e-light-100-2MA

Art.-Nr.: 044200 01 000X 000X XX

eks Engel FOS GmbH & Co. KG
Schützenstraße 2-4
57482 Wenden-Hillmicke
Germany

Tel: **+49 (0) 2762 9313-600**
Fax: **+49 (0) 2762 9313-7906**
E-Mail: **info@eks-engel.de**
Internet: **www.eks-engel.de**

Legal notice

This manual contains important notes and warnings that could lead to serious personal and property damage if ignored. Please read this manual carefully prior to commissioning the ***EL-100-2MA*** switches. Correct transport, correct storage, and installation and careful operation and maintenance of the ***EL-100-2MA*** are critical for safe operation.

Intended use

The devices in the ***EL-100-2MA*** product family may only be operated as described in this manual. These may only be used free of damage and according to the indicated environmental conditions. The enclosure of the ***EL-100-2MA*** may only be opened by eks technicians; the devices do not contain any components that must be maintained by the customer. The ETHERNET connections are only intended for connection to computer networks (LANs) and must not be connected to telephone networks or telecommunication lines.

Personnel requirements

Installation and commissioning of the ***EL-100-2MA*** may only be completed by trained personnel who are familiar with this operating manual. Furthermore, all work on electrical systems may only be completed by an electrician or under their direction and supervision. Applicable local and national safety conditions must be maintained at all times.

Voltage supply

The devices in the ***EL-100-2MA*** product family have been designed for operation with NEC Class 2 conform voltage supplies.

The shielding of the RJ45 sockets is connected with the enclosure of the ***EL-100-2MA*** to discharge faults. Note any possible short circuits when using shielded cables.

Laser equipment safety

The devices in the ***EL-100-2MA*** product family include LED or LASER components as per IEC 60825-1 (2014): class 1 laser/LED product.

Warning!

Do not use optical instruments (e.g. lenses, microscope) to look into the beam of the optical transceivers! Ignoring this warning may result in eye damage.

CE conformity

The devices in the ***EL-100-2MA*** product family match the regulations of the EU guideline

2014/30/EU

Directive of the Council… regarding electromagnetic compatibility

with the following standard and standardizing documents in the currently applicable version:

DIN EN61000-6-2	**Electromagnetic compatibility (EMC) – part 6-2:**
	Generic standards – Immunity for industrial environments
DIN EN55032 cl. A:2016-2	**Information technology equipment**
	Radio disturbance characteristics – Limits and methods of measurement

Warning!

This is a class A product. It may cause radio disturbances in living areas; in this case, the operator can be required to take appropriate measures and to be responsible for these.

The installation instructions in this manual must be followed exactly so that the EMC threshold values indicated are maintained.

Disposal notes

The devices must not be disposed with normal household waste but can be returned to eks Engel FOS GmbH & Co. KG for disposal.

WEEE-identification: DE 900 53 255

Foreword

Overview of the *EL-100-2MA* product family

The devices in the ***EL-100-2MA*** product family are industrial Ethernet switches including management features that can be configured comfortably and easily via a web application. These enable low-cost installation of industrial Ethernet bus, star, and ring structures with switching functionality.

In addition to the basic version of the ***EL-100-2MA***, which is delivered without fiberoptic connections, there are versions with two or four fiberoptic connections. These devices can be equipped with the most diverse transceivers for single mode or multi-mode featuring plug connector types ST or SC.

Properties

- Web application for configuration
- Redundant voltage supply 12 VDC to 60 VDC with reverse voltage protection
- Monitoring of individual input voltages via configurable alarms
- Two relay contacts controlled via configurable alarms
- 10BASE-T/100BASE-TX (RJ45) and 100BASE-FX (MM or SM)
- PHY and MAC completely compatible to IEEE 802.3, IEEE802.3u, and IEEE 802.3x
- Auto MDI/MDI-X crossover function for 100BASE-T and 10BASE-T ports
- Store-and-forward switching architecture with 2048 MAC address table
- Quality of Service (QoS) with four priority queues
  Prioritize via IEEE 802.1p Class of Service (COS), Type of Service (TOS)/DiffServ or port priority
  Limitation of incoming and outgoing packets
- Port mirror for TX or TX and RX packets
- Port-based VLAN/802.1Q Tagged VLAN
- Simple Network Time Protocol (SNTP)
- Simple Mail Transfer Protocol (SMTP) for signaling alarms
- Internet Gateway Management Protocol Snooping (IGMP Snooping)
- Dynamical Host Configuration Protocol (DHCP) client function
- Simple Network Management Protocol (SNMP)
- Update, save, and back up the system configuration via TFTP, HTTP and USB

- Profinet (Conformance Class B, Netload Class III)

Note:

Depending on the version of the programmed software, devices can be delivered featuring other functions.

1 Table of contents

2 Hardware Description

The front of the ***EL-100-2MA*** switches is equipped with extensive displays, which provide information concerning the current status of the devices. In addition to USB data line connections and the RS232 line for configuration, there is also a reset button for resetting the device to the factory settings in case of an unknown IP address and a labeling field for entering the programmed IP address.

2.1 Front view

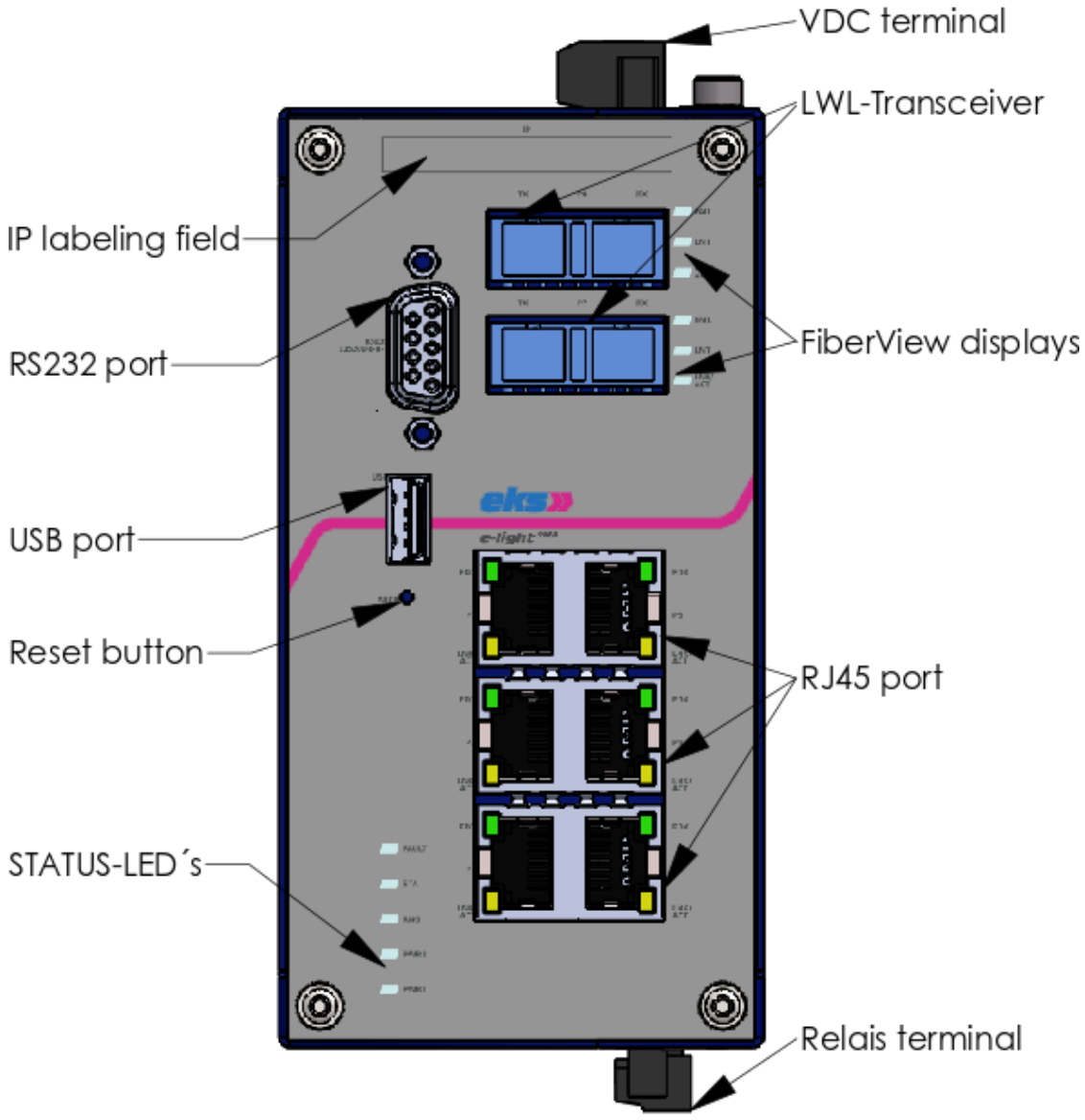


Figure 1: Front view of the *EL-100-2MA* switch with 2 LWL transceivers

2.2 Reset button

The reset button can be used to restart the switch or to reset the configuration to the initial value:

- **Restart:** Hold the button pressed down for 5 seconds and release it as soon as all LEDs light up. The switch is now restarted.
- **Reset to initial value:** Hold down the button for 10 seconds. The switch resets the complete configuration to the standard settings and signals this after shutting off all LEDs briefly.
- Config mode can be used to make certain settings (see chapter 3 Config mode)

2.3 DIP switches

Devices manufactured up to 31.07.2018 had a 9-pin DIP switch on the front, without function. From 01.08.2018 manufactured ***EL-100-2MA*** devices are delivered without DIP switches.

2.4 LED displays

The front panel of the switch features 5 diagnosis LEDs. Furthermore, each of the Ethernet ports features two status LEDs. Optical ports feature optical ports FiberView (5.5.4.FiberView). The LED displays offer real-time information regarding the status of the ***EL-100-2MA*** switch. For a detailed description, please refer to **Fehler! Verweisquelle konnte nicht gefunden werden.** below.

LED	Status	Meaning
VDC1	Green	The VDC1 connection possesses sufficient voltage (>= 12VDC)
	Off	The VDC1 connection does not possess sufficient voltage
VDC2	Green	The VDC2 connection possesses sufficient voltage (>= 12VDC)
	Off	The VDC2 connection does not possess sufficient voltage
Ring	Green	The switch is the manager in the MRP ring
	Off	The switch is not the manager in the MRP ring
Status	Geen	Profinet-AR-Status Online
	Off	Profinet-AR-Status Offline
Fault	Red	Configured alarm active
	Off	No alarm condition fulfilled

LED	Status	Meaning
LNK/ACT (Optischer Port)	Green	Connection available
	Blinking	Sending or receiving packets
	Off	No connection
LIMIT (Optischer Port)	Yellow	Low signal level
	Off	Sufficient signal level
Fail (Optischer Port)	Red	No connection
	Off	Connection available
FDX (Kupfer Port – RJ45)	Green	Full duplex mode
	Off	No connection (LNK/ACT off) or half-duplex (LNK/ACT on)
LNK/ACT (Kupfer Port – RJ45)	Yellow	Connection available
	Blinking	Sending or receiving packets
	Off	No connection available

Table 1: LED description

2.5 Ports

2.5.1 RJ-45 ports

The ***EL-100-2MA*** features four, six or eight RJ-45 ports, depending on the design, each with transfer rates of 10 mbps or 100 mbps. The ports detect the data rate automatically. Sending and receiving lines are crossed appropriately via MDI/MDI-X auto-crossover so that connections are able to be established with other devices, independent of the cable type used (1:1 or crossed).

2.5.2 Optical ports

The ***EL-100-2MA*** is equipped with up to four 100Base-FX ports, depending on the design. Depending on the variation ordered, the LWL ports may have ST- or SC- plug connectors and be suitable for different fiber types (multi-mode, single-mode).

Please make sure that the transceivers of the ***EL-100-2MA*** are always connected with transceivers of other devices that are suitable for the same wavelength and the same fiber type.

With the exception of Bidi transceivers, which cannot send and receive simultaneously via one fiber, the

transmitters of a device must always be connected with the receiver of the opposite device and vice-versa.

2.5.3 **Wiring**

- Use twisted-pair cable of category 5 or better to connect the RJ-45 ports. The electrical connection cable between the switch and the connection partner (switch, hub, workstation, etc.) may not be longer than 100 meters. Use metal shielded connectors on the cables.
- Connect the multi-mode transceiver with 50/125 µm or 62.5/125 µm multi-mode optical fiber cables.
- Connect the single-mode transceiver with 9/125 µm single-mode optical fiber cables.

2.5.4 **Voltage supply connection**

Connect the supply voltage to VDC1 and GND clamping terminals. The redundant supply voltage may now be connected to the VDC2 and GND clamping terminals. The terminal block for the voltage supply is clamping and can be locked using two screws. Both voltage inputs feature reverse voltage protection.

The permissible range for the input voltage is between 12 VDC and 60 VDC. The voltage must be SELV/LPS-conform voltage as per IEC 60950-1/EN60950-1/VDE0805-1. Please observe the instructions for SELV voltages according to the legal instructions at the beginning of this operating manual.

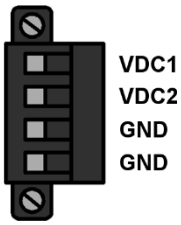


Figure 2: VDC connection terminal

Note: Please tighten the screws and check that all connections are stable.

Note: Please note the corresponding cable cross-section of at least 0.5 mm^2 or 12~ 24 AWG during wiring.

2.5.5 Failure relay connection

Clamping terminals K1/K2 and K3/K4 each feature two potential-free failure relay contacts. The relays act as alarm receivers and can be connected in the software with different alarm triggers. Depending on the configuration, they activate, for example, in case of a voltage failure, RJ45 port error or a LWL port error. In the software, the relay between K1 and K2 is marked relay 1, and the relay between K3 and K4 is marked relay 2.

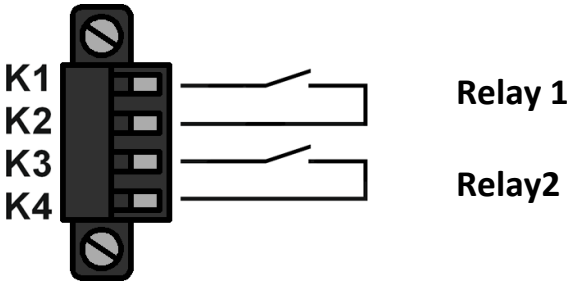


Figure 3: Relay terminal clamp

Note: The capacity of the relay contact amounts to 25 VDC (1A) of 60 VDC (0.3A).

2.6 Installation on DIN mounting rail

The ***EL-100-2MA*** switches are equipped with a fastener for 35 mm top-hat rails as per DIN EN 60175. To install the top-hat rails, snap the devices onto the top side of the rail (Figure 4 left) and then press downward against the spring force in the top-hat rail clip (1) and then into the assembly plate (2). The top-hat rail fastener locks via spring force (3) as depicted in the Figure 4 right.

To remove the device from the DIN rail, press the housing down (overcome the spring force of the DIN rail clip), then pull the device towards you and remove it from the mounting rail.

Optional to the top-hat rail fastener, a wall installation mount can be delivered. If the system is fastened with the wall installation mount, then the top-hat rail fastener must be removed first.

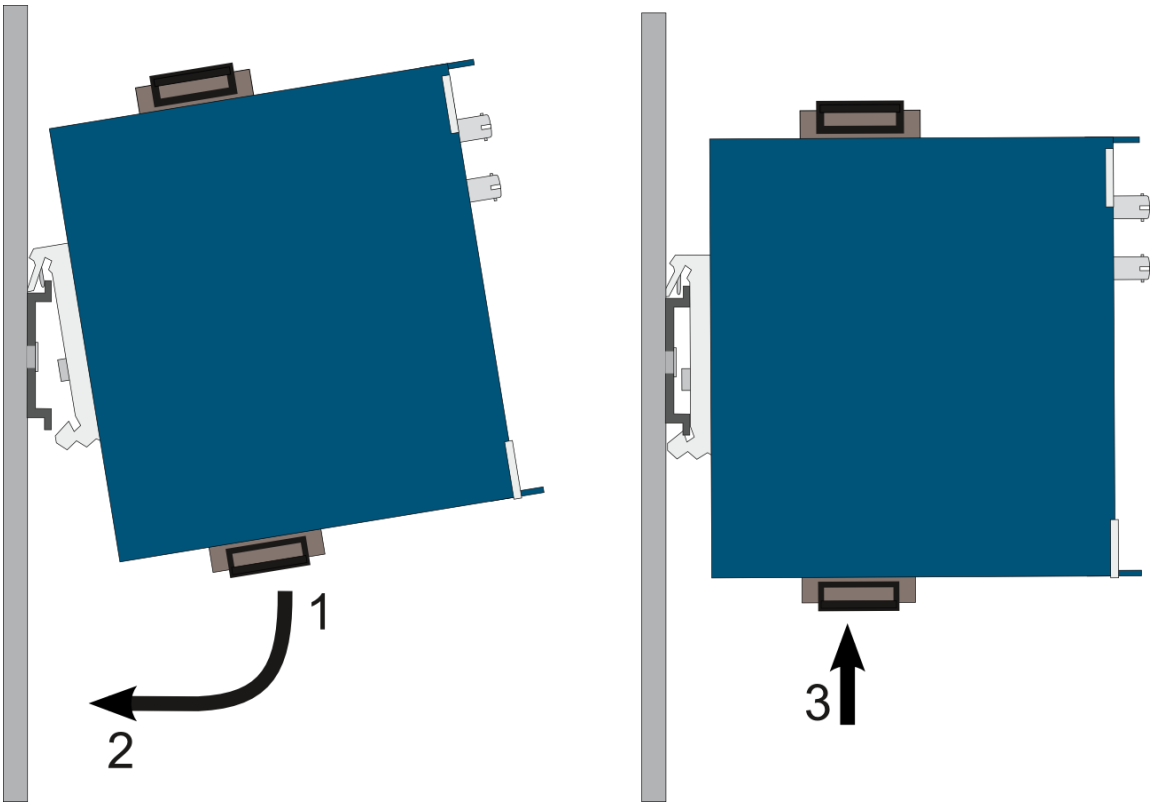


Figure 4: Installation on DIN mounting rail

Warning!

Do not mount ***EL-100-2MA*** switches directly beside devices that produce strong electromagnetic interference fields, e.g. transformers, contactors, frequency inverters, etc.

Warning!

Do not mount ***EL-100-2MA*** switches directly next to heat producing devices and protect the switch against direct sunlight in order to prevent unwanted heating.

Warning!

When operating in ambient temperatures above 50°C, the enclosure of the ***EL-100-2MA*** switches may heat above 70°C. Do not install the devices in areas that are accessible by unqualified personnel.

Warning!

When operating in ambient temperatures above 50°C, measurements must be taken to check how severely the plug connectors of the cables used heat up. Use of special cables that are suitable for ambient temperatures above 80°C may be required.

Note:

In case of use on ships, ***EL-100-2MA*** switches may not be fastened with the top-hat rail fastener on a 35 mm rail. The top-hat rail does not provide secure mounting. On ships, ***EL-100-2MA*** switches must be fastened using the wall installation mounting.

2.7 Dimensions

Figure 5 indicates the dimensions of the ***EL-100-2MA***.

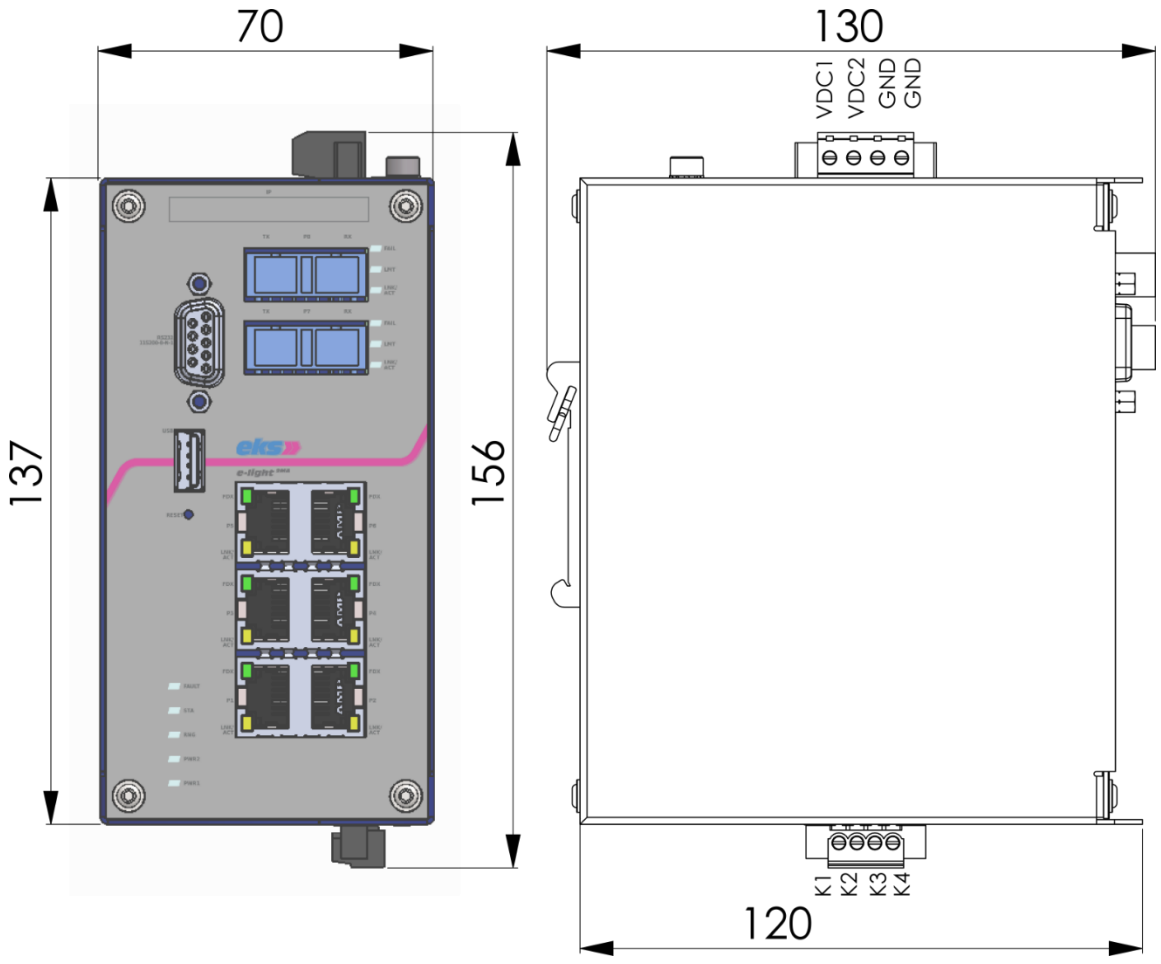


Figure 5: Dimensions of the *EL-100-2MA* switch

3 Config-Mode

By utilizing the reset button and status LEDs of the device, ***EL-100-2MA*** switches can be configured without having access to the Web interface using the Config-Mode.

3.1 Config-Mode usage

The Config-Mode is activated by tapping the Reset button 3 times within a 2 second time window. Once it active, the green Ring LED starts flashing.

To switch between the different available options the reset button has to be tapped again. With each tap the mode switches on until the last option is active. If the button is pressed again, the Config-Mode switches back to the first option.

To leave the Config-Mode the reset button has to be pressed for at least 3-4 seconds without being released (no LED is blinking).

Once the Config-Mode is exited, the selected option is executed.

The settings in Config Mode do not cause the connection to be interrupted. Communication between the connected devices continues undisturbed.

3.2 Config-Mode options

3.2.1 Overview

Falshing LEDs (Status LEDs)	Meaning
Ring	Leave without changes
Status	Activate default IP settings
Ring + Status	Delete IP settings
Fault	Block access to the Management interface
Ring + Fault	Allow access to the Management interface
Status + Fault	Disable Profinet functionality
Ring + Status + Fault	Enable Profinet functionality

Table 2: Overview Config-Mode options

3.2.2 **Leave without changes**

Upon activation of this option, Config-Mode is exited without performing any changes.

3.2.3 **Activate default IP settings**

Upon activation of this option the following changes will be made:

- The device's IP address is set to 192.168.10.1
- The device's subnet mask is set to 255.255.255.0
- The device's default gateway is set to 0.0.0.0
- The DHCP mode is deactivated

3.2.4 **Delete IP settings**

Upon activation of this option the following changes will be made:

- The device's IP address, subnet mask and default gateway are set to 0.0.0.0
- The DHCP mode is deactivated

3.2.5 **Block access to the Management interface**

Upon activation of this option the following changes will be made:

- The device's IP address, subnet mask and default gateway are set to 0.0.0.0
- The DHCP mode is deactivated
- All Profinet functionality is disabled

3.2.6 **Allow access to the Management interface**

Upon activation of this option the following changes will be made:

- The device's IP address is set to 192.168.10.1
- The device's subnet mask is set to 255.255.255.0
- The device's default gateway is set to 0.0.0.0
- All Profinet functionality is enabled

3.2.7 **Disable Profinet functionality**

Upon activation of this option all functionality regarding Profinet is disabled.

3.2.8 **Enable Profinet functionality**

Upon activation of this option all functionality regarding Profinet is disabled.

4 Network topologies/redundancy

The devices in the EL-100-2MA product family can be used with various protocols in addition to use in star-shaped switched-Ethernet networks and in redundant networks such as meshed networks or rings.

4.1 Star structure

Classic Ethernet star structures, see Figure 6, can be networked using devices in the ***EL-100-2MA*** product family without additional configuration. The devices are immediately ready to function.

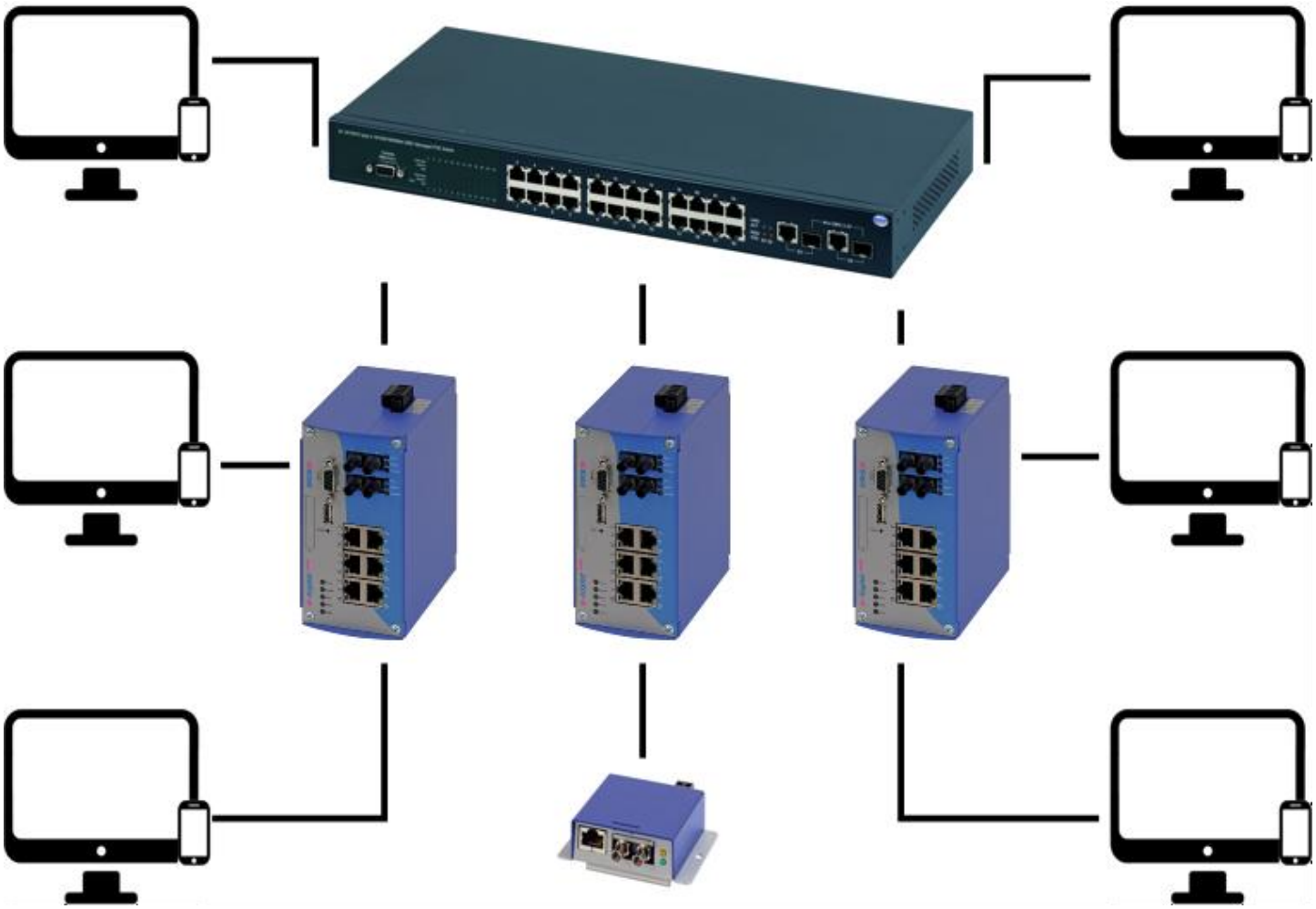


Figure 6: *EL-100-2MA* in a star-shaped network

4.2 Meshed networks

Use of the Rapid Spanning Tree protocol (RSTP) enables any Ethernet structures to be built, for example, as displayed in Figure 7. STP and RSTP break these structures up into a tree structure and reconfigure this tree structure in case of changes to the topology. The reconfiguration time is typically less than 1 s for Rapid Spanning Tree.

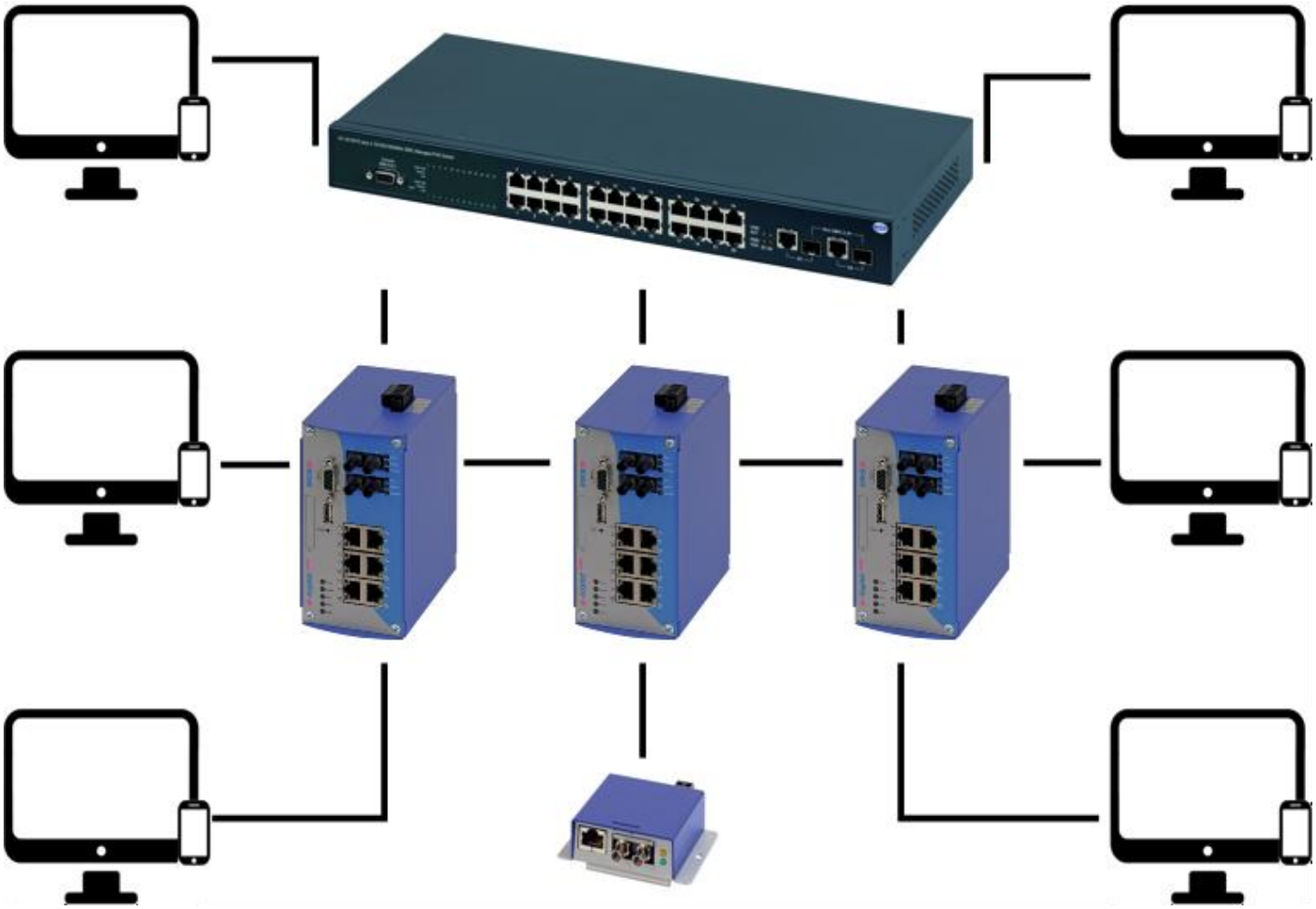


Figure 7: *EL-100-2MA* in a meshed network

4.3 Ring structure

The ***EL-100-2MA*** supports the Media Redundancy Protocol as per IEC 62439 (MRP ring), which enables the system to recover from network failures within 200 ms or less. The MRP ring increases the reliability of the network in this way. Figure 8 shows an example for use with ring functionality. The switch can be configured as Manager and Client.

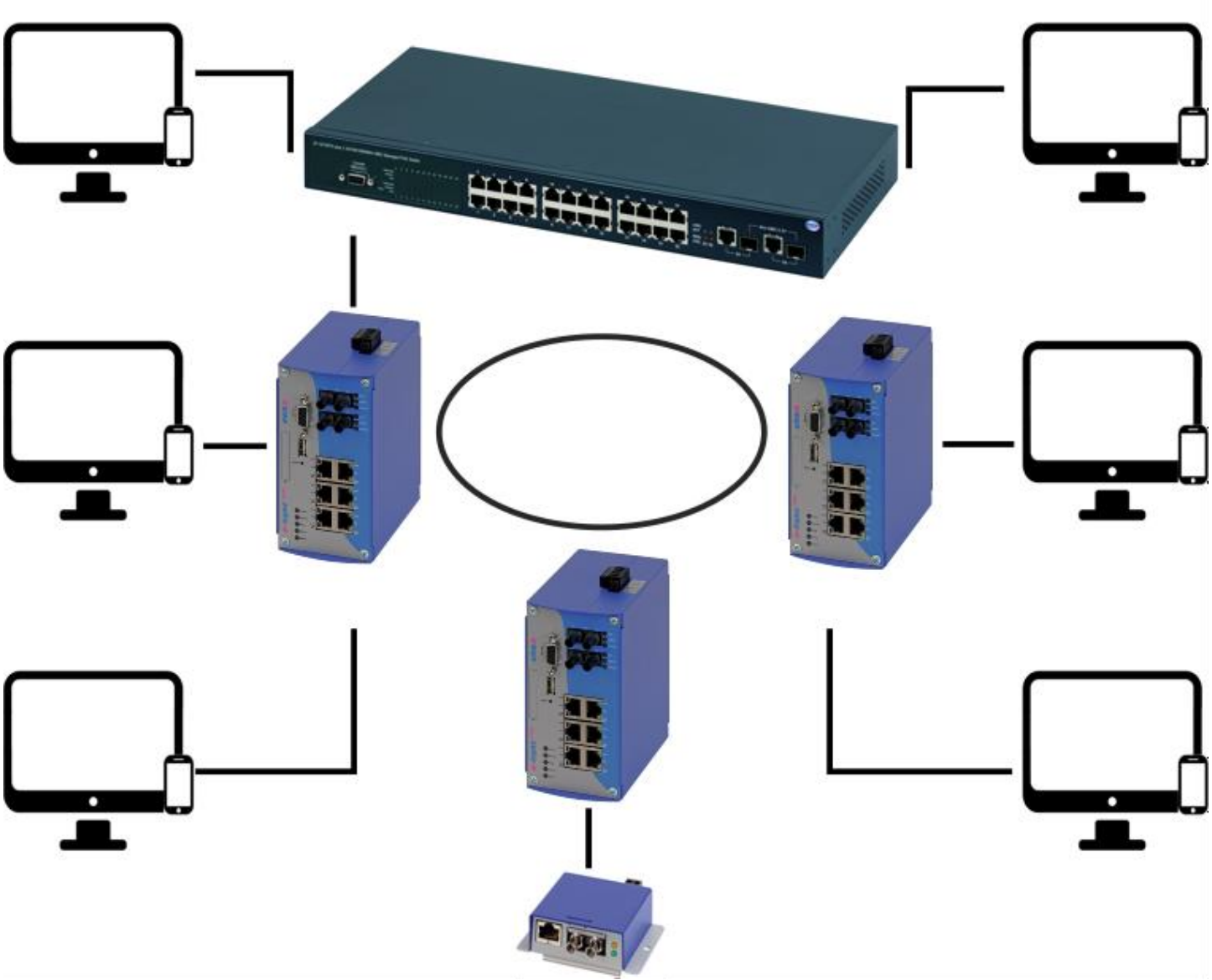


Figure 8: *EL-100-2MA* in a ring-shaped network

5 Web application

EL-100-2MA switches are equipped with a modern web interface so that they can be configured conveniently using any web browser.

5.1 Preparations

Before you use the web management feature, install the ***EL-100-2MA*** switch in the network and ensure that the PC intended for configuration of the switch is in the same subnet to be able to access the switch via the web browser. The device credentials set upon delivery are available here:

- User name: **admin**
- Password: **admin**

Alternatively to administrator access, guest access with fewer permissions and adjusted menu guidance is also available. The guest user does not have access to the switching and maintenance functions and their sub-items. The access data are:

- User name: **guest**
- Password: **guest**

Note:
Please change the passwords of the admin and guest users, before you use the device in your network.

With factory settings the device has the fixed IP-Address 192.168.10.1. In Profinet-Projects please set the IP-Address with the Automation Framework (e.g. TIA Portal). In non Profinet applications setup tools that are capable of setting Device-Names and IP-Addresses via DCP may be used (e.g. Profinet Commander)[1].

[1] https://profinetcommander.com/

5.2 System login

1. Start a web browser on your computer.
2. Enter the configured IP address of the ***EL-100-2MA*** switch used by you and then press the "**Enter**" key.
3. The login mask of the device now appears on the screen.

Figure 9: Login Window

4. Select the desired menu language.
5. Now enter the user name and password.
6. Press the "**Enter**" key or click "**Login**". You will now enter the web interface for the switch.

5.3 Web interface

The web interface of the ***EL-100-2MA*** comprises the menu bar on the left edge, the information bar in the top area, the actual configuration in the center, and the help on the right edge, see Figure 10.

5.3.1 Menu bar

The menu guide enables you to access the individual screens and complete settings there. The menu items displayed are divided into additional sub-items.

5.3.2 Information bar

The information bar shows you the device type, Profibus name, location, and the IP address. The current user is shown under the logout button on the right end of the bar. By pressing the button, you can log out and lock the webgui of the device. The help button shows instructions and explanations for the individual screens.

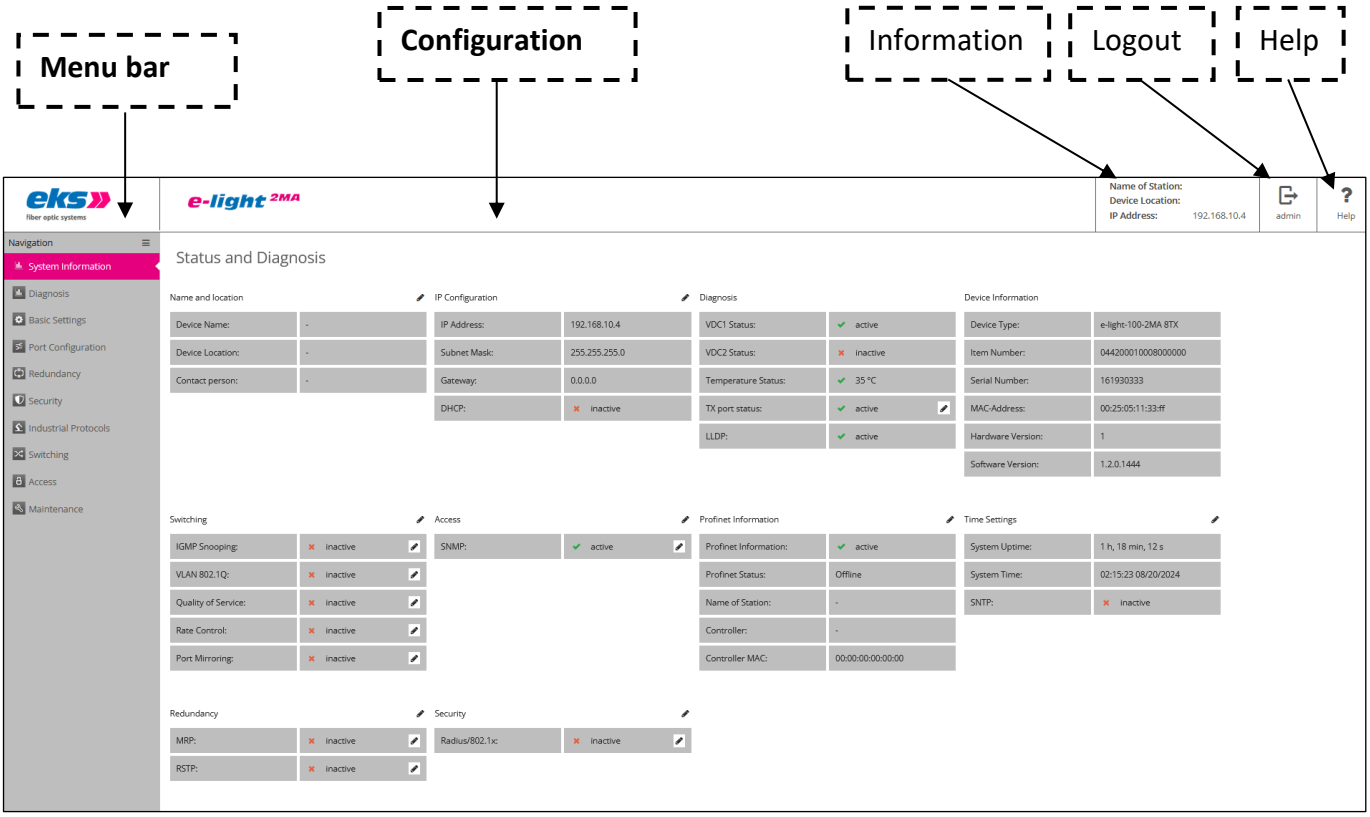


Figure 10: Status and diagnosis

5.4 System information

The "System Information" page provides a complete overview of the status and current configuration of the ***EL-100-2MA*** switch. In addition to the serial number and hardware and software versions of the device, you will find an overview of the enabled and disabled protocols and functions. Using the edit buttons, you can directly access the corresponding protocols and functions to make adjustments.

5.5 Diagnosis

The "Diagnostics" menu item is divided into several subpoints that provide comprehensive information about the status of the ***EL-100-2MA*** switch and its network environment. The individual subpoints will be

explained in more detail below.

5.5.1 **Alarms/Notifications**

The menu item alarms/notifications is used to define alarm triggers and alarm receivers. Alarm triggers indicate which alarms of the software should be observed. If alarms occur for which an alarm trigger is defined, then a log entry will be created and the Fail LED will be activated. In turn, alarm receivers connected with the alarm trigger are informed or activated. Alarm triggers include, for example:

- a status change at a port
- temperature that is too high or too low
- a supply voltage outage
- Media Redundancy Protocol Error
- Wrong Neighbor in Profinet-Projects

Alarm receivers are:

- two error relays
- SNMP traps
- E-mail addresses

Overview table

The configured alarm assignments are displayed in a table with a consecutive ID.

Individual columns in the table can be sorted using pull-down menus in the table headings. If you click on a table heading, a small up arrow 

appears to the right of it. If you click again, the arrow 

points downwards, allowing you to switch between sorting the entries in ascending or descending order. If the pull-down menu is clicked a third time, the arrow 

disappears again and the sorting corresponds to the chronological order in which the entries were created. (The columns are sorted either by number (ID) or alphabetically (alarm triggers and assigned alarm receiver). Only one column can be sorted at a time.

Figure 11: Overview Alarms and Notifications

With the help of the alarm trigger and alarm receiver screen tabs, the view can be switched between:

- Alarm trigger with assigned receiver
- Alarm receiver with assigned trigger

Add and edit alarm trigger

The alarm trigger screen tab (Figure 12) enables new alarms to be added by clicking the "+" button. If alarms are already present, then they can be edited or deleted using the button on the right in the table. When adding and editing alarms, the associated receiver can be selected in the lower part of the screen and linked to the alarm trigger in this way. The following alarm triggers are possible:

- The Ethernet ports can trigger an alarm in case of activity, inactivity, and status change.
- The optical ports may also report a weak signal in addition to activity, inactivity, and a status change.
- Alarms can be configured if an upper temperature limit is exceeded or if a lower temperature limit dropped below.
- The input voltages can be monitored individually. If one or both voltages are below 12 VDC, then an alarm can be triggered.
- MRP events (ring interruption, ring connected again, generic warning) may create an alarm.
- The device is connected to another device than configured in the Automation Portal. (Wrong Neighbor

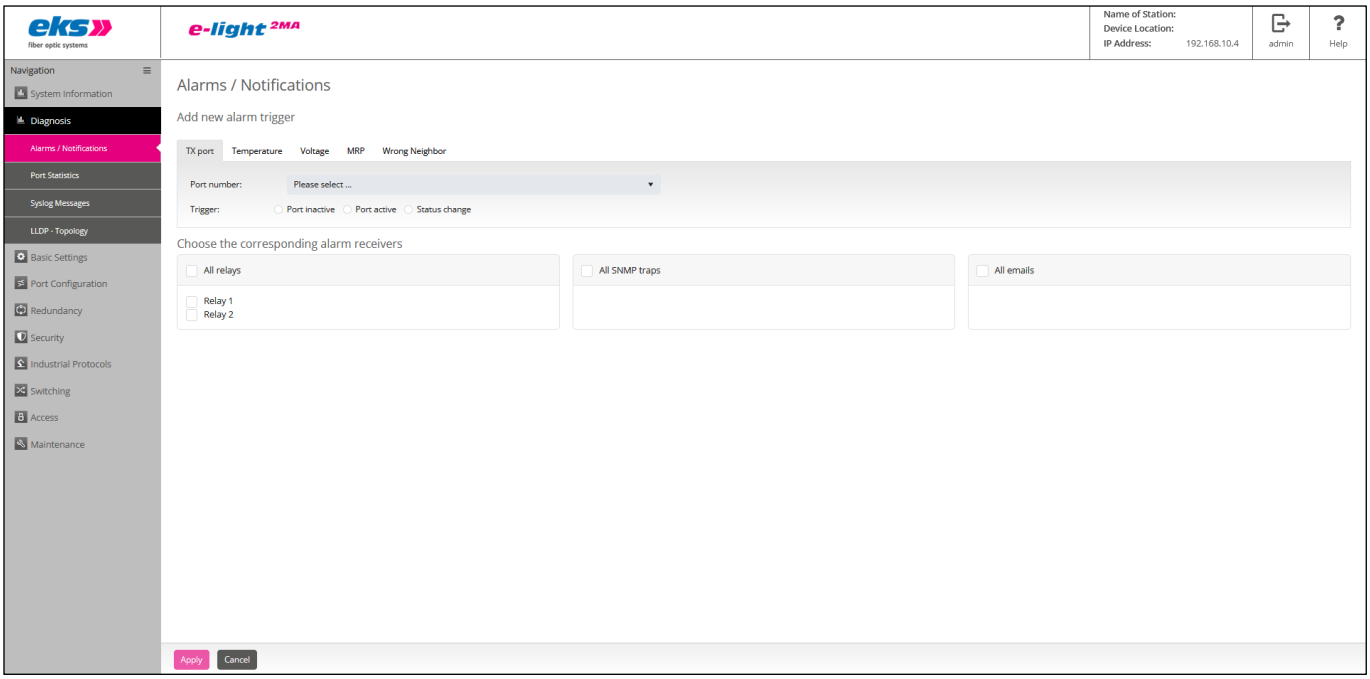


Figure 12: Alarms/notifications: Adding an alarm trigger

Add and edit alarm receiver

By clicking the "+" buttons below the alarm receiver screen tab (Figure 13), new receivers can be added. Both relays are already available as alarm receivers and may not be deleted, but rather only linked with alarm triggers. SNMP traps and e-mail in-boxes can be added as new alarm receivers.

- With the simple network management protocol (SNMP), the generated error messages of the device (which acts as agent) are sent to the management station which IP-address is specified in the field “Trap receiver IP”. The receiver will not send acknowledgement messages. So there is no guarantee that the trap receiver received the information. Furthermore you have to define a community string to ensure the communication between the management station and the agent. The settings will be confirmed by clicking the Create button.
- With the email notification, administrators can be notified about errors. Enter an email address and a SMTP-server IP (simple mail transfer protocol) to configure receivers. The device will send email messages if a configured alarm is triggered. If required set up authentication credentials according to your needs. For this you have to select the checkbox “Authentication needed:” and define a SMTP password. Optionally, the encryption can be activated by selecting the checkbox. Subsequently, the port and the type of encryption can be defined.

  The setting will be confirmed by clicking the Create button.

With the Button “Send test email” you can verify if the email setup works before the alarm receiver is created.

In the lower part of the screen, the alarm receivers can be assigned to previously added alarm triggers.

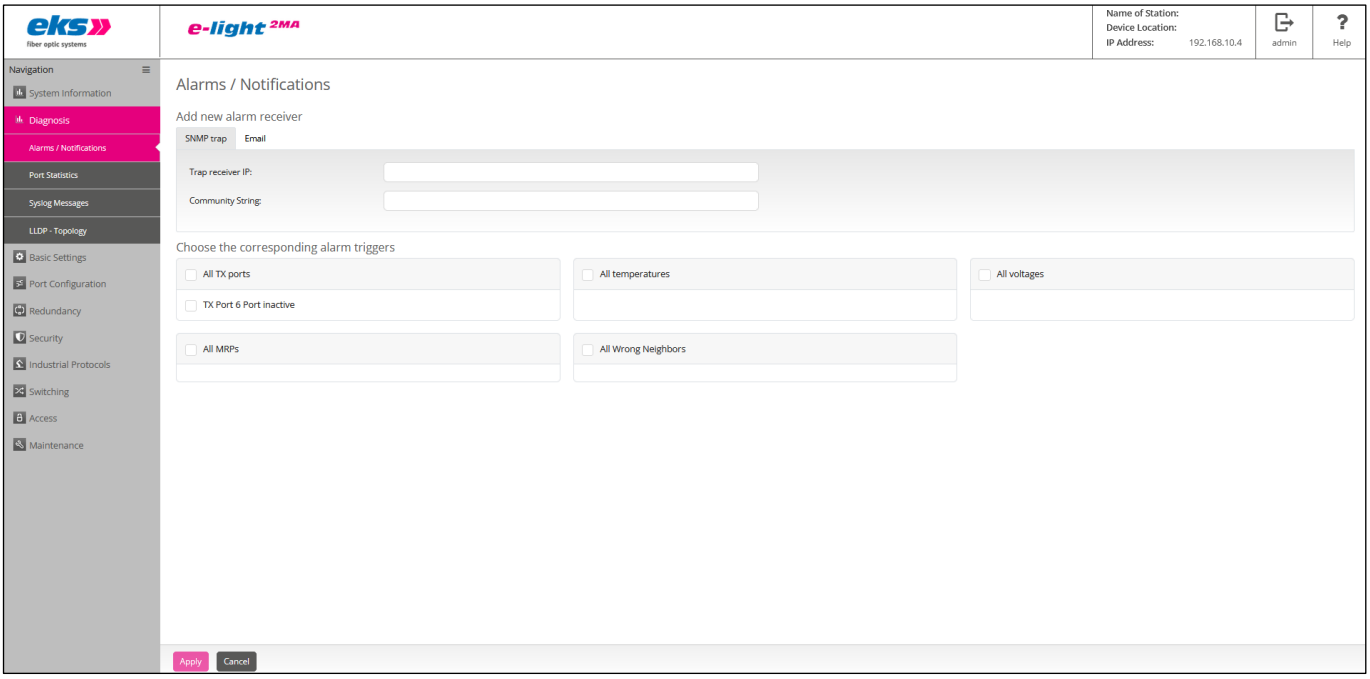


Figure 13: Adding an alarm receiver

5.5.2 Port statistics

The port statistics screen (Figure 14) provides information about the data traffic on the individual ports, which is helpful for diagnosis purposes in case of network problems. The complete number of sent, received, faulty, and colliding packets is displayed. Furthermore, the size of the individual packets is recorded statistically up to a variety of threshold values.

Sent packets are differentiated in terms of:

- Number of packets
- Number of Unicast packets (packets to one receiver)
- Number of non-Unicast packets (packets to multiple receivers)

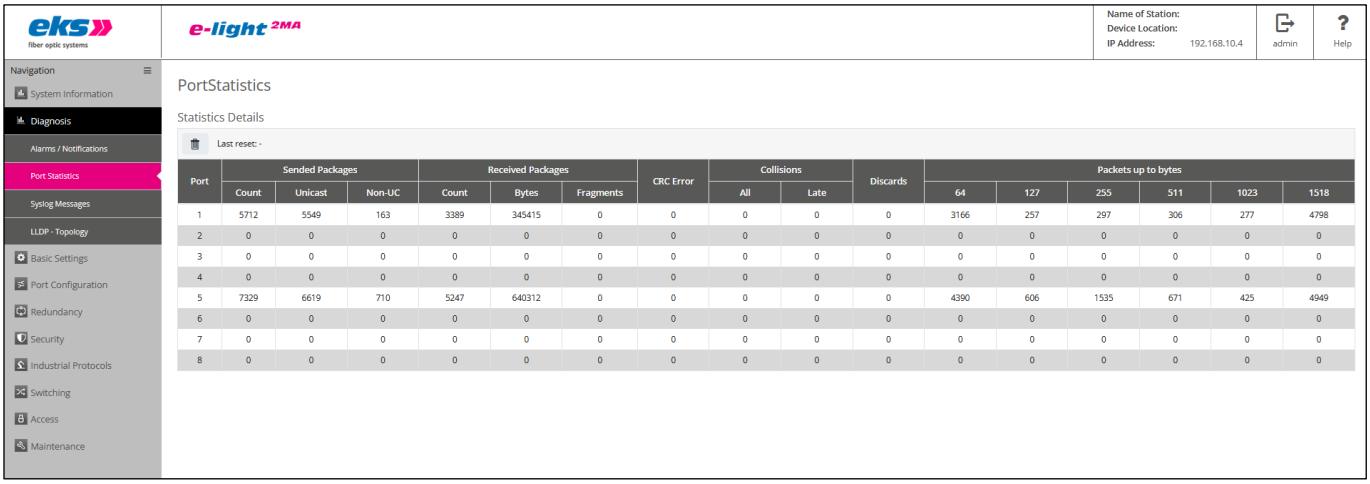
Received packets are differentiated in terms of:

- Number of all packets
- Total number of bytes received
- Total number of fragments received

The CRC errors column provides information about the number of faulty received data packets. The cyclical redundancy test, CRC (Cyclic Redundancy Check), specifies a test value using the transferred data. This value is sent together with the data and evaluated by the receiver. Fault packets are detected and discarded in this way.

The total number of all collisions and the late collisions are displayed in the collisions column.

The packets up to bytes column provides information about the number of packets in diverse sizes. In this case, the number of packets received up to 64, 127, 255, 511, 1023, or 1518 bytes in size is recorded.



Port	Sended Packages			Received Packages			CRC Error	Collisions		Discards	Packets up to bytes					
	Count	Unicast	Non-UC	Count	Bytes	Fragments		All	Late		64	127	255	511	1023	1518
1	5712	5549	163	3389	345415	0	0	0	0	0	3166	257	297	306	277	4798
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	7329	6619	710	5247	640312	0	0	0	0	0	4390	606	1535	671	425	4949
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 14: Port statistics

Reset the values

In the status bar above the table, a button can be used to reset the counters of all ports and thus start a new evaluation. The time at which the new evaluation was started is displayed in the status bar as the last reset.

5.5.3 Syslog messages

The Syslog messages (Figure 15) provide the user help for receiving status and error messages about the various functions and protocols. The messages are displayed in the overview including the date and time, plus a code, a description, and a reference. Because the log entries are not saved in the device, they are no longer available after the device is restarted or if the voltage is interrupted. In order to archive the messages permanently, the option is available to use an external Syslog server or USB flash drive.

Using the Syslog server

In order to archive the messages on a Syslog server or to save them, activate this function via the selection field in the top bar. Enter the IP address of the Syslog server in decimal points and save the settings using the apply button that appears below. Please check if the server is able to be reached and if the messages are being saved in a file.

Syslog to USB flash drive

To archive and save messages on a sub flash drive, connect an usb-device with the usb-port of the ***EL-100-2MA*** device and activate this function. After that save the settings with the apply button. Please check that there is enough memory free on the usb-device and if it saves the messages in a file.

- To use this functionality, USB access must be enabled under section 5.12 Access.

Export and reset the entries

The following buttons are available for this:

- The CSV export button creates a CSV file (Comma-Separated Values) including all entries from the table and saves these in the download folder of the browser. The messages are written in a file separated into rows by a comma.
- The button for deleting the log file removes all entries from the table. After that all messages that occurred after this time are shown. The time that the entries were deleted is visible via the first log entry that appears.

Search for Entries

With the search bar, you can specifically search for certain entries in the list of Syslog messages. This is

particularly useful when the list is extensive, allowing you to determine if a specific event has occurred, how often it happened, or which events were recorded on a particular day. The search can be applied to all columns of the table (Date, Code, Description, and Reference). Only entries that match your search query will be displayed, and the search is case-insensitive. To view all entries again, you need to clear the search bar.

Sort Entries

Individual columns of the Syslog messages can be sorted using dropdown menus in the table headers. For example, clicking on the "Date" header will display a small arrow pointing up next to it; a second click will change the arrow to point down, allowing you to toggle between ascending and descending sorting of the entries.

In the "Date" column, sorting is done chronologically, while the "Code" column is sorted based on ascending or descending error codes, with only the first digit being relevant. The "Description" and "Reference" columns are sorted alphabetically, based on the initial letter.

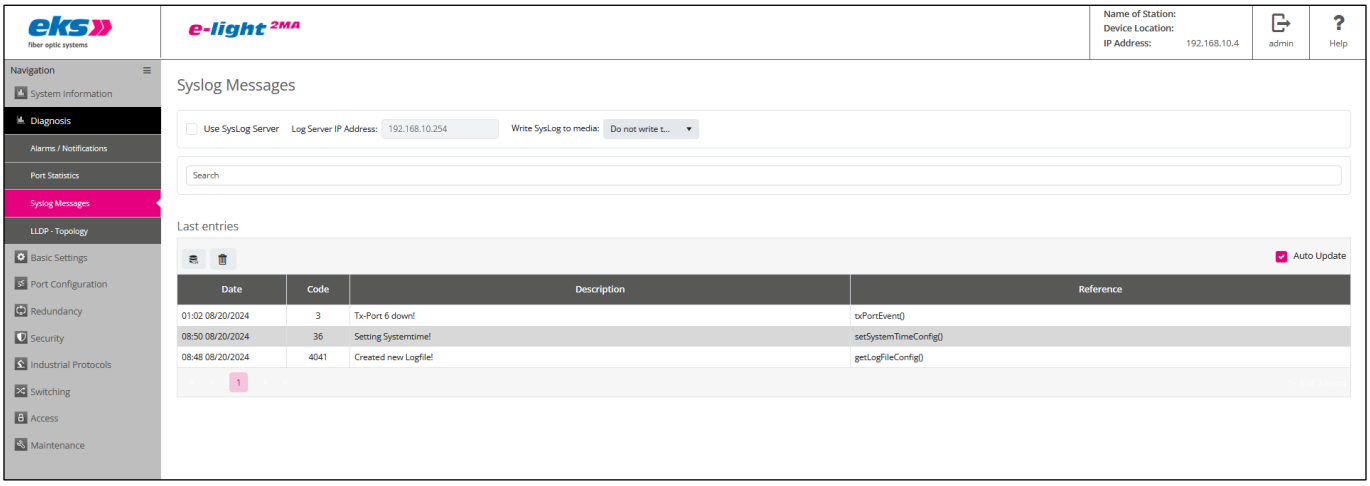


Figure 15: Syslog messages

5.5.4 FiberView

FiberView is a status display for optical ports. The three colors that are arranged as a traffic light, i.e. green, yellow, and red, intuitively indicate if the received light output is sufficient or if 3 dB reserve are available up to the sensitivity threshold.

The FiberView menu (Figure 16) also indicates the names assigned in the port configuration to make the diagnosis easier.

FiberView differentiates between the following conditions:

- Green: The path is intact and the receiver is receiving a good signal level.
- Green/yellow: The signal level in the fiber is close to the threshold value. The green LED indicates that the communication remains possible via the path. Nevertheless, checking the path is recommended.
- Red: The connection at this port is interrupted.

Figure 16: FiberView

In order to detect FiberView status messages immediately at this port as well, the states are displayed directly next to the ports using colored LEDs. This allows quick identification of the current status of the optical fiber cable connections.

Note: Light output as required for Profinet including specification of the received power in dB is not supported. Threshold values that deviate from the 3 dB system reserve may therefore not be specified.

5.5.5 Link Layer Discovery protocol – topology

The Link Layer Discovery protocol (Figure 17) is a manufacturer-independent Layer-2 protocol, which is defined as per the IEEE-802.1AB[1] standard and offers the option to exchange information between neighboring devices. On every device that supports the LLDP, a software component operates as the so-called LLDP agent. This sends information in periodic intervals concerning the actual status and receives

information from neighboring devices permanently. Because this occurs independently of each other, the LLDP is also referred to as a one-way protocol. Before sending the information, no connection to the other devices is established.

The following information is compiled by the LLDP and sent:

- System name
- System description
- Port description
- Chassis ID
- IP-Address

System name, System description and Port description are set according to the values given in SNMP-MIB2. These values are read-only. The Chassis ID is the assigned Profinet device Name. In case no device name is assigned the MAC-Address is transmitted. The IP-Address is automatically set to the current device IP

LLDP interval

The LLDP interval parameter can be used to specify the time intervals (in seconds) in which the device sends its own LLDP telegram to the neighboring devices.

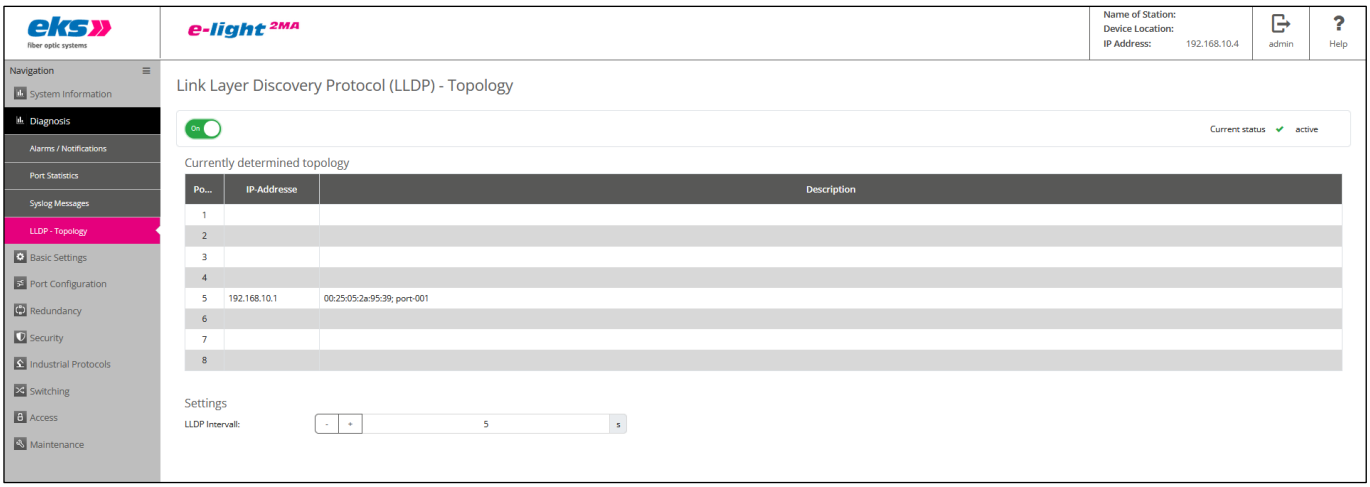


Figure 17: Link Layer Discovery protocol (LLDP)

- On / Off switch: The LLDP can be switched on or off using the switch.

- Save settings: The settings can be saved by clicking on the "Apply" button under the LLDP interval setting. If the Cancel button is clicked, the new settings are discarded. Both buttons are only visible when a setting on the page has been changed.

5.6 Basic settings

The basic settings screen (Figure 18) offers you the option to assign the device a clear name, a location, and a contact partner.

- Device name: Assign the ***EL-100-2MA*** a name to clearly identify the device.
- Location: The location provides you an additional option for identifying the device.
- Contact partner: A contact partner responsible for the device can be saved in the third field.

The input fields are configured so that up to 50 characters can be used. At least one character has to be set. The use of special characters is possible. The location is displayed in the information bar in the above right and helps you to assign the web interface to a device.

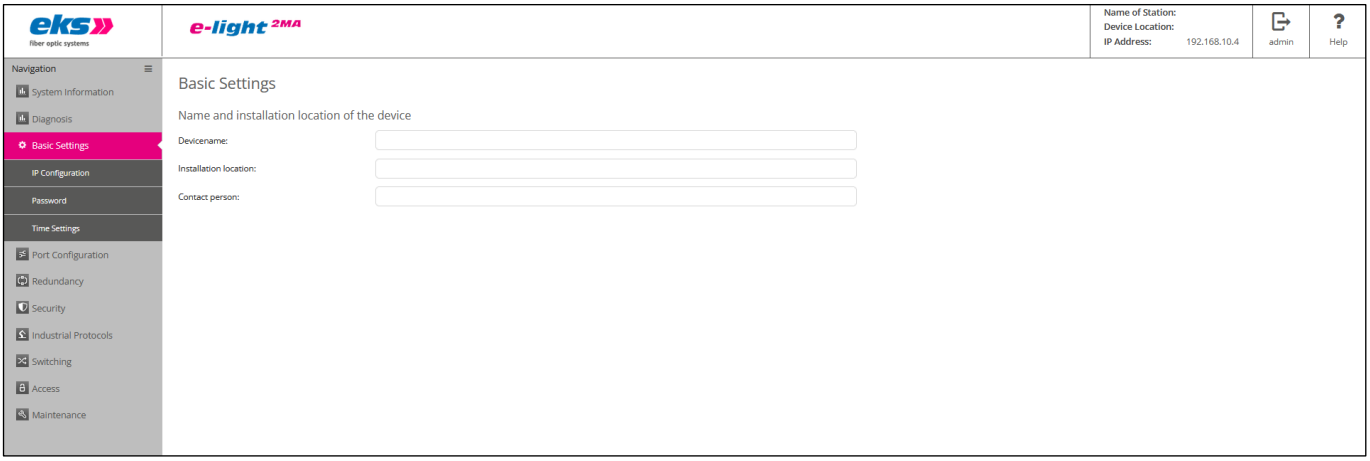


Figure 18: The basic settings of the *EL-100-2MA*

5.6.1 IP configuration

You can either execute the IP configuration (Figure 19) automatically with the help of the Dynamic Host Configuration Protocol (DHCP) or adjust the settings manually.

Automatic

In order to receive a configuration for the IP-Address, the subnet mask and the standard gateway from a

server working in the network with the corresponding functionality, activate the DHCP client function. After you have saved the settings by clicking the apply button, the device sends a query to the network and accepts the configuration received by the DHCP server. Because the device has now received a new IP address, it is no longer able to be reached via the previously configured IP. Please contact your network administrator to receive a new IP address.

Manual

If your network does not possess a DHCP or BootP server, or if the settings should be made by hand, then select the manual IP configuration via the top area of the screen. Please check exactly which settings you change so that problems involving duplicate IP addresses do not result, since these could have a negative influence on the entire network. The format of the IP address, the subnet mask, and the gateway must be entered in decimal point format. The following settings are required:

Figure 19: Changes to the IP configuration

- IP address: Please note that the set IP address must be able to be reached from your PC so that you can connect again with the device in order to make additional settings.
- Subnet mask: Enter the subnet mask IP address; this separates the IP address into a network component and a device component. This specifies which IP addresses are able to be reached in the network and which addresses are located in other subnets and only accessible via routers.
- Gateway: Specify the standard gateway of switches. The gateway is used to communicate with devices outside of the subnet.

PROFINET-DCP

If you configure the device in a profinet project the IP-Address is set with the DCP-Protocol by the Profinet-Controller depending on the device name. If the device has an active connection to a Profinet-Controller it is not possible to set the IP-Address in the Webinterface.

5.6.2 Password

On the password screen (Figure 20), the pre-set standard password for administrator and guest user can be changed. The current or former password must be known and entered. The user names and rights of the administrator and guest are specified permanently and cannot be changed.

Figure 20: Change the password for administrator and guest access

The following form fields are available:

- New password: Please enter the password specified by you in this field for the previously selected user. Please also note the instructions for providing passwords in the section below.
- Confirm the password: To ensure that you have entered your password correctly, repeat the input in this field.
- Current password: Please enter the password used up until now, which should now be changed.

Instructions concerning passwords: The safety of your system depends significantly on the security of your passwords. For passwords, we therefore generally recommend:

- Do not use dictionary entries
- Please use passwords that are as complex as possible
- Combine letters, numbers, and special characters
- Use lower case and capital letters
- Your password should consist of at least eight characters
- Do not write down the passwords

5.6.3 Time setting

The status bar in the top area of the screen for setting the time (Figure 21 / Figure 22) displays the system time and the date. The device running time is featured in the center. The far right features the currently applied settings for the time zone.

When setting the date and time, select between the use of a time server and manual configuration. The automatic configuration of the system time via Simple Network Time protocol (SNTP) has the advantage that the time setting is updated in regular intervals. An exact system time is especially sensible if the log file should be evaluated in case of a fault.

Set system time automatically via SNTP

In order to set the system time via SNTP, a connection to an SNTP server on the Internet is required. The following settings are required when using SNTP:

- SNTP server IP address: Enter the IP address of a time server that can be reached on the Internet or locally. Please use the decimal point format.
- SNTP server IP address (redundancy): In this field, you may enter the IP address of a second, redundant time server. If the first server is not able to be reached, then the time will be synchronized via this SNTP server.
- Update interval: Please enter the time intervals at which the device should synchronize with the time server here. In this case, note that the system time may possibly deviate severely from the real time in case of large time spans.

- Time zone: Please enter the time zone where the device is located.

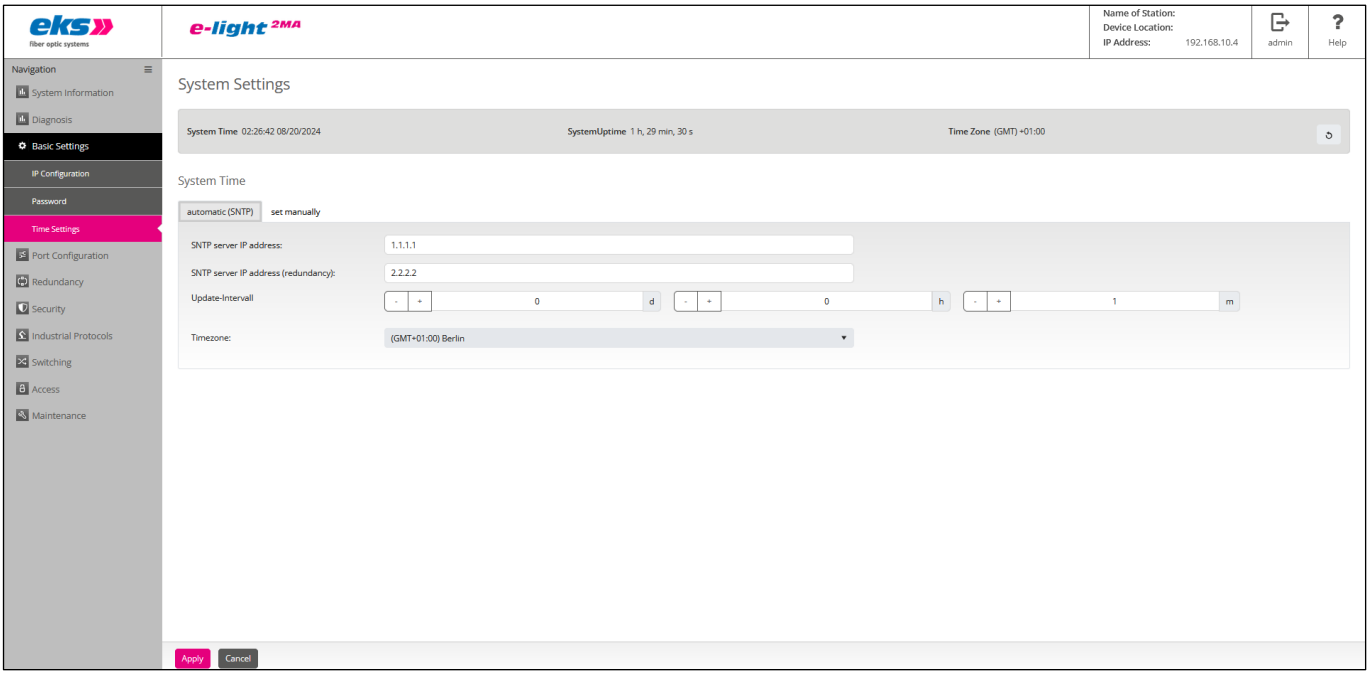


Figure 21: Automatically time settings configuration (SNTP)

Set the system time by hand

If the system time is set by hand, then you have the option of using the browser time or entering the time and the date by hand and saving this.

To use the browser time, press the use browser time button, check the correct time/date, save the correct date/time and save the values with the apply button.

If you want to make the settings manually, first select the current date using the input field. You can also enter the date using the keyboard, first two digits for the month, then two for the day and finally two or four digits for the year. Alternatively, you can use the small calendar button next to the input field and set the date and time graphically with a mouse click. Enter the time and the corresponding time zone. Save the settings using the Apply button and check that everything has been applied correctly.

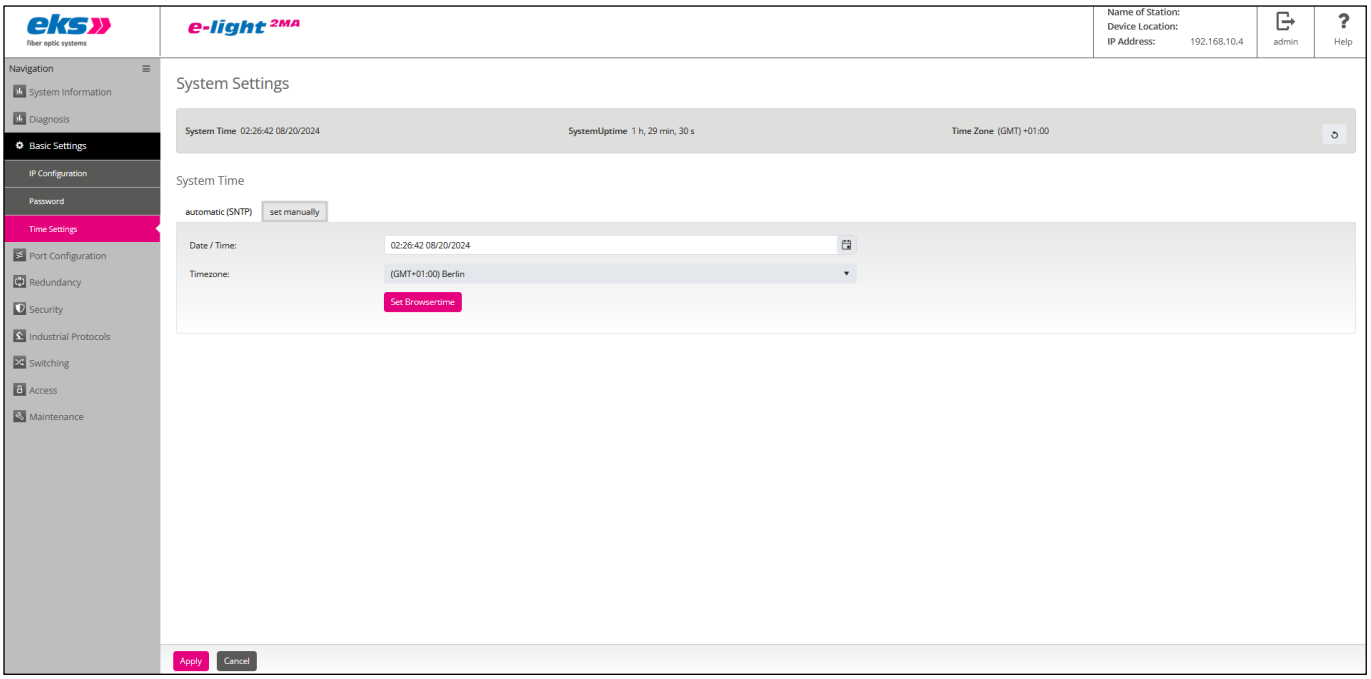


Figure 22: Manually time settings configuration

5.7 Port configuration

The table for the port configuration (Figure 23) provides an overview of the current configuration of the individual ports. The columns Activated, Auto Negotiation, Flow Control, and Designation may also be configured. The remaining fields are partially changed by configuring the ports and updated by reloading the screen, or they provide an improved overview.

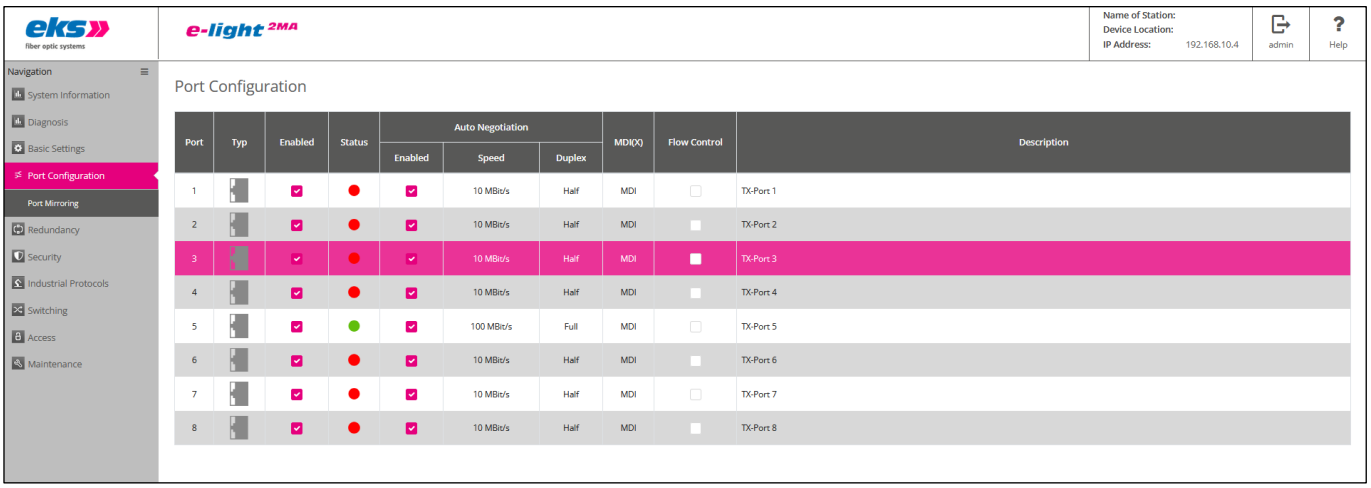


Figure 23: Overview of the port configuration table

The following columns are displayed:

- Port: Indicates the port number, which is also labeled on the enclosure (P1 to P8).
- Type: Indicates via the help symbol if the port is an RJ45 port or an optical port.
- Activated: The individual ports can be activated or deactivated here. This specifies whether a port is able to be used or not.
- Status: Status signals the current status of the ports:
  - Green: The port is activated and a connection is present.
  - Red: The port is activated, but there is no connection.
  - Grey: The port is deactivated. A connection is not possible.
  - Green/yellow: The LWL port is active and a connection is present. The path should be checked.
- Auto Negotiation: If this function is activated, the configuration of transfer speed and duplex mode via the ***EL-100-2MA*** and the connected recipient will take place automatically. If Auto Negotiation is deactivated, then the settings can be set manually, and the communicating devices must work with these settings:
  - Speed: The data rate of the ports can be assigned permanently. The option of setting a data rate 10 mbps or 100 mbps is possible.
  - Duplex: Duplex modus can be switched between half and full duplex. This setting is therefore specified permanently for a connection.

Note: If both link partners use Auto Negotiation, then it cannot be guaranteed that the link partners will settle on 100 mbps full duplex. There will also be a duplex mismatch with output impairment if one link partner uses Auto Negotiation and the other is set permanently to 100 mbps. We recommend setting link partners permanently to one speed and one duplex mode.

- MDI(X): The ***EL-100-2MA*** switch may complete an auto-crossover by default. This means that the switch independently recognizes whether a subscriber is connected via a crossed or uncrossed cable.
- Flow control: The flow control ensures that overloading at a port signals to the opposite subscriber that it should send slower. If QoS (Quality of Service) is used, then the flow control should be deactivated.
- Designation: You can give the ports a name in this column. The names are often displayed during configuration and facilitate selection of the correct settings and diagnosis in case of an error. The port

designations can be edited directly in the row where they are displayed.

5.7.1 Port Mirroring

Port Mirroring (Figure 24) is a method for mirroring the data traffic of a port in a network (source) on a second port (target) in order to analyze it. Either only sent or sent and received packets are able to be mirrored. The following settings can be made:

- Port and port name: All of the ports are displayed here in order to select a target and one or multiple source ports.
- Target port: If port mirroring is active, then the port can be selected here to which the data should be duplicated.
- The source port indicates from which ports sent (TX) or sent and received (TX and RX) data packets should be forwarded to the target port.

After you have set the respective parameters, click the apply button to save and apply the settings.

Note:

Deactivate port mirroring in normal mode and only apply it for problem analysis.

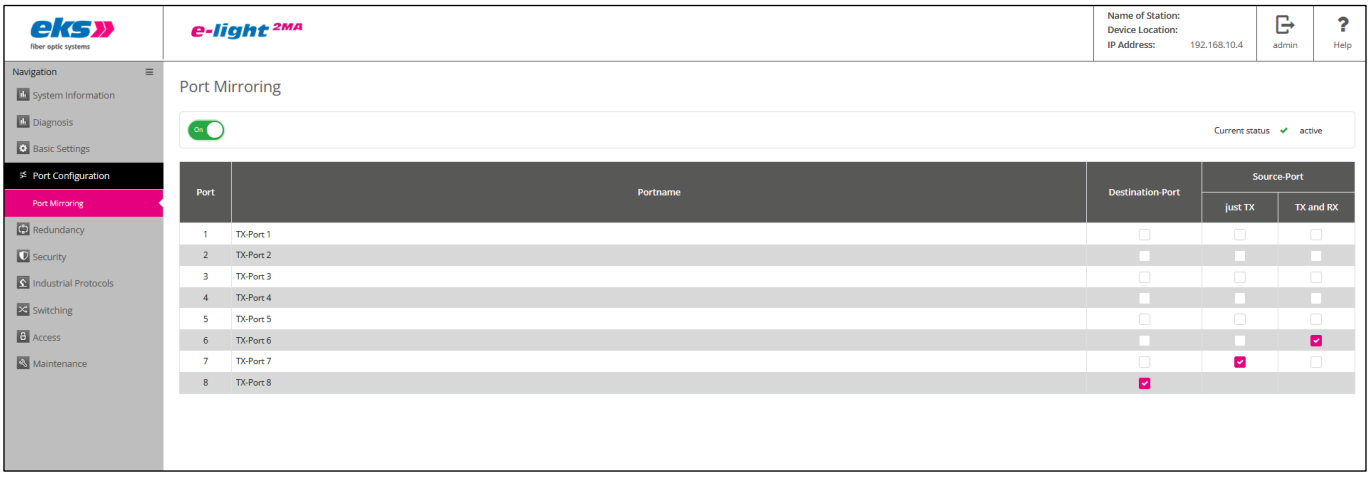


Figure 24: Port Mirroring

5.8 Redundancy

The Redundancy page provides you with an overview of the available redundancy protocols and their

status. It is not possible to activate several redundancy protocols at the same time, so only one can have the status active. If one of the two protocols is active, you will receive the following message on the configuration page of the other: “To enable RSTP you have to disable MRP first” and you will not be able to make any settings on this page.

The edit button can be used to access the protocols, where the configuration can be made.

Figure 25: Menu Redundancy

The following protocols are available:

- MRP: Media Redundancy Protocol
- RSTP: Rapid Spanning Tree Protocol

Use of the redundancy protocols guarantees your network increased failure security and availability in case of faults.

5.8.1 Media Redundancy Protocol (MRP)

The Media Redundancy Protocol (Figure 26) is a ring protocol for highly available networks. The MRP switches form a ring via the two respective dedicated ports. Exactly one switch in the ring is configured as a redundancy manager. This redundancy manager uses special test packets to test the flow capacity of the ring and completes a redundant connection if the ring is interrupted by a fault.

The guaranteed reconfiguration time for up to 50 devices in the ring amounts to 200 ms. In a typical application, the reconfiguration time normally amounts to less than 50 ms.

Attention! The ring may only physically be completed if MRP is configured completely.

Ring configuration

The following settings are required for MRP:

- First ring port: Please select a port that should work as the primary ring port.
- Second ring port: Specify a second port that should work as the secondary ring port. Please note that the secondary ring port cannot simultaneously function as the primary ring port.
- Ring Settings: Please specify whether the ***EL-100-2MA*** should act as manager or client. Please note that only one manager can be used for each ring.

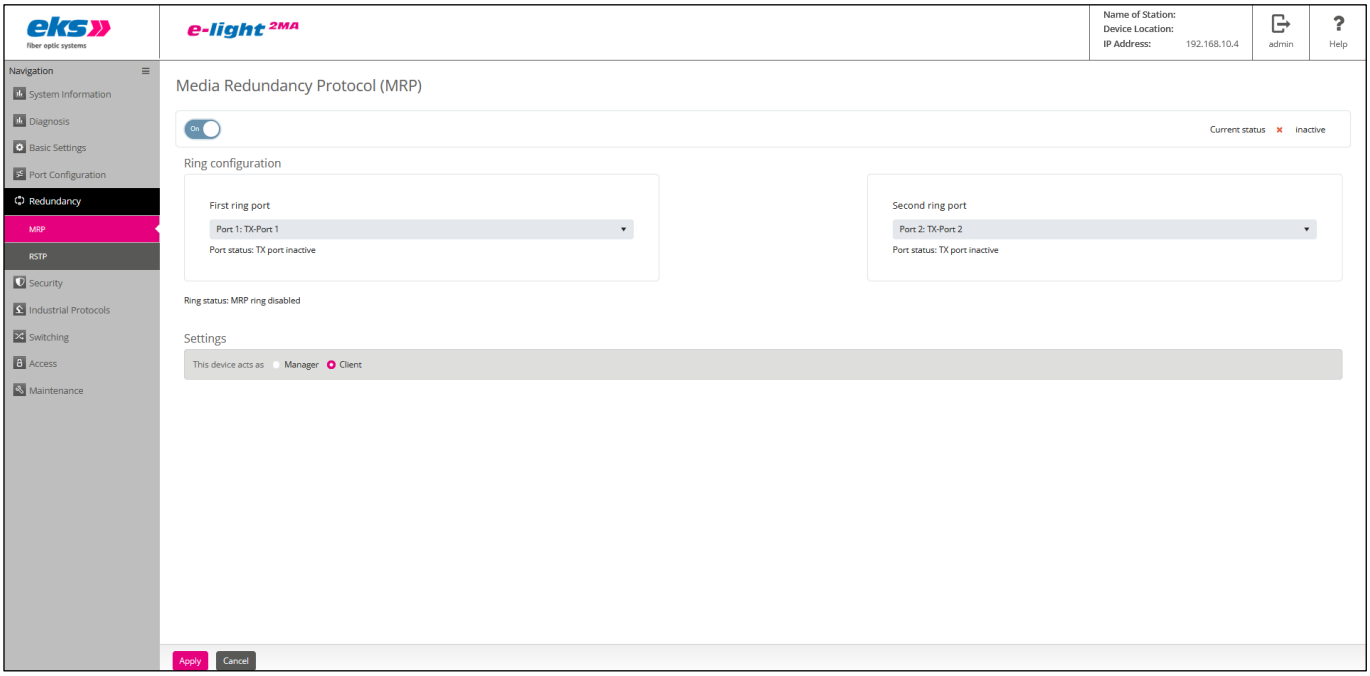


Figure 26: Media Redundancy protocol (MRP)

5.8.2 Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) (Figure 27 / Figure 28) is a standardized method that can be used to establish network structures including a ring. The protocol breaks the network into a logical tree and deactivates redundant paths or activates them as required. The first step is to select a root bridge, which depicts the root of the tree to be created. Starting from the root bridge, the path to all of the other bridges in the network is specified. The paths that can be used for communication are detected via the path costs to the individual bridges.

Device settings

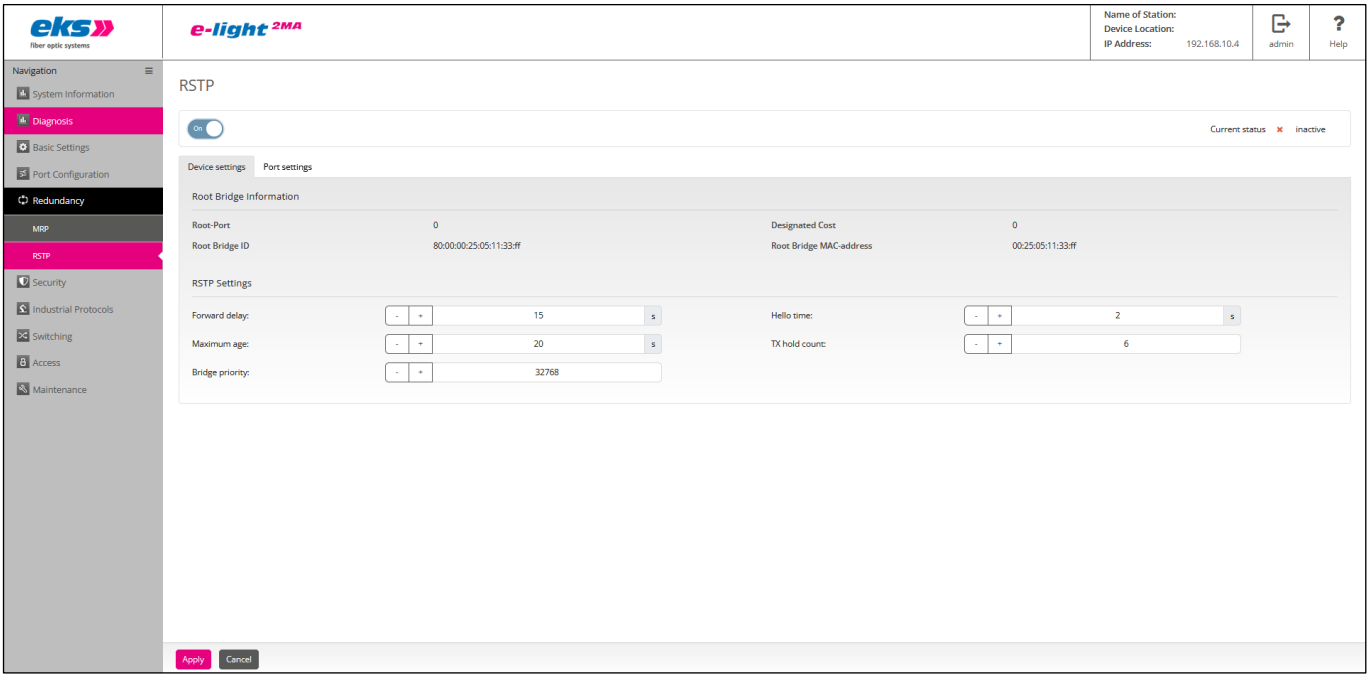


Figure 27: Rapid Spanning Tree Protocol – device settings

Root Bridge Information

The following parameters are displayed in this field:

- Root port: Shows which port works as the root port, i.e. the connection with the lowest path costs to the root bridge.
- Root bridge ID: The bridge ID is a combination of bridge priority and MAC address of a bridge. The bridge with the lowest bridge ID is selected as the root bridge. The Root bridge ID is the bridge ID of the selected root bridge.
- Designated cost: Path costs for root bridge
- Root bridge MAC address: Displays the MAC address of the root bridge.

RSTP settings

In order to discover the RSTP tree, every port of the switch completes a process involving the port states before the ports transfer useful data. The time span that the ports remain in the individual states is specified by timers. Under RSTP settings, the following can be adjusted:

- Forward Delay: The waiting time before a port switches from the status Learning/Listening (still no

transfer of useful data) to Forwarding (transfer of useful data). A time between 4 s and 30 s can be entered. The basic setting features a forward delay of 15 s.

- Maximum Age: The time that a bridge waits before attempting a new configuration if it does not receive messages from the Spanning Tree configuration protocol. A time between 6 s and 40 s can be entered. In the basic setting, the Maximum Age amounts to 20 seconds.
- Bridge Priority: This value is used to specify the root bridge. The bridge with the lowest value selected as the root bridge. The value must be between 0 and 61440 and a multiple of 4096. Changes to this value require a switch restart.
- Hello Time: The time in which the switch sends a BPDU packet (Bridge Protocol Data Unit) to check the current status of the RSTP. A time between 1 s and 10 s can be entered. The basic setting for the Hello Time is 2 s.
- TX Hold Count: The maximum number of hello packets of an interval transferred. Between 1 and 10 packets can be selected. In the basic setting, the TX Hold Count amounts to 3.

Note: Observe the following rules to configure the forward delay, maximum age, and hello time:

2 * (Forward Delay Time - 1) >= Maximum age >= 2 * (Hello Time + 1).

Recommended approach: Select a value for the "Hello Time" and calculate using the formula 2*(Hello Time + 1) according to the rule indicated above to determine the lower limit for the Maximum Age. Select a value for the "Forward Delay Time" and calculate using the formula 2*(Forward Delay Time - 1) according to the rule indicated above to determine the upper limit for the Maximum Age. Select a maximum age between 6 and 40 seconds between the calculated limits.

After clicking apply, the RSTP protocol reconfigures itself and indicates any possibly changed root bridge parameters in the top part of the screen.

Port settings

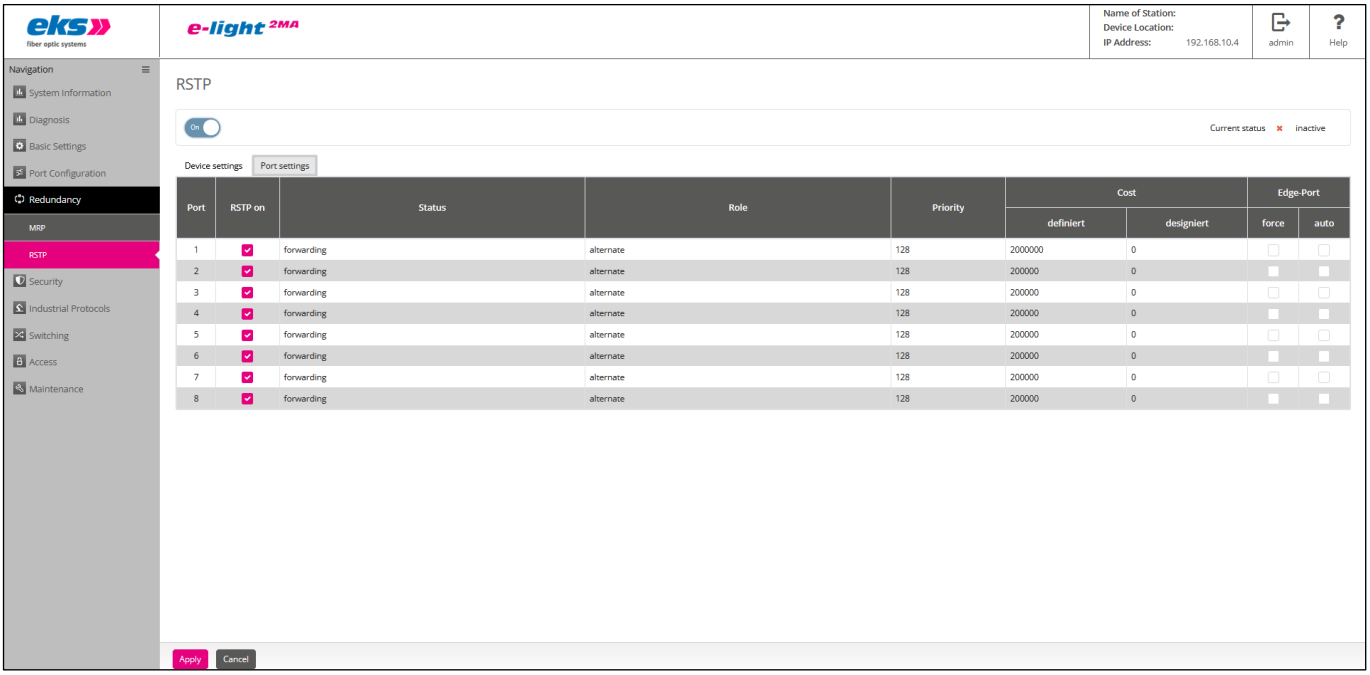


Figure 28: Rapid Spanning Tree Protocol – port settings

The port settings screen tab enables the following settings to be made:

- Port: Displays the port number.
- RSTP on: RSTP can be activated or deactivated for each port.
- Status: This column displays the status of the individual ports. This is differentiated between:
  - Blocking: Discards packets; does not learn addresses; does not receive and processes BPDUs (Bridge Protocol Data Units = RSTP protocol packets)
  - Listening: Discards packets; does not learn addresses; receives, processes, and transfers BPDUs
  - Learning: Discards packets; learns addresses; receives, processes, and transfers BPDUs
  - Forwarding: Forwards packets; learns addresses; receives, processes, and transfers BPDUs
  - Disabled: Discards packets; does not learn addresses; does not receive and process BPDUs
- Role: Each port is able to run in one of the following modes:
  - Root Port: A port in the forwarding state that was selected for the best tree structure.
  - Designated Port: A port in the forwarding state that has been selected for any switched LAN segment.
  - Alternative Port: An alternative port to the root bridge that is also available in addition to the current root port.

- Backup Port: A reserve path that is provided via a designated port in the direction of the branches of the tree structure.
- Deactivated Port: A port that does not have any operating function in the tree structure.

» Priority: Decides which port is treated with priority if the path costs to multiple ports are the same. Priority must be a multiple of 16 between 0 and 240.

» Costs: The path costs from this bridge to the opposite bridge. The costs can be between 1 and 200,000,000.

- Defined: The costs of the connection to the root bridge can be specified to include cable lengths or maximum data rates.
- Designed: Calculated path costs.

» Edge port: Indicates a port that is connected directly with an end station. These ports cannot cause loops and therefore immediately change to forwarding mode. The status change of an edge port will not lead to a change in the topology.

- Force: The port is configured by default as an edge port.
- Auto: The configuration as edge port takes place automatically.

After setting the RSTP parameters, these must be saved by clicking the apply button.

5.9 Security

The ***EL-1000-4GM*** switch has two security functions with which you can increase network security in your network by allowing only authorized devices to access your network. In addition, the ***EL-1000-4GM*** switch offers you the option of authenticating against a Radius server (Radius/802.1x) and the option of access control via MAC addresses (MAC filter)

5.9.1 **Radius/802.1x**

Radius 802.1x is a standard for port-based network control. In conjunction with a Radius server, it enables the authentication of devices or users before they gain access to the network. This significantly increases network security.

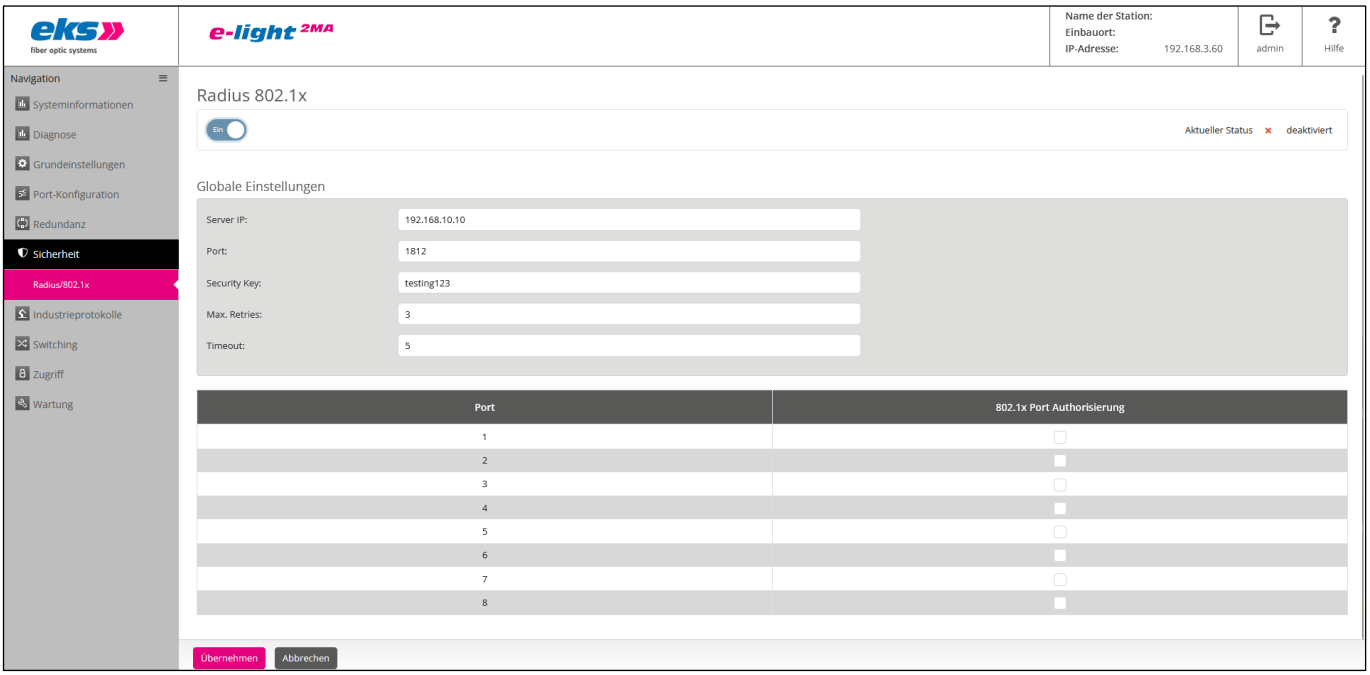


Figure 29: Page Radius/802.1x

You can use the slider to set whether authentication via Radius should be active.

Global Settings

The global settings required to authenticate against the Radius server are made in the upper table.

- Server IP: IP address of the Radius server.
- Port: Network port on which the Radius server receives requests. This is usually port 1812.
- Security Key: Key for encrypted communication. The security key must match that of the Radius server, which is usually port 1812.
- Max. Retries: Maximum number of retries if no response is received from the Radius server.
- Timeout: Waiting time in seconds, this time is waited after a failed server request before a new request is sent

In the table below, you can activate for each port individually whether it should authenticate itself against the Radius server. This is done by ticking the checkbox under 802.1x port authorization for the corresponding port.

After setting the Radius parameters, these must be saved by clicking the apply button.

Note: If new Radius settings are to be applied, please switch the port that is affected briefly off and on again under Port configuration (5.7). This ensures that the radius settings for this port are applied correctly.

5.10 Industrial Protocols

5.10.1 **Profinet**

Profinet is the abbreviation for Process Field Network and describes the open industrial Ethernet-standard for the automation. The ***EL-100-2MA*** switch is developed as a Profinet IO-Device for the connection of decentralized periphery to a Profinet controller. The device supports conformance class B and Netload Class III.

On the webpage you can activate the Profinet functionality and the other settings.

GSD-File: The downloadable configuration file offers the device description of the Profinet field device. The file is written in General Markup Language (GSDML). The file includes information needed during project planning with the Profinet controller.

Attention! For proper operation in a Profinet network we highly recommend that the Quality of Service feature is enabled and configured to use class based scheduling of traffic (Class of Service First or Class of Service only) and enable the weighted fair queuing priority setting. The Traffic Classes 6 (Internetwork Control) and 7 (Network Control) should be set to highest priority. Please also check chapter 5.11.3.

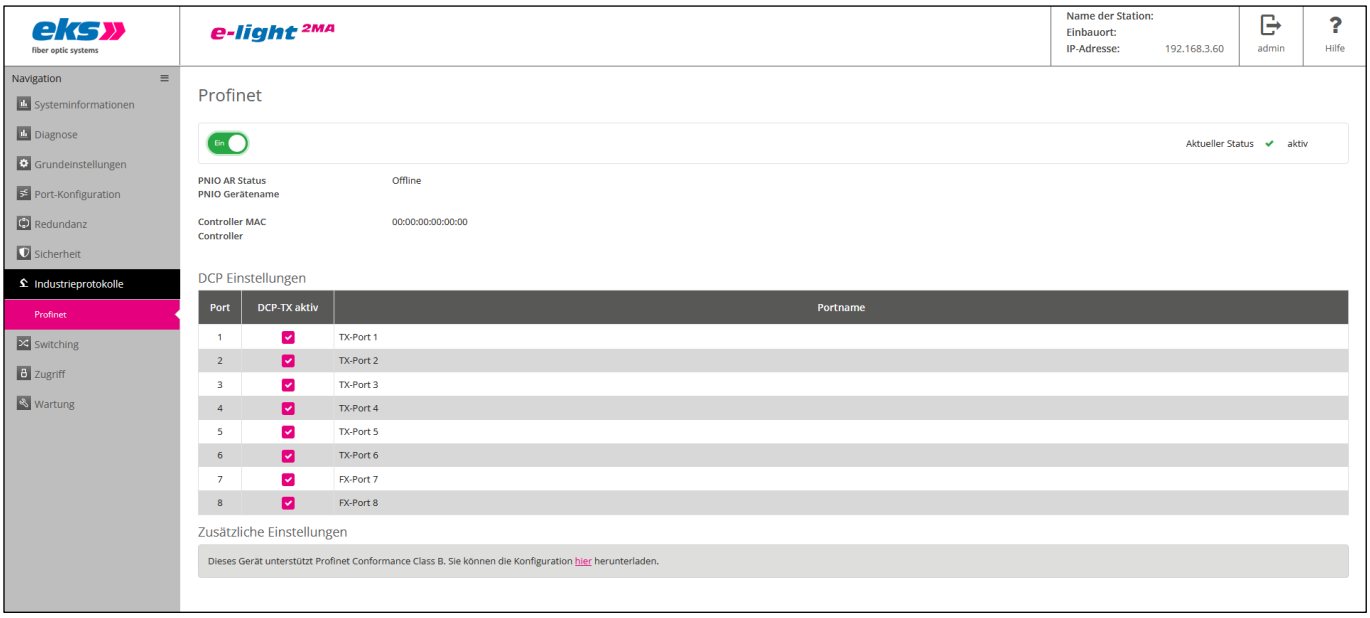


Figure 30: Profinet and DCP configuration

5.11 Switching

The switching screen offers an overview of activated and deactivated functions in the switching area.

Aging Time: This indicates the period of time during which a MAC address remains after removal from the port or switching of the device. You can select values between 16 and 4080 seconds in steps of 16 seconds. The default value is 304 seconds.

5.11.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) is used by switches, routers, and hosts to set up multi-cast groups. If IGMP is activated, multi-cast data traffic does not need to be sent to every individual multi-cast receiver, but rather only to each group. This severely reduces the network load.
IGMP snooping works on Layer 3 of the OSI model and is extended by the Layer 2 protocol IGMP snooping (Figure 31). IGMP snooping listens to the IGMP data traffic and learns via which ports the multi-cast data must be sent.

IGMP snooping settings

The following settings are displayed and can be adjusted:

- VLAN ID: IGMP snooping operates on VLAN basis and can be activated for each individual VLAN ID.
- Fast Leaver: If a multi-cast group should be removed, then there is normally a query whether no subscriber is really available in the group (query message). Fast Leaver is a port that removes a multi-cast group without any additional query. This setting is interesting for ports that are only connected with one multi-cast receiver.
- Learned Ports: Shows which ports are connected with multi-cast receivers and which ports should be forwarded the corresponding multi-cast data.
- Static Ports: Freely configurable ports that should always receive multi-cast data independent of IGMP messages.
- VLAN name: The name of VLANs.

Additional Settings

- Activate querier: If no multi-cast router is present in the VLAN and the IGMP queries are sent, you can configure here that query packets should be created from this switch.
- Suppress report: If receivers join multi-cast groups or leave them, then they transfer status reports to the IGMP protocol. This status data can be bundled by the IGMP snooping protocol by activating "suppress report". By limiting the necessary reports, the network load is reduced.

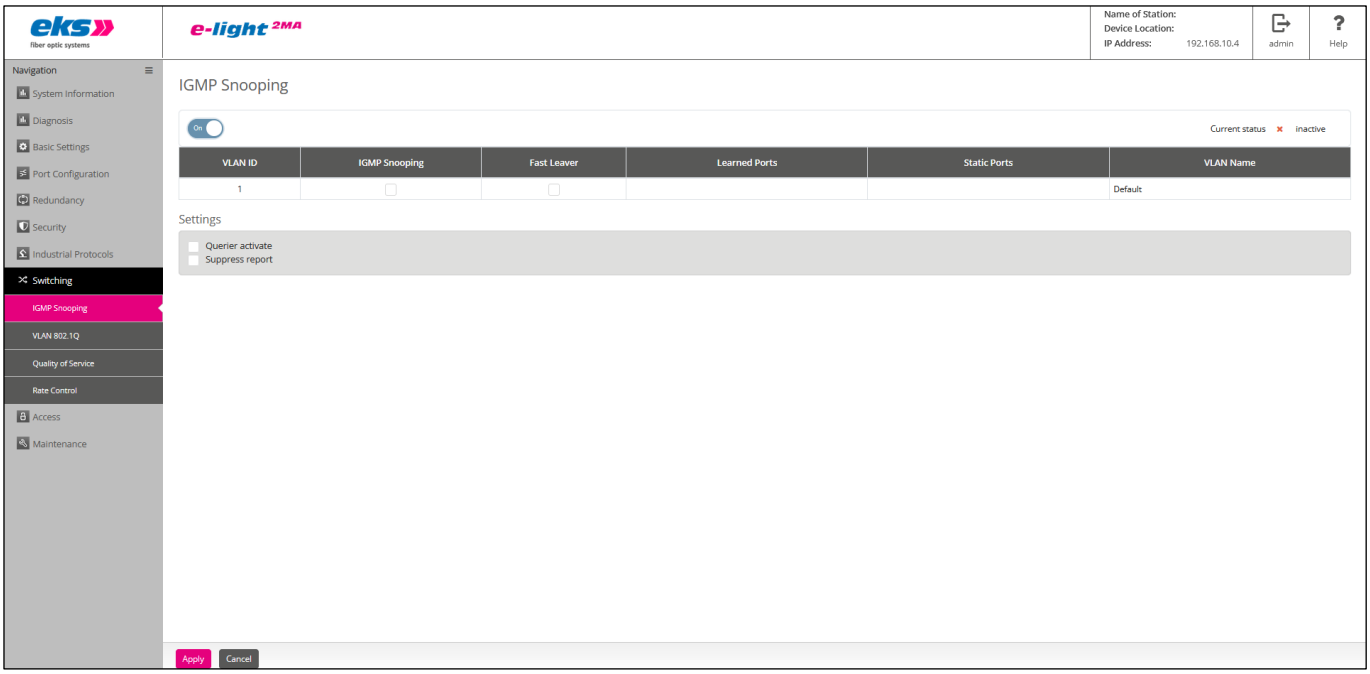


Figure 31 : IGMP Snooping

5.11.2 VLAN 802.1Q

A virtual LAN (VLAN) is a group of ports that may be somewhere in the network, but communicate as if they were in the same area. VLANs can be used to separate departments (R&D, marketing), applications (e.g. E-mail), or multi-cast groups for video transfers, which thereby simplifies network management.

In 802.1Q VLANs, Ethernet data packets are tagged with a VLAN tag, which includes a VLAN ID that uniquely identifies the VLAN to which the data packet belongs. You can conveniently configure and clearly display in the web interface menu which ports should send data packets with VLAN tags and which ports should send packets without VLAN tags, as well as which ports are assigned to each VLAN.

Figure 32: VLAN 802.1Q

Additionally, you can create, configure, and delete new VLANs here. When adding VLANs using the "+" button or editing them with the edit button, the following settings can be adjusted:

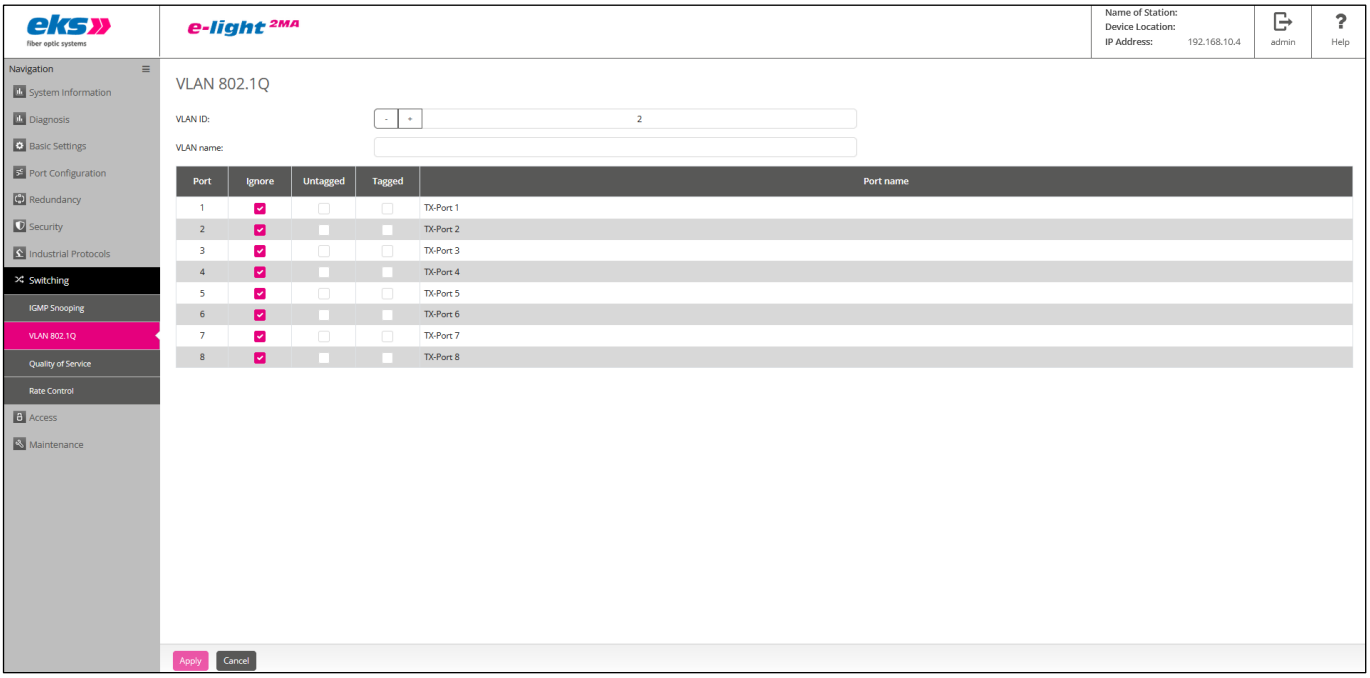


Figure 33: VLAN add / edit

- **VLAN ID**: This identification number is uniquely assigned to a VLAN. VLAN IDs can range from 1 to 4094. (This entry is fixed when editing an existing VLAN.)
- **VLAN Name**: Any name you choose for the VLAN.
- **Port Settings**: You can specify whether the port should be ignored in this VLAN or whether it should send tagged or untagged packets.

Using the delete button, you can remove any VLANs except for the default VLAN (VLAN ID 1).

Ports Tab

This page provides a clear overview of the port assignments for the ***EL-100-2MA*** switch to the configured VLANs. Each row represents a port, with the columns "Untagged in VLANs" and "Tagged in VLANs" indicating which VLANs (VLAN IDs) are assigned to the port in those respective configurations.

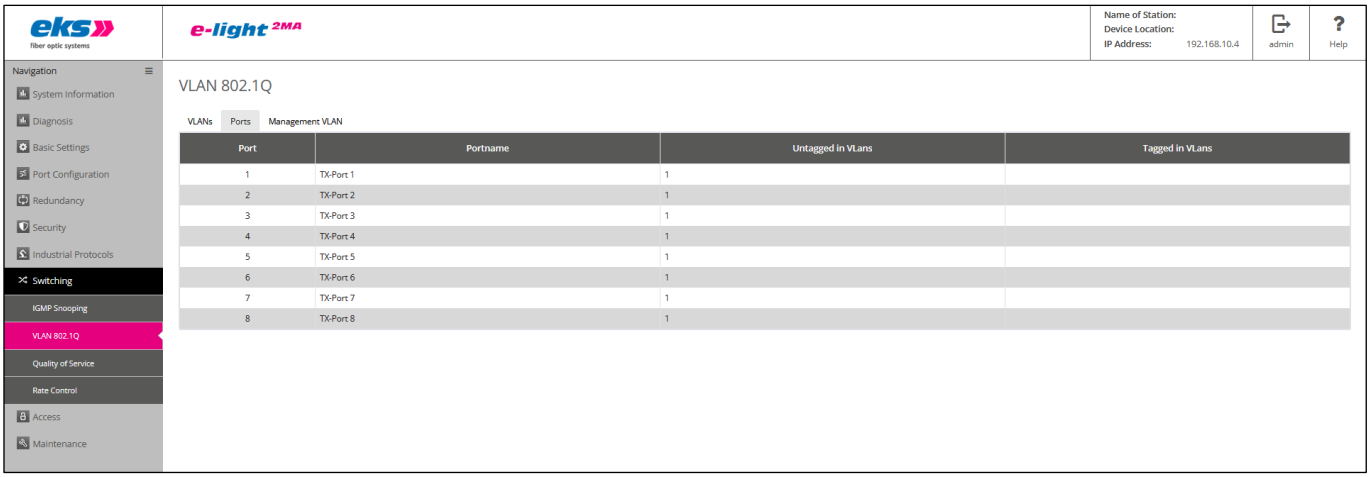


Figure 34: VLAN - Port overview

Management VLAN Tab

Here, you can configure which VLAN should be designated as the management VLAN. Access to the device, such as through the web interface, is only possible via the ports assigned to the management VLAN.

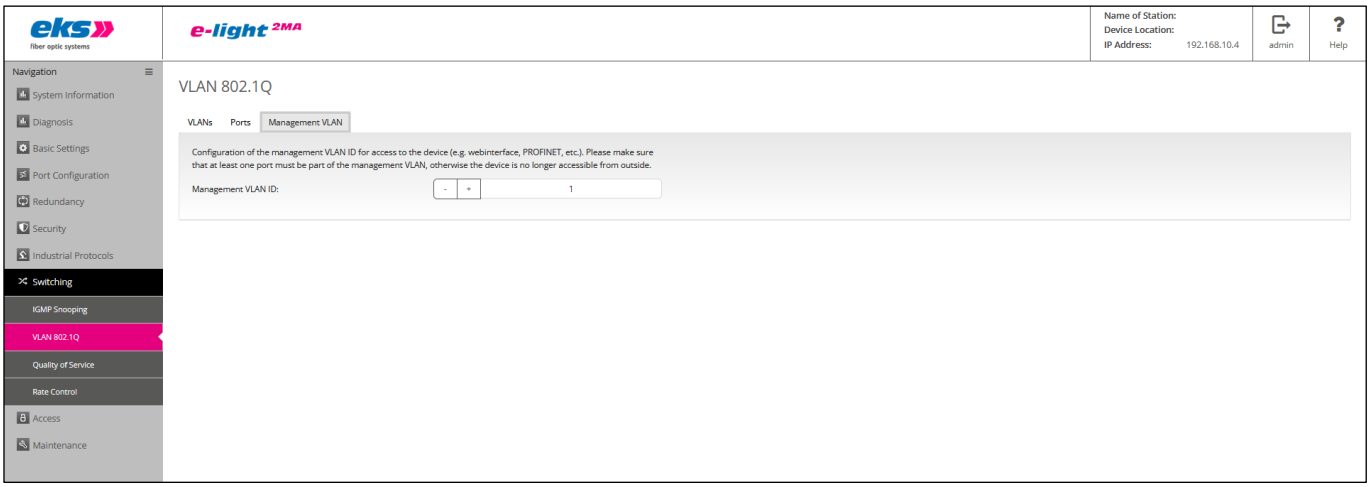


Figure 35: Management VLAN Assignment

Use of VLANs as per VLAN 802.1Q

If data packets that do not include a VLAN tag are received by a port, then they receive the VLAN-ID of the VLAN for internal processing that is configured as the untagged receiver port. Each port may therefore be configured as untagged for a VLAN. If data packets are received that contain a VLAN tag, then these are discarded if their VLAN-ID does not correspond with the default VLAN-ID or the VLAN-ID of a VLAN that is assigned to the receiving location tagged or untagged.

All incoming data packets therefore possess a VLAN-ID internally. This internal VLAN-ID decides which ports the data packets are exported on. The data of the default VLAN is exported to all ports, while the data of other VLANs are only exported to ports that are assigned to the VLAN with the VLAN-ID of the data packets.

If the data packets are sent with or without a VLAN tag is decided by the type of port assignment to the VLAN. If a port is assigned to a VLAN tagged, then data packets are sent with the VLAN-ID of the VLAN on the corresponding port with a VLAN tag. If the VLAN is assigned untagged, then the packets are sent on the port without a VLAN tag.

Attention! Packets of the default VLAN are output to all ports. The default VLAN should therefore be used for management packets. Ports without a VLAN assignment must be assigned to a VLAN that is not used so that packets that are received on these ports are not able to enter the default VLAN (see).

Attention! Packets with the VLAN tag 1 are received on all ports and output to all ports.

5.11.3 Quality of Service (QoS)

Quality of Service influences the data traffic in the switch so that services are available to the receiver with a specified quality. In addition to this, data packets are sorted depending on different priority processes (port-based, class of service, type of service) into four priority queues, which are emptied at the exit corresponding with a priority mode (strictly and weighted).

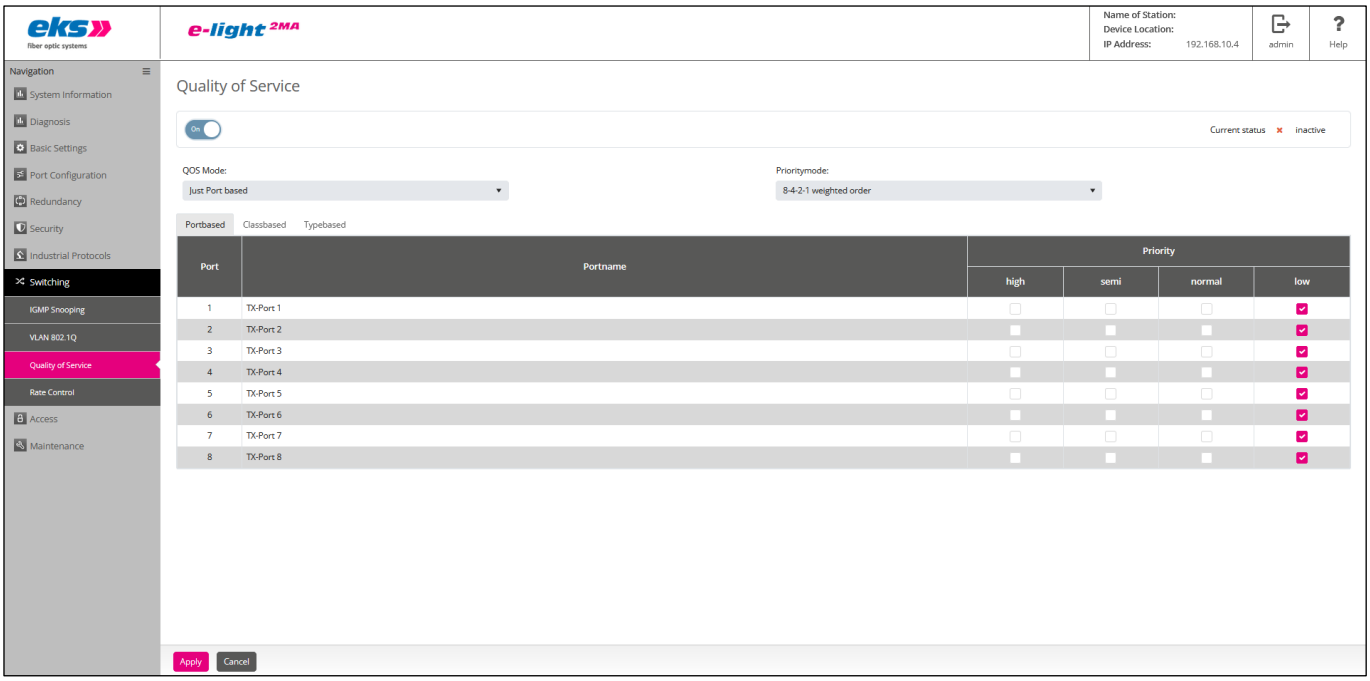


Figure 36: Quality of Service

Priority process

The following priority processes can be selected:

- Port-based only: The priority takes place exclusively based on the port priority.
- Class of Service (CoS) only: The priority takes place based on the CoS fields in the VLAN tag of the data packets. Non VLAN packets are guided to the priority queue with the lowest priority.
- Type of Service (ToS) only: The priority takes place based on the ToS fields in the IP header of the IP data packets. Packets without ToS field or non-IP packets are guided into the priority queue with the lowest priority.
- Class of Service first: Packets with COS information in the VLAN tag are prioritized after this. Packets without CoS information are prioritized according to the ToS field in the IP header or according to port priority in case of a missing ToS field.
- Type of Service first: Packets with ToS field in the IP header are prioritized after this. Packets without ToS information are prioritized according to the CoS field in the VLAN tag or according to port priority in case of a missing VLAN tag.

Priority mode

- Strict priority diagram: In case of a strict priority diagram, all of the packets from the higher priority queue are sent first, and then packets from the next lower priority queue are sent.
- 8-4-2-1 weighted sequence: After 8 packets in the highest priority queue have been sent, 4 packets in the second-highest, 2 packets in the third-highest, and 1 packet in the lowest priority queue will be sent. This approach avoids extreme waiting times for packets with the lowest priority.

Note: If Quality of Service is used, the flow control must be switched off, since activated flow control will transfer data packets throttled and independent of the priority (see section 0).

Attention! If the device is used in a Profinet setup it is highly recommended to enable the Quality of Service feature and use a weighted fair scheduling (8-4-2-1 Priority Mode). Furthermore either COS only mode or COS first mode with highest priority for traffic classes 6 (Internetwork Control) and 7 (Network Control) should be configured in order to allow secure and reliable communication in automation networks.

5.11.4 Rate Control

The rate control feature (Figure 37) can be used to limit different types of packets to an adjustable data rate. This can be used, for example, to ensure that an excessive number of broadcast packets (packets that are sent to all subscribers) do not disturb the normal Unicast data traffic (packets that are only sent to one subscriber).

The following settings can be made:

- Port: Indicates the port number.
- Type of incoming packets: Indicates which types of data packets should be limited:
  - All: All packets are limited.
  - Broadcasts: Only broadcast packets are limited.
  - Multi-casts: Only multi-cast packets (packets to receiver groups) are limited.
  - Unknown Unicasts: Only Unicast packets from unknown receivers are limited.
- Limit incoming packets: The data rate limits of incoming data. 128 kbps, 256 kbps, 512 kbps, 1 mbps,

2 mbps, 4 mbps and 8 mbps are possible. "No limit" is defined as a standard value.

- Limit outgoing packets: The data rates limits for outgoing packets. These always relate to all packet types. 128 kbps, 256 kbps, 512 kbps, 1 mbps, 2 mbps, 4 mbps and 8 mbps are possible. "No limit" is defined as a standard value.

The desired settings can be saved by pressing the apply button.

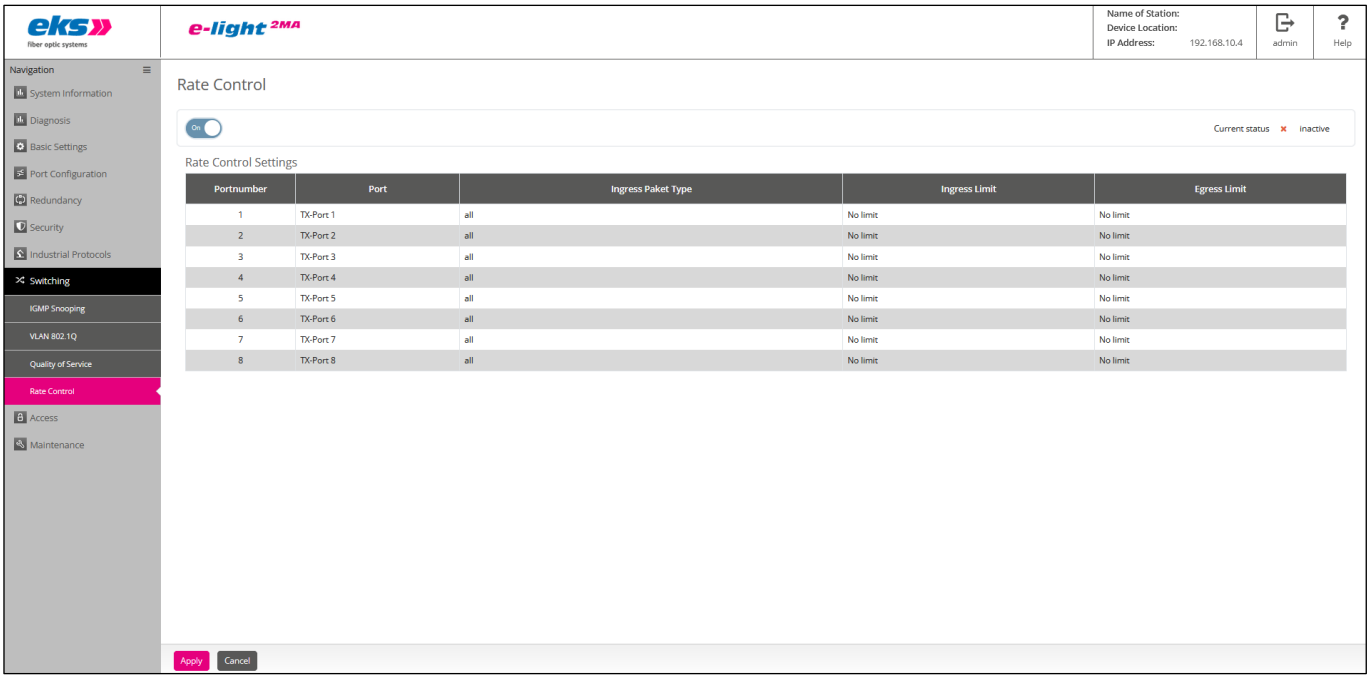


Figure 37: Rate Control settings

5.12 Access

The access menu item is used to specify the paths that will be used to access the ***EL-100-2MA*** switch.

Figure 38: Selection of access options

- Ping: In order to check if the device is able to be reached in your network, you can send queries to the device, which will send a response. The responses to these ping packets are suppressed if you deactivate ping under access.
- Config Mode: The ***EL-100-2MA*** switch can be configured via Config mode without requiring access to the web interface. If this setting is deactivated, Config mode can no longer be used. (Further explanations on Config mode can be found in chapter 3 Config-Mode)
- USB Port: It is possible to connect a USB stick to the ***EL-100-2MA*** switch. This can be used to update or restore the configuration and to back up the current configuration of the ***EL-100-2MA*** switch. Syslog messages can also be automatically transferred to the USB stick (5.5.3 Syslog messages). If this setting is deactivated, USB sticks are no longer integrated by the ***EL-100-2MA*** switch and it is no longer possible to restore or import a firmware update or save the configuration or syslog messages via USB.
- Device Identifier: The device identifier is used to uniquely identify the ***EL-100-2MA*** switch whose web interface is currently being accessed. If the Execute button is pressed, the Fault, Status and Ring LEDs flash simultaneously for 30 seconds.

Settings

There are two setting options for configuring access to the web interface of the ***EL-100-2MA*** switch.
The apply button can be used to save the settings.

- Time until automatic logout: The time until automatic logout defines how long a session in web management remains without activity until an automatic logout takes place. The time can be configured between 3 minutes and 30 minutes.
- Webgui Access Mode:
  - http: The web interface of the ***EL-100-2MA*** switch can only be accessed unencrypted.
  - https: The web interface of the ***EL-100-2MA*** switch can only be accessed encrypted. A valid https certificate is required for this.
  - http and https: The web interface of the ***EL-100-2MA*** switch can be accessed both encrypted and unencrypted.
- Use your own HTTPS certificate: You can set that an HTTPS certificate should be uploaded and used. If the box is checked, you are given the option of uploading an HTTPS certificate. This is then used. If the checkmark is removed again, the HTTPS certificate is deleted from the device and the standard HTTPS

certificate is used instead.

The apply button can be used to save the settings.

5.12.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is used to monitor and control network elements via a central station. Which settings in a network element can be changed and which values can be queried is not defined in the SNMP, but rather in the so-called MIBs (Management Information Base). In addition to several generally applicable MIBs, most of the devices also feature manufacturer-specific MIBs with device-specific information. The device-specific MIB for the ***EL-100-2MA*** switch can be downloaded from the Maintenance page under Licenses.

The ***EL-100-2MA*** switch supports both SNMP V1/2c and SNMP V3.

- SNMP V1/2c: queries are sent from the management station with a so-called community string, which represents a simple access limit. Responses are only provided for queries featuring a community string that matches a community string that is defined in the switch. Because the community string is sent in plain text via the network, its use does not necessarily increase the security.
- SNMP V3: Compared to SNMP V1/2c, SNMP V3 offers enhanced security features, including authentication, encryption and integrity protection. These features ensure that only authorized users can access network data and that the transmitted information remains protected and unchanged during communication.

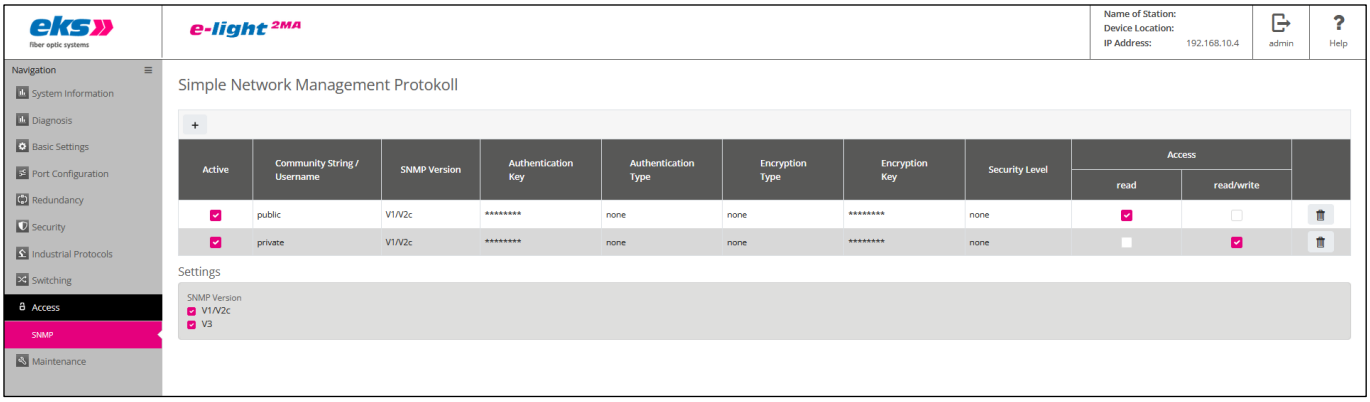


Figure 39: Overview of currently available SNMP accesses

Create SNMP access

Additional accesses can be created in the SNMP menu (Figure 39) of the ***EL-100-2MA*** switch. To do this, select the "+" button to open a new view in which you can first set the name and access level for the access. By default, new entries are always created as SNMP V1/2c.

Delete SNMP access

Additional community strings can be deleted in the SNMP menu (Figure 39) of the ***EL-100-2MA*** switch. By clicking on the small "trash can" button to the right of the entry, the entry is marked for deletion. Click the Apply button to apply the settings and delete the entry.

Configure SNMP access

Community strings can be edited in the SNMP menu (Figure 39) of the ***EL-100-2MA*** switch. The following settings can be configured:

For both SNMP V1/2C and SNMP V3:

- Active: Shows which strings are active at which community and which are not
- Community string: The accesses are defined via a clear name, which can be set here. A name may feature a maximum 32 characters.
- Read only: Queries with this community string are answered, but they cannot adjust settings at the switch.
- Read and write: Queries with this community string are answered and may adjust settings at the switch.
- Remove: Delete the community strings

Additionally for SNMP V3:

- Security level: SNMP V3 offers 3 different security levels.
  - NoAuthNoPriv: No authentication and encryption mechanisms are used at this level. Consequently no information is required for the authentication protocol and authentication key as well as for the encryption protocol and encryption key.
  - AuthNoPriv: At this level authentication is performed but no encryption. Therefore an authentication protocol and an authentication key must be set for this entry. No information is

required for the encryption protocol and encryption key.

- AuthPriv: This level provides authentication and encryption mechanisms. Therefore both an authentication protocol and an authentication key as well as an encryption protocol and an encryption key must be set.

- Authentication protocol: The authentication protocol ensures that only authorized users can access the SNMP data by checking the login data (user name and authentication key). It ensures that the transmitted data has not been tampered with. During transmission a hash value (e.g. HMAC) is created to check the integrity of the message. SNMP V3 offers two authentication protocols:
  - MD5: An older authentication protocol that creates a hash value for authentication. However, it is considered less secure as it is susceptible to collisions.
  - SHA: A more modern and secure authentication protocol that offers better security features and is more robust against many attacks.
- Authentication key: Enter the password required for authentication here. The password must be at least 8 digits long
- Encryption protocol: The encryption protocol is crucial for ensuring data security. SNMP V3 offers two encryption protocols:
  - Data Encryption Standard (DES): An older encryption method that uses a 56-bit key length
  - Advanced Encryption Standard (AES): A modern and more secure encryption method that offers stronger security and is considered the current standard for data encryption.
- Encryption key: Enter the password required for encryption here. The password must be at least 8 digits long.

Settings

You can select which SNMP version (V1/2c or V3) is active. It is possible to activate only one version or both versions in parallel. If no version is active, SNMP is deactivated. Save the settings by clicking the Apply button.

5.13 Maintenance

The maintenance menu item is divided into the items backup, restore, firmware update, factory settings, and restart, which are described in the following.

5.13.1 Backup

This menu item offers you the option to save the current configuration of the ***EL-100-2MA*** as a file. The backup can be stored via TFTP-server (Trivial File Transfer Protocol), as download or via usb-device. In connection with restoring, the backup function enables you to save all settings and reload them later to the device or use the current configuration in other devices.

The device creates a file with all settings. You have to store this file and can load it again to the device with the restore function.

In order to save the configuration via TFTP, a TFTP server must be set up on a computer in the network. Various TFTP server programs are available for download as freeware on the Internet.

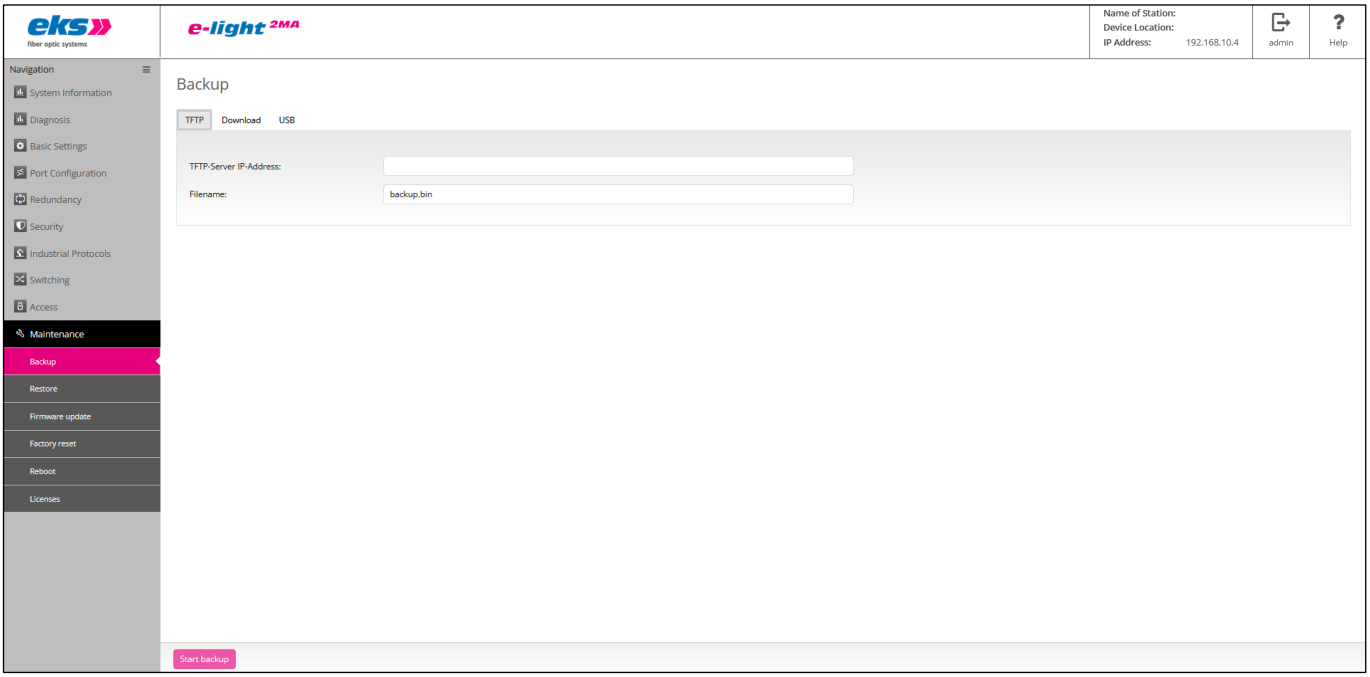


Figure 40: Settings for saving a configuration

TFTP Settings

- TFTP Server IP address: IP address of the TFTP server available in the network in decimal point notation.
- File name: File name under which the switch configuration file is to be saved on the TFTP server.

Settings Download

- No settings can be made, the backup is saved in the browser's standard download directory under the name backup.bin.

Settings USB

- File name: File name under which the switch configuration file is to be saved on the USB stick.
- To be able to use this functionality, access via USB must be activated under 5.11 Access.

If the parameters have been entered correctly, the backup can be executed by clicking on "Start backup".

5.13.2 Restore

This menu item is used to import a configuration that was previously saved as a backup file. It can be loaded vie tftp-server, as an upload or vie usb-device. Additionally, you can use this feature to transfer the configuration from one ***EL-100-2MA*** switch to other ***EL-100-2MA*** switches. This is done by creating a backup on one ***EL-100-2MA*** switch and then using this option to restore it to additional ***EL-100-2MA*** switches.

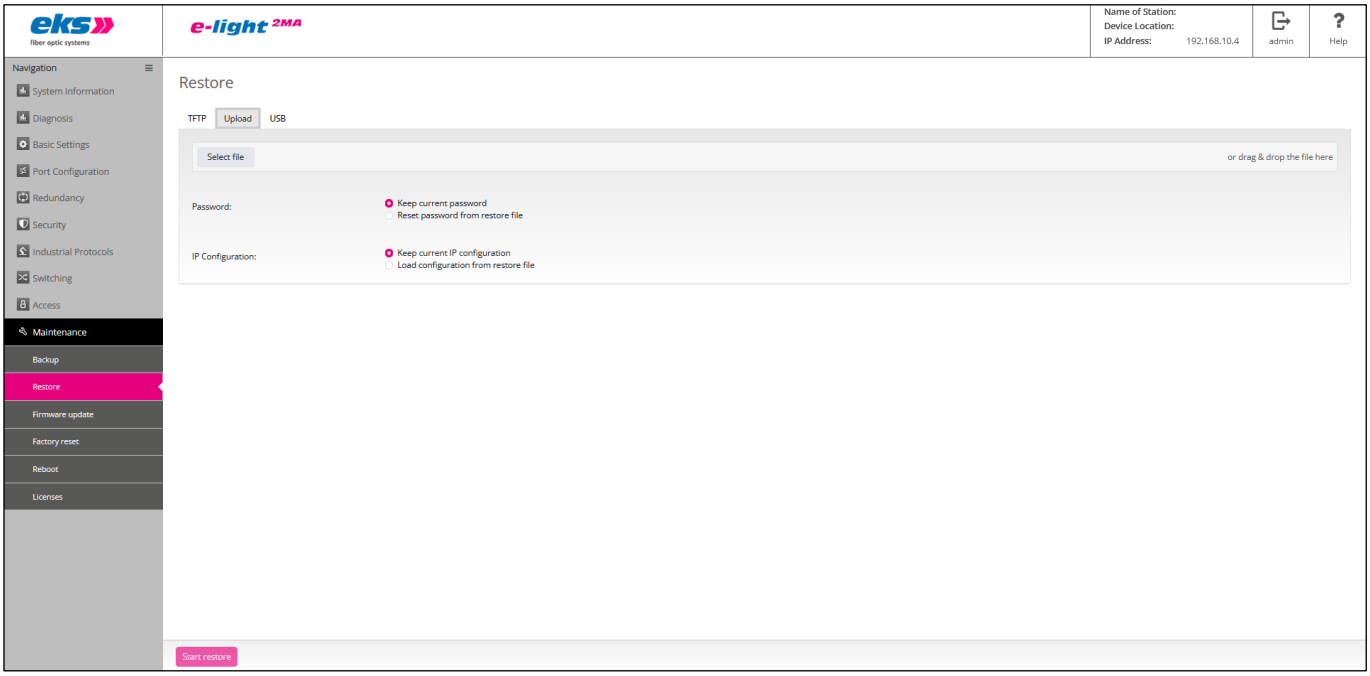


Figure 41: Settings for restoring a configuration

Settings

These settings are the same regardless of whether the backup is to be imported from a TFTP server, a USB stick or via the web interface.

- Password: Specifies whether the current password settings should be retained when restoring the

configuration or overwritten with the settings from the configuration file.

- IP configuration: Specifies whether the currently set IP address, subnet mask and gateway should be retained or overwritten with the settings from the configuration file.

TFTP Settings

- TFTP Server IP address: IP address of the TFTP server available in the network in decimal point notation
- File name: The file name of the switch configuration file that was saved on the TFTP server and is to be imported to the ***EL-100-2MA*** switch.

Settings Upload

- Select file: By selecting the “Select file” button, you can navigate to the switch configuration file to be imported. Alternatively, the file can be dragged and dropped onto this button.

Settings USB

- File name: The file name of the switch configuration file that was saved on the USB stick and is to be imported to the ***EL-100-2MA*** switch.
- To be able to use this functionality, access via USB must be activated under 5.11 Access.

Press the button "Start restore" to start the restore process. Doublecheck the settings in the popup window and confirm to reload the settings. After the process is done the device will reboot.

5.13.3 Restore via USB stick

The ***EL-100-2MA*** switch may also be restored without web interface access, provided a USB stick with a configuration file is present while the device is starting. The file name of the configuration file decides if the IP configuration of the switch should be overwritten or not.

If the configuration file configWithoutIp.bin is present on the USB-Drive (in the root folder) while the device is starting, all ***EL-100-2MA*** settings up to the IP configuration are replaced by the settings from the file. If the file is not available and a configWithIp.bin is not available on the USB stick, then all of the settings of the ***EL-100-2MA*** including the IP configuration will be replaced with the settings from this file.

If one of these configuration files is available, the ***EL-100-2MA*** switch several seconds after starting up with the settings from the configuration file. This is indicated when all of the LEDs light up again. The file is remove after a successful restore process.

The password settings are always kept for this type of configuration. If both files are present on the USB-Drive the file configWithoutIp.bin will be used.

» To be able to use this functionality, access via USB must be activated under 5.11 Access.

5.13.4 **Firmware update**

The menu item firmware update can be used to update the firmware of the ***EL-100-2MA***. Please only use firmware versions that are recommended by eks Engel FOS GmbH & Co. KG and have been developed for the devices of the ***EL-100-2MA*** series. Before starting the update process it is important to stop the redundancy protocols and to open the MRP ring. The device can get the new firmware by downloading it from a directly connected USB-Device or a TFTP-Server, which is accessible in the network. With the option upload it is possible to use a firmware which is stored on the computer or server in your network and store it on the ***EL-100-2MA***. To switch between the different options for applying a firmware update, simply click on the appropriate tab at the top of the page. There, you will find the available options.

Figure 42: Firmware Update

Attention! Please **do not** complete this action if you have not been authorized to do so by the manufacturer beforehand. This function should only be used if problems occur that are only able to be corrected by changing the device software. For this reason, you will only receive new or changed firmware if the manufacturer considers it to be necessary.

Update via TFTP-Server

To update the firmware by using a TFTP-Server, the new firmware file has to be stored in the TFTP-Server root directory. Please write down the name of the file or remember it. Now open the web interface of the ***EL-100-2MA*** and choose Firmware update over TFTP. Insert the IP-Address (Version 4) of the TFTP-Server in the field "TFTP-Server IP Address" and the name of the firmware file in the field filename. Press the button "Start Firmware update" to install the new firmware on the device.

Update via Upload

Press the button "select file" and a new window will open and show you the content of your computer. Select the firmware file and press the button open, to upload the file to the ***EL-100-2MA***. The upload of the firmware file will start and you can see the progress status. When the upload has finished the progress window will close and you can check the name of the uploaded file in the field Filename. Press the button "Start Firmware update" to install the new firmware on the device.

Update via USB

To update the firmware by using the usb-function store the file with the new firmware in an usb-device and write down or remember the name of the file. Connect the usb-device to the ***EL-100-2MA*** and choose the point Firmware update over usb. Insert the name and extensions of the file in the field filename. Press the button "Start Firmware update" to install the new firmware on the device.

» To be able to use this functionality, access via USB must be activated under 5.12 Access.

Attention. Please follow these rules during the firmware update:

- » Do not disconnect the device from the supply voltage.
- » Do not disconnect or replace any network connections.
- » Do not press the reset button on the front side of the device.

During the update, a progress display appears in the web interface. As soon as the update is completed, the ***EL-100-2MA*** switch will restart.

5.13.5 Factory settings

This menu item is used to reset the device to the factory settings.

Settings:

- Password: Specifies whether the password settings should be maintained if the configuration is reset or if they should be overwritten with the factory settings.
- IP configuration: Specifies whether the IP address, subnet mask, and gateway should be maintained or if they should be overwritten with the factory settings.

By clicking the "Set factory settings" button, the ***EL-100-2MA*** switch is reset.

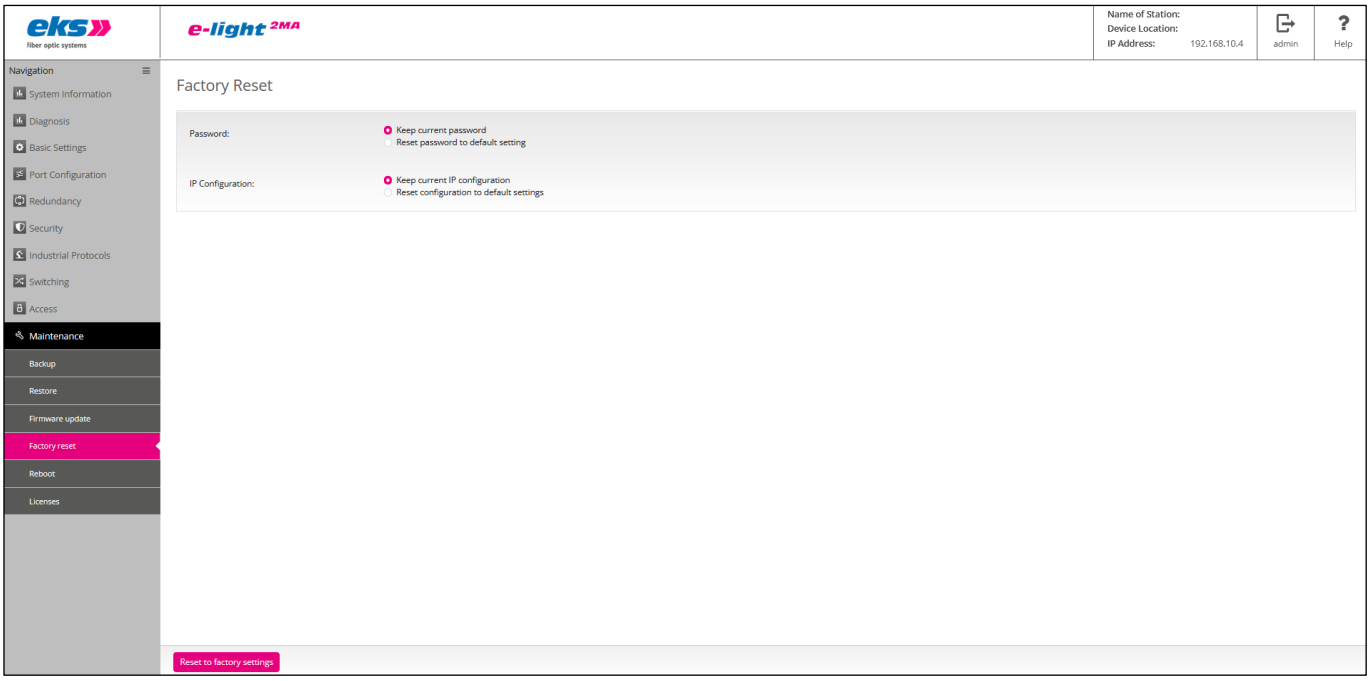


Figure 43: Factory Settings

5.13.6 Reboot

A reboot or software reset can be executed here. By clicking the reboot button, the switch's program is stopped and the device is rebooted. The reset button on the front side of the device has the same function and restarts the software, see section Reset button. Alternatively, you can switch both supply voltages of

the switch on and off to complete a hardware reset.

5.13.7 Licenses

Manufacturer information

Get in contact with the eks Engel FOS GmbH & Co. KG as manufacturer of the ***EL-100-2MA*** switch if you have serious problems during the configuration of the switch, or if you have questions to which you don't get an answer in the data sheet or in the manual. Read the chapter in the help text of the device and the manual before you get in contact with our support.

User manual

With this link you can download or open the manual of the ***EL-100-2MA*** in the portable document format (*.pdf). To read the manual a pdf-viewer is necessary which you can download in the internet for free. For example you can use the adobe acrobat reader.

SNMP-MIB File

The SNMP-MIB (**S**imple **N**etwork **M**anagement **P**rotocol - **M**anagement **I**nformation **B**ase)–File is available for download on the device. It provides all device-specific information that can be accessed using an SNMP browser.

License information

The linked file license.txt contains information concerning the used "open source software".

Profinet GSD file

The GSD-file describes the functionality of the ***EL-100-2MA*** to integrate the device into the profinet environment. The GSDML-File (generic station description markup language) is a xml-file which is language independent.

6 Instructions for troubleshooting

- Check the correct voltage supply. One of the VDC LEDs must be glowing green.
- Check the link/act LEDs of the wired RJ45 sockets and the optical fiber cable transceiver. If the connection is established, the link LEDs will light up, and they will flash in case data is being transmitted.
- Check the wiring of the RJ45 sockets. Select the correct network cable. Use "unshielded twisted pair" (UTP) or "shielded twisted pair" (STP) for RJ45 connections to establish the network: 100Ω category 3, 4, 5 or better cables for connections with 10 mbps or 100Ω category 5 or bettercables for connections with 100 mbps. Make sure that the cables are no longer than 100 meters.
- In case of doubt, disconnect redundant network structures and set the ***EL-100-2MA*** switch to the factory settings. If the communication functions, enter your settings gradually and observe which settings result in the error.

7 Technical specifications

8 Tx	EL100-2MA-8TX			
Item Number	044200 01 0008 0000 00			
6Tx, 2Fx	**EL100-2MA-6TX-2FX-MM-ST**	**EL100-2MA-6TX-2FX-MM-SC**	**EL100-2MA-6TX-2FX-SM-ST**	**EL100-2MA-6TX-2FX-SM-SC**
Item Number	044200 01 0006 0002 31	044200 01 0006 0002 33	044200 01 0006 0002 51	044200 01 0006 0002 53
100 FX Ports	2 x ST	2 x SC	2 x ST	2 x SC
Fibertype	Multimode		Singlemode	
Fibertype	50/125 µm		9/125 µm	
Typical Attenuation	1 dB/km		0,3dB/km	
Wavelength	1300 nm		1310 nm	
Budget	10 dB (+ 3 dB system reserv)		18 dB (+ 3dB system reserv)	
Max.-Distance	5000 m		30 km (others on request)	
4Tx, 4Fx	**EL100-2MA-4TX-4FX-MM-ST**	**EL100-2MA-4TX-4FX-MM-SC**	**EL100-2MA-4TX-4FX-SM-ST**	**EL100-2MA-4TX-4FX-SM-SC**
Item-Number	044200 01 0004 0004 31	044200 01 0004 0004 33	044200 01 0004 0004 51	044200 01 0004 0004 53
100 FX Ports	4 x ST	4 x SC	4 x ST	4 x SC
Fibertype	Multimode		Singlemode	
Fibertype	50/125 µm		9/125 µm	
Typical Attenuation	1 dB/km		0,3dB/km	
Wavelength	1300 nm		1310 nm	
Budget	10 dB (+ 3 dB system reserve)		18 dB (+ 3dB system reserve)	
Max.-Distance	5000 m		30 km (others on request)	

Table 3: Port specification (FX ports) of the *EL-100-2MA* models

10/100 Base Tx-Ports	RJ45 / auto-negotiation / Auto MDI / MDI-X / Supports cables up to 100m
Power supply	12-60 VDC redundant voltage supply
Power consumption	Maximum 8 W
Electrical isolation	500 V
Dimensions	B: 70mm, H: 156mm, D: 130mm
Weight	850 g
Enclosure	Stainless steel, powder-coated
Storage temperature	-40°C – +85°C
Operating temperature	-40°C – +55°C
Humidity	Moisture 5-95% RHD non-condensing
EMC	EN 61000-6-2 / EN 55032 Class A
LED display	Status LEDs / port LEDs (yellow / green) / voltage supply (green)

Table 4: Technical specification of the *EL-100-2MA* models

IEEE	IEEE 802.3 10Base-T Ethernet / IEEE 802.3u 100Base-TX and 100Base-FX Fast Ethernet / IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree / IEEE 802.1p class of service / IEEE802.1Q VLAN Tag
Protocol	CSMA/CD
Management	SNMP management, Web interface management
SNMP MIB	RFC 1213 MIBII / RFC 1493 Bridge MIB / RMON RFC 1757 / RFC 2674 VLAN MIB / RFC 1643 EtherLike-MIB / RFC 1215 Trap MIB Private MIB for switch information, ring, port alarm, TFTP firmware update, reset, port mirror, IP security management, IGMP management MIB
Technology	Store and forward switching architecture, Profinet Class B, Netload Class III
SNMP trap	Trap receiver / cold start / port link up / port link down / authentication fault / private trap for power status / port alarm configuration / fault alarm ring
Transfer rate	14,880 pps for 10 Base-T Ethernet port 148,800 pps for 100 Base-TX/FX Fast Ethernet port
MAC address table	2K MAC address table
Packet filters	4 types of packet filter rules with different packet combinations
Ring	2 ports for the ring in order to guarantee a recovery time below 200 ms
VLAN	Port-based VLAN Tagged VLAN IEEE 802.1Q
Class of Service	IEEE802.1p Class of Service with 4 priority queues per port
Spanning Tree	IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree
IGMP	IGMP v1 and query mode with up to 256 groups
SNTP	SNTP for time synchronization
SMTP	SMTP server and e-mail accounts for event messages
Port Mirror	Only TX packets or TX and RX packets
Firmware Update	Firmware update, TFTP backup and restore via TFTP, USB; HTTP
Alarm contact	Relay contact 25 VDC (1A) / 60 VDC (0.3 A)
Bandwidth control	Ingress and egress with combination options
DHCP Client	DHCP client function to receive an IP address from the DHCP server

Table 5: Functions, standards and technologies of the *EL-100-2MA* models

8 GPL/LGPL guarantee and liability exclusion

The ***EL-100-2MA*** switches from eks Engel GmbH & Co. KG (referred to as eks in the following) also include open source software components in addition to proprietary software. The open source software is provided to you according to the conditions of the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL) free of license fees. It was written by third parties and is subject to copyright. You are entitled to use open source software according to the conditions of the GPL or LGPL. In case of a conflict between eks license conditions and the conditions of the GPL or the LGPL, the GPL and LGPL shall apply to the open source components of the software.

The GPL and LGPL licenses and additional license information are available via the following URL on the device (IP address upon delivery): http://<insert-device-ip>/download/license.txt

If the source code of the open source software is not delivered with the ***EL-100-2MA***, then you may request it via the following e-mail address (together with the associated copyright instructions): info@eks-engel.de. The source code will be sent to you for the price the of copying and delivery costs.

All source code queries must be submitted within three years after purchasing the ***EL-100-2MA***. Please include a copy of the purchase receipt with your request. Please also include the exact name of the device and the version number of the installed software.

Use of the open source software delivered with ***EL-100-2MA*** in any other way with the ***EL-100-2MA*** hardware shall take place at your own risk without any liability claims against eks. For more information about guarantee claims involving the authors of the open source software delivered with the ***EL-100-2MA***, we refer to the GPL and the LGPL.

We exclude all liability for damage that results from any changes completed by third parties other than eks on parts of the software or the configuration. We exclude all liability on behalf of eks if the open source software violates copyrights of third parties. In case of changes that were not made to the software by eks, we shall not provide any technical support.

9 Table of figures

10 List of tables