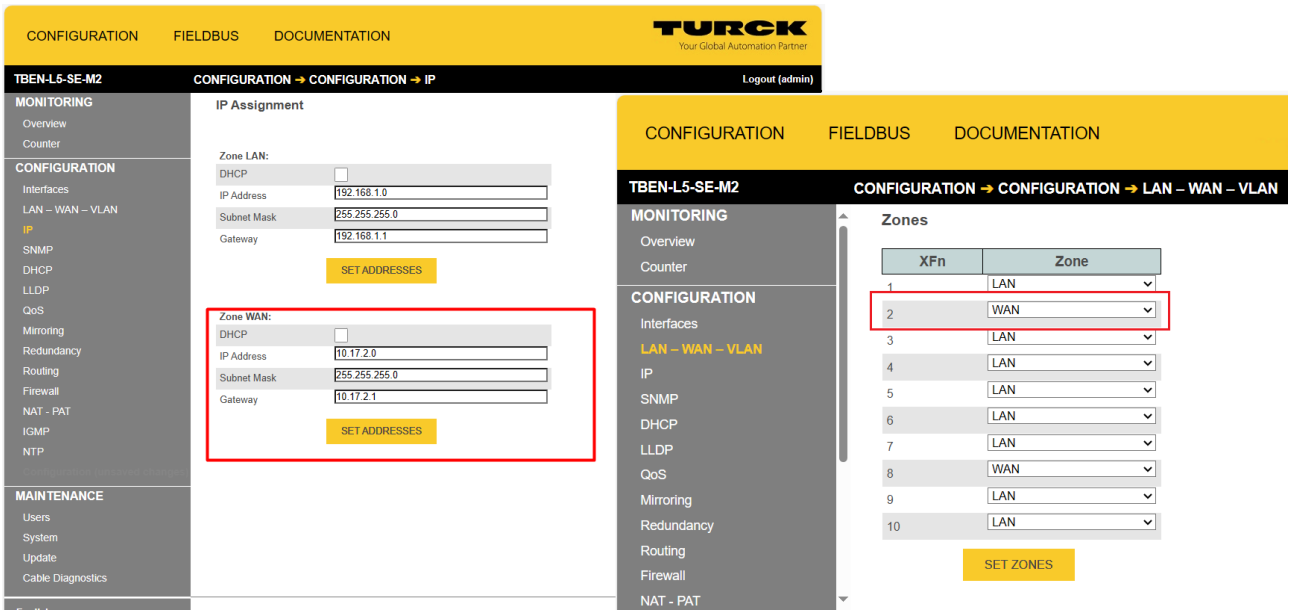

Fig. 65: IP addresses for LAN and WAN zone

Make the following settings and add rules using **ADD**.

Function	Value	Meaning
Source network	10.17.2.12	Address of network node 1 in the WAN zone
Source Subnet Mask	255.255.255.0	Subnet mask of the WAN zone
Outgoing Zone	LAN	
Next Hop/Gateway	192.168.1.100	IP address of network node 2
Metric	0	Number of networks in between

8.1.11 Firewall: configuring firewall rules

The firewall is deactivated when the device is delivered and must first be activated, e.g. via a block-any rule (all telegrams are blocked). After that, exceptions to this rule can be defined.

Firewall rules can be created separately for incoming and outgoing packets.

In addition, forwarding rules can be defined.

NOTE
The firewall is only required if two networks (e.g. LAN and WAN) are used.

Application example – defining firewall rules

Access to the switch via HTTP (port 80) is blocked. The device can only be accessed from outside the WAN via HTTPS. For this purpose, port 443 is enabled for HTTPS. All other ports are blocked.

- First incoming rule, which allows access via port 433 for HTTPS:

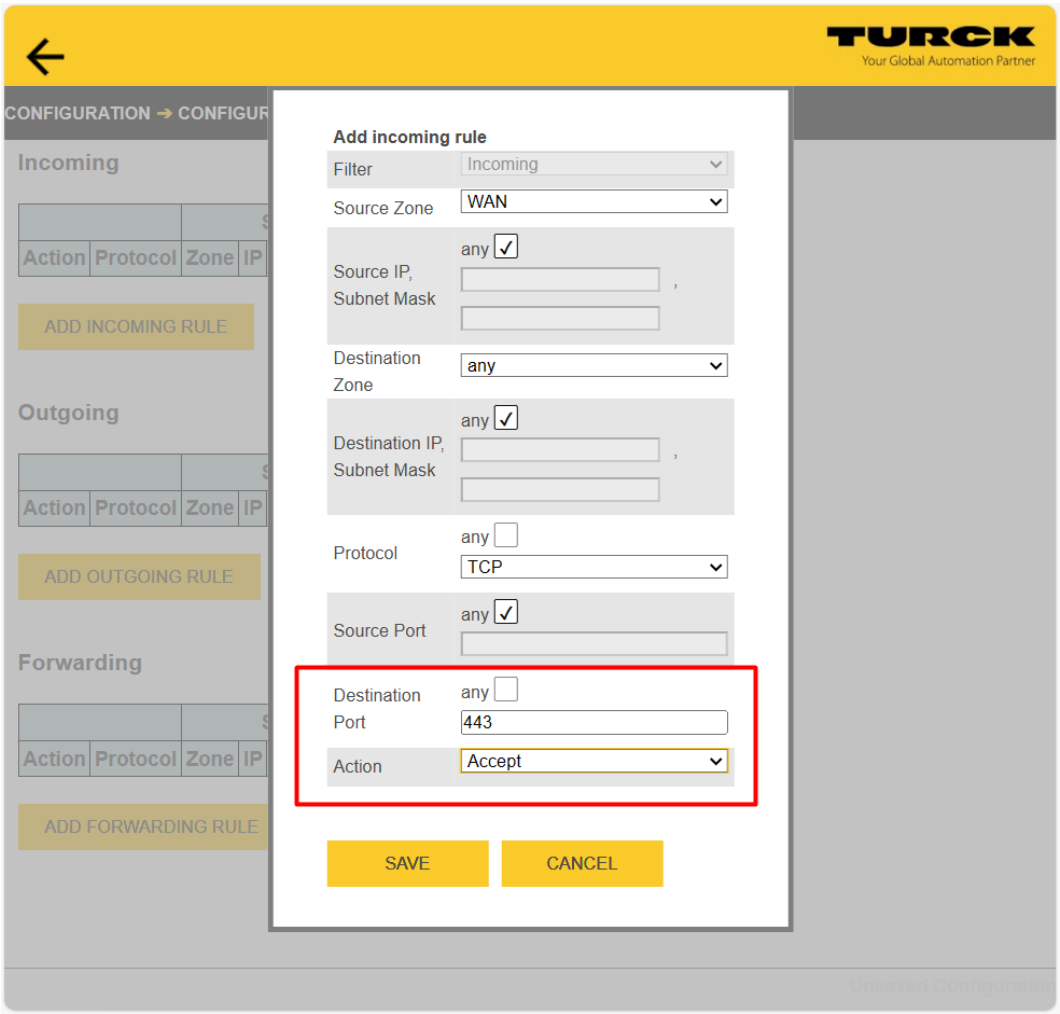

Fig. 66: Enable access via HTTPS

- Define the firewall rule via **SAVE** .
- Set up second incoming rule that blocks access via HTTP (port 80):

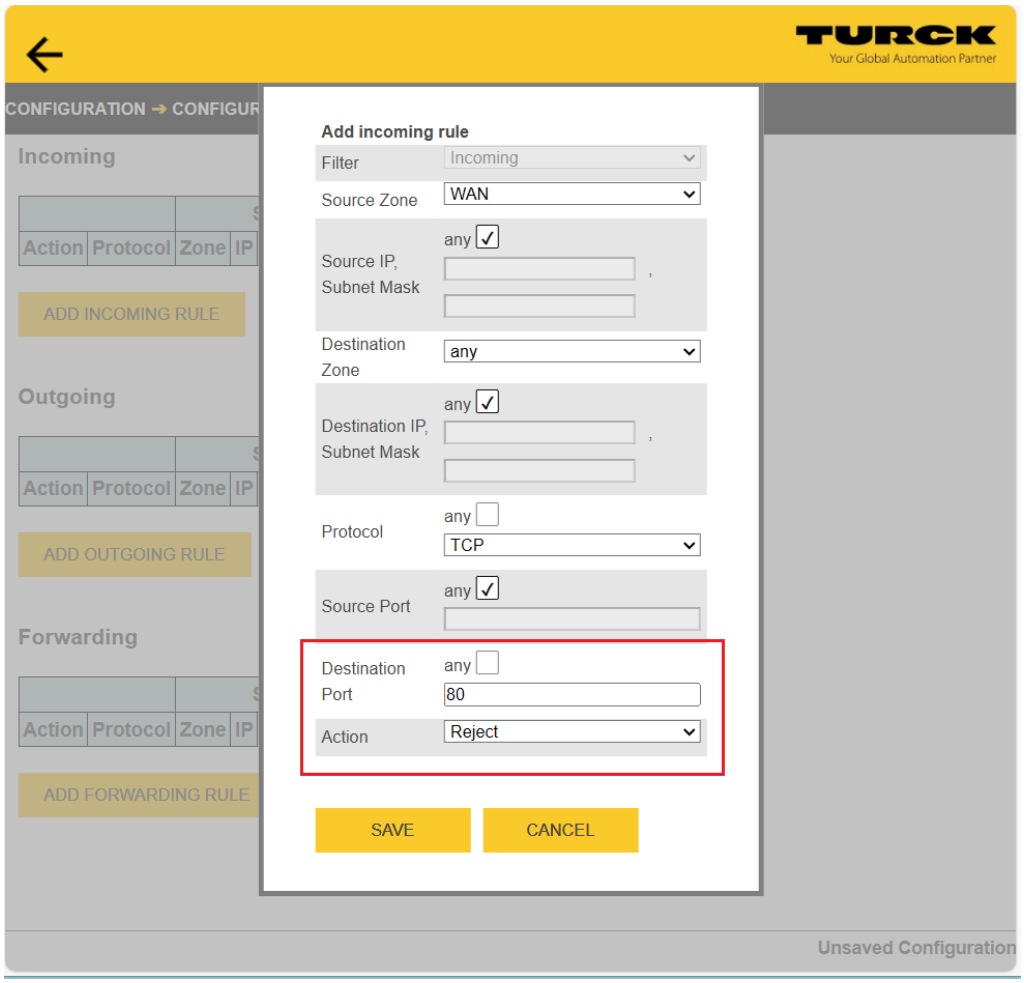

Fig. 67: block access via HTTP

▶ Create firewall rule via **SAVE** .

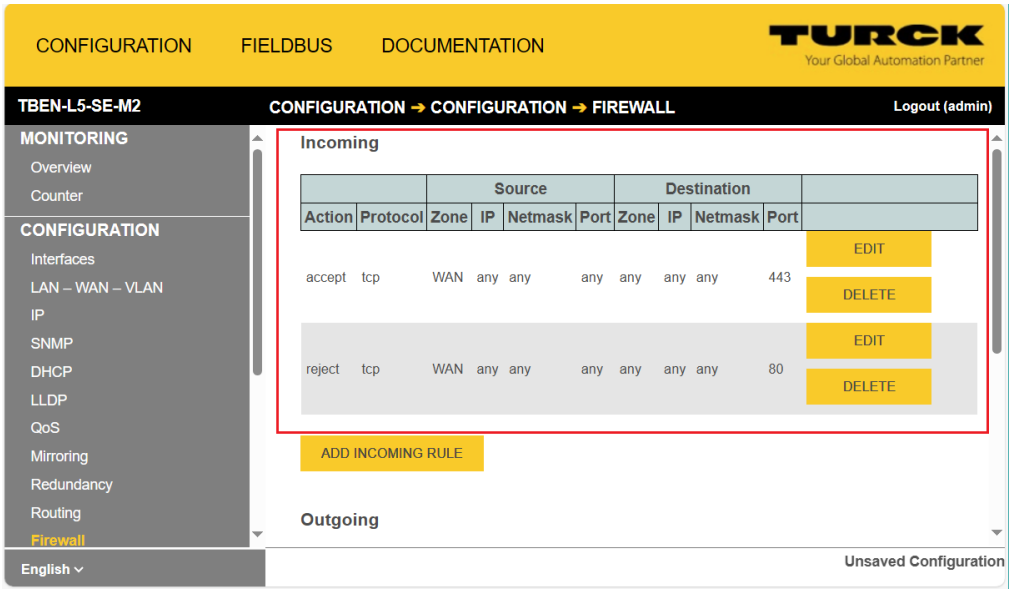

Fig. 68: Incoming Rules

8.1.12 NAT: configuring NAT/PAT rules

The NAT – PAT page is used to configure rules for NAT (Network Address Translation) and PAT (Port Address Translation).

NAT (Network Address Translation)

In NAT, IP addresses of one network are translated into IP addresses of another network.

PAT (Port Address Translation)

With PAT, all IP addresses of a network are mapped with port numbers (TCP/UDP ports). PAT rules define how data traffic is redirected from an incoming port to another port.

NOTE
IP forwarding (forwarding of data packets between networks with different IP address ranges) must be activated.

Add NAT Rule (Source NAT)

In the **Add NAT Rule** section, rules for the translation of IP addresses for outgoing telegrams are created.

Example:

Function	Value	Meaning
Desired priority	1…50	Order number to prioritize the rules, beginning with 1 and assigned consecutively
Source IP Network	12.222.2.0	IP address of an external network
Source IP Subnet Mask	255.255.255.0	Subnet mask of the external network
Outgoing Zone	LAN WAN	IP addresses of telegrams which are set here and sent from the network zone to participants of the source network (Source IP Network) are translated into IP addresses of the other network.

- ▶ Create a Source NAT rule.
- ▶ Add the rule via **ADD** and send it to the device.

Add Destination NAT/PAT Rule (Destination NAT)

Under **Add Destination NAT/PAT Rule**, rules for the translation of IP addresses are created. For PAT rules, port numbers are specified in addition to IP addresses.

Function	Value	Meaning
Index	1…64	Order number to prioritize the rules, beginning with 1 and assigned consecutively
Incoming Zone	LAN WAN	Network zone from which incoming telegrams are to be forwarded
Original IP	12.222.2.95	IP address assigned to the device in the external network
Destination IP	192.168.1.15	IP address in the internal network via which an external device device is to be accessed
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the service (e.g. web server = port 80)
Outgoing Dest. Port	80	

- ▶ Sett the NAT/PAT rule.
- ▶ Add the rule via **ADD** and send it to the device.

Example:

The web server of a TBEN-L5-PLC-10 (original IP: 12.222.2.95) in a plant network (WAN: 12.222.2.0) is accessed from a PC in the company network (LAN: 192.168.1.0) via a defined IP address (destination IP).

For this purpose, two PAT rules are defined, one for each communication direction.

- PAT rule 1:

Function	Value	Meaning
Index	1	
Incoming Zone	WAN	Plant network
Original IP	12.222.2.95	IP address of the TBEN-L5-PLC-10 in the WAN that is to be accessed via the LAN IP address 192.168.1.15 (Destination IP)
Destination IP	192.168.1.15	
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the web server
Outgoing Dest. Port	80	

- PAT rule 2:

Function	Value	Meaning
Index	2	
Incoming Zone	LAN	Factory network
Original IP	192.168.1.15	IP address in the LAN via which the TBEN-L5-PLC-10 is to be accessed
Destination IP	12.222.2.95	IP address of the TBEN-L5-PLC-10 in the WAN that is to be accessed via the LAN IP address 192.168.1.15 (Destination IP)
Protocol	TCP	Defines for which telegrams the rule applies (TCP, UDP, all = OFF).
Incoming Dest. Port	80	Port number of the web server
Outgoing Dest. Port	80	

8.1.13 IGMP: configuring Multicast

The device supports the functions **IGMP Snooper** and **IGMP Querier**.

The IGMP configuration is only effective if **Flood unknown Multicasts/Unicasts** under **Interfaces → Switching** is set to **off** or **IGMP only**.

NOTE
In PROFINET networks, the **IGMP Snooper** function must be deactivated.

Function	Value	Meaning
Snooper		If the IGMP Snooper function is activated, IGMP telegrams are received and evaluated. The device logs on to receive multicast telegrams by sending IGMP messages to a router and is recorded as a receiver in a multicast table.
Querier		If the IGMP Querier function is activated, the device itself also sends IGMP requests, which trigger responses from connected IGMP-capable participants.
Version	1	A host can join a multicast group. Logoff is not implemented. After a timeout, the host is deregistered.
	2	Starting with IGMP version 2, devices can log off from receiving IGMP messages with a leave message.
Interval [s]	0.01…1000000 s	Query (Snooper) or transmit interval (Querier)
Time out [s]	0.01…1000000 s	Time after which a device no longer receives multicast telegrams and is automatically deleted from the multi-cast table.

IGMP Settings

In the **IGMP Settings** section, the IGMP settings are made separately for the two networks LAN and WAN.

- Under LAN or WAN, activate the IGMP **Snooper** and/or or **Querier** function.
- Select the IGMP version.
- Define the polling or transmission interval.
- Send settings to the device via **SET IGMP**.

Active IGMP

The **Active IGMP** table shows all active IGMP requests and responses from connected devices.

8.1.14 NTP: configuring the time server

The switch is an NTP relay. The device requests date and time information from an external NTP server and makes it available to the connected devices.

- Enable time synchronization via NTP server with **enable** .
- Define NTP time server using the IP address of the server. In this example, the time server of the TU Berlin with the IP address 130.149.17.21 is used.
- Set the interval for the time query.
- Use **SET CONFIG** to send changes to the device.

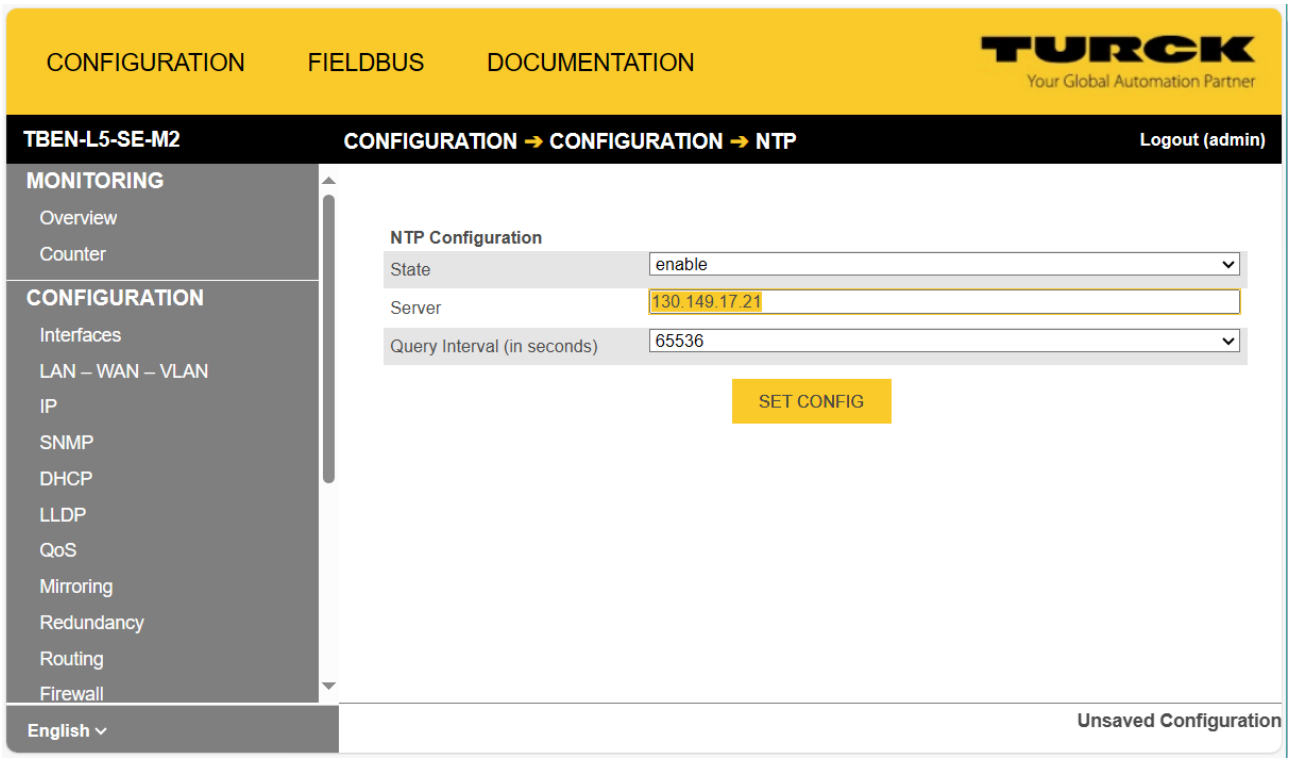

Fig. 69: Configuring the NTP server

8.1.15 Configuration. accept, reset, load or download the configuration

NOTE
If changes have been made to the configuration compared to the configuration stored in the device, this is indicated by the entry **Unsaved Configuration** at the bottom of the web server screen. Configuration changes are only stored in the device until a device failure or power reset.

- If the configuration is to be accepted as a permanent configuration:
  Use **Make current configuration persistent** → **SAVE** and save it as permanent configuration.

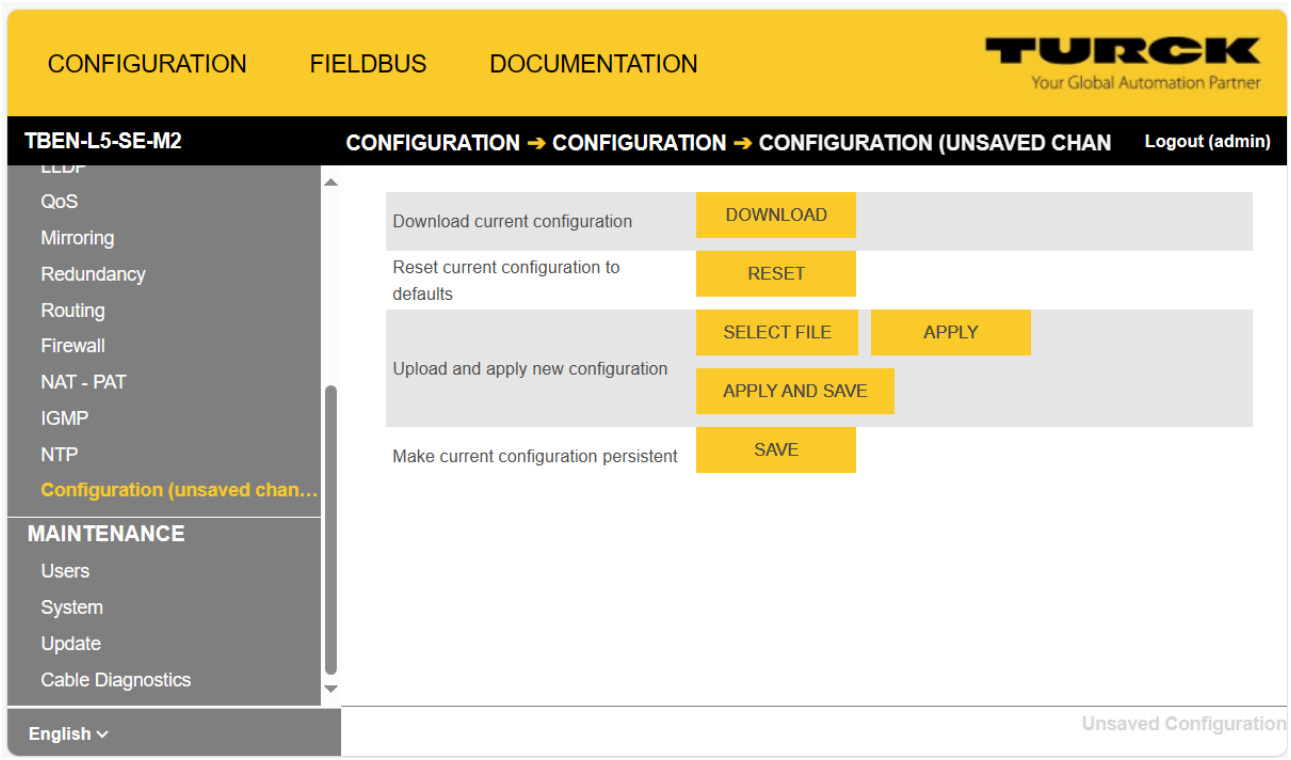

Fig. 70: Load, reset etc. the configuration

Save configuration permanently in the device

- Accept the changed configuration via **Make current configuration persistent** as the permanent configuration.

Reset current configuration to default configuration

- Use **Reset current configuration to defaults** to reset the configuration.

Load saved configuration

- Select the file with the stored configuration (*.cfg) via **Upload and apply new configuration → SELECT FILE** .
- Use **APPLY** to write the configuration to the device. The configuration is not stored permanently in the device.
- To save the configuration permanently in the device, use **Make current configuration persistent → SAVE** and save it as permanent configuration.

Storing the configuration

- Use **Download current configuration** to store the configuration. The configuration is stored in the folder that is defined as the download folder in the browser.

8.2 Downloading the configuration to the device via USB stick

The configuration is transferred via a USB stick using a command file (cmd.json). The file can be created in a text editor as shown below.

✓ The configuration of the device was downloaded from the web server via **Configuration → Download current configuration**.

▶ Load the file **cmd.json** from the folder **…\usb_commands\apply_and_save_config** and load the configuration file **config.cfg** onto the USB stick.

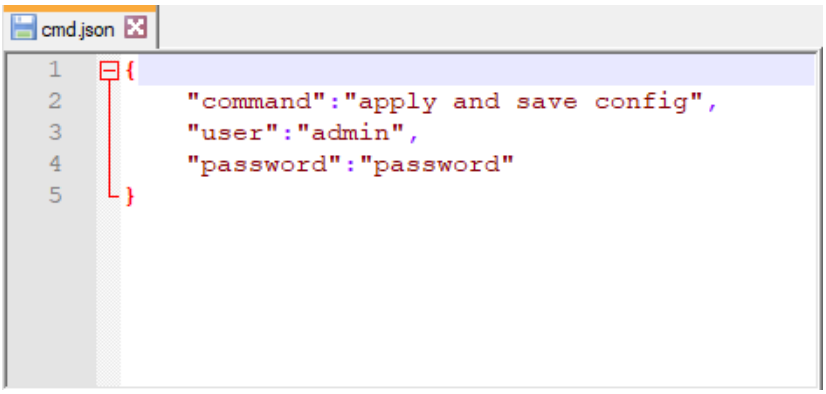

Fig. 71: Program file "cmd.json"

Program code:

```
{"command":"apply and save config",
"user":"admin",
"password":"password"}
```

▶ Open the service window above the switches.
▶ Insert the USB stick with the file **cmd.json** into the device.
⇨ The RUN LED flashes 3 × green at 1 Hz.
⇨ The RUN LED flashes green green at 0.5 Hz.
▶ Press the SET-button within the next 30 seconds for at least 3 seconds to start the update.
⇨ The RUN LED turns off.
⇨ When the RUN LED flashes green (1 Hz), the transfer of the configuration to the device is complete.
▶ Remove the USB stick.
▶ NOTICE! IP67 or IP69K protection is not guaranteed when the cover over the rotary coding switches is opened. Device damage through penetrating foreign objects or liquids is possible. Tightly close the service window.

Compatible USB sticks

FAT or FAT32 formatted USB sticks can be connected to the USB host port. It is not possible to connect NTFS formatted sticks or USB devices such as external hard disks, keyboards, PC mice, etc.

8.3 Parameters for the fieldbus integration

Word no.	Bit no.															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Fieldbus control																
0x00	FBUS LAST PORT								-	-	-	-	-	-	-	EN FB CTRL
Netload diagnostics																
0x01	-	-	-	-	-	-	-	-	-	-	-	-	-	EN NL ALARM	EN NL WARN	EN NL DIAG
0x02	-	-	-	-	-	-	-	-	TH NL WARN							
0x03	-	-	-	-	-	-	-	-	TH NL ALARM							
Frame error diagnostics																
0x04	-	-	-	-	-	-	-	-	-	-	-	-	-	EN FRM ALARM	EN FRM WARN	EN FRM DIAG
0x05	FRM TB															
0x06	TH FRM WARN															
0x07																
0x08	TH FRM ALARM															
0x09																
Duplex and link speed diagnostics																
0x0A	-	-	-	-	-	-	EN LS ALARM	EN LS DIAG	-	-	-	-	-	-	EN DUP ALARM	EN DUP DIAG
Port De-/Aktivierung																
0x0B	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	EN PORT CTRL
0x0c	-	-	-	-	-	-	XF10 activ-ated	XF9 activ-ated	XF8 activ-ated	XF7 activ-ated	XF6 activ-ated	XF5 activ-ated	XF4 activ-ated	XF3 activ-ated	XF2 activ-ated	XF1 activ-ated
PROFINET DHC (PROFINET only)																
0x0D	-	-	-	-	-	-	-	-	-	-	-	-	-	EN DHC ALARM	EN DHC WARN	EN DHC DIAG
0x0E	TH DHC WARN															
0x0F	TH DHC ALARM															
RSTP																
0x10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	EN RSTP

Meaning of parameter bits

Default values are shown in **bold**.

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
Fieldbus control				
EN FB CTRL Enable fieldbus control	0	0x0	No	The number of ports for which fieldbus control is activated cannot be limited.
	1	**0x1**	**Yes**	The number of ports for which fieldbus control is activated can be limited via the "Last port with fieldbus functionality" (FBUS LAST PORT) parameter.
FBUS LAST PORT Last port with fieldbus functionality	01…**10**	0x01… **0x0A**		The parameter can only be set if the parameter "Enable fieldbus control" (EN FB CTRL) is activated. The number of ports (port 1 to port…) for which fieldbus control is to be activated is limited (default: 0x0A = fieldbus control activated for all ports). Example: FBUS LAST PORT = 8 → fieldbus control activated for ports XF1…XF8. **Note:** The PLC must be connected to one of the defined ports. If the parameter is changed independently of the PLC program in the web server or similar (e.g. restriction of the ports with fieldbus control in the above example to FBUS LAST PORT = 6), the PLC will no longer have access to the device.
Netload diagnostics				
EN NL DIAG Enable netload diagnostics	0	0x0	No	Netload diagnostics deactivated
	1	**0x1**	**Yes**	Netload diagnostics activated Input data, warnings or alarms about netload will be sent.
EN NL WARN Enable warnings for netload diagnostics	0	0x0	No	Sending of warnings for netload deactivated
	1	**0x1**	**Yes**	Sending of warnings for netload activated.
EN NL ALARM Enable alarms for netload diagnostics	**0**	**0x0**	**No**	Sending of alarms for netload deactivated
	1	0x1	Yes	Sending of alarms for netload activated
TH NL WARN Threshold for netload warnings in %	0…100, **30**	0x0000… 0x0064, **0x001E**		If the threshold defined here is exceeded, warnings are issued for network load diagnostics. The parameters "Enable netload diagnostics (EN NL DIAG)" and "Enable warnings for netload diagnostics" (EN NL WARN) have to be activated.
TH NL ALARM Threshold for netload alarms in %	0…100, **80**	0x0000… 0x0064, 0x0050		If the threshold defined here is exceeded, alarms are issued for network load diagnostics. The parameters "Enable netload diagnostics (EN NL DIAG)" and "Enable warnings for netload diagnostics" (EN NL ALARM) have to be activated.
Frame error diagnostics				
EN FRM DIAG Enable frame error diagnostics	0	0x0	**No**	Frame error diagnostics deactivated
	1	**0x1**	Yes	Frame error diagnostics activated Input data, warnings or alarms for frame errors will be sent.

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
EN FRM WARN Enable warnings for frame error diagnostics	0	0x0	**No**	Sending of warnings for frame errors deactivated
	1	**0x1**	Yes	Sending of warnings for frame errors activated
EN FRM ALARM Enable alarms for frame error diagnostics	**0**	**0x0**	**No**	Sending of alarms for frame errors deactivated
	1	0x1	Yes	Sending of alarms for frame errors activated
FRM TB Time base for frame error diagnostics	0…65535, **60**	0x0… 0xFFFF, **0x3C**		Period of time in s in which the number of frame errors is calculated and returned
TH FRM WARN Threshold for frame error warnings	0… 4294967295, **100**	0x0… 0xFFFFFFFF, **0x64**		If the threshold defined here is exceeded, warnings are issued for frame error diagnostics. The parameters "Enable frame error diagnostics (EN FRM DIAG)" and "Enable warnings for frame error diagnostics" (EN FRM WARN) have to be activated.
TH FRM ALARM threshold for frame error alarms	0… 4294967295, **1000**	0x0… 0xFFFFFFFF, **0x03E8**		If the threshold defined here is exceeded, alarms are issued for frame error diagnostics. The parameters "Enable frame error diagnostics (EN FRM DIAG)" and "Enable warnings for frame error diagnostics" (EN FRM ALARM) have to be activated.
Duplex and link speed diagnostics				
EN DUP DIAG Enable full duplex diagnostics	**0**	**0x0**	**No**	Half duplex diagnostics deactivated
	1	0x1	Yes	Half duplex diagnostics activated Input data, warnings or alarms for half duplex diagnostics will be sent.
EN DUP ALARM Enable half duplex diagnostics	**0**	**0x0**	**No**	Sending of alarms for half duplex diagnostics deactivated
	1	0x1	Yes	Sending of alarms for half duplex diagnostics activated
EN LS DIAG Enable half duplex diagnostics	**0**	**0x0**	**No**	Link speed diagnostics deactivated
	1	0x1	Yes	Link speed diagnostics activated Input data, warnings or alarms for link speed diagnostics will be sent.
EN LS ALARM Enable link speed diagnostics	**0**	**0x0**	**No**	Sending of alarms for link speed diagnostics deactivated
	1	0x1	Yes	Sending of alarms for link speed diagnostics activated
Port control				
EN PORTCTL Enable port control	0	0x0	No	Port control enabled The ports cannot be switched on or off via the field-bus.
	1	**0x1**	**Yes**	Port control activated The ports can be enabled or disabled via the para-meter "Activate XF…" (XF… STATE) parameter.
XF… activated Activate XF1… activate XF10	0	0x0	No	Port XF… deactivated
	1	**0x1**	**Yes**	Port XF… activated

Parameter name	Value		Meaning	Description
	Dec.	Hex.		
PROFINET DHC (PROFINET only)				
EN DHC DIAG Enable PN DHC diagnostics	**0**	**0x0**	**No**	Diagnostics for PROFINET DHC (Data Hold Counter) deactivated
	1	0x1	Yes	Diagnostics for PROFINET DHC (Data Hold Counter) activated Input data, warnings or alarms for PROFINET DHC diagnostics will be sent.
EN DHC WARN Enable warnings for netload diagnostics	**0**	**0x0**	**No**	Sending of warnings for PROFINET DHC diagnostics deactivated
	1	0x1	Yes	Sending of warnings for PROFINET DHC diagnostics activated
EN DHC ALARM Enable alarms for PROFINET DHC diagnostics	**0**	**0x0**	**No**	Sending of alarms for PROFINET DHC diagnostics deactivated
	1	0x1	Yes	Sending of alarms for PROFINET DHC diagnostics activated
TH DHC WARN Threshold for PN DHC warnings	**2**…255	**0x02**…0xFF		If the threshold defined here is exceeded, warnings are issued for PROFINET DHC diagnostics. The parameters "Enable PROFINET DHC diagnostics (EN DHC DIAG)" and "Enable warnings for PROFINET DHC diagnostics" (EN DHC WARN) have to be activated.
TH DHC ALARM Threshold for PN DHC alarms	2…255, **3**	0x02…0xFF, **0x03**		If the threshold defined here is exceeded, alarms are issued for PROFINET DHC diagnostics. The parameters "Enable PROFINET DHC diagnostics (EN DHC DIAG)" and "Enable alarms for PROFINET DHC diagnostics" (EN DHC ALARM) have to be activated.
RSTP				
FB RSTP Enable RSTP	**0**	**0x0**	**No**	RSTP for LAN deactivated
	1	0x1	Yes	RSTP for LAN activated

9 Operating

9.1 Process input data

Word no. / Offset	Bit no. 15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Fieldbus control																
0x00	-	-	-	-	-	-	-	-	FBUS LAST PORT							
Netload diagnostics, Basic																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
Netload diagnostics, Advanced																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0x01	-	-	-	-	-	-	-	-	NL MAX							
0x02	-	-	-	-	-	-	-	-	NL MAX PLC							
Netload diagnostics, Full																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	NL ALARM	NL WARN
0x01	-	-	-	-	-	-	-	-	NL MAX							
0x02	-	-	-	-	-	-	-	-	NL MAX PLC							
0x03	-	-	-	-	-	-	NL WARN RX XF10	NL WARN RX XF9	NL WARN RX XF8	NL WARN RX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
0x04	-	-	-	-	-	-	NL WARN TX XF10	NL WARN TX XF9	NL WARN TX XF8	NL WARN TX XF7	NL WARN TX XF6	NL WARN TX XF5	NL WARN TX XF4	NL WARN TX XF3	NL WARN TX XF2	NL WARN TX XF1
0x05	-	-	-	-	-	-	NL ALARM RX XF10	NL ALARM RX XF9	NL ALARM RX XF8	NL ALARM RX XF7	NL ALARM RX XF6	NL ALARM RX XF5	NL ALARM RX XF4	NL ALARM RX XF3	NL ALARM RX XF2	NL ALARM RX XF1
0x06	-	-	-	-	-	-	NL ALARM TX XF10	NL ALARM TX XF9	NL ALARM TX XF8	NL ALARM TX XF7	NL ALARM TX XF6	NL ALARM TX XF5	NL ALARM TX XF4	NL ALARM TX XF3	NL ALARM TX XF2	NL ALARM TX XF1
Frame error diagnostics, Basic																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
Frame error diagnostics, Advanced																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0x01	FE MAX															
0x02																

Word no. Offset	Bit no. 15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Frame error diagnostics, Full																
0x00	-	-	-	-	-	-	-	-	-	-	-	-	-	-	FE ALARM	FE WARN
0x01	FE MAX															
0x02																
0x03	FE MAX PLC															
0x04																
0x05	-	-	-	-	-	-	FE WARN XF10	FE WARN XF9	FE WARN XF8	FE WARN XF7	FE WARN XF6	FE WARN XF5	FE WARN XF4	FE WARN XF3	FE WARN XF2	FE WARN XF1
0x06	-	-	-	-	-	-	FE ALARM XF10	FE ALARM XF9	FE ALARM XF8	FE ALARM XF7	FE ALARM XF6	FE ALARM XF5	FE ALARM XF4	FE ALARM XF3	FE ALARM XF2	FE ALARM XF1
Duplex diagnostics																
0x00	-	-	-	-	-	-	DUP XF10	DUP XF9	DUP XF8	DUP XF7	DUP XF6	DUP XF5	DUP XF4	DUP XF3	DUP XF2	DUP XF1
Link speed diagnostics																
0x00	-	-	-	-	-	-	LS XF10	LS XF9	LS XF8	LS XF7	LS XF6	LS XF5	LS XF4	LS XF3	LS XF2	LS XF1
Port status																
0x01	-	-	-	-	-	-	PS XF10	PS XF9	PS XF8	PS XF7	PS XF6	PS XF5	PS XF4	PS XF3	PS XF2	PS XF1
Counter for lost PROFINET RT frames (only for PROFINET)																
0x00	-	-	-	-	-	-	-	-	MAX PN RT FRAMES PLC							
0x01	-	-	-	-	-	-	-	-	MAX PN RT FRAMES							
Module status																
0x02	-	-	-	-	-	-	-	DIAG	-	FCE	-	-	-	COM	V1	-

Meaning of the process data bits

Name	Value		Meaning
Fieldbus control			
FBUS LAST PORT	0…10		Number of the last port with fieldbus functionality
Netload diagnostics			
NL WARN	No	0	-
	Yes	1	Netload warning at one of the ports
NL ALARM	No	0	-
	Yes	1	Netload alarm at one of the ports
NL MAX	0…100		Max. current netload (%)
NL MAX PLC	0…100		Maximum netload since last PLC connection in %
NL WARN RX XF1… XF10	No	0	-
	Yes	1	RX netload warning at port

Name	Value		Meaning
NL WARN TX XF1… XF10	No	0	-
	Yes	1	TX netload warning at port
NL ALARM RX XF1… XF10	No	0	-
	Yes	1	RX netload alarm at port
NL ALARM RX XF1… XF10	No	0	-
	Yes	1	TX netload alarm at port
Frame error diagnostics			
FE WARN	No	0	-
	Yes	1	Frame error warning at one of the ports
FE ALARM	No	0	-
	Yes	1	Frame error alarm at one of the ports
FE MAX	0…4294967295 (0…0xFFFFFFFF)		Max. frame errors Counter for the maximum number of frame errors that detected on any port within the parameterized time period (s. parameter "FRM TB (Time base for frame error diagnostics)".
FE MAX PLC	0…4294967295 (0…0xFFFFFFFF)		Max. number frame errors (peak) since last PLC connection Counter for the maximum number of frame errors since the last PLC connection.
FE WARN XF1… XF10	No	0	-
	Yes	1	Frame error warning at port
FE ALARM XF1…XF10	No	0	-
	Yes	1	Frame error alarm at port
Duplex diagnostics			
DUP XF1…DUP XF10	No	0	-
	Yes	1	Half duplex detected at XF…
Link speed diagnostics			
LS XF…	No	0	-
	Yes	1	10 Mbps detected at XF…
Port status			
PS XF1…XF10	No	0	-
	Yes	1	Active connection at port XF…
Counter for consecutively lost PROFINET RT frames			
MAX PN RT FRAMES PLC	0…255		Maximum number of consecutively lost PN-RT frames since last PLC connection
MAX PN RT FRAMES	0…255		Max. number of successively lost PN RT frames wihtin the last 10 minutes
Module status	See status and control word [▶ 134]		

9.2 LED displays

The device has the following LED indicators:

- Power supply
- Status

LED PWR	Meaning
Off	No voltage connected or under voltage at V1 (LED ERR is constantly red)
Green	Voltage at V1 OK

NOTE
Each of the Ethernet ports XF1…XF10 has an LED L/A.

LED L/A	Meaning
Off	No Ethernet connection
Green	Ethernet connection established,100 Mbps (XF1…XF10) or respectively 1 Gbps (XF9 and XF10)
Yellow	Ethernet connection established, 10 Mbps
Green flashing	Data transfer, 100 Mbps (XF1…XF10) or respectively 1 Gbps (XF9 and XF10)
Yellow flashing	Data transfer, 10 Mbps

LED BUS	Meaning
Off	Fieldbus inactive
Green	Active connection to a master
Green flashing (1 Hz)	IP address received, waiting for PLC connection
Red	IP address conflict, restore mode active or Modbus connection timeout
Red/green (1 Hz)	Waiting for IP address assignment in DHCP or BootP mode

LED ERR	Meaning
Off	Fieldbus inactive
Green	No diagnostics
Red	Diagnostic message pending

NOTE
The flashing pattern of the RUN LED indicates the configuration process when using the USB host function [▶ 125].

LED RUN	Meaning
Off	No USB function active
Green flashing (twice, 1 Hz)	USB host function is being activated
Green flashing (0.5 Hz)	USB function active

LED APP	Meaning
White flashing	Wink command active

9.3 Status- and control word

Status word

EtherNet/IP/ Modbus	PROFINET	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 0	Byte 1	-	-	-	-	-	-	-	DIAG
Byte 1	Byte 0	-	FCE	-	-	-	COM	V1	-

Bit	Description
COM	Internal Error The device-internal communication is disturbed.
DIAG	Diagnostic message at the device
FCE	DTM Force Mode is activated.
V1	Undervoltage at supply voltage V1 (threshold, s. technical data), DXP channels switch off

The status word is mapped into the module's process data.

In EtherNet/IP the mapping can be deactivated via the Gateway Class (VSC 100).

NOTE
Activating or deactivating the status and control word modifies the process data mapping in den standard Assembly Instances 103 and 104 EtherNet/IP standard classes, Assembly Object (0x04).

Control word

The control word has no function.

9.4 Software diagnostic messages

Except for the PROFINET DHC error diagnostics, the diagnostic data is also mapped into the process input data of the module.

Byte no.	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Netload diagnostics								
0	-	-	-	-	-	-	NL ALARM	NL WARN
1	-	-	-	-	-	-	-	-
2	NL WARN RX XF8	NL WARN RX XF7	NL WARN RX XF6	NL WARN RX XF5	NL WARN RX XF4	NL WARN RX XF3	NL WARN RX XF2	NL WARN RX XF1
3	-	-	-	-	-	-	NL WARN RX XF10	NL WARN RX XF9
4	NL WARN TX XF8	NL WARN TX XF7	NL WARN TX XF6	NL WARN TX XF5	NL WARN TX XF4	NL WARN TX XF3	NL WARN TX XF2	NL WARN TX XF1
5	-	-	-	-	-	-	NL WARN TX XF10	NL WARN TX XF9
6	NL ALARM RX XF8	NL ALARM RX XF7	NL ALARM RX XF6	NL ALARM RX XF5	NL ALARM RX XF4	NL ALARM RX XF3	NL ALARM RX XF2	NL ALARM RX XF1
7	-	-	-	-	-	-	NL ALARM RX XF10	NL ALARM RX XF9
8	NL ALARM TX XF8	NL ALARM TX XF7	NL ALARM TX XF6	NL ALARM TX XF5	NL ALARM TX XF4	NL ALARM TX XF3	NL ALARM TX XF2	NL ALARM TX XF1
9	-	-	-	-	-	-	NL ALARM TX XF10	NL ALARM TX XF9
Frame Error diagnostics								
0	-	-	-	-	-	-	FE ALARM	FE WARN
1	-	-	-	-	-	-	-	-
2	FE WARN XF8	FE WARN XF7	FE WARN XF6	FE WARN XF5	FE WARN XF4	FE WARN XF3	FE WARN XF2	FE WARN XF1
3	-	-	-	-	-	-	FE WARN XF10	FE WARN XF9
4	FE ALARM XF8	FE ALARM XF7	FE ALARM XF6	FE ALARM XF5	FE ALARM XF4	FE ALARM XF3	FE ALARM XF2	FE ALARM XF1
5	-	-	-	-	-	-	FE ALARM XF10	FE ALARM XF9
Duplex diagnostics								
0	DUP XF8	DUP XF7	DUP XF6	DUP XF5	DUP XF4	DUP XF3	DUP XF2	DUP XF1
1	-	-	-	-	-	-	DUP XF10	DUP XF9
Link speed diagnostics								
0	LS XF8	LS XF7	LS XF6	LS XF5	LS XF4	LS XF3	LS XF2	LS XF1
1	-	-	-	-	-	-	LS XF10	LS XF9
PROFINET DHC error diagnostics (PROFINET only)								
0	-	-	-	-	-	-	DHC WARN AR2	DHC WARN AR1
1	-	-	-	-	-	-	DHC ALARM AR2	DHC ALARM AR1

Meaning of diagnostic bits

Name	Value		Meaning
Netload diagnostics			
NL WARN	No	0	-
	Yes	1	Netload warning at one of the ports
NL ALARM	No	0	-
	Yes	1	Netload alarm at one of the ports
NL WARN RX XF1… XF10	No	0	-
	Yes	1	RX netload warning at port
NL WARN TX XF1… XF10	No	0	-
	Yes	1	TX netload warning at port
NL ALARM RX XF1… XF10	No	0	-
	Yes	1	RX netload alarm at port
NL ALARM RX XF1… XF10	No	0	-
	Yes	1	TX netload alarm at port
Frame error diagnostics			
FE WARN	No	0	-
	Yes	1	Frame error warning at one of the ports
FE ALARM	No	0	-
	Yes	1	Frame error alarm at one of the ports
FE MAX	0…4294967295 (0…0xFFFFFFFF)		Max. frame errors Counter for the maximum number of frame errors that detected on any port within the parameterized time period (s. parameter "FRM TB (Time base for frame error diagnostics)".
FE MAX PLC	0…4294967295 (0…0xFFFFFFFF)		Max. number frame errors (peak) since last PLC connection Counter for the maximum number of frame errors since the last PLC connection.
FE WARN XF1… XF10	No	0	-
	Yes	1	Frame error warning at port
FE ALARM XF1…XF10	No	0	-
	Yes	1	Frame error alarm at port
Duplex diagnostics			
DUP XF1…DUP XF10	No	0	-
	Yes	1	Half duplex detected at XF…
Link speed diagnostics			
LS XF…	No	0	-
	Yes	1	10 Mbps detected at XF…
PROFINET DHC error diagnostics (PROFINET only)			
DHC WARN AR…	No	0	-
	Yes	1	PN DHC warning AR1 or AR2
DHC ALARM AR…	No	0	-
	Yes	1	PN DHC alarm AR1 or AR2

9.4.1 PROFINET diagnostics

Station diagnostics (slot 0 according to configuration tool)	PROFINET diagnostics Error code
Undervoltage	
V1	0x0002

I/O diagnostics (Slot 1 according to configuration tool)	PROFINET diagnostics Error code
Netload diagnostics	
Netload warning	0x1712
Netload alarm	0x1713
RX netload warning at port XF1	0x1714
…	…
RX netload warning at port XF10	0x1723
TX netload warning at port XF1	0x1724
…	…
TX netload warning at port XF10	0x1733
RX netload alarm at port XF1	0x1734
…	…
RX netload alarm at port XF10	0x1743
TX netload alarm at port XF1	0x1744
…	…
TX netload alarm at port XF10	0x1753
Frame error diagnostics	
Frame error warning	0x1754
Frame error alarm	0x1755
Frame error warning at port XF1	0x1756
…	…
Frame error warning at port XF10	0x1765
Frame error alarm at port XF1	0x1766
…	…
Frame error alarm at port XF10	0x1775
Duplex diagnostics	
Half duplex detected at XF1	0x1776
…	…
Half duplex detected at XF10	0x1785
Link speed diagnostics	
10 Mbps detected at XF1	0x1786
…	…
10 Mbps detected at XF10	0x1795
PROFINET DHC error diagnostics	
PN DHC warning AR1	0x1796
PN DHC warning AR2	0x1797

I/O diagnostics (Slot 1 according to configuration tool)	PROFINET diagnostics Error code
PN DHC alarm AR1	0x1798
PN DHC warning AR2	0x1799

9.5 Cable diagnostics

The cable diagnostics measures the length of the Ethernet line for the selected port or detects line breaks, open line ends, etc.

NOTE
The switch briefly deactivates the selected port for the line test. If the line test is activated for the port via which the connection to the PC (web server) is established, this connection is also interrupted and the web server displays a timeout message. The length check can only be carried out if no device is connected to the selected port or the connected device is switched off.

- ▶ Select the Ethernet ports for which line diagnostics are to be performed.
- ▶ Start the line diagnostics via **START CABLE DIAGNOSTCS** .
- ⇨ The lines on the selected Ethernet ports are checked.
- ⇨ Line breaks are detected and localized wire by wire.

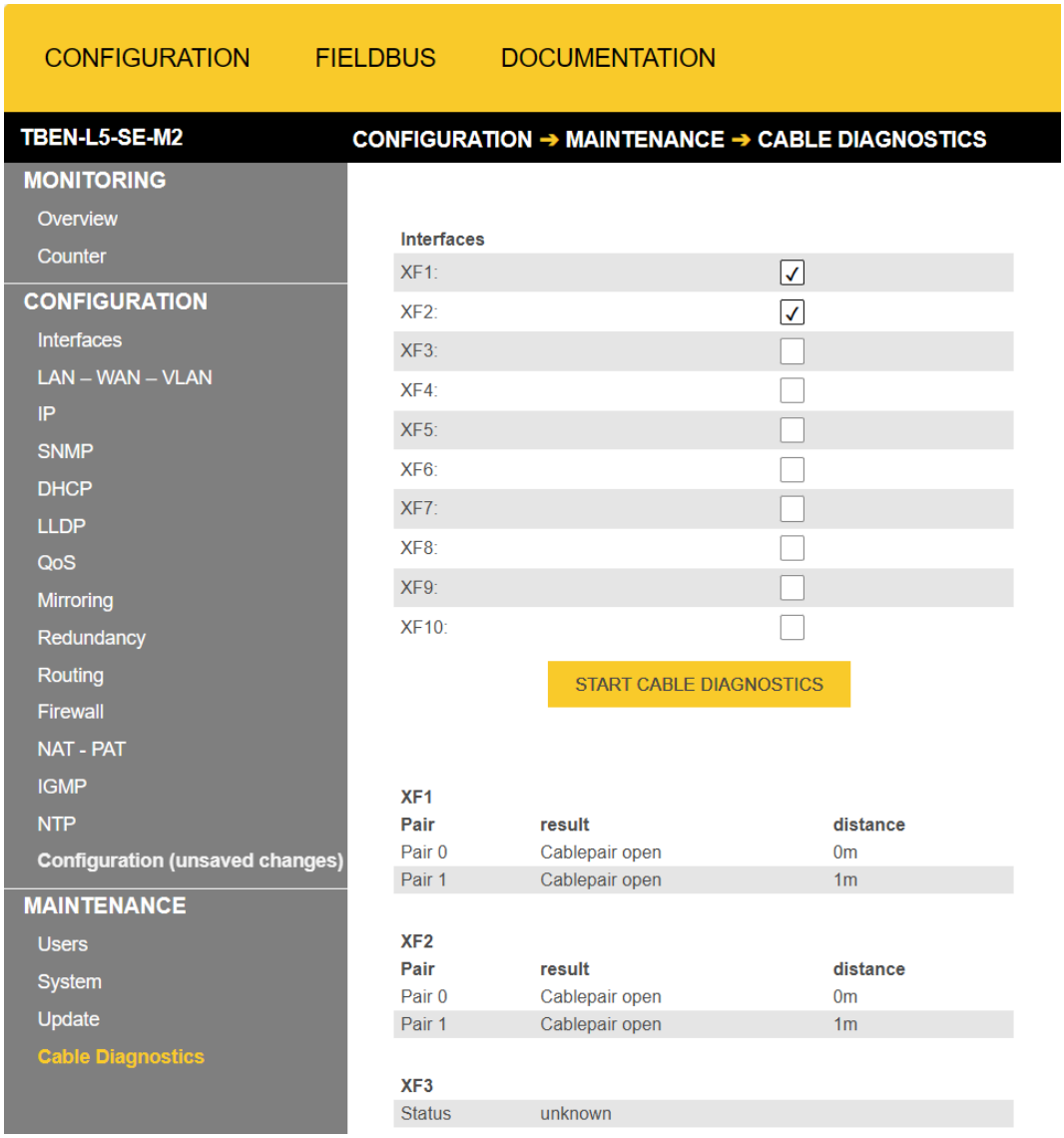

Fig. 72: Cable diagnostics in the web server

9.6 Monitoring function

9.6.1 Monitoring – Overview (device overview)

Overview shows an overview of all Ethernet interfaces of the device, the device data (name, firmware version, etc.) and the current device settings (VLAN, DHCP, routing, etc.).

A click on the respective entries opens the corresponding configuration page.

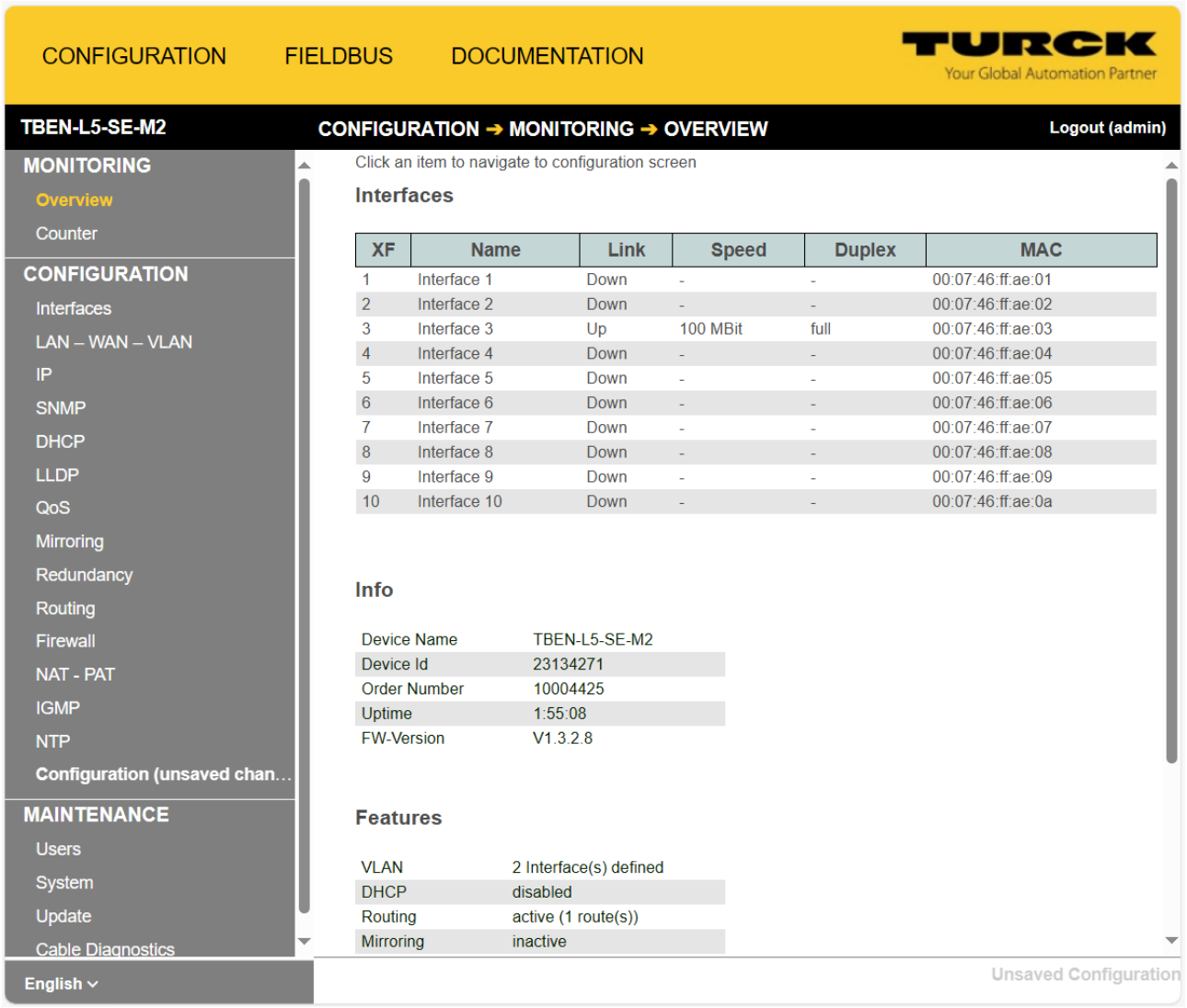

Fig. 73: Overview in the web server

9.6.2 Monitoring – Counter (network load monitoring)

Counter shows all sent and received telegrams as well as the calculated network load in %.

The values can also be displayed graphically:

- Select the values by double-clicking.
- Use the button **Graph** to switch to the graphical view.

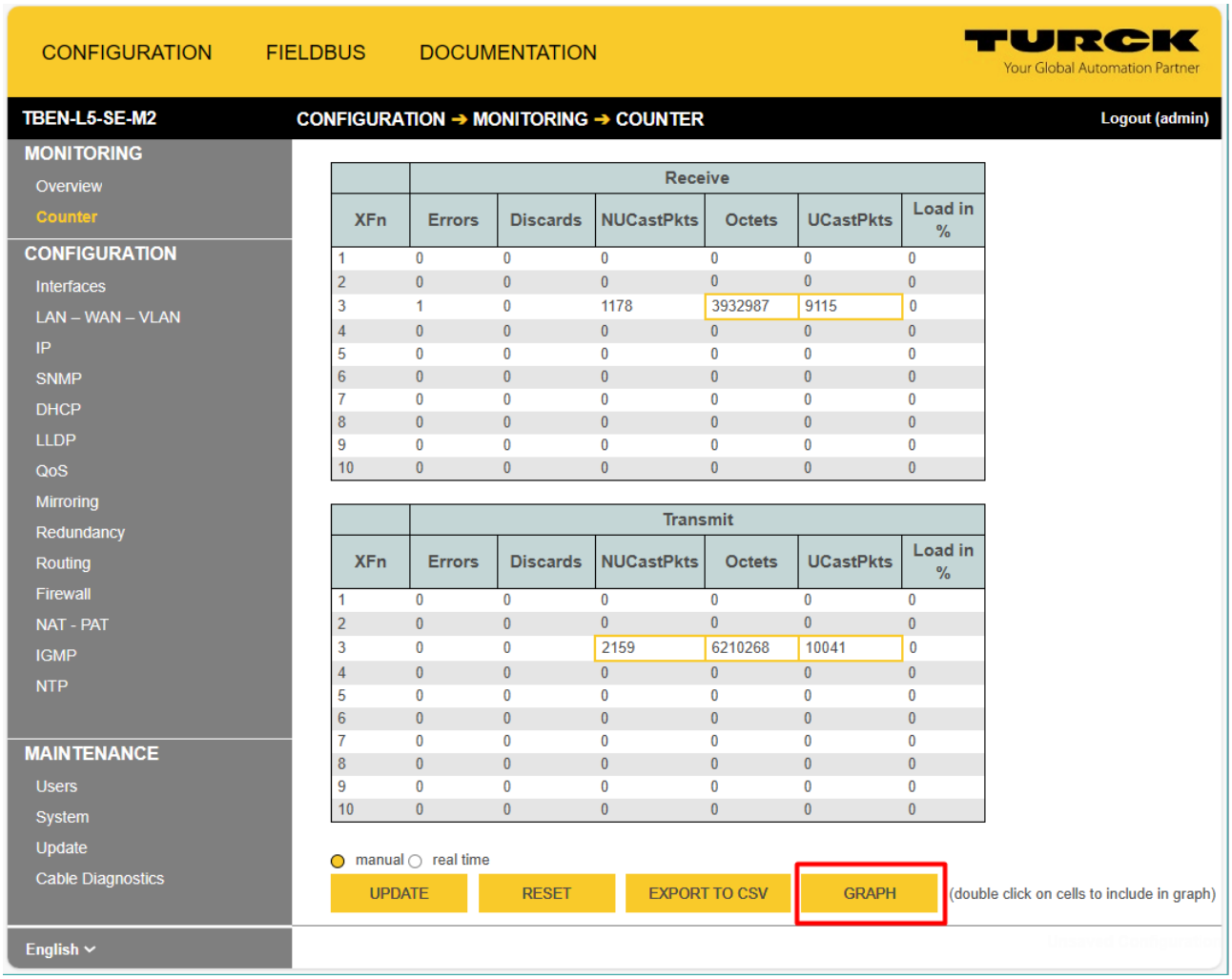

Fig. 74: Counter (tables) in the web server

➪ The values are displayed graphically.

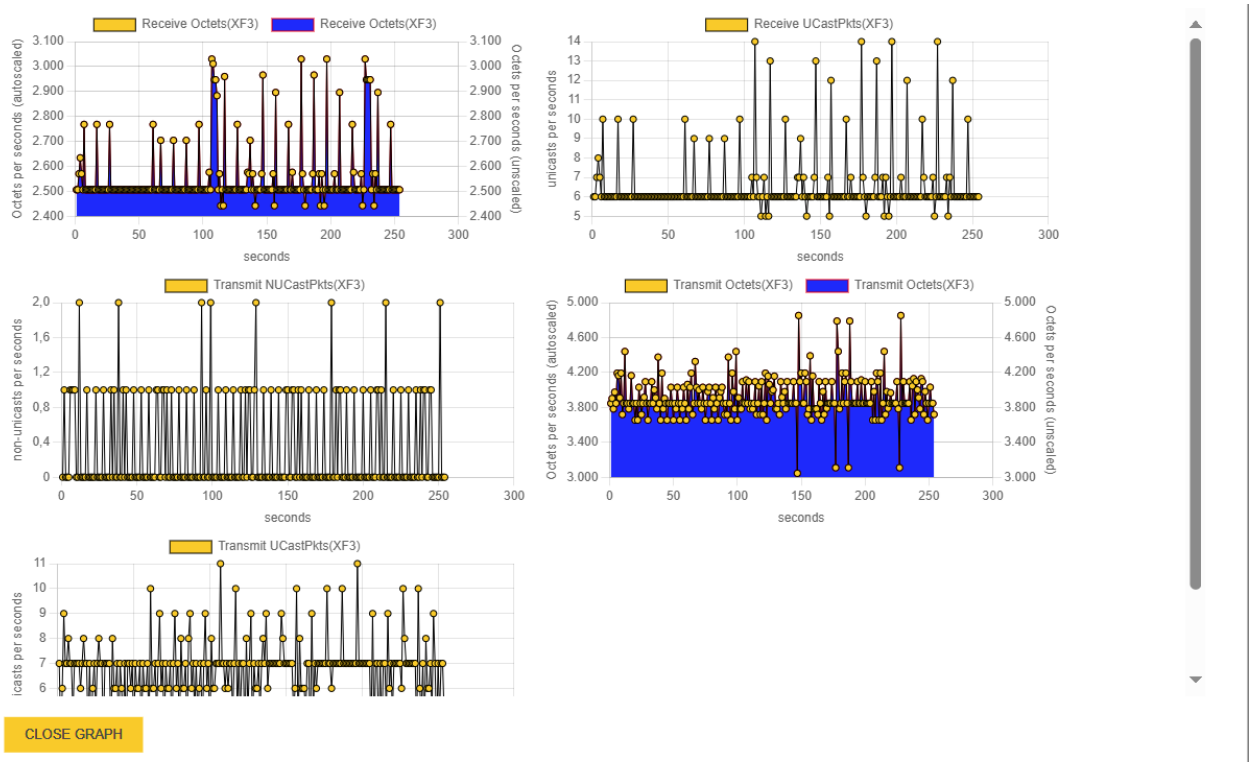

Fig. 75: Counter (graphic display) in the web server

10 Troubleshooting

If the device does not function as expected, first check whether ambient interference is present. If there is no ambient interference present, check the connections of the device for faults.

If there are no faults, there is a device malfunction. In this case, decommission the device and replace it with a new device of the same type.

11 Maintenance

Ensure regularly that the plug connections and cables are in good condition.

The devices are maintenance-free, clean dry if required.

11.1 Executing the firmware update via the web server

- Open the web server and log in.
- Select the storage location of the file and select file.
- Start the firmware update via the **UPDATE FIRMWARE** Button.
- Restart the device after the firmware update has been completed.

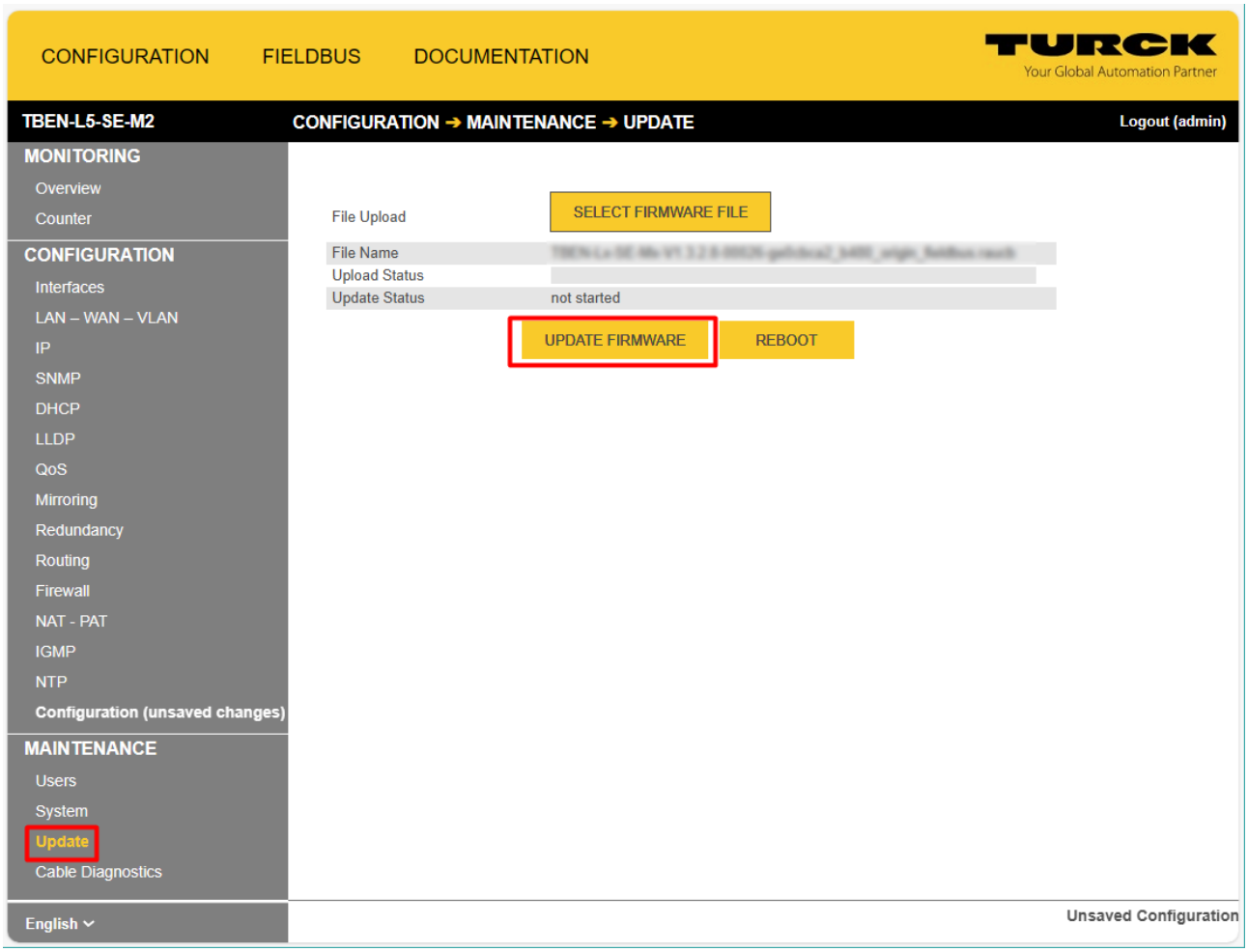

Fig. 76: Updating the firmware via the web server

12 Repair

The device is not intended for repair by the user. The device must be decommissioned if it is faulty. Observe our return acceptance conditions when returning the device to Turck.

12.1 Returning devices

If a device has to be returned, bear in mind that only devices with a decontamination declaration will be accepted. This is available for download at
https://www.turck.de/en/return-service-6079.php
and must be completely filled in, and affixed securely and weather-proof to the outside of the packaging.

13 Disposal

The devices must be disposed of properly and do not belong in the domestic waste.

14 Technical data

Technical data	
Supply	
Supply voltage	24 VDC
Permissible range	8…30 VDC with load dump protection
Current feed-through	
■ TBEN-L4/TBEN-L5 (X1 to X2)	Max. 9 A per voltage group
■ TBEN-LL (XD1 to XD2)	Max. 16 A per voltage group
■ Ex derating	S. document "Notes on Use in Ex zone 2 and 22" (ID 100022986)
Current consumption at 24 VDC	Max. 200 mA
Power loss	≤ 4.8 W
Connectors	
Supply	
■ TBEN-L4	■ X1: 7/8" male connector, 4-pin ■ X2: 7/8" female connector, 4-pin
■ TBEN-L5	■ X1: 7/8" male connector, 5-pin ■ X2: 7/8" female connector, 5-pin
■ TBEN-LL	■ XD1: M12 male connector, 5-pin, L-coded ■ XD2: M12 female connector, 5-pin, L-coded
Ethernet	2 x M12, 8-pin, X-coded 8 x M12, 4-pin, D-coded
Permissible torques ■ Ethernet ■ Mounting (M6 screws)	 0.6 Nm 1.5 Nm
Isolation voltages	
V1 to V2	≤ 500 V AC
V1/V2 to fieldbus	≤ 500 V AC
System data	
Transmission rate	XF1…XF8: 10/100 Mbps XF9…XF10: 10/100/1000 Mbps
Max. cable length	
■ Ethernet	100 m (per segment)
System data	
Transmission rate	10 Mbps/100 Mbps
Protocol detection	Automatic
Web server	Integrated
Service interface	Ethernet via XF1 or XF2
Modbus TCP	
Address assignment	Static IP, BOOTP, DHCP
Supported Function Codes	FC3, FC4, FC6, FC16, FC23
Number of TCP connections	8
Input register, start address	0 (0x0000)
Local port	Port 502, fix setting

Technical data	
EtherNet/IP	
Address assignment	According to EtherNet/IP standard
Device Level Ring (DLR)	Supported
Quick Connect (QC)	< 150 ms
Min. RPI (Requested Packet Interval)	2 ms
Number of Class 3 connections (TCP)	3
Number of Class 1 connections (CIP)	10
Input Assembly Instance	103
Output Assembly Instance	104
Configuration Assembly Instance	106
PROFINET	
Address assignment	DCP
MinCycle Time	1 ms
Fast Start Up (FSU)	< 150 ms
Diagnostics	According to PROFINET alarm handling
Automatic address setting	Supported
Media Redundancy Protocol (MRP)	Supported
Web server	Integrated Default IP address: 192.168.1.254
Mounting	
Type of mounting	Via 2 mounting holes, Ø 6.3 mm
Mounting distance (device to device)	≥ 50 mm Valid for operation in the ambient temperatures mentioned below, with sufficient ventilation as well as maximum load (horizontal mounting). For low simultaneity factors and low ambient temperatures, mounting distances of < 50 mm may also be realizable.
Standard/directive conformity	
Vibration test	According to EN 60068-2-6
Acceleration	Up to 20 g
Shock test	According to EN 60068-2-27
Drop and topple	According to IEC 60068-2-31/IEC 60068-2-32
Electromagnetic compatibility	According to EN 61131-2
Approvals and certificates	CE UL UV-resistant according to DIN EN ISO 4892-2A (2013)
General Information	
Dimensions (B × L × H)	64 × 230.4 × 39 mm
Operating temperature	-40…+70 °C
Storage temperature	-40…+85 °C
Relative humidity	100 %, indoor use (UL only)
Overvoltage category	II

Technical data	
Weight	605 g
Operating height	Max. 5000 m
Degree of protection	IP65/IP67/IP69K (not evaluated by UL)
Pollution degree	2
MTTF	
■ TBEN-L4-SE-M2 and TBEN-L5-SE-M2	82 years acc. to SN 29500 (Ed. 99) 20 °C
■ TBEN-LL-SE-M2	81 years acc. to SN 29500 (Ed. 99) 20 °C
Housing material	PA6-GF30
Halogen-free	Yes

Note on FCC

NOTE
This device complies with the limit values for a Class A digital device in accordance with Part 15 of the FCC regulations. Operation of this device in a residential area may cause harmful interference. In this case users must rectify the interference at their own cost.

15 Turck branches — contact data

Germany	Hans Turck GmbH & Co. KG Witzlebenstraße 7, 45472 Mülheim an der Ruhr www.turck.de
Australia	Turck Australia Pty Ltd Building 4, 19-25 Duerdin Street, Notting Hill, 3168 Victoria www.turck.com.au
Austria	Turck GmbH Graumanngasse 7/A5-1, A-1150 Vienna www.turck.at
Belgium	TURCK MULTIPROX Lion d'Orweg 12, B-9300 Aalst www.multiprox.be
Brazil	Turck do Brasil Automação Ltda. Rua Anjo Custódio Nr. 42, Jardim Anália Franco, CEP 03358-040 São Paulo www.turck.com.br
Canada	Turck Canada Inc. 140 Duffield Drive, CDN-Markham, Ontario L6G 1B5 www.turck.ca
China	Turck (Tianjin) Sensor Co. Ltd. 18,4th Xinghuazhi Road, Xiqing Economic Development Area, 300381 Tianjin www.turck.com.cn
Czech Republic	TURCK s.r.o. Na Brne 2065, CZ-500 06 Hradec Králové www.turck.cz
France	TURCK BANNER S.A.S. 11 rue de Courtalin Bat C, Magny Le Hongre, F-77703 MARNE LA VALLEE Cedex 4 www.turckbanner.fr
Hungary	TURCK Hungary kft. Árpád fejedelem útja 26-28., Óbuda Gate, 2. em., H-1023 Budapest www.turck.hu
India	TURCK India Automation Pvt. Ltd. 401-403 Aurum Avenue, Survey. No 109 /4, Near Cummins Complex, Baner-Balewadi Link Rd., 411045 Pune - Maharashtra www.turck.co.in
Italy	TURCK BANNER S.R.L. Via San Domenico 5, IT-20008 Bareggio (MI) www.turckbanner.it
Japan	TURCK Japan Corporation ISM Akihabara 1F, 1-24-2, Taito, Taito-ku, 110-0016 Tokyo www.turck.jp

Korea	Turck Korea Co, Ltd. A605, 43, Iljik-ro, Gwangmyeong-si 14353 Gyeonggi-do www.turck.kr
Malaysia	Turck Banner Malaysia Sdn Bhd Unit A-23A-08, Tower A, Pinnacle Petaling Jaya, Jalan Utara C, 46200 Petaling Jaya Selangor www.turckbanner.my
Mexico	Turck Comercial, S. de RL de CV Blvd. Campestre No. 100, Parque Industrial SERVER, C.P. 25350 Arteaga, Coahuila www.turck.com.mx
Netherlands	Turck B. V. Ruiterlaan 7, NL-8019 BN Zwolle www.turck.nl
Poland	TURCK sp.z.o.o. Wroclawska 115, PL-45-836 Opole www.turck.pl
Romania	Turck Automation Romania SRL Str. Siriului nr. 6-8, Sector 1, RO-014354 Bucuresti www.turck.ro
Sweden	Turck AB Fabriksstråket 9, 433 76 Jonsered www.turck.se
Singapore	TURCK BANNER Singapore Pte. Ltd. 25 International Business Park, #04-75/77 (West Wing) German Centre, 609916 Singapore www.turckbanner.sg
South Africa	Turck Banner (Pty) Ltd Boeing Road East, Bedfordview, ZA-2007 Johannesburg www.turckbanner.co.za
Turkey	Turck Otomasyon Ticaret Limited Sirketi Inönü mah. Kayisdagi c., Yesil Konak Evleri No: 178, A Blok D:4, 34755 Kadiköy/ Istanbul www.turck.com.tr
United Kingdom	TURCK BANNER LIMITED Blenheim House, Hurricane Way, GB-SS11 8YT Wickford, Essex www.turckbanner.co.uk
USA	Turck Inc. 3000 Campus Drive, USA-MN 55441 Minneapolis www.turck.us

TURCK

Your Global Automation Partner

Over 30 subsidiaries and
60 representations worldwide!

100013016 | 2024/10

www.turck.com