

# Enhanced Ethernet Switch

## USER MANUAL

March 2024

# CONTENT

|          |                                                               |           |
|----------|---------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction .....</b>                                     | <b>5</b>  |
| 1.1      | About this document.....                                      | 5         |
| 1.1.1    | Scope.....                                                    | 5         |
| 1.1.2    | Validity.....                                                 | 5         |
| 1.1.3    | Glossary.....                                                 | 6         |
| <b>2</b> | <b>Safety and warranty .....</b>                              | <b>7</b>  |
| 2.1      | General operating and safety strategy of TE products.....     | 7         |
| 2.2      | General design rules for the power supply of TE products..... | 7         |
| 2.3      | Warranty and safety information.....                          | 8         |
| 2.4      | RoHS certificate of compliance.....                           | 10        |
| <b>3</b> | <b>Product description.....</b>                               | <b>11</b> |
| 3.1      | Functionality.....                                            | 11        |
| 3.2      | Features.....                                                 | 11        |
| 3.3      | Technical data.....                                           | 12        |
| 3.4      | Startup Time.....                                             | 12        |
| 3.5      | Scope of Delivery .....                                       | 13        |
| <b>4</b> | <b>Hardware .....</b>                                         | <b>14</b> |
| 4.1      | Connectors and controls.....                                  | 14        |
| 4.1.1    | Connectors.....                                               | 15        |
| 4.1.2    | Push-button (1).....                                          | 15        |
| 4.1.3    | Power MQS connector (2).....                                  | 15        |
| 4.1.4    | SFP slots (4).....                                            | 17        |
| 4.1.5    | Host port (5).....                                            | 17        |
| 4.1.6    | Service connector (6) .....                                   | 17        |
| 4.1.7    | BASE-T connector (7).....                                     | 17        |
| 4.1.8    | Other interfaces .....                                        | 17        |
| 4.1.8.1  | LEDs (3).....                                                 | 17        |
| 4.1.8.2  | Link LEDs (4).....                                            | 18        |
| <b>5</b> | <b>Configuration.....</b>                                     | <b>19</b> |
| 5.1      | Home screen.....                                              | 19        |
| 5.1.1    | Switch configuration tab.....                                 | 21        |
| 5.1.2    | Show configuration (1).....                                   | 21        |

|         |                                        |    |
|---------|----------------------------------------|----|
| 5.1.3   | Global configuration (2)               | 22 |
| 5.1.4   | BASE-T ports (3)                       | 23 |
| 5.1.4.1 | Port statistics                        | 23 |
| 5.1.4.2 | Port configuration                     | 23 |
| 5.1.5   | SFP+ Ports (4)                         | 27 |
| 5.1.5.1 | Port Statistics                        | 27 |
| 5.1.5.2 | Port Configuration                     | 27 |
| 5.1.6   | CPU port (5)                           | 31 |
| 5.1.7   | Control port (6)                       | 31 |
| 5.1.7.1 | Port statistics                        | 32 |
| 5.1.7.2 | Port configuration                     | 32 |
| 5.1.8   | Switch                                 | 34 |
| 5.1.8.1 | Port segmentation                      | 34 |
| 5.1.8.2 | Address resolution table               | 35 |
| 5.1.8.3 | VLAN configuration                     | 37 |
| 5.1.8.4 | Advanced filter                        | 39 |
| 5.1.8.5 | Traffic Shaping                        | 42 |
| 5.1.8.6 | TimeSync                               | 46 |
| 5.1.8.7 | Ingress rate limiter                   | 55 |
| 5.2     | Control panel tab                      | 59 |
| 5.2.1   | Configuration                          | 59 |
| 5.2.1.1 | Import a configuration                 | 59 |
| 5.2.1.2 | Export a configuration                 | 59 |
| 5.2.1.3 | Default configuration                  | 59 |
| 5.2.2   | Password write-protection:             | 59 |
| 5.2.3   | Power                                  | 60 |
| 5.2.3.1 | Reset System                           | 60 |
| 5.2.3.2 | Sleep System                           | 60 |
| 5.2.4   | SFP options                            | 60 |
| 5.2.4.1 | Automatic traffic shaping on SFP ports | 60 |
| 5.2.5   | Sleep parameters                       | 60 |
| 5.2.5.1 | Sleep mode                             | 60 |
| 5.2.5.2 | Wake-Up line 1 actuator                | 61 |

|           |                                                           |           |
|-----------|-----------------------------------------------------------|-----------|
| 5.2.5.3   | Wake-Up line 2 actuator .....                             | 61        |
| 5.2.5.4   | Wake-Up lines signaling timeout (in seconds).....         | 61        |
| 5.2.5.5   | Sleep timeout (in seconds).....                           | 61        |
| 5.2.6     | Network .....                                             | 61        |
| 5.2.6.1   | Controller IP Address .....                               | 61        |
| 5.2.6.2   | TECMP unit identifier .....                               | 61        |
| 5.2.6.3   | TECMP Device ID .....                                     | 62        |
| 5.2.6.4   | TECMP Ports.....                                          | 62        |
| 5.3       | System information tab.....                               | 63        |
| 5.3.1     | License information.....                                  | 63        |
| 5.3.2     | Device information .....                                  | 64        |
| <b>6</b>  | <b>Maintenance .....</b>                                  | <b>65</b> |
| 6.1       | Firmware update.....                                      | 65        |
| 6.1.1     | Preconditions and important information .....             | 65        |
| 6.1.1.1   | Update via host port .....                                | 65        |
| <b>7</b>  | <b>Remote control API .....</b>                           | <b>68</b> |
| <b>8</b>  | <b>Appendix.....</b>                                      | <b>69</b> |
| 8.1       | UDP Discovery messages .....                              | 69        |
| 8.1.1     | Broadcast discovery request .....                         | 69        |
| 8.1.1.1   | Unicast discovery response.....                           | 69        |
| 8.2       | UDP Configuration messages .....                          | 70        |
| 8.2.1     | Set Configuration mode .....                              | 72        |
| 8.2.2     | Restart device .....                                      | 72        |
| 8.2.3     | Mute/Unmute PHY .....                                     | 73        |
| 8.2.4     | Import configuration.....                                 | 73        |
| 8.2.5     | Export configuration.....                                 | 74        |
| <b>9</b>  | <b>Contact .....</b>                                      | <b>76</b> |
| <b>10</b> | <b>Declaration of conformity (EES RJ-45 variant).....</b> | <b>77</b> |

# 1 Introduction

## 1.1 About this document

This user manual contains important information for the proper and safe operation of Technica Engineering 's Enhanced Ethernet Switch.

Read this user manual carefully before using the device for the first time and follow the instructions, paying special attention to the safety-related parts.

For the latest version of this document please check the customer portal.

©2024 Technica Engineering GmbH

The content in this document is copyrighted by Technica Engineering GmbH. Copying or reproducing its content in full or in parts is not allowed. Technical contents in this document are subject to change without prior notice. Third-party content and trademarks are the property of the corresponding vendors.

### 1.1.1 Scope

This document includes instructions about how to use Technica Engineering's Enhanced Ethernet Switch properly, together with information about some of the complex use cases that can be covered by this device.

Troubleshooting is not part of the scope of this document. For support queries, please contact Technica Engineering via [Support](#).

Please note that, due to the dynamic development of the Enhanced Ethernet Switch, the information in this document is subject to change without prior notice to adapt to technical changes and updates. Some features may not be described yet in the user manual or maybe described incompletely.

Make sure to always use the correct version of this document, matching the firmware and hardware versions in operation (check next section).

### 1.1.2 Validity

This user manual applies to Enhanced Ethernet Switch with:

- Firmware version: v014.001
- Hardware version: v2.1 for RJ-45 variant and v3.2(for non-RJ-45 variants)
- TECMP version: v3.0 (specification document v1.6.1)

## 1.1.3 Glossary

| Term  | Definition / Explanation                                                                                 |
|-------|----------------------------------------------------------------------------------------------------------|
| AVB   | Audio Video Bridging                                                                                     |
| AVTP  | (Layer 2) Audio-Video Transport Protocol                                                                 |
| DUT   | Device Under Test                                                                                        |
| Eth   | Ethernet                                                                                                 |
| FCS   | Frame Check Sequence. Error-detecting code is added at the end of an Ethernet frame                      |
| gPTP  | Generic Precision Time Protocol, IEEE 802.1AS                                                            |
| HW    | Hardware                                                                                                 |
| IVN   | In-Vehicle Network                                                                                       |
| IFG   | The interframe gap between two ethernet frames                                                           |
| PTP   | Precision Time Protocol, IEEE 1588                                                                       |
| TECMP | Technically Enhanced Capture Module Protocol, used for encapsulation of captured in-vehicle network data |
| TSN   | Time-Sensitive Networking                                                                                |

Table 1-1: Glossary

Additionally, the following symbols are used throughout the document to highlight important information:



Information: Useful tips, hints, or background information.



Warning: Important information to consider for the correct use of the device.

## 2 Safety and warranty

### 2.1 General operating and safety strategy of TE products

Technica Engineering products are designed for operation in automotive systems and for supply voltages of nominal 12 V. The applicable limit, values adhere to the standard norms for 12 V automotive onboard power systems correspondingly and can be found in the mentioned norms.

Should Technica Engineering products be operated in voltage ranges beyond those specified in the norms, which represents a breach of the conditions of operation, then this will void the product warranty and Technica Engineering will assume no liability whatsoever for the results and/or consequences thereof.

This is especially valid whenever the voltage level reaches or exceeds the limits of the low voltage directive. In this case, damage to the devices cannot be excluded. Due to the manufacturing characteristics of the devices, there is no imminent fire hazard from the device itself, if the devices are being operated in an environment according to the conditions of use. A secondary fire hazard cannot be excluded, should those conditions not be met. Protection against overvoltage cannot be provided in such a breach of the conditions of use.




### 2.2 General design rules for the power supply of TE products

The power supply circuit of Technica Engineering products is equipped with self-protection hardware components. This protects the devices against excessive temperature and too high a voltage supply by switching the device off. This automatic switch-off function is independent of any software function.




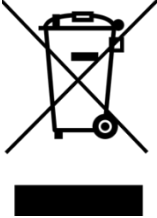

The root cause of excessive temperature in the power supply circuit can eventually be due to a too high environmental temperature or due to an internal failure of the device. In both cases, the automatic switch-off function will switch the power supply of the device off to avoid further damage.

The protection against too high a voltage supply protects the device even in case of an internal failure of the Technica Engineering device.

## 2.3 Warranty and safety information

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Before operating the device, read this manual thoroughly and keep it for your reference.</p> <p>The latest documentation for the Enhanced Ethernet Switch can be found at the customer portal.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|    | <p>As a user of this device, you may only perform tasks that are described in this document and valid for the corresponding firmware version.</p> <p>Technica Engineering assumes no liability for any kind of damages arising from the use of or concerning the use of our devices. The full responsibility of operation rests on the side of the end user.</p> <p>Manufacturer warranty of Technica Engineering products only applies as long as the user ensures proper installation, configuration, and use of the device as described in this user manual.</p> <p>Use the device only as described in this manual.<br/>       Use only in dry conditions.<br/>       Do not insert any foreign object in the slots/openings of the housing.<br/>       Do not apply power to a damaged device.<br/>       The device is to be used only by specialists.</p> |
|  | <p>Do not open the device. Otherwise, the warranty will be lost.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>This product is intended for use in automotive-like environments. An automotive-like environment includes test setups or test benches in the office, laboratory, and workshop areas. In the test setups, the same environmental conditions apply as in-vehicle electrical systems. Technica Engineering products are not intended to be used as standard IT equipment. The test systems and products from Technica Engineering are designed as customer and application-specific test modules that are only used by specialists for the development and test facilities.</p> <p>When integrating the modules in a vehicle or test setup, the user must ensure appropriate ventilation or air convection for the device(s). Technica Engineering products must not be considered as a safety element out of context when using safety-critical systems and must be included in the safety assessment when used. The development class in a safety system must be considered with standard QM referred to as ISO26262.</p> |
|  | <p> The device can get hot.</p> <p>Do not cover the device due to fire danger.<br/>         Do not place the device near highly flammable materials due to fire danger.<br/>         Do not use the device above the specified operating temperature.<br/>         The operating temperature is the ambient temperature of the installation space.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|  | <p>This symbol is only valid in the European Union. If you wish to discard this product, please contact your local authorities or dealer, and ask for the correct method of disposal. Technica Engineering GmbH is registered as a manufacturer of the brand "Technica Engineering" and the device type "Small devices of Information and Telecommunications technology for exclusive use in non-private households". WEEE Reg. No. DE 20776859</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|  | <p>Please refer to <a href="#">CHAPTER 10</a> for the EU Declaration of Conformity In accordance with directive 2014/30/EU.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 2.4 RoHS certificate of compliance

Technica Engineering's Enhanced Ethernet Switch complies with the RoHS (Restriction of Hazardous Substances Directive) certificate of compliance.

## 3 Product description

Ethernet is a point-to-point technology. This means to construct a network based on Ethernet, a switch is needed. The purpose of the switch is to intelligently communicate between the devices connected to it avoiding dedicated point-to-point connections.

Technica Engineering's Enhanced Ethernet Switch (EES) allows users to connect and loop through up to 8 10/100/1000BASE-T-based devices. This switch can establish virtual point-to-point connections using single VLAN tags (802.1Q) and double VLAN tags (802.1q-in-q), thus enabling filtering and control over data streams (mirroring and forwarding). This platform allows strong AVB/TSN capabilities intended for testing and analyzing onboard vehicle networks.

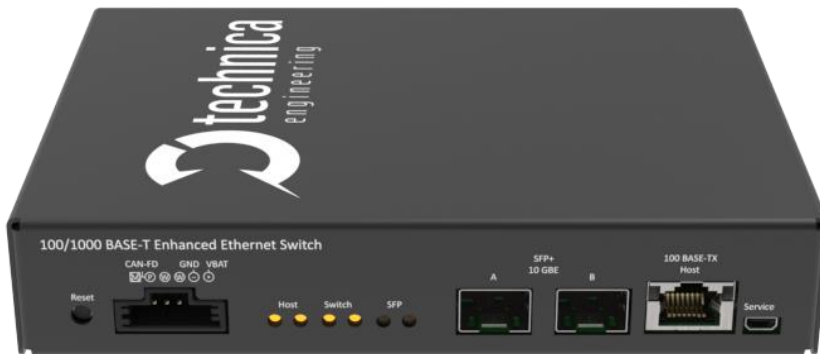



Figure 3-3-1: Enhanced Ethernet Switch

 The Enhanced Ethernet Switch RJ-45 variant is **not** optimized for automotive use.

### 3.1 Functionality

The main task of the Technica Engineering Enhanced Ethernet Switch is to act as a switch for the data collected from in-vehicle (IVN) communication systems via its multiple ports. Other features such as time synchronization of time-aware systems, segmentation of traffic, and supervising various streams of traffic are added intelligence provided by the switch. In this way, a user can set up specific solutions fitting the user's needs. The device is equipped with standard ethernet interfaces making it possible to use a regular computer for configuration and analysis.

### 3.2 Features


The main features of the Enhanced Ethernet switch are summarized below:


- 8x 10/100/1000BASE-T ports
- 2x SFP+ Ports for Logging data output (up to 10Gbps each)
- 1x 100BASE-TX Fast Ethernet Port for configuration
- Easy configuration via webserver and remote configuration messages
- Import and export of configurations
- Wake-up / sleep functionality
- Possibility to reset to default settings by push button
- Automotive ethernet variants are 10/100/1000BASE-T1 capable
- Time synchronization using a subset of 802.1AS automotive profile (gPTP)
- Stream Reservation & Traffic Shaping (802.1Qav)
- Individual use cases for the following TSN functionalities can be provided on-demand, Qci, Qbv, Qbu (check with our Technical Sales Team)
- Extended voltage range: 12-to-24-volt automotive battery voltage systems compatible
- Robust steel case


The following features – and more – make this device appropriate for general-purpose testing:

### 3.3 Technical data

|                           |                                                   |
|---------------------------|---------------------------------------------------|
| Voltage requirement:      | 6.5 to 28 Volt DC (nominal 12 Volt DC)            |
| Power consumption:        | 8 to 14 Watt (depending on connected SFP Modules) |
| Size:                     | 164 x 118 x 27 mm                                 |
| Weight:                   | 0.57Kg                                            |
| International Protection: | IP 2.0                                            |
| Operating temperature:    | -40°Celsius to 85°Celsius                         |


 Operating temperature is the guaranteed range of temperature under which all the device features are available and working. Outside this range, the user operates the device at their own risk.

 The temperature conditions where the device can be placed while not in use should not exceed 50° for the device to have consistent performance for longer periods.

 When SFP+ interfaces are used then the operating temperature can be a **maximum of up to 60°C** as the SFP modules generate extra heat

### 3.4 Startup Time

|                                                                                                                             |       |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| PowerUp and Processor Boot Time:<br>The time from power-up until all hardware related to switching operations is configured | 80 ms |
|-----------------------------------------------------------------------------------------------------------------------------|-------|

 The 100BASE-TX Host port needs about 3-4 seconds of linkup time in Auto-negotiation mode

## 3.5 Scope of Delivery

The delivery includes:

-  1x Enhanced Ethernet Switch

Cable sets can be ordered separately. For details, please consult the cable set document or contact [Technical Sales](#).

## 4 Hardware

The Enhanced Ethernet Switch has been designed for multiple use cases. Therefore, several hardware versions of the switch have been developed so far. Differences between the versions are collected in the table below:

| HW variant | Properties                                                                                                                                                                                                       |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v2.0       | <ul style="list-style-type: none"> <li>With RJ-45 connectors for 1000BASE-T interfaces (article number TE-2002)</li> </ul>                                                                                       |
| v2.1       | <ul style="list-style-type: none"> <li>Minor changes</li> </ul>                                                                                                                                                  |
| V3.1       | <ul style="list-style-type: none"> <li>With MATEnet connectors for 1000BASE-T1 interfaces (article number TE-2000)</li> <li>With H-MTD connectors for 1000BASE-T1 interfaces (article number TE-2001)</li> </ul> |
| v3.2       | <ul style="list-style-type: none"> <li>Minor changes</li> </ul>                                                                                                                                                  |

Table 2 Hardware variants

### 4.1 Connectors and controls

The Enhanced Ethernet Switch is equipped with several connectors and control elements that are distributed between the front and back sides of the device. This document focuses on

- The Enhanced Ethernet Switch RJ-45 variant

There is a separate user manual for:

- Enhanced Ethernet Switch MateNet variant
  - Enhanced Ethernet Switch hMTD variant

On the front side of the Enhanced Ethernet Switch, we can find:

- 1x Power connector including
    - 2x Wake up lines
    - 1x CAN-FD connection
  - 1x RJ-45 Ethernet connector (for configuration only)
  - 2x SFP+ slots
  - Several LEDs

The backside of the device is reserved for the interfaces used to 10/100/1000BASE-T devices. This means:

- 8x 10/100/1000BASE-T ports

## 4.1.1 Connectors

Here user can see an overview of all the HW interfaces of the Enhanced Ethernet Switch

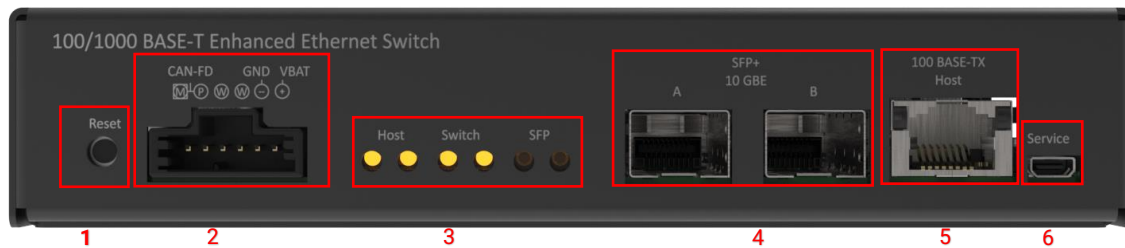


Figure 4-1: Front side of Enhanced Ethernet Switch

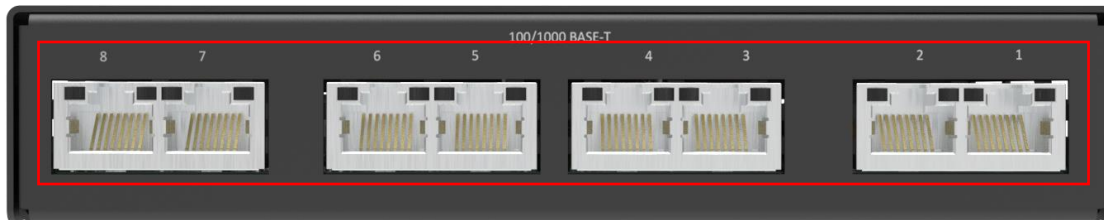


Figure 4-2 Backside of Enhanced Ethernet Switch RJ-45

## 4.1.2 Push-button (1)

The push-button will reset all settings to factory default settings. Press this button for 5 seconds. After that:

- IP Address is set to default (10.0.0.200)
- The complete configuration is lost and is set to default



If the device is blocked and all LEDs are lit (not blinking), the device must be sent to Technica Engineering. To avoid problems please make sure that the Host LED (orange) is blinking slowly (once per second) and the power supply is stable before the reset.

## 4.1.3 Power MQS connector (2)

A black MQS connector on the front side (8 pins, one row) is used to supply the power to the Enhanced Ethernet Switch

- The power supply for the device is supplied by pin 1 (12 Volt) and pin 2 (Ground)
- Requirements for the device itself: 12 Volt DC up to 1 ampere (typically 600 mA).

Next to the pins for the power supply, the pins corresponding to two independent wake-up lines can be found, identified with the letter “W” in the device housing. For each of them:

- As a digital input, the line consumes approximately 0.7 mA.
- As digital output, the line supplies a maximum of approximately 60 mA.

Next to the pins for wake-up lines, the pins for a CAN-FD connection can be found. Currently, this function is under development.

The connector Tyco Electronics Micro Quad Lock System (MQS) is used, as described in the table below:




| Name                                             | Picture                                                                             | Part Number                                        |
|--------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------|
| TE connectivity<br>6pos MQS .63 header 90deg THR |   | 1-1418888-5                                        |
| TE connectivity<br>MQS BU-GEH 6P                 |  | 1-969508-2<br>Distributor: mouser.de               |
| TE connectivity<br>MQS crimp contact             |  | 928999-1<br>Distributors:<br>Mouser.de; Digikey.de |

Table 3: Parts of Tyco MQS Connector

| Pin | Function               |
|-----|------------------------|
| 1   | CAN-FD Minus           |
| 2   | CAN-FD Plus            |
| 3   | Wake up line 2         |
| 4   | Wake up line 1         |
| 5   | Power Ground           |
| 6   | Battery +12 Volt Input |

Table 4: Pinning of black MQS connector



#### 4.1.4 SFP slots (4)

There are two SFP slots for SFP+ modules in the switch. For details on configuration, please check [CHAPTER 5.1.5](#).

The following modules have been tested and can be used with the switch:

- BEL SFP-1GBT-05 SFP 10/100/100 Mbps RJ-45 Module.
- 10Gtek 10GBASE-T SFP+ Transceiver, RJ-45 SFP+ CAT.6a up to 30 meters.

#### 4.1.5 Host port (5)

There is one RJ-45 Standard Ethernet connector for Fast Ethernet on the front side, labeled as 100BASE-TX Host, that can be used for the configuration of the device.

The in-built LEDs in the RJ-45 connector show the status of the 100BASE-T configuration port.

- The left (red LED) is lit by a link-up.
- The right (orange LED) will blink on data traffic.

#### 4.1.6 Service connector (6)

The Enhanced Ethernet Switch is provided with an interface to be used for service only.

#### 4.1.7 BASE-T connector (7)

The Enhanced Ethernet Switch RJ-45 variant is equipped with 8x 10/100/1000BASE-T ports allowed through the RJ-45 connectors. Standard Ethernet cables can be used with these connectors to connect to the devices

#### 4.1.8 Other interfaces

These interfaces include LED indicators for various interfaces.

##### 4.1.8.1 LEDs (3)

The Enhanced Ethernet Switch has 4 Status LEDs and 2 LEDs related to SFP slots on the front side of the case.

| LED      | Description                                              |
|----------|----------------------------------------------------------|
| Host LED | Green: Always lit, during normal operation of the switch |

|                   |                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <p>Orange:</p> <p>Blink slowly (once/second) during normal operation of the device</p> <p>Blink fast (flicker) suggesting the device is in bootloader mode</p> |
| <b>Switch LED</b> | Green; Currently not in use                                                                                                                                    |
|                   | Orange; Currently not in use                                                                                                                                   |
| <b>SFP</b>        | The 2 SFP LEDs show if the inserted SFPs in the SFP+ slots have a linkup                                                                                       |

Table 5 Details for Status LEDs

#### 4.1.8.2 Link LEDs (4)

There are two types of link LEDs corresponding to the interface

The 8 port status LEDs (on the backside next to every RJ-45 connector) of all 10/100/1000BASE-T ports monitor the link status of the corresponding port.

##### 1Gbps mode

- The left (red LED) is lit by a link-up.
- The right (orange LED) will blink on data traffic.

##### 100Mbps/ 10Mbps:

- The left (red LED) is not used.
- The right (orange LED) is lit by a link-up and is blinking on data traffic.


## 5 Configuration

The Enhanced Ethernet Switch is a highly configurable device, offering the user great flexibility to include it in many different scenarios.

Out-of-the-box, access to the webserver is possible by connecting the device via the Host port (RJ-45) to a computer. The default IP address for the device is 10.0.0.200. The recommended subnet mask is 255.255.255.0.

Once connected to the device (through the 100BASE-TX Host RJ-45 connector):

1. Please go to the network adapter settings and adjust the IP in the same range as your Enhanced Ethernet Switch. For example, 10.0.0.20 with subnet mask 255.255.255.0.
2. Enter the IP address in your standard web browser.

 Firefox is the recommended browser.

### 5.1 Home screen

The following website should appear. The user can select the corresponding ports for further configuration.

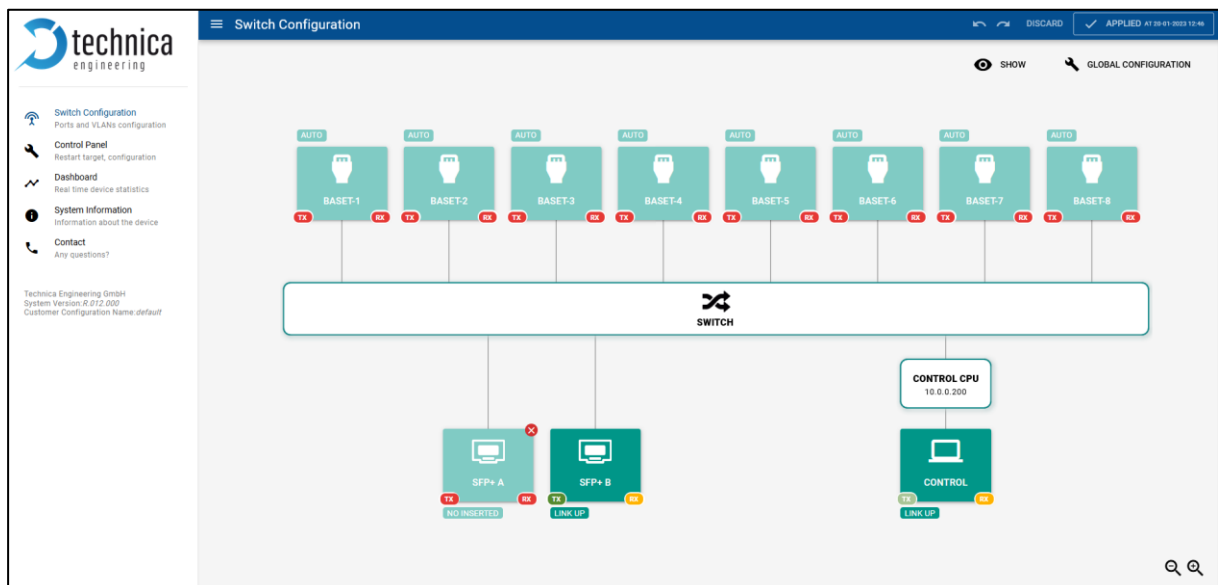


Figure 5-1: Home Screen Enhanced Ethernet Switch

Please select one of the tabs for further configuration. Each tab is described in detail in the next sections of this document.


Any change in the configuration will lead to the following hint appearing at the top of the current web page:



This option sends data from the webpage to the memory of the device. There is no need to save every time this hint appears. All the desired changes can be done at once and the configuration can be saved at the end. To do that, please click **“SAVE CONFIGURATION”**. Please note that the configuration will not be applied unless the device is restarted.



By clicking on this option, the user is prompted to introduce an optional name for the configuration file and to accept the changes. By selecting **“OK”** the configuration is saved similar to the option **“SAVE CONFIGURATION”**. It also restarts the device, applying the saved configuration.

-  Note that without **“SAVE & APPLY CONFIGURATION”**, the configuration of the device will not be fully updated. To be sure that all changes have been applied, a restart of the device is necessary.

## 5.1.1 Switch configuration tab

The following options can be explored in the switch configuration tab.

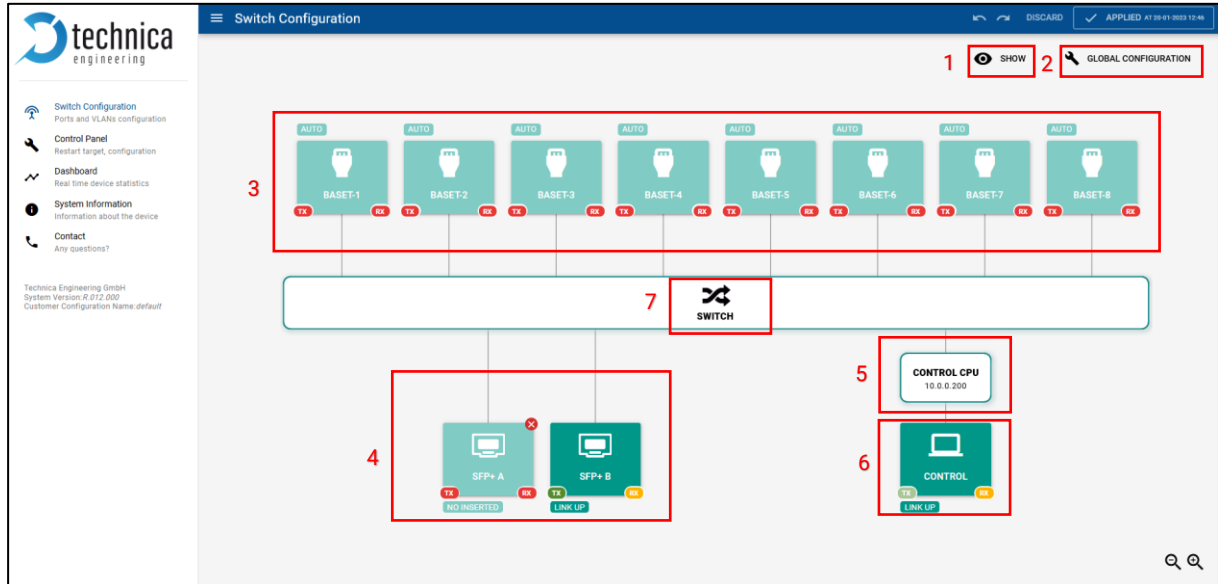



Figure 5-2 Switch Configuration Tab

## 5.1.2 Show configuration (1)

This tab visualizes the settings on the switch

-  **Show VLANs:** When this option is checked, the user can add VLAN IDs that can be visualized on the switch configuration page. A maximum of 7 sections are allowed

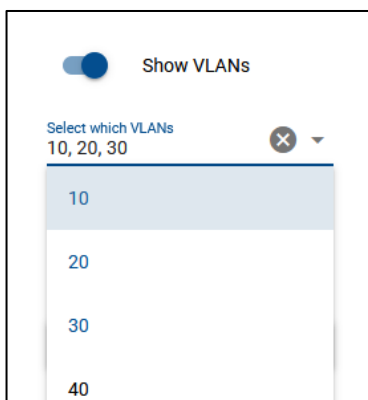


Figure 5-3 Selection of VLANs

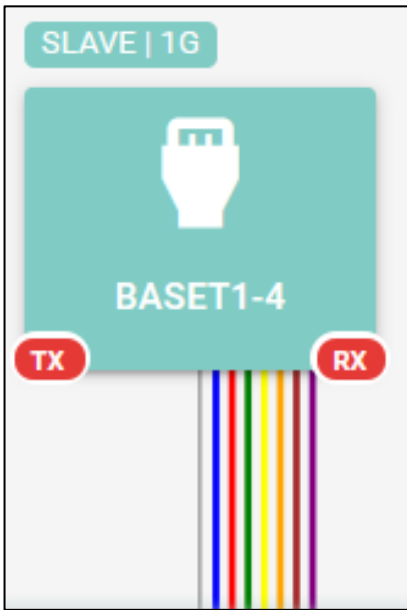



Figure 5-4 Visualization of VLANs

- 
**Show Mirroring:** When this option is checked, all the mirroring ports are visualized. Mirroring can only be selected on the SFP+ A and SFP+ B ports. When visualized mirroring is shown as “dotted lines.”

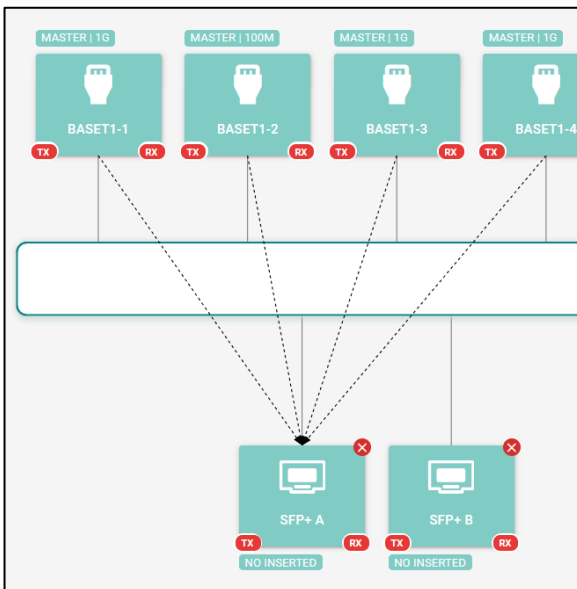


Figure 5-5 Visualization of Mirroring

### 5.1.3 Global configuration (2)

This option permits the user to enable port settings on the switch.

- **Port Segmentation:** When this option is checked, the user can make segments of ports that are allowed to exchange traffic. See [CHAPTER 5.1.8.1](#)
- **VLAN:** When this option is checked, the user can configure VLAN Tags (802.1q) and is allowed to facilitate VLAN-based traffic. See [CHAPTER 5.1.8.3](#)
- **Double Tagging:** When this option is checked, the user can configure double VLAN Tags (802.1q-in-q) and facilitate double VLAN-tagged traffic. The user is also free to enter any TPID for the second tag in hex. By default, the TPID is 0x88A8. See [CHAPTER 5.1.8.3](#)
- **TimeSync:** When this option is checked, the user can configure the ports of the switch for gPTP. The user can create partitions for time synchronization. See [CHAPTER 5.1.8.6](#).
- **Advanced Filter:** When this option is checked, the user can define rules for filtering traffic. See [CHAPTER 5.1.8.4](#)
- **Traffic Shaping:** When this option is checked, the user can configure 802.1Qav related parameters on each port. See [CHAPTER ERROR! REFERENCE SOURCE NOT FOUND](#).
- **Ingress Rate Limiter:** When this option is checked, the user can configure token buckets for streams of traffic on ingress. See [CHAPTER 5.1.8.7](#).
- **Address Table:** Here the user can view and manipulate entries on the address resolution table. See [CHAPTER ERROR! REFERENCE SOURCE NOT FOUND](#).

 At a time, only one option between [VLAN](#) and [Double Tagging](#) can be selected.

## 5.1.4 BASE-T ports (3)

The switch is provided with 8 RJ-45 ports (BASE-T-1 to BASE-T-8). The switch configuration tabs show basic information about the configuration of the port. This includes:

- **10M/100M/1G/Auto:** The selected BASE-T port is configured at 10M/100Mbps/1Gbps/in auto-negotiation mode
- **Signal Strength:** The selected port has the following signal strength for TX/RX
- **Automatic Base-T1 parameters search:** A loupe icon on the top right indicates that the automatic Base-T1 search is enabled, and role and speed will be detected automatically.
- **Reverse Polarity:** A warning icon in the upper left corner shows that the positive and negative wires in the connection have been swapped.

### 5.1.4.1 Port statistics

The user can see the summary of the configuration of a port along with some statistics by placing the cursor on the desired port.

### 5.1.4.2 Port configuration

The user can click on the desired port for configuration.

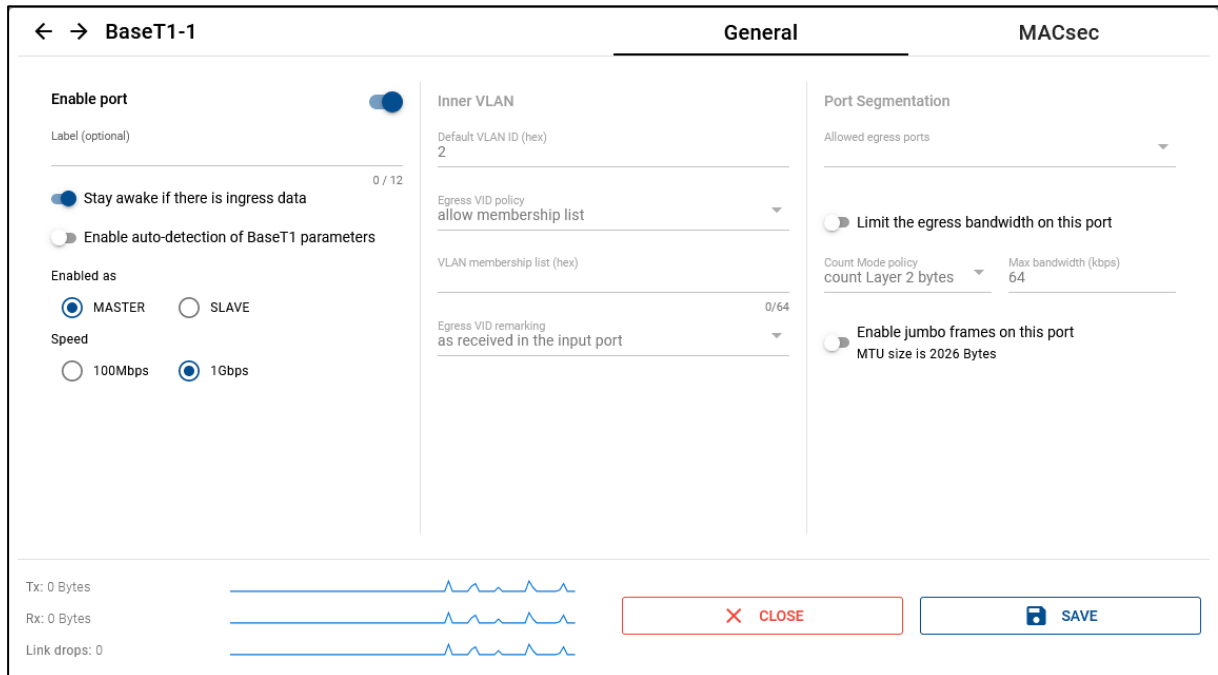


Figure 5-6 Configuration Menu for BASET-1 Port

**Enable Port:** The user can enable or disable the port. Once the port is disabled the color of the port is changed to grey



Figure 5-7 Disabled & Enabled Port

**Label:** The user can add a name for a particular port. A maximum of 12 characters can be used for the name.

**Stay awake:** When this option is enabled the Port stays up as long as there is traffic on the port.

**Auto-detection of BaseT1 parameters:** When this option is enabled the device tries all combinations to identify the speed (100 or 1000 Mbps) and the role (master or slave). The role (master/slave) and speed options are greyed out when this option is enabled, as the equipment will detect the neighbouring device's configuration by itself.

**Speed:**



- **10Mbps:** The selected BASE-T port is operating with a 10Mbps speed
- **100Mbps:** The selected BASE-T port is operating with a 100Mbps speed
- **1Gbps:** The selected BASE-T port is operating with a 1Gbps speed
- **Auto:** The selected BASE-T port is operating in auto-negotiation


**TX:** The decimal value of sent octets on this port along with the graph

**RX:** The decimal value of received octets on this port along with the graph

**Link drops:** The decimal value of the number of times the link was dropped on the connected ports along with the graph

#### Inner/Outer VLAN:

In this section, the user can change and add settings about VLANs. Depending on the selection made in [Global Configuration](#), the user can configure Inner or Outer VLANs.

 The switch cannot be enabled to configure inner and outer VLAN tags at the same time. So, at one point in time, only one of the two settings between [VLAN \(inner VLAN\)](#) and [Double Tagging \(outer VLAN\)](#) can be selected.

**Default VLAN ID:** The user can define one hexadecimal value between 0x2 and 0xFFF. Incoming traffic is single-tagged with this value, if not already tagged. If the traffic comes with a tag, the VLAN ID is not overwritten.

 VLAN ID 0x01 is used internally so it cannot be used.

**Egress VID policy:** The user can select what should be done with the traffic once it is ready to be egressed out of the port. There are several options.

- **Allow all:** Allow all the traffic to be egressed by this port
- **Allow membership list:** Allow only the traffic that is tagged with VLANs present in the membership list
- **Allow all but membership list:** Allow all traffic except the ones that are tagged with VLANs present in the membership list

**VLAN membership list:** The user can input any values between 0x2 and 0xFFF. These values can be defined separated by "," [E.g.: 100, 101, EDF, ...]. A range of VLANs can be defined using the character "-". [E.g. 100-105]. Outgoing traffic is allowed to egress the switch on this port if the data is tagged with one of the defined VLAN-IDs

#### Egress VID remarking:

- **As received in the input port:** The tags on VLAN IDs mentioned in the VLAN membership list are kept as received on the ingress

- **Removed:** The tags on VLAN IDs mentioned in the VLAN membership list are removed on the egress
- **Normalized:** If the packet is received without a VLAN tag, at egress, it is tagged with the default VLAN in the ingress port of the packet. If it is received with a VLAN tag, act as the option, [as received in the input port](#).
- **Custom:** The VLANs mentioned in [the VLAN egress removed list](#) are removed while the VLANs mentioned in [the VLAN egress normalized list](#) are forced.

**Port Segmentation:** The section allows the user to add ports to create segments

**Selected Ports:** The user can mention ports here that are desired to be part of the segments. The user can select which ports the packets ingressed on this port can be forwarded to the allowed egress ports. More information can be found in the chapter on Port segmentation.

**Limit the egress bandwidth on this port:** This feature allows the user to limit the overall output bandwidth of the selected port. Traffic shaping can be set up to limit the bandwidth using the payload of layers 1 to 3 (OSI Model Layers). The following three options can be selected for traffic shaping.

- **Count Layer 1 bytes:** When selected the user can limit traffic starting from the first byte of a frame (from intergap to CRC).
- **Count Layer 2 bytes:** When selected the user can limit traffic starting after the header of the Data link layer (Layer 2) of a frame (from Destination MAC to end of payload).
- **Count Layer 3 bytes:** When selected the user can limit traffic starting after the header of the network layer (Layer 3) of a packet (only the ethernet payload).
- **Maximum bandwidth (kbps):** The user can define the bandwidth to limit in kbps. The range of this field is between 64kbps to 1000000kbps. More information can be found in the chapter for bandwidth reservation.

**Enable jumbo frames on this port:** This feature allows the user to enable or disable the reception of jumbo frames on the selected port.

- When the option is disabled the maximum transmission unit (MTU) is 2026 Bytes
- When the option is enabled the maximum transmission unit (MTU) is 10218 Bytes



When Jumbo frames are enabled all time-aware functions of the switch are affected. This involves features like [TimeSync](#), [Ingress Rate Limiter](#), [Traffic Shaping](#), etc.

To identify any possible error in the cabling, the EES reports if a cable polarity inversion is detected. If the port is set to 100 Mbps polarity inversion can only be identified if the PHY is set as slave. If the port is set to 1Gbps polarity inversion can be identified

regardless of whether the role is master or slave. Once polarity inversion is detected the EES shows a sign in the top right corner of the port.

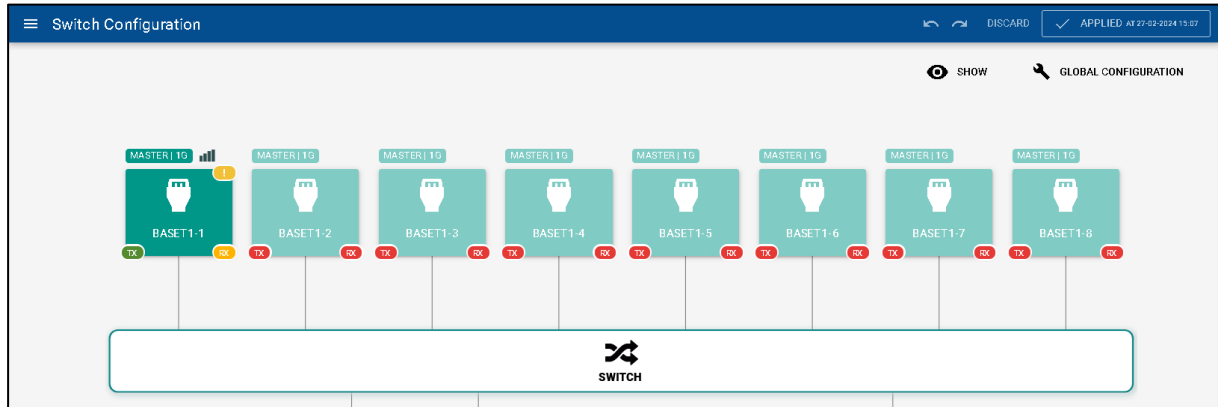


Figure 5-8 Polarity inversion detected

## 5.1.5 SFP+ Ports (4)

The switch is provided with 2 SFP+ ports that are capable of supporting the 10GBASE-R standard. Users can insert 10GBASE-T1 transceivers in these slots to operate these ports in 10Gbps mode.

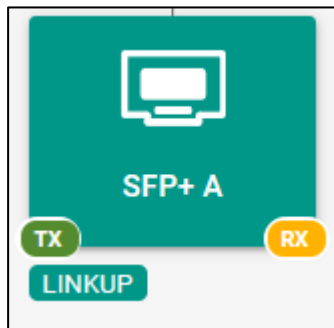


Figure 5-9 SFP+ Port Visualization

### 5.1.5.1 Port Statistics

The user can see the summary of the configuration of a port along with some statistics by placing the cursor on the desired port.

### 5.1.5.2 Port Configuration

The user can click on the desired port for configuration.

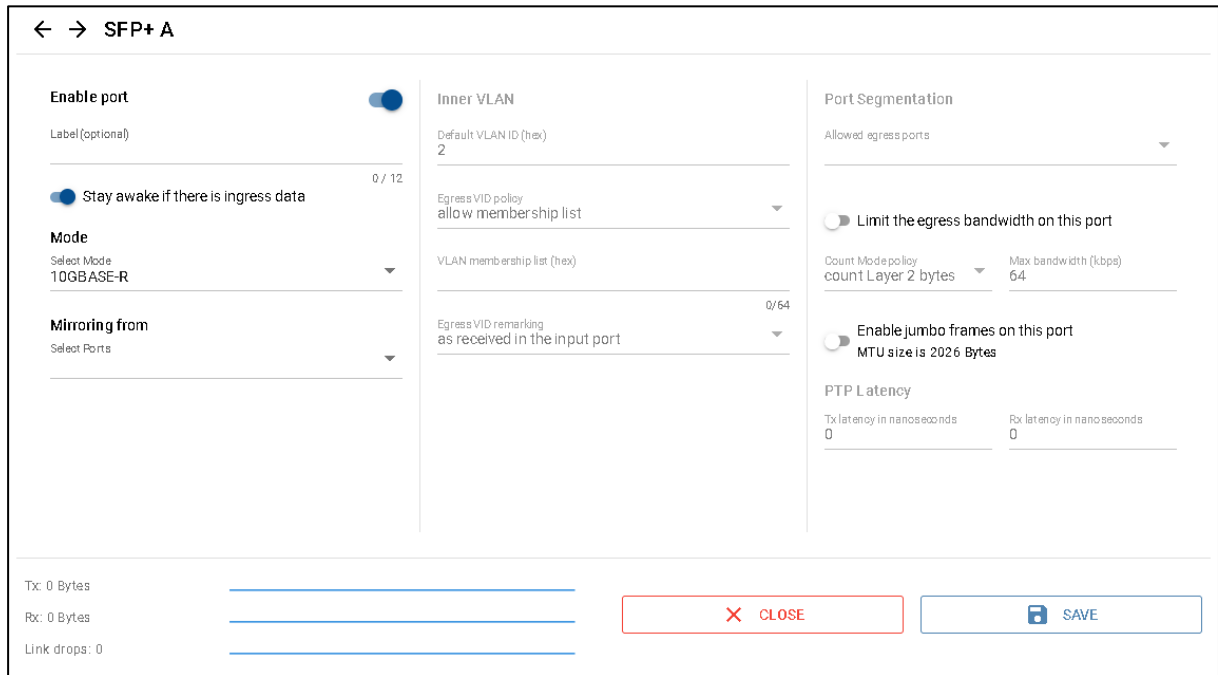


Figure 5-10 Configuration Menu for SFP+ A Port

**Enable Port:** The user can enable or disable the port. Once the port is disabled the color of the port is changed to grey.

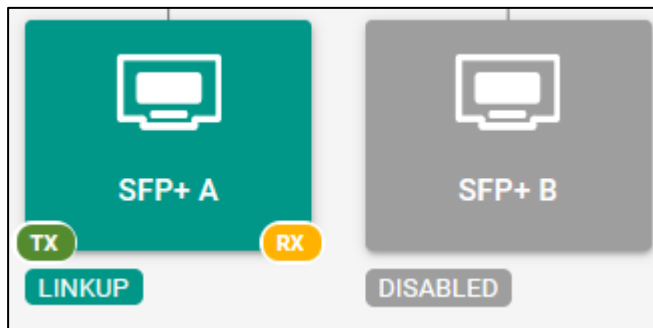


Figure 5-11 Disabled & Enabled Port

**Label:** The user can add a name for a particular port. A maximum of 12 characters can be used for the name.

**Stay awake:** When this option is enabled the Port stays up as long as there is traffic on the port

**Mode:**

- **SGMII:** This option needs to be selected when the SFP cages are equipped with 100/1000BASE-T1 SFPs.
- **10GBaseR:** This option needs to be selected when the SFP cages are equipped with 10G SFPs

➤ **Other modes:** Other modes are 1000BASE-X, 2500BASE-X, 5GBASE-R, and USXGMII.

**Mirroring from:** The following option can be used to mirror the traffic on the selected ports to the selected SFP+ port. All the traffic that is received on the ports added in the selected ports panel will be mirrored on the given SFP+ port.

**TX:** The decimal value of sent octets on this port along with the graph.

**RX:** The decimal value of received octets on this port along with the graph.

**Link drops:** The decimal value of the number of times the link was dropped on the connected ports along with the graph.

#### Inner/Outer VLAN:

In this section, the user can change and add settings about VLANs. Depending on the selection made in [Global Configuration](#), the user can configure Inner or Outer VLANs.

**i** The switch cannot be enabled to configure inner and outer VLAN tags at the same time. So, at one point in time, only one of the two settings between [VLANs \(inner VLAN\)](#) and [Double Tagging \(outer VLAN\)](#) can be selected.

**Default VLAN ID:** The user can define one hexadecimal value between 0x2 and 0xFFF. Incoming traffic is single-tagged with this value, if not already tagged. If the traffic comes with a tag, the VLAN ID is not overwritten

**i** VLAN ID 0x01 is used internally so it currently cannot be used

**Egress VID policy:** The user can select what should be done with the traffic once it is ready to be egressed out of the port. There are several options.

- **Allow all:** Allow all the traffic to be egressed by this port
- **Allow membership list:** Allow only the traffic that is tagged with VLANs present in the membership list
- **Allow all but membership list:** Allow all traffic except the ones that are tagged with VLANs present in the membership list

**VLAN membership list:** The user can input any values between 0x2 and 0xFFF. These values can be defined separated by “,” [E.g.: 100, 101, EDF, ...]. A range of VLANs can be defined using the character “-”. [E.g. 100-105]. Outgoing traffic is allowed to egress the switch on this port if the data is tagged with one of the defined VLAN-IDs

#### Egress VID remarking:

- **As received in the input port:** The tags on VLAN IDs mentioned in the VLAN membership list are kept as received on the ingress

- **Removed:** The tags on VLAN IDs mentioned in the VLAN membership list are removed on the egress
- **Normalized:** If the packet is received without a VLAN tag, at egress, it is tagged with the default VLAN in the ingress port of the packet. If it is received with a VLAN tag, act as the option, [as received in the input port](#).
- **Custom:** The VLANs mentioned in [the VLAN egress removed list](#) are removed while the VLANs mentioned in [the VLAN egress normalized list](#) are forced.

**Port segmentation:** The section allows the user to add ports to create segments

**Selected ports:** The user can mention ports here that are desired to be part of the segments. The user can select which ports the packets ingressed on this port can be forwarded to the allowed egress ports. More information can be found in the chapter on Port segmentation.

**Limit the egress bandwidth on this port:** This feature allows the user to limit the overall output bandwidth of the selected port. Traffic shaping can be set up to limit the bandwidth using the payload of layers 1 to 3 (OSI Model Layers). The following three options can be selected for traffic shaping.

- **Count Layer 1 bytes:** When selected the user can limit traffic starting from the first byte of a frame (from intergap to CRC).
- **Count Layer 2 bytes:** When selected the user can limit traffic starting after the header of the Data link layer (Layer 2) of a frame (from Destination MAC to end of payload).
- **Count Layer 3 bytes:** When selected the user can limit traffic starting after the header of the Network layer (Layer 3) of a packet (only the Ethernet payload).
- **Maximum bandwidth (kbps):** The user can define the bandwidth to limit in kbps. The range of this field is between 64kbps to 1000000kbps More information can be found in the chapter for bandwidth reservation.

**Enable jumbo frames on this port:** This feature allows the user to enable or disable the reception of jumbo frames on the selected port.

- When the option is disabled the maximum transmission unit (MTU) is 2026 Bytes
- When the option is enabled the maximum transmission unit (MTU) is 10240 Bytes



When Jumbo frames are enabled all time-aware functions of the switch are affected. This involves features like [TimeSync](#), [Ingress Rate Limiter](#), [Traffic Shaping](#), etc.

**PTP Latency:** This is an expert option for the user to compensate PTP latencies of the used SFP modules. These latencies have to be provided by the SFP manufacturer.

## 5.1.6 CPU port (5)

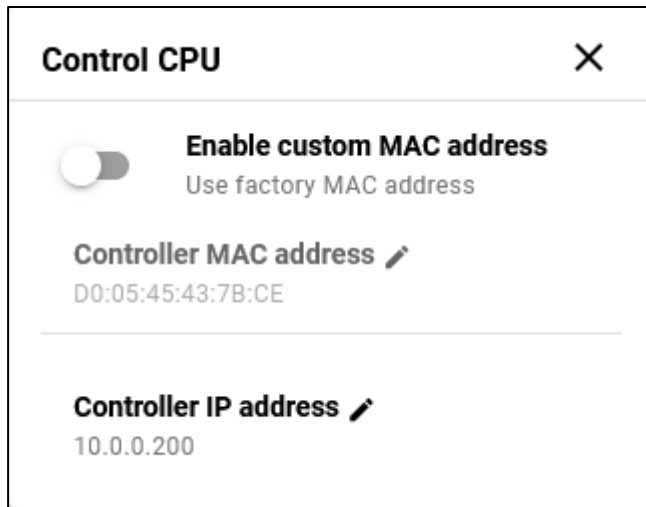



Figure 5-12 Control CPU

This port allows the user to change the MAC Address and the IP Address of the switch. Technica assigns a unique MAC address to each device. If this MAC address needs to be changed, the custom MAC address toggle must be enabled and then the Controller MAC Address field must be populated with the new MAC address. The factory MAC address is never lost, so disabling the custom MAC address toggle will force the device to ignore the controller MAC address entered and use the factory MAC address.

By default, the IP address is 10.0.0.200.

-  The MAC and IP Address can also be changed in the [NETWORK DETAILS](#) (See [CHAPTER 5.2.6.1](#) section of the [SYSTEM INFORMATION TAB](#)).

## 5.1.7 Control port (6)

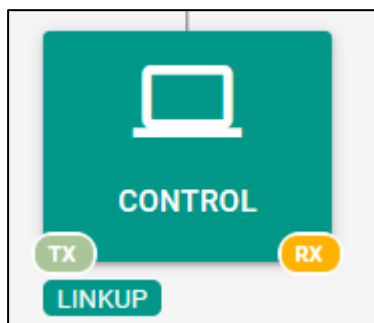


Figure 5-13 Enabled Control Port

The user can click on the desired port for configuration.

### 5.1.7.1 Port statistics

The user can see the summary of the configuration of a port along with some statistics by placing the cursor on the desired port.

### 5.1.7.2 Port configuration

The user can click on the desired port for configuration.

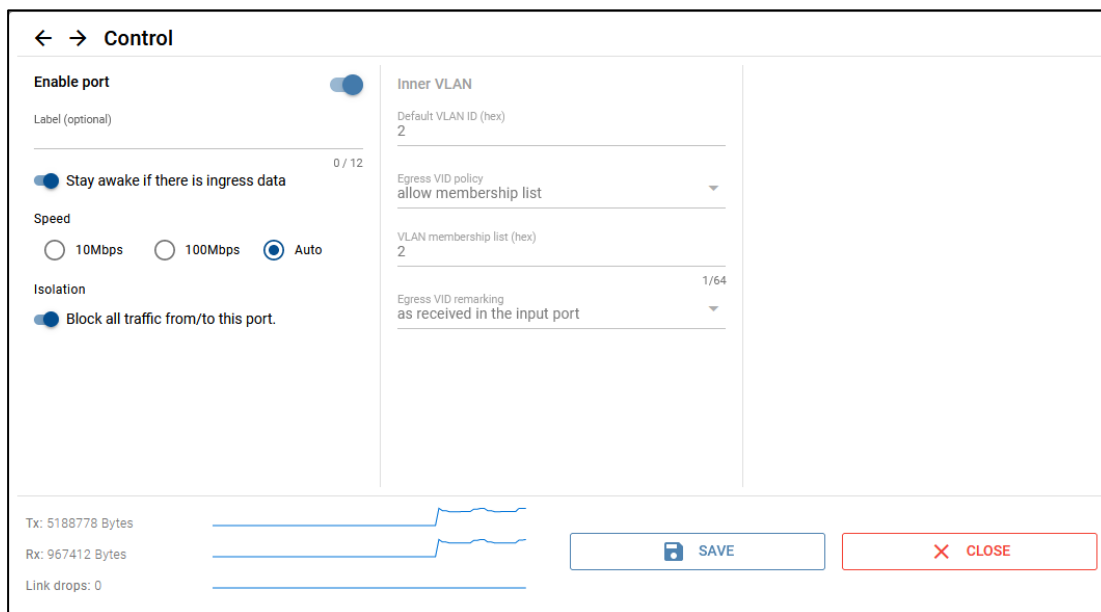


Figure 5-14 Configuration Menu for Control Port

**Enable Port:** This port cannot be disabled because this port is used for the configuration of the device.

**Label:** The user can add a name for a particular port. A maximum of 12 characters can be used for the name.

**Stay awake:** When this option is enabled the Port stays up if there is traffic on the port.

**Speed:**

- 🔄 **10Mbps:** The selected 100BASE-TX configuration port is operating with 10Mbps speed
- 🔄 **100Mbps:** The selected 100BASE-TX configuration port is operating with 10Mbps speed
- 🔄 **Auto:** The selected 100BASE-TX configuration port is operating in auto-negotiation mode

**Isolation:**



This option can be used to isolate traffic to or from the configuration port to the rest of the ports of the switch


**TX:** The decimal value of sent octets on this port along with the graph.

**RX:** The decimal value of received octets on this port along with the graph.

**Link drops:** The decimal value of the number of times the link was dropped on the connected ports along with the graph.

#### Inner/Outer VLAN:




In this section, the user can change and add settings about VLANs. Depending on the selection made in [Global Configuration](#), the user can configure Inner or Outer VLANs.

 The switch cannot be enabled to configure inner and outer VLAN tags at the same time. So, at one point in time, only one of the two settings between [IEEE 802.1q mode \(inner VLAN\)](#) and [Double Tagging \(outer VLAN\)](#) can be selected.

**Default VLAN ID:** The user can define one hexadecimal value between 0x2 and 0xFFFF. Incoming traffic is single-tagged with this value, if not already tagged. If the traffic comes with a tag, the VLAN ID is not overwritten.



 VLAN ID 0x01 is used internally so it currently cannot be used.

**Egress VID policy:** The user can select what should be done with the traffic once it is ready to be egressed out of the port. There are several options.

-  **Allow all:** Allow all the traffic to be egressed by this port
-  **Allow membership list:** Allow only the traffic that is tagged with VLANs present in the membership list
-  **Allow all but membership list:** Allow all traffic except the ones that are tagged with VLANs present in the membership list

**VLAN membership list:** The user can input any values between 0x2 and 0xFFFF. These values can be defined separated by “,” [E.g.: 100, 101, EDF, ...]. A range of VLANs can be defined using the character “-”. [E.g. 100-105]. Outgoing traffic is allowed to egress the switch on this port if the data is tagged with one of the defined VLAN-IDs

#### Egress VID remarking:

-  **As received in the input port:** The tags on VLAN IDs mentioned in the VLAN membership list are kept as received on the ingress
-  **Removed:** The tags on VLAN IDs mentioned in the VLAN membership list are removed on the egress

- **Normalized:** If the packet is received without a VLAN tag, at egress, it is tagged with the default VLAN in the ingress port of the packet. If it is received with a VLAN tag, act as the option, [as received in the input port](#).
- **Custom:** The VLANs mentioned in [the VLAN egress removed list](#) are removed while the VLANs mentioned in [the VLAN egress normalized list](#) are forced

## 5.1.8 Switch

This tab is used to configure the switch. The various functions offered by the Enhanced Ethernet Switch can be configured and modified graphically using this tab.

### 5.1.8.1 Port segmentation

This sub-tab is used to isolate the subsets of ports. When this option is enabled in [Global configuration](#) ( See [CHAPTER 5.1.3](#)), the user can create subsets where the user can allow the traffic ingressed to be egressed only out of the mentioned ports. This way traffic on some ports can be isolated from other ports. For example, in [FIGURE 5-15](#) Port Segmentation a port segment is created between BASET1-4 and BASET1-5. The traffic ingressed on BASET1-4 can only be egressed to BASET1-5. In case bi-directional isolation is needed BASET1-5 must enable BASET1-4, that way the traffic ingressed on BASET1-5 can be egressed on BASET1-4 as well as establishing a bi-directional isolation tunnel for the traffic exchanged on these two ports. The user must connect both ports but if “Edit Symmetrically” is enabled, the device automatically selects the other way when a connection is enabled.

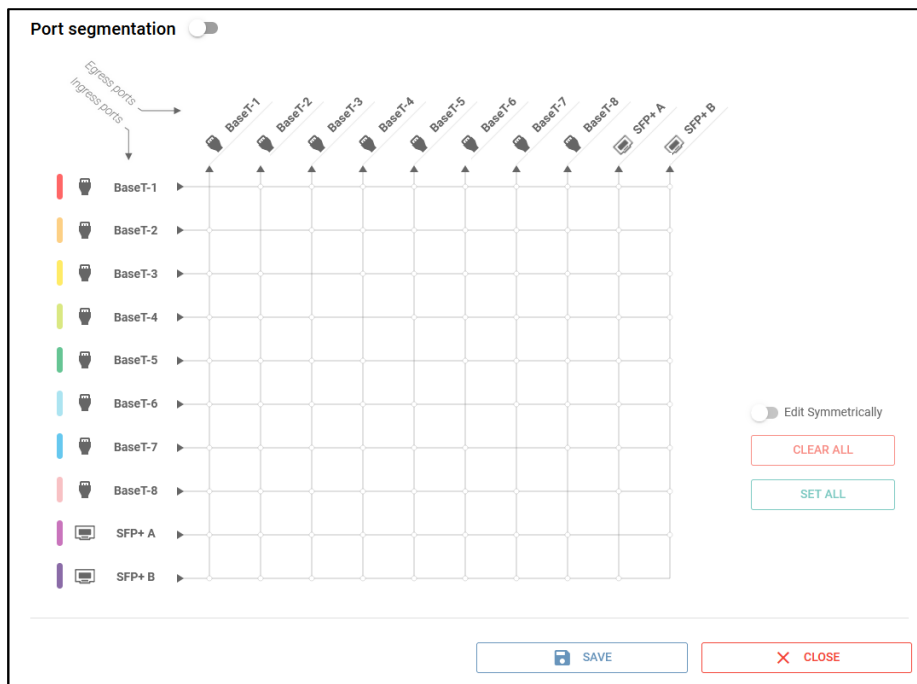
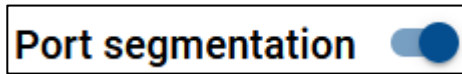
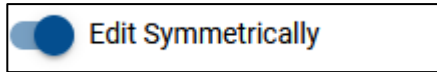


Figure 5-15 Port Segmentation

The following options can be found in this tab:



Enables the feature port segmentation



Enables bi-directional communication between port segments. Disabling this option creates only one-way port segments



Deletes all the configured port segments



Create port segments between all ports



Port segmentation can work alongside VLANs. However, it is not possible to override port segmentation by VLAN configuration. Port segmentation has more priority over VLAN configuration.

### 5.1.8.2 Address resolution table

This sub-tab is used to display the mapping of MAC addresses to the physical ports.

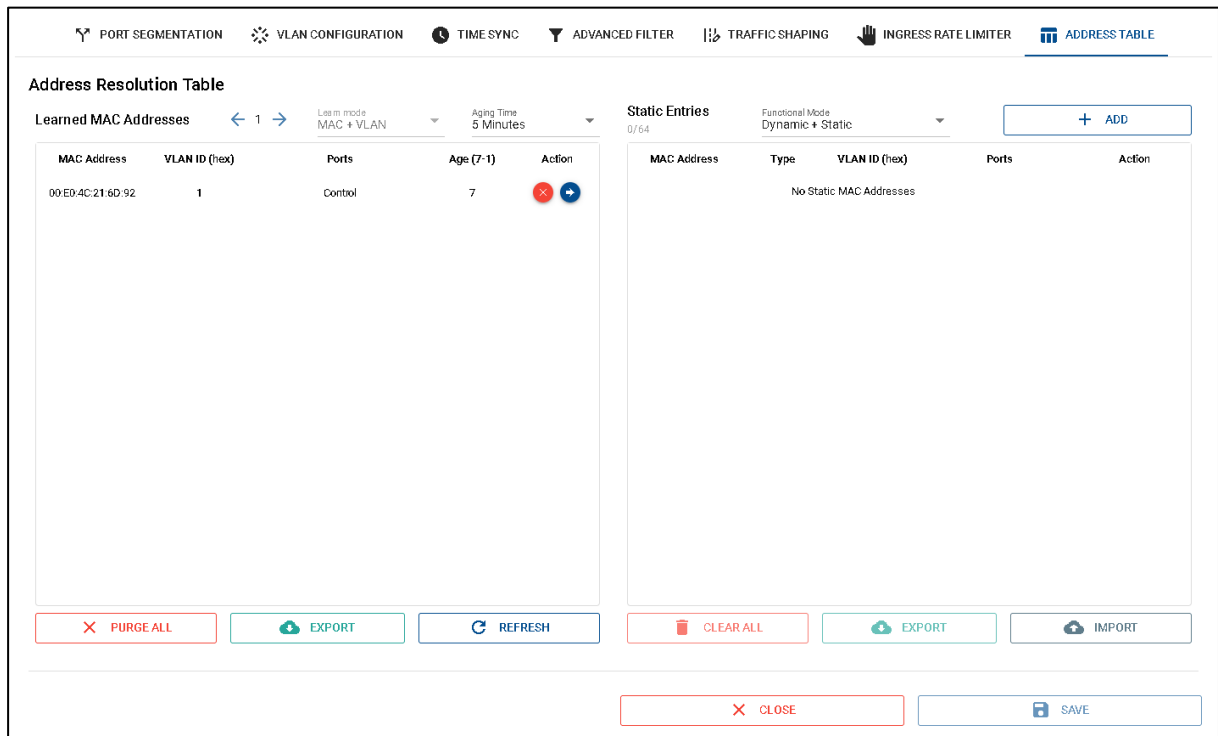






Figure 5-16 Address Resolution Table


The left-hand side shows a table of [Learned MAC Addresses](#). When the VLAN mode is enabled, the user has the choice how the [Learn mode](#) will learn the MAC Addresses for the table. Either the MAC Address will be learned together with the VLAN or the table can learn only the MAC Address. The user can select the [aging time](#) to specify for how long the switch wants to remember the corresponding MAC address. If the aging time is “disabled” the switch never forgets all learned MAC addresses. The following buttons can be used in the section of [Learned MAC Addresses](#).


 Opens a dialog to create a new static MAC entry using the learned MAC address information

 Deletes the corresponding entry


 Deletes all the entries in the Learned MAC Address table


 The learned table can be exported to the connected PC


 Refreshes the table for new entries or removes expired entries


The right-hand side shows a table of manually added Static (and Dynamic) entries. The user can select the functional mode of the address resolution table to [static+dynamic](#) or only static entries. Up to 64 static entries can be added by the user in this table. To add the entries the user can select  and input the MAC address and port manually.


The following buttons can be used in the section of [Static Entries](#).

 Enables the user to create or edit a new entry for mapping between the MAC address and the port

 Enables the user to clone an existing entry for mapping between the MAC address and the port

 Deletes the corresponding entry

 Deletes all the entries in the Learned MAC Address table

 The learned table can be exported to the connected PC



The learned table can be imported from the connected PC

**i** The tables can be imported or exported in .json format

**i** While adding an entry in the addressing resolution table, ingress VLANs can be used to distinguish packets from different endpoints that have the same MAC addresses but different VLANs.

### 5.1.8.3 VLAN configuration

| VLAN ID | BaseT-1          | BaseT-2          | BaseT-3          | BaseT-4          | BaseT-5          | BaseT-6          | BaseT-7          | BaseT-8          | SFP+ A           | SFP+ B           | Action |
|---------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|--------|
| 10      | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | +      |
| 20      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | Not Allowed      | +      |
| 30      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | Tag Removed      | +      |
| 40      | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | Tag Normalized   | +      |

Figure 5-17 Configuration of VLANs

If **VLAN (inner VLAN)** is enabled port-based single VLANs are activated. In this mode, the forwarding of frames through the Enhanced Ethernet Switch is defined by the configuration on each port. Users can also make these configurations using this sub-tab. This sub-tab shows all the ports with the ability to different processing mechanisms based on the selection made for egress. The sections of this sub-tab are described below

| VLAN ID | BaseT1-1         | BaseT1-2         | BaseT1-3         | BaseT1-4         | BaseT1-5         | BaseT1-6         | BaseT1-7         | BaseT1-8         | SFP+ A           | SFP+ B           | Action |
|---------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|--------|
|         | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership | Allow Membership |        |

Figure 5-18 Egress VID Policy

The options mentioned in [Figure 5-18 Egress VID Policy](#) provide the same parameters to be configured as in the individual port configuration for VLANs under the field Egress VID Policy (See [CHAPTER 5.1.4.2](#)). The user can select between the following options:

- [Allow all](#): Allow all the traffic to be egressed by this port
- [Allow membership list](#): Allow only the traffic that is tagged with VLANs present in the membership list
- [Allow all but membership list](#): Allow all traffic except the ones that are tagged with VLANs present in the membership list



When a new VLAN is added using the button above, the user can select what should be done with the mentioned VLAN while egressing out of the corresponding port. The options mentioned in [Figure 5-19 Egress VID remarking](#) can also be configured inside the individual ports (See [CHAPTER 5.1.4.2](#)) under the field [Egress VID remarking](#).

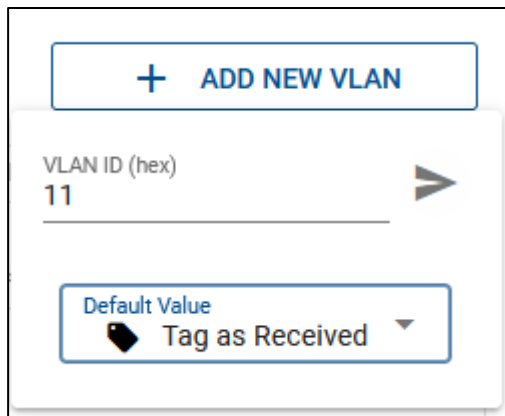


Figure 5-19 Egress VID remarking

The user can select between the following options:

- [As received in the input port](#): The tags on VLAN IDs mentioned in the VLAN membership list are kept as received on the egress
- [Removed](#): The tags on VLAN IDs mentioned in the VLAN membership list are removed on the egress
- [Normalized](#): If the traffic is not received with an Outer VLAN then place a tag on the traffic on egress. If it is received with a tag, act as the option, as received in the input port.
- [Custom](#): The VLANs mentioned in [the VLAN egress removed list](#) are removed while the VLANs mentioned in [the VLAN egress normalized list](#) are kept

These options can be edited using the panel shown in [Figure 5-20 Egress VID remarking editing](#) editing from one option to another.



Figure 5-20 Egress VID remarking editing

The following buttons can be used in the section



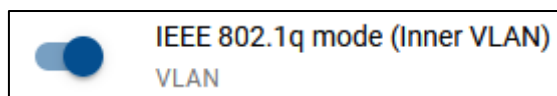
Enables the user to clone a setting (egress VID policy) for a new VLAN ID



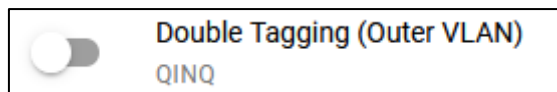
Deletes the corresponding entry



Applies to the corresponding entry



When enabled user can configure the inner tag of VLANs (802.1q)



When enabled user can configure the outer tag of VLANs( 802.1q-in-q)



Enables the user to add a new VLAN



Deletes all the configured VLANs



The switch cannot be enabled to configure inner and outer VLAN tags at the same time. So at one point in time, only one of the two settings [VLAN \(inner VLAN\)](#) and [Double Tagging \(outer VLAN\)](#) can be selected.

#### 5.1.8.4 Advanced filter

This sub-tab provides extended flexibility by defining filters for the received traffic.

The user can define a filter rule via



It allows the user to inspect the content of the packet. Depending on the content of the packet the user can trigger some actions.

**Ingress filter match:** The user must choose the ingress ports here. Specific conditions can be defined to inspect the type of traffic ingressed through these ports. Ingress filters can work in two modes.

- Normal mode
- Expert Mode

#### Normal mode:

In normal mode, the following options are available for ingress traffic.

Is the frame double-tagged? When enabled the ingress traffic inspects the outer tag (802.1q-in-q).

**i** Double tagging must be enabled in the [Global Configuration](#)

**i** Users can select the attributes of inspection for ingress traffic. Users can also select the **AND** operator to combine more than one rule for filtering the traffic. Attributes for a protocol like Ethernet, IPv4, IPv6, and ARP can be selected. The following attributes can be used for inspection.


|                                |
|--------------------------------|
| Destination MAC                |
| Source MAC                     |
| Outer VLAN PCP                 |
| Outer VLAN DEI                 |
| Outer VLAN ID                  |
| Inner VLAN TPID                |
| Inner VLAN PCP                 |
| Inner VLAN DEI                 |
| Inner VLAN ID                  |
| EtherType or Length            |
| IP version (IPv4 / IPv6)       |
| IPv4 Internet Header Length    |
| IPv4 TTL                       |
| IPv4 Protocol                  |
| IPv4 Source address            |
| IPv4 Destination address       |
| ARP Operation                  |
| ARP Sender Hardware Address    |
| ARP Sender Protocol Address    |
| ARP Receiver Hardware Address  |
| ARP Receiver Protocol Address  |
| IPv6 Source Address            |
| IPv6 Destination Address       |
| IPv6 NDP Solicitation Address  |
| IPv6 NDP Advertisement Address |
| IPv6 NDP Operation             |
| IPv6 Next Header               |
| IEEE1722 AVTP Header Type      |
| IEEE1722 AVTP Protocol Subtype |
| IEEE1722 AVTP Stream ID valid  |
| IEEE1722 AVTP Stream ID        |
| TECMP Device ID                |
| TECMP Message Type             |
| TECMP Data Type                |



|                      |
|----------------------|
| TECMP Interface ID   |
| UDP Source Port      |
| UDP Destination Port |
| TCP Source Port      |
| TCP Destination Port |





### Expert mode:


The user can define a filter based on any Byte that is received on the ingress port within the first 96 Bytes. The user can click on the Byte that needs to be inspected for filtering and define an **Offset**, **Data**, and **Mask**.

 Two 48Bytes rules are not the same as 96 Byte rule

### Egress action:

The user can define an action to be implemented on the traffic received on the ports selected in the **ingress filter match** section. The following actions can be performed:

-  **Mirror**: Mirror the packets to other ports
-  **Drop at egress**: Drop the packets at egress
-  **Force output port**: Allows modifying the normal forwarding and forces a new egress port for the traffic
-  **Avoid further filtering**: Allows to mirror everything except a particular kind of traffic.

 The field **Mask** in **Ingress filter match** specifies which bits in the **Value** field should matter. Users can input “1”s and “0”s in this field where 1 means the corresponding bit in the **Value** field stays the same and 0 means the corresponding bit in the **Value** field could be a “don’t care” value.

**Select the bound TCAM Flow ID**: The user can define a filter for FlowIDs described in the **ingress rate limiter** (See **CHAPTER5.1.8.7**)

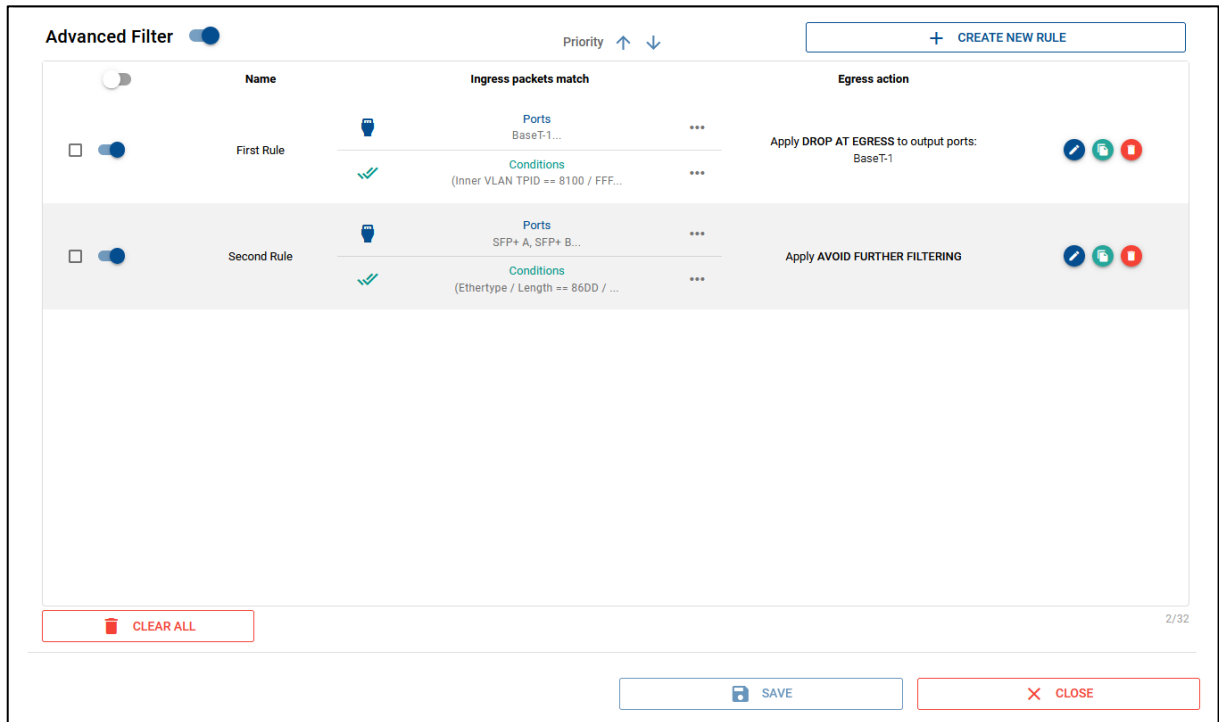


Figure 5-20 Advanced Filter

### 5.1.8.5 Traffic Shaping

This is a licensed feature. This sub-tab enables the user to fully configure the traffic shaping options that the EES provides.

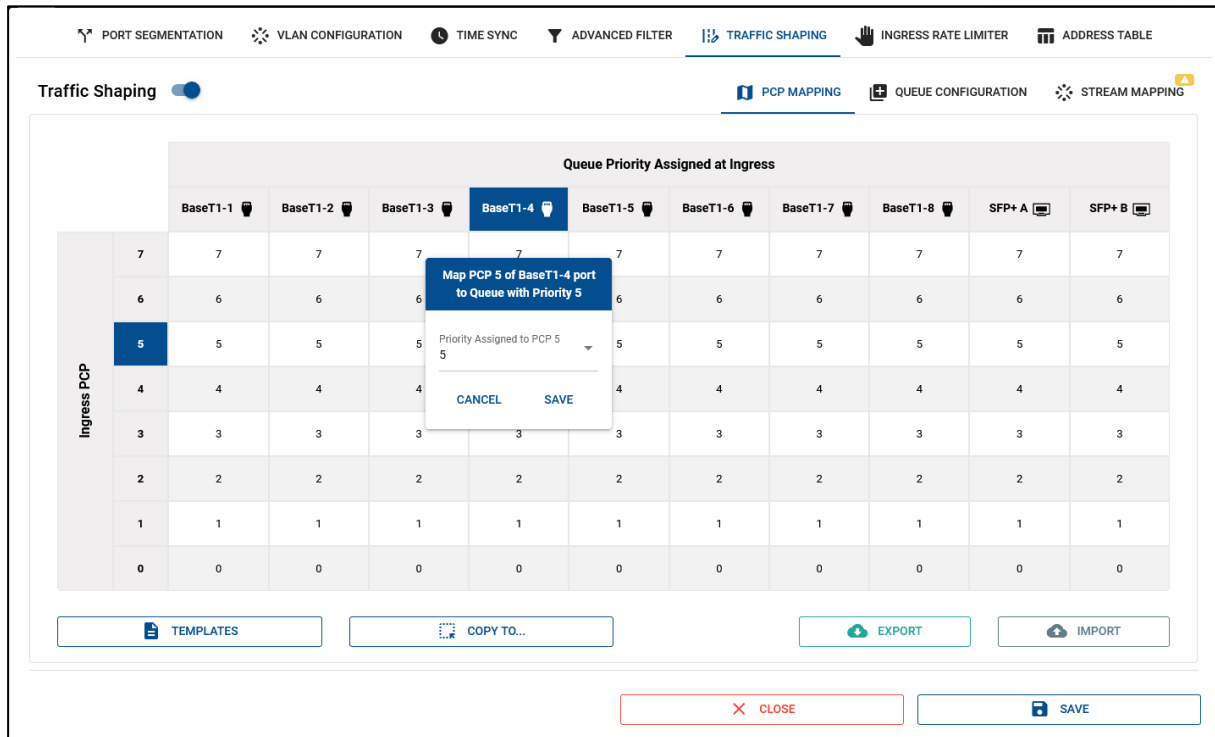


Figure 5-21 Traffic Shaping. PCP Mapping View

The first tab of this function, "PCP MAPPING", configures the carrier priority mapping of the PCP field in the VLAN header. On entry, when a packet arrives at the switch, each packet is assigned a priority from 0 to 7, where 7 corresponds to the highest priority. The switch uses the PCP to assign a different priority depending on the value of the PCP field. The default configuration provides a one-to-one mapping of PCP to priority, but a different mapping can be configured. Clicking on a cell brings up a dialog box that allows to assign a different queue priority on the corresponding port and PCP value.

The template button offers a couple of pre-configured mapping:

- The Default template that maps one-to-one the PCP to priority (the default configuration)
- An AVB template that sets a predefined mapping typically used in AVB scenarios.

It is also possible to copy the assignments of a selected port to other ports using the Copy to .... option.

Exporting and importing of mappings is possible using the corresponding buttons on the configuration window.

Untagged frames will be assigned to the priority 0.

**Traffic Shaping**

PCP MAPPING **QUEUE CONFIGURATION** STREAM MAPPING

|                |   | Credit Based Shaper Bandwidth Assigned at Egress |          |          |          |          |          |          |          |        |        |
|----------------|---|--------------------------------------------------|----------|----------|----------|----------|----------|----------|----------|--------|--------|
|                |   | BaseT1-1                                         | BaseT1-2 | BaseT1-3 | BaseT1-4 | BaseT1-5 | BaseT1-6 | BaseT1-7 | BaseT1-8 | SFP+ A | SFP+ B |
| Queue Priority | 7 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 6 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 5 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 4 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 3 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 2 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 1 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |
|                | 0 | ----                                             | ----     | ----     | ----     | ----     | ----     | ----     | ----     | ----   | ----   |

CLEAR ALL COPY TO... EXPORT IMPORT

CLOSE SAVE

Figure 5-21 Traffic Shaping. Queue Configuration view

Based on the priority assigned at ingress according to the configuration done in the [PCP Mapping](#) window, the packet is pushed to the corresponding queue of the Egress port.

Each queue output has its own Credit Based Shaper (CBS) that can be configured by clicking onto the field. Here the [CBS](#) can be enabled and a [CBS Bandwidth](#) can be configured.

The scheduler reads the packets from the queues following a "strict" policy, no packets will be sent from a queue if there are packets pending to be sent in a queue of higher priority.

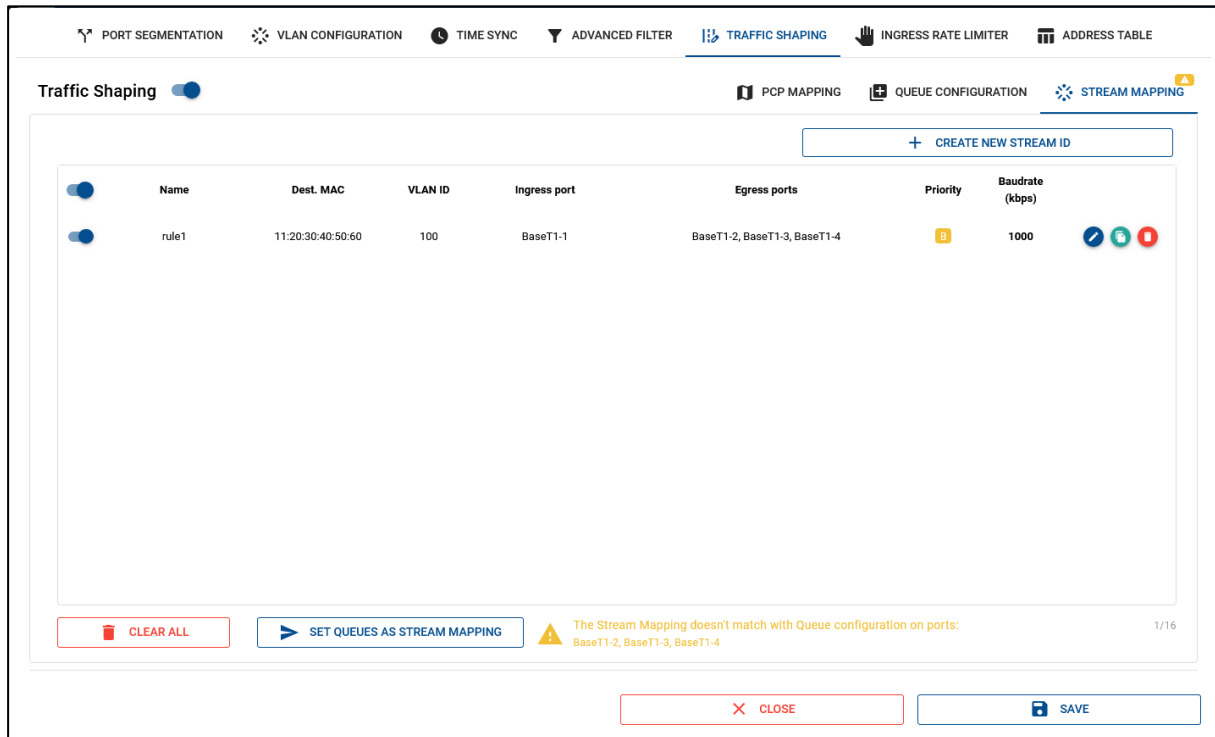



Figure 5-22 Traffic Shaping. Stream Mapping view.

For this feature the VLAN Mode needs to be enabled. A notification will inform the user about this necessity.

The Stream mapping view allows to define several streams within the switch. A stream is identified by its ingress port, its destination MAC address and its VLAN ID. For each defined flow, it is necessary to configure the ports over which the packets will be forwarded, the class A or B where A is a higher priority (a reference to the standard 802.1qat) than B and the maximum bandwidth assigned to. The user can

add their own desired values of bandwidth by clicking on , where the user can input Max Payload Size in Bytes, Frame overhead, and Max Frames per Interval. For 1000BASE-T1 ports, the maximum limit is 1000Mbps and for SFP+ ports the maximum limit is 10Gbps, respectively.

The user can define multiple stream reservation rules via [+ Create New Stream ID](#).

Once the flows have been defined, it is necessary to translate their configuration into an appropriate Queue Configuration. If the current Credit Base Shaper configuration is not able to match the stream configuration, a warning will be displayed to the right of the SET QUEUES AS STREAM MAPPING button. The SET QUEUES AS STREAM MAPPING button allows transferring the stream mapping configuration to the queue configuration in two different modes:

- Replace the Queue Configuration according to Stream Mapping: In this mode the CBS of the queues will be replaced to match exactly the configuration on the Stream Mapping.
- Adjust the Queue Configuration to accommodate the Stream Mapping: In this mode the CBS of the queues will be only modified if the bandwidth is not enough to fit all the streams configured.

### 5.1.8.6 TimeSync

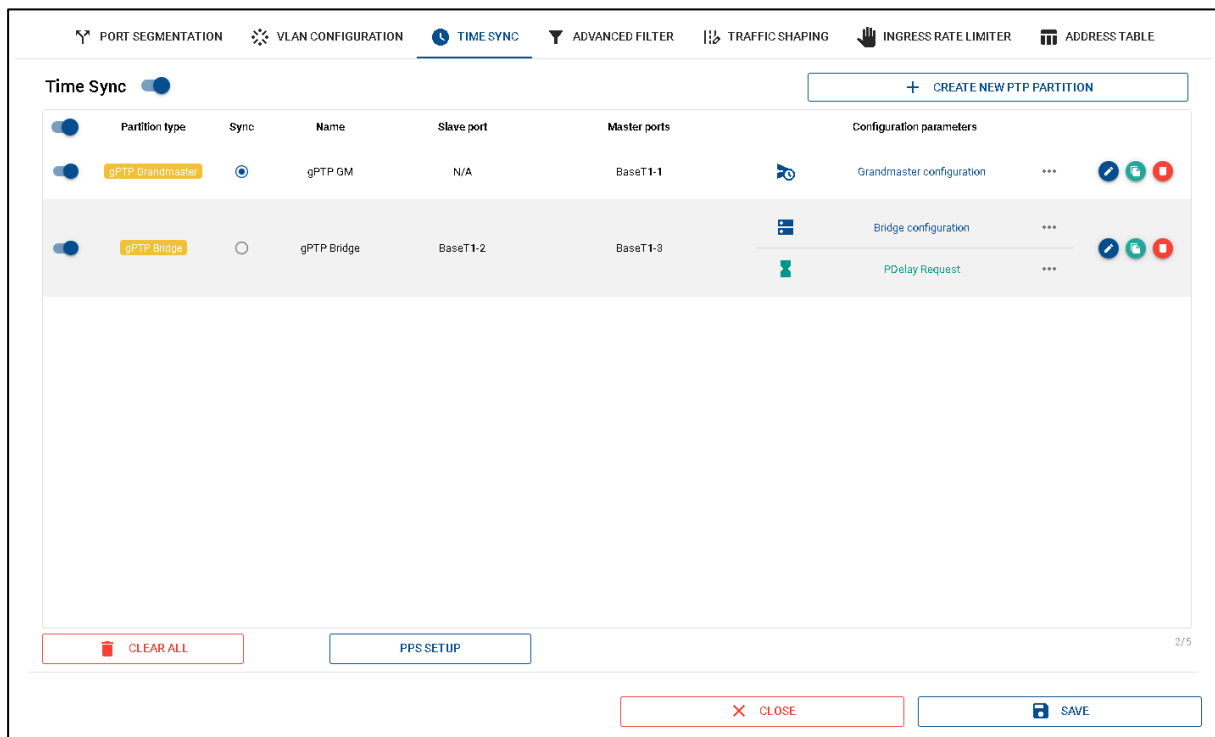


Figure 5-24 TimeSync configuration

To adopt an open approach for the configuration of time synchronization Technica Engineering developed its PTP stack. The implemented stack follows the gPTP standard from AVNU Alliance and also includes the IEEE1588-2008 standard. Using this stack, the user can define more than one bridge slave port per switch. This is achieved in the switch using partitioning inside the switch. The partitioning enables the user to divide the ports of a switch into multiple sections. Each section is an independent partition. The synchronization information received in one partition stays in the same partition. Each partition contains a set of ports. These ports can be Grand Master, Bridge Master, or Bridge Slave. A port can only be assigned to one partition at a time. Up to 5 partitions can be set in the switch. For Grandmaster partitions (gPTP or PTPv2) the switch provides the option of PPS output. When clicking on the **PPS Setup** and enabling the **Pulse Per Second output** the user can configure the **PPS out signal width**. The user can choose between 1, 10 or 100 milliseconds width.

## Concept

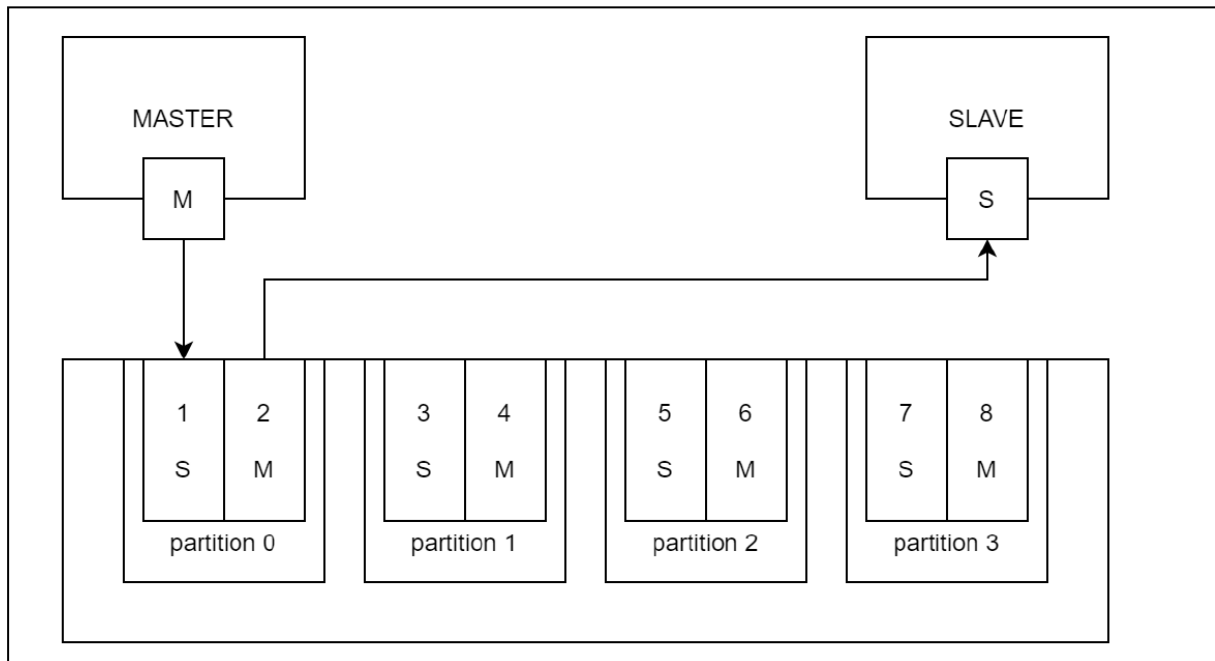


Figure 5-25 Time Sync Partitioning in EES

Five types of partitions can be defined in the switch.

- **Bridge Partition:** This forwards the synchronization information for the slave port to multiple master ports. Only one slave port per bridge can be configured while multiple master ports can be configured.
- **Grand Master Partition:** The synchronization is generated using the internal oscillator of the switch. The synchronization information can be distributed to multiple master ports.
- **PTPv2 to gPTP Bridge:** This is a licensed feature. The PTPv2 to gPTP bridge forwards synchronization information from the PTPv2 master node to several gPTP slave nodes
- **PTPv2 Grand Master Partition:** This is a licensed feature. The synchronization is generated using the internal oscillator of the switch. The synchronization information can be distributed to multiple master ports.
- **PTPv2 Transparent Clock:** This is a licensed feature. The PTPv2 Transparent Clock forwards synchronization information from the PTPv2 master node to several PTPv2 slave nodes.

**i** Time synchronization in multiple partitions of the switch is a licensed feature.

## Configuration

### Configuring Time Synchronization on the switch

In the sub-tab [TimeSync](#), the user can configure Time Sync partition(s).

[Set partition name](#): The user can name the partitions created in the switch.

[Select partition type](#): Here user can create either a Bridge partition or a Grand Master partition.

[Select transport layer](#): The user can choose the physical transporter layer for the partition. The transport layer can be selected between Ethernet (Layer 2) and IP4/UDP (Layer 3). (Only available for PTPv2 partitions)

[Select delay mechanism](#): The user can choose the delay mechanism for the partition. The path delay measurement can be selected between “End to End” and “Peer to Peer”. (Only available for PTPv2 partitions)

[Bridge partition](#): The following setting can be made in this mode.

[Select slave port \(only Bridge mode\)](#): Here the user can select the port that needs to be connected to the master so that the switch can be used as a bridge. Apart from the selection of the slave port on the switch. The user can enable/disable VLAN on the slave port. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for gPTP frames that are already tagged. The user can also enable/disable the forwarding of announce messages to the master ports. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

[Select master ports](#): Here the user can select the port that needs to be connected to the master ports so that the switch can be used as a bridge. Apart from the selection of the master ports on the switch. The user can enable/disable VLAN on the master ports. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for gPTP frames that are tagged. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

[Sync timeout counter on slave port](#): Here the user can define the number of sync messages between 1-5 that must be lost to consider a timeout event.

[Proxy operation \(only in Bridge mode\)](#):

If the synchronization is lost in the slave port, the bridge must enter “Proxy Mode” the master ports must keep sending synchronization using the latest valid information and updating it with its internal clock. When “Proxy Mode” is enabled, the user can define the following parameters.



- If the **Proxy operation** is set to true, the proxy operation will be triggered if the synchronization on the slave is lost
- If the **Proxy operation** is set to false, the partition will never jump to the proxy operation

#### Default Date / Time:

The date/time sent by master ports when working in proxy mode and no valid synchronization information has been received on the slave port

Users can configure other parameters for fine-tuning, but they have default values in case they are not changed. These parameters are:

- **Startup timeout (in seconds):** This is the wait time to jump to proxy mode if at startup the slave port does not receive any synchronization information

**Default Sync interval on master ports:** If proxy mode is enabled, then the default sync interval shows the synchronization message interval used on master ports until a valid synchronization is received on the slave port. The master port sends a message to synchronize. The interval for the synchronization message can be set here. The current selection offers the following choices.

- 31.25 milliseconds
- 62.5 milliseconds
- 125 milliseconds
- 250 milliseconds
- 500 milliseconds
- 1 second

**Initial PDelay Request configures (only in Bridge Mode):** The slave port sends a message to calculate path delay. The interval for a path delay request message can be set here. If 1 second is selected it means the slave port sends a path delay request every second until the system considers the measurements to be stable. Currently, the following selections can be made.

- 500 milliseconds
- 1 second
- 2 seconds
- 4 seconds
- 8 seconds

**Operational PDelay request interval:** After the system considers the measure of path delay request to be stable, the user can define an interval for transmitting path delay requests in this field. An operation path delay request enables the user to define a time for transmitting path delay requests after the system has achieved stability thus avoiding overloading the system with unnecessary path delay requests. The current selection offers four choices

- 500 milliseconds
- 1 second
- 2 seconds
- 4 seconds
- 8 seconds

**Grandmaster partition:** The following setting can be made in this mode:

**Select master ports:** Here the user can select the port that acts as PTP master(s). The user can enable/disable VLAN on the master port(s). Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for PTP frames that are tagged. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

**Sync interval period on master ports:** This defines the synchronization interval: The master port sends a message for synchronization. The interval for the synchronization message can be set here. The current selection offers the following choices.

- 31.25 milliseconds
- 62.5 milliseconds
- 125 milliseconds
- 250 milliseconds
- 500 milliseconds
- 1 second

**Initial Date / Time:** The date/time sent by master ports when it starts operating as grandmaster can be defined here.

**Initial Time, nanoseconds part:** The nanoseconds parts of the Initial Date/Time.

**Announce interval period on master ports:** This defines the announce message interval: The master port sends a message announce message. The interval for the announce message can be set here. The current selection offers the following choices.

- Disable announce message (default)
- 500 milliseconds
- 1 second
- 2 seconds
- 4 seconds
- 8 seconds

**UTC offset valid:** If enabled the flag “currentUtcOffsetValid” is set in the announce message.

**UTC offset in seconds:** The value set in the “currentUtcOffset” field of the announce message.

**Clock Priority 1, Clock Priority 2, Clock Class, Clock Accuracy, Clock Variance, and Time Source:** The values set in the “grandmasterPriority1”, “grandmasterPriority2”, “grandmasterClockQuality” and “timeSource” fields of the announce message.

**PTPv2 to gPTP bridge:**

- There is no support for BMCA (Best Master Clock Algorithm), neither in PTPv2 nor in gPTP.
- The PTPv2 port receives the synchronization, so it can only take the role of slave. The received information is forwarded to all gPTP ports defined in the partition, so these ports can only take the role of master.
- Only one PTPv2 port per partition. Up to 5 different partitions can be defined in the switch.

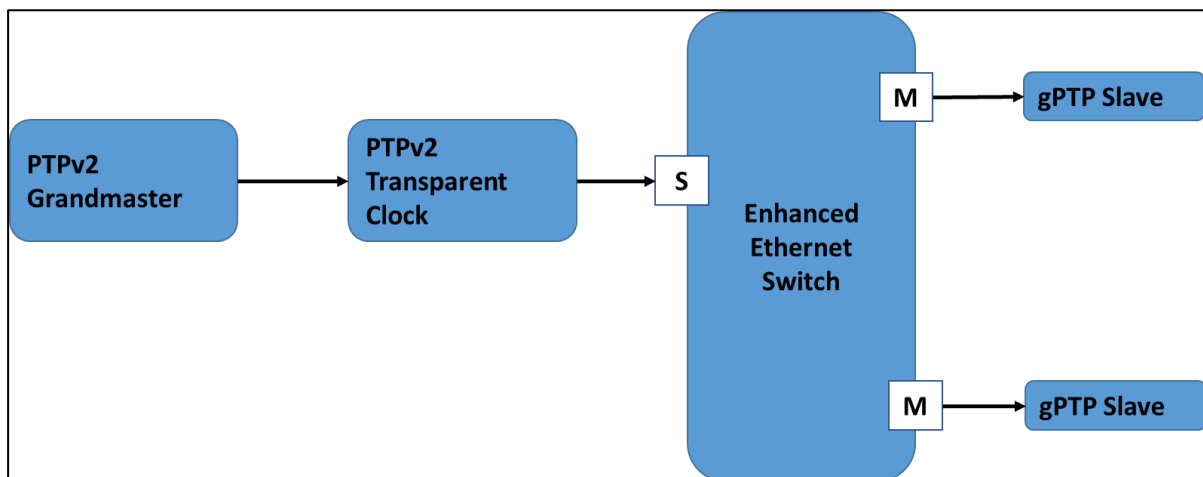


Figure 5-26 PTPv2 to gPTP Bridge

The following parameters can be configured for PTPv2 to gPTP Bridge:

**Select slave port (only Bridge mode):** Here the user can select the port that needs to be connected to the PTPv2 master so that the switch can be used as a bridge. Apart from the selection of the slave port on the switch, the user can enable/disable VLAN on the slave port. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for the frames that are already tagged. The user can also enable/disable the forwarding of announce messages to the master ports. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

**Select master ports:** Here the user can select the port that needs to be connected to the master ports so that the switch can be used as a bridge. Apart from the selection of

the master ports on the switch. The user can enable/disable VLAN on the master ports. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for the frames that are tagged. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

**Sync interval period on master ports:** This defines the initial synchronization interval: The master port sends a message for synchronization. The interval for the synchronization message can be set here. The current selection offers the following choices.

- 31.25 milliseconds
- 62.5 milliseconds
- 125 milliseconds
- 250 milliseconds
- 500 milliseconds
- 1 second

**Sync timeout counter on slave port:** Here the user can define the number of sync messages between 1-5 that must be lost to consider a timeout event.

**Domain number:** This defines the domain number that the PTPv2 slave port must respond to for synchronization. This can range from 0 to 255.

**Current UTC offset mode:** The user can select how the current UTC offset of the Announce message is applied. There are three options:

- Apply depending on the current UTC offset valid flag
- Always apply the offset
- Never apply the offset

**Proxy operation (only in Bridge mode):**

If the synchronization is lost in the slave port, the bridge must enter “Proxy Mode” the master ports must keep sending synchronization using the latest valid information and updating it with its internal clock. When “Proxy Mode” is enabled, the user can define the following parameters.

- If the **Proxy operation** is set to true, the proxy operation will be triggered if the synchronization on the slave is lost
- If the **Proxy operation** is set to false, the partition will never jump to the proxy operation

**Default Date / Time:**

The date/time sent by master ports when working in proxy mode and no valid synchronization information has been received on the slave port

Users can configure other parameters for fine-tuning, but they have default values in case they are not changed. These parameters are:

- **Startup timeout (in seconds):** This is the wait time to jump to proxy mode if at startup the slave port does not receive any synchronization information

**Delay request interval:** This defines the mean Delay request generation interval for synchronization

**Delay Request timeout counter on slave port:** This field enables the user to specify the number of Path Delay Responses that must be lost to consider a timeout event. The user can enter any value between 1 to 5.

**PTPv2 Grand Master Partition:** The following setting can be made in this mode:

**Select master ports:** Here the user can select the port that acts as PTPv2 master(s). The user can enable/disable VLAN on the master port(s). Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for PTPv2 frames that are tagged.

**Sync interval period on master ports:** This defines the initial synchronization interval: The master port sends a message for synchronization. The interval for the synchronization message can be set here. The current selection offers the following choices.

- 31.25 milliseconds
- 62.5 milliseconds
- 125 milliseconds
- 250 milliseconds
- 500 milliseconds
- 1 second

**Initial Date / Time:** The date/time sent by master ports when it starts operating as grandmaster can be defined here.

**Initial Time, nano seconds part:** The nano seconds parts of the Initial Date/Time.

**Announce interval period on master ports:** This defines the announce message interval: The master port sends a message announce message. The interval for the announce message can be set here. The current selection offers the following choices.

- Disable announce message
- 500 milliseconds
- 1 second
- 2 seconds (default)
- 4 seconds
- 8 seconds

**UTC offset valid:** If enabled the flag “currentUtcOffsetValid” is set in the announce message.

**UTC offset in seconds:** The value set in the “currentUtcOffset” field of the announce message.

**Clock Priority 1, Clock Priority 2, Clock Class, Clock Accuracy, Clock Variance, and Time Source:** The values set in the “grandmasterPriority1”, “grandmasterPriority2”, “grandmasterClockQuality” and “timeSource” fields of the announce message.

**PTPv2 Transparent Clock:** The following setting can be made in this mode:

**Select slave port (only Bridge mode):** Here the user can select the port that needs to be connected to the PTPv2 master so that the switch can be used as a transparent clock. Apart from the selection of the slave port on the switch, the user can enable/disable VLAN on the slave port. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for the frames that are already tagged. The user can also enable/disable the forwarding of announce messages to the master ports. The user can also enable the mirroring of the egress PTP messages on the slave port and select any port that is not already used by a PTP partition.

**Select master ports:** Here the user can select the port that needs to be connected to the master ports so that the switch can be used as a bridge. Apart from the selection of the master ports on the switch. The user can enable/disable VLAN on the master ports. Once enabled, the user can define VLAN-ID and priority for the corresponding VLAN. This can be useful for the frames that are tagged. The user can also enable the mirroring of the egress PTP messages on the master ports and select any port that is not already used by a PTP partition.

**Sync timeout counter on slave port:** Here the user can define the number of sync messages between 1-5 that must be lost to consider a timeout event.

**Domain number:** This defines the domain number that the PTPv2 slave port must respond to for synchronization. This can range from 0 to 255.

## 5.1.8.7 Ingress rate limiter

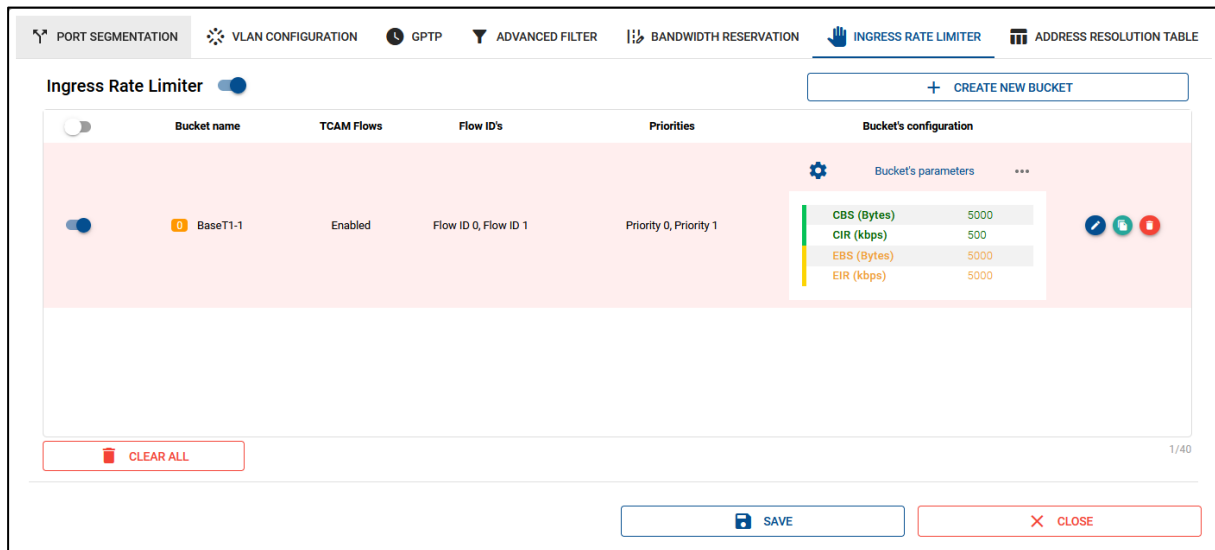


Figure 5-27 Ingress rate limiter

This is a licensed feature. For the switch receiving multiple streams simultaneously, per-stream filtering and policing enable a bridge or endpoint component to detect whether components in the network are conforming to the agreed rules. For example, a node gets allocated a certain amount of bandwidth and when this bandwidth is exceeded due to a component failure, or malicious act, appropriate action can be taken to protect the network. This feature includes procedures to perform frame counting, filtering, policing, etc. Policing and filtering functions are useful for detecting and enabling the elimination of disruptive transmissions, thus improving the robustness of the network.

In the Enhanced Ethernet switch -up to 4 available FlowIDs per port can be defined so up to 4 buckets per port are available. Frames are selected using an advanced filter rule and marked with a FlowID which is used as an ingress filter rule by ingress rate limiter.

## Concept

When a stream ingresses the switch, it passes through multiple blocks to be serviced by an ingress rate limiter. These blocks are described below

1. Stream marking: The ingress stream enters the stream marking block. Here the TCAM Flow ID rule defined in the advanced filter isolates the stream based on the parameters defined. The parameters that are used to isolate the traffic are ingress port, source MAC address, destination MAC address, VLAN, priority, egress action, and TCAM Flow ID. In automotive applications streams are defined statically in each one of the resources in the network. The advanced filter feature, implemented in the switch, is used to mark a specific stream to be metered by an ingress rate limiter flow meter.
2. Flow metering: The stream from the stream marking block enters the flow metering block. Here users can define token buckets to limit the ingress rate. These token buckets can be defined using the following parameters.
  - Committed burst size (CBS)
  - Committed information rate (CIR)
  - Excess burst size (EBS)
  - Excess information rate (EIR).

The ingress rate limiter limits the bandwidth through token buckets. Three different types of token buckets can be configured.

1. Two-color single rate
2. Three color single rate
3. Three color double rate

## Two-color single rate

The user can define the size of the bucket in Bytes in the field committed burst size(CBS). All the ingress traffic can be accumulated in the bucket and egressed out by the rate defined through the committed information rate(CIR). If the ingress traffic is more than the size of the committed bucket rate, the bucket is over-filled and excessive traffic is dropped.



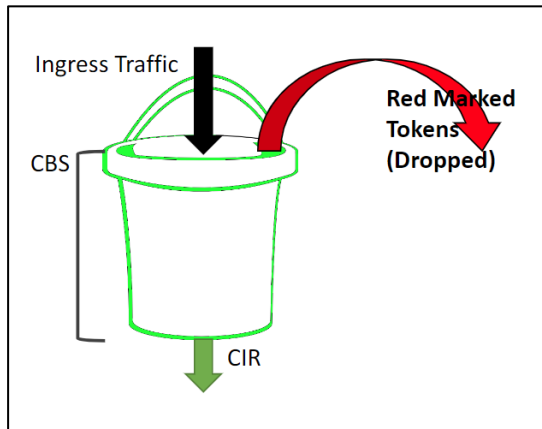


Figure 5-23 Two-color marker

### Three color single rate

The user can define the size of the bucket in Bytes in the field committed burst size(CBS). The user can also define excess burst size (EBS). This means in case of congestion the yellow packets (EBS) will not be serviced. If there is no congestion, all the ingress traffic (CBS and EBS) will be serviced. In case of no congestion, all the ingress traffic can be accumulated in the bucket and egressed out by the rate defined through committed information rate (CIR). Since the bucket has only one egress, the committed information rate (CBS) should be equal to the excessive information rate(EBS).

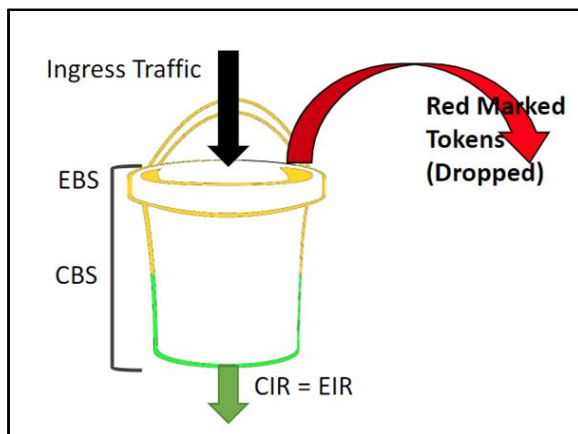


Figure 5-29 Three color single rate

### Three color double rate

The user can define the size of the bucket in Bytes in the field committed burst size (CBS). The user can also define excess burst size (EBS). This means in case of congestion the yellow packets (EBS) will not be serviced. If there is no congestion, all the ingress traffic (CBS and EBS) will be serviced. In case of no congestion, all the

ingress traffic can be accumulated in the corresponding buckets and egressed out by the rate defined through the committed information rate (CIR) and the excessive information rate (EIR).

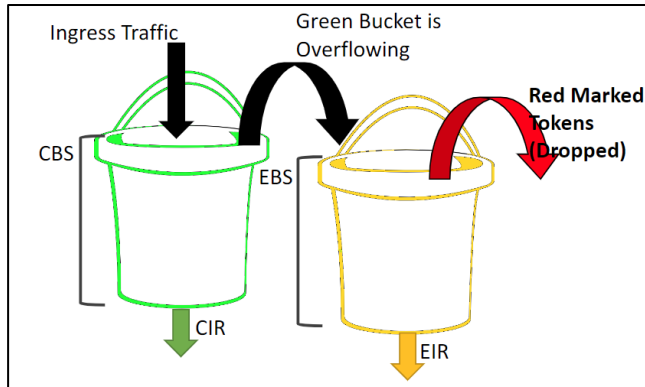


Figure 5-30 Three color double rate

## Configuration

In the sub-tab [Ingress rate limiter](#), the user can configure the following parameters

[Select ingress port](#): The user can select the ingress port where the limiting of the rate is desired.

[Select ingress traffic](#): The flow meters are implemented as token buckets. The user can select the FlowIDs to be applied to the bucket. More than one stream/priority can be metered by a single bucket.

[Select priorities](#): The user can select priorities between 0-7 to be applied to the buckets.

[Set bucket parameters](#): The following parameters can be defined to form a bucket

- [Committed burst size \(CBS\)](#): This defines the size of the bucket in Bytes
- [Committed information rate \(CIR\)](#): This defines the number of tokens periodically egressing the bucket in kbps.
- [Excess burst size \(EBS\)](#): This defines the size of the bucket in Bytes
- [Peak information rate \(PIR\)](#): This defines the sum of excess information rate (EIR) tokens periodically egressing the bucket and the committed information rate (CIR)
- [Calculated rate error \(%\)](#): Since the flows can vary how much information is expressed based on the internal elements, in this field the user can define how much deviation from the EIR can be tolerated.

## 5.2 Control panel tab

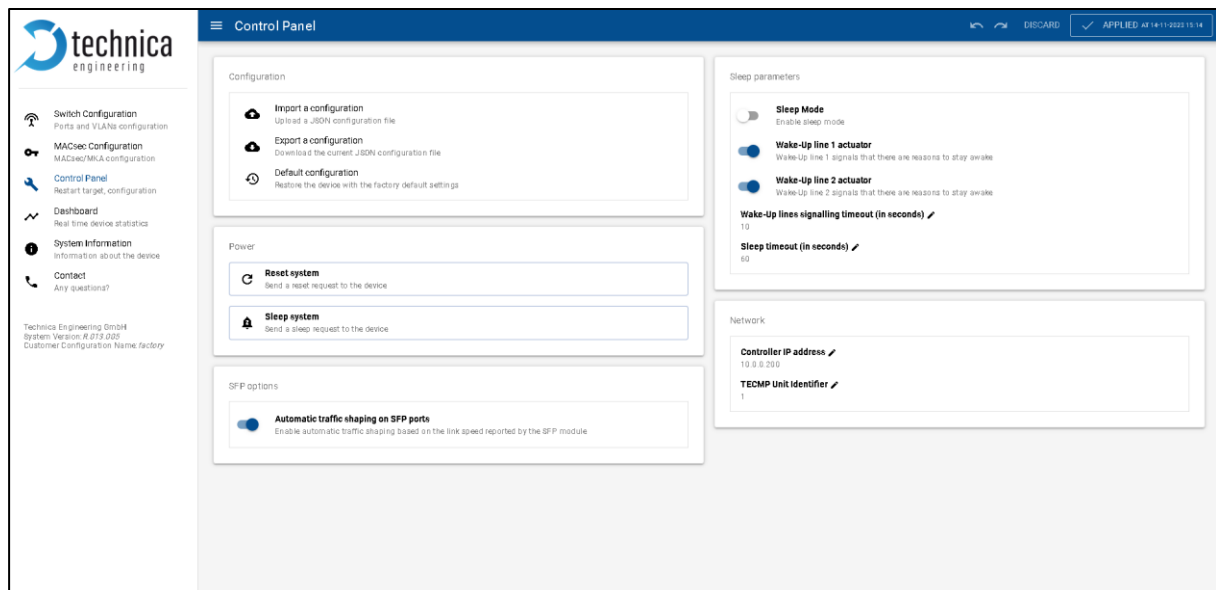


Figure 5-31 Control Panel Tab

### 5.2.1 Configuration

Users can make general settings of the configuration in the switch in this tab

#### 5.2.1.1 Import a configuration

Through this option, the user can import a configuration from the computer to the switch in .json format.

#### 5.2.1.2 Export a configuration

Applied changes can be exported to the computer through this option. The exported configuration is in \*.json file extension format.

#### 5.2.1.3 Default configuration

Through this option, the switch is reset to the default configuration. The IP address remains the same and is not reset to default.

### 5.2.2 Password write-protection:

The user can protect the configuration with a password (min. 8 digits), so only authorized persons can modify the configuration. The configuration can still be

exported but for uploading another configuration the password has to be inserted. The password can be changed or cleared on the webpage by inserting the current password. With the factory HW button on the EES the configuration can be set to default what also removes the password protection

## 5.2.3 Power

This section offers settings for power and sleep functions.

### 5.2.3.1 Reset System

When this option is selected, the device can trigger a power reset.

### 5.2.3.2 Sleep System

This option sends a sleep request to the device.

## 5.2.4 SFP options

This section offers settings about the SFP ports.

### 5.2.4.1 Automatic traffic shaping on SFP ports

When this feature is enabled the EES automatically sets traffic shaping based on the link speed reported by the SFP module for the SFP port. However if the user manually sets traffic shaping for the SFP ports and the configured value is lower than the reported speed by the SFP module the manually set value will be used.

## 5.2.5 Sleep parameters

This section offers settings about sleep and wake-up features.

### 5.2.5.1 Sleep mode

When disabled, the device is working without entering into sleep mode. If this option is enabled, the device will go to sleep if no activity is recognized according to the observed ports. The user must use a Wakeup line to wake the device up if the device goes to sleep.



Please see the configuration of each port in [Sections 4.1.4, 4.1.5, and 4.1.7](#).

### 5.2.5.2 Wake-Up line 1 actuator

There are two WakeUp Lines. Both WakeUp lines can be output.

- If this option is enabled, the wakeup line provides the same voltage as the voltage on the powerline (kind of loop-through). It provides power as long as there is a reason to stay awake
- If this option is disabled, this wakeup line is only input and wakes up the device when supplied

### 5.2.5.3 Wake-Up line 2 actuator

- If this option is enabled, the wakeup line provides the same voltage as the voltage on the powerline (kind of loop-through). It provides power as long as there is a reason to stay awake
- If this option is disabled, this wakeup line is only input and wakes up the device when supplied

### 5.2.5.4 Wake-Up lines signaling timeout (in seconds)

Here user can define the time in seconds, which must go by before the actuator of the wakeup lines is set to ground. The default value is 10 seconds.

### 5.2.5.5 Sleep timeout (in seconds)

Here user can define the time in seconds, which must go by with no communication on the supervised ports before the switch goes to sleep. Reasonable values are between 15s and 300s.

## 5.2.6 Network

This section offers settings about the network address and identifiers used for the switch.

### 5.2.6.1 Controller IP Address

The IP address assigned to the switch can be changed here. By default, the IP address is 10.0.0.200.

### 5.2.6.2 TECMP unit identifier

The TECMP Unit Identifier is used for TECMP status and configuration messages. By default, the identifier is 1.

### 5.2.6.3 TECMP Device ID

The TECMP Unit Identifier is used for TECMP status and configuration messages. By default, the identifier is 0x00BC. 4 possible values are assigned to the EES (from 0x00BC to 0x00BF both included). Beside these values, any other value can be entered, but a warning will be shown indicating that a non-standard value is used.

### 5.2.6.4 TECMP Ports

This field allows to configure on which ports TECMP messages will be sent. By default only the Control port is configured, but any other combination of ports is possible.

## 5.3 System information tab

On the tab “System Information”, some status information about the device is displayed.

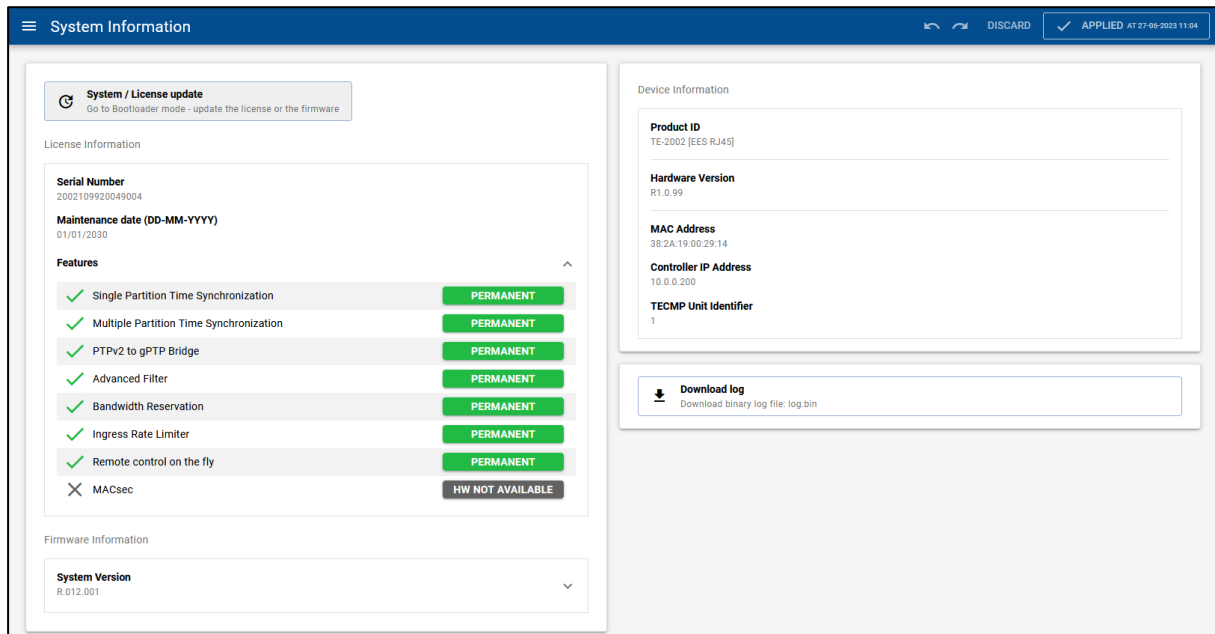


Figure 5-24 System Information Tab

### 5.3.1 License information

**System update:** This option is used to update the firmware on the device. The process of updating a firmware/license is explained in [CHAPTER 6](#) When clicking on this option, the device goes into bootloader mode and loses its normal operation. The bootloader mode can also be verified by the fast toggle of the status LED (see [CHAPTER 4.1.8.1](#)) which in normal mode is in slow toggle mode. If this option is selected by mistake, please select “go back to application mode” to exit the bootloader mode.

**Serial number:** Serial number that identifies the device unequivocally.

**Maintenance date (DD-MM-YYYY):** The date when the license is valid.

**Maintenance date (DD-MM-YYYY):** The date when the license is valid.

**Features:** The list of all the features that are covered under the license is mentioned here. There can be several modes of license.

1. **Unlicensed:** No license is available for this feature.
2. **Temporal:** The license is granted for the limited amount of time mentioned on the webpage.

3. **Permanent:** The license is granted permanently for this device.
4. **Expired:** The license for the feature mentioned is expired and the feature cannot be used anymore.

Currently, Enhanced Ethernet Switch has the following features that need a license.

- 🔗 [Single Partition Time Synchronization](#)
- 🔗 [Multiple Partition Time Synchronization](#)
- 🔗 [PTPv2 to gPTP Bridge](#)
- 🔗 [Advanced Filter](#)
- 🔗 [Bandwidth Reservation](#)
- 🔗 [Ingress Rate Limiter](#)
- 🔗 [Remote control on the fly \(See Chapter 7\)](#)
- 🔗 [MACsec](#)


## 5.3.2 Device information

**Product Id:** This shows the name of the device

**Hardware version:** The version of your hardware of the switch is displayed here

**MAC address:** This MAC address should be the same as on the label at the bottom of the device.

**Controller IP address:** The user can change the IP address of the switch, in this field. If the user wants to use multiple devices in one network, the user must configure a unique IP address for each device.

 If you forgot the IP address of your device, you could reset it to default settings as described in [Section 4.1.2](#).

**TECMP unit identifier:** The TECMP Unit Identifier is used for TECMP status and configuration messages. By default, the identifier is 1.

**Download log:** This enables the user to download the logs of the switch in binary format.









## 6 Maintenance

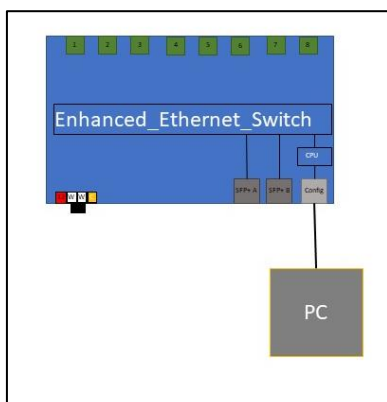
### 6.1 Firmware update

The latest firmware and documentation for the Enhanced Ethernet Switch can be requested at [Technical Sales](#).

#### 6.1.1 Preconditions and important information

-  To update the device to release 10 and onwards, the user must update the firmware to release 9 first and then update to release 10. A direct update from a lower release to release 10 can cause the device to break
-  If an error occurs during the update, please perform a power reset, and try again
-  Make sure your network adapter is configured in the correct IP address range. The subnet mask should be 255.255.255.0
-  The device can only be flashed/updated through the 100BASE-TX Host port
-  Please follow these update instructions to avoid erroneous states of the device. Technica Engineering may charge support fees for repair services.
-  A stable 12 Volt DC power supply is required. Do not switch off the power supply during the update process

##### 6.1.1.1 Update via host port



Pre-requisites:

-  Please set the device to default settings

Figure 6-1 Update through Host port

**Steps:**

1. Open the website through the host port and by typing the IP of the device. The Default IP address is 10.0.0.200
2. Go to the "System Information" tab and click System update

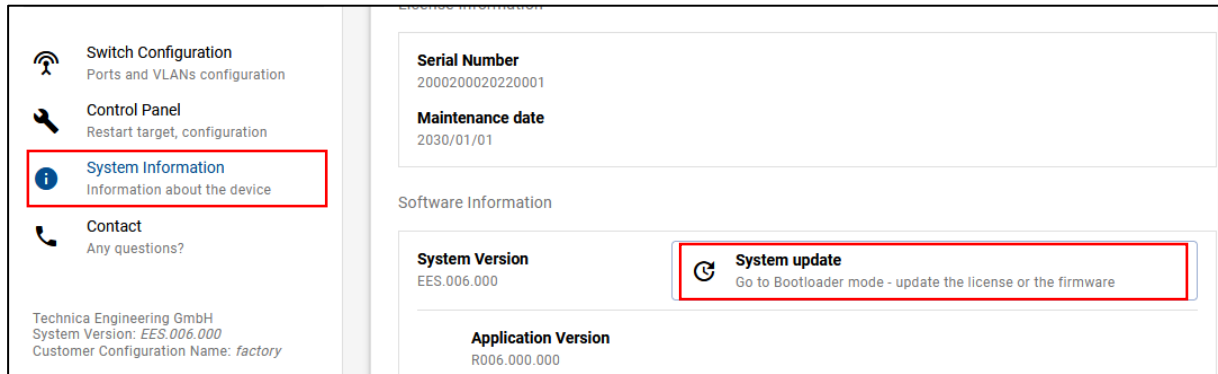


Figure 6-2 System information tab

The device is now in bootloader mode and the following website should appear:

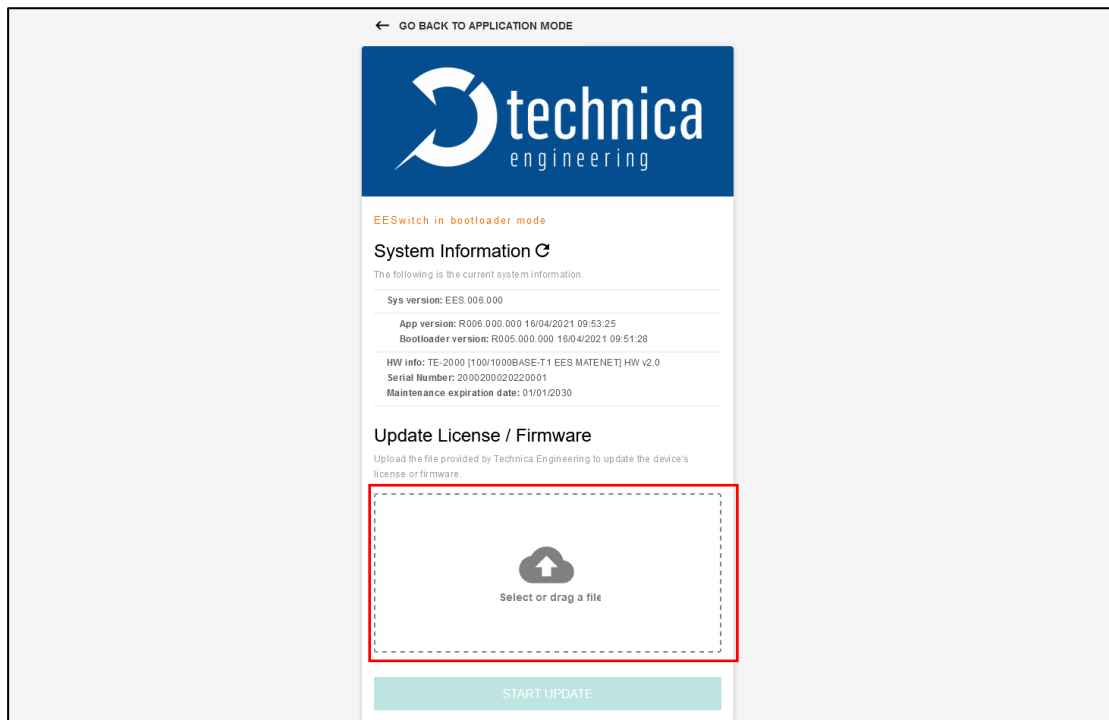



Figure 6-3 Firmware upload

3. Please click into the framed field and open the file [firmware\\_full.tefw](#) for new firmware or open new license files. Alternatively, it is possible to drag and drop the mentioned files into the framed field
4. Press [start update](#) 

5. Wait until you are prompted by the following window:

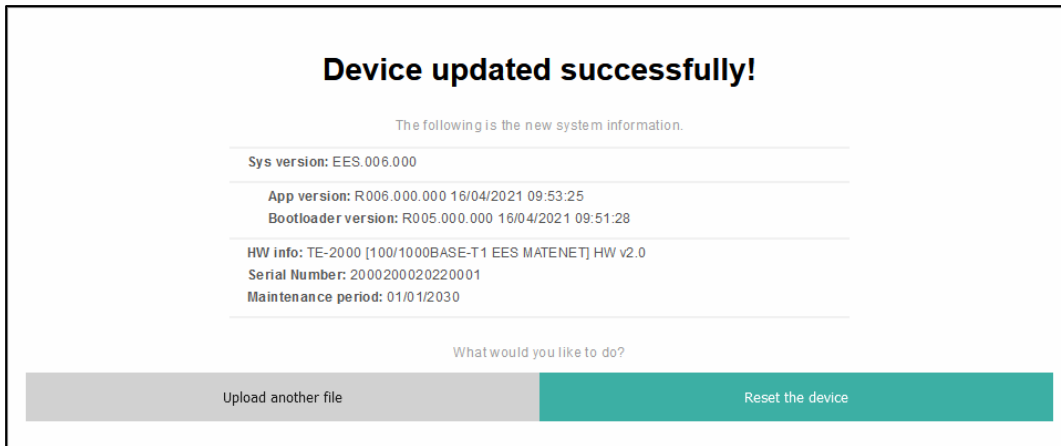


Figure 6-4 Firmware update successful

6. Press “Reset the device” if you are finished with updating.
7. The device will jump into application mode and show you the website again for configuration.

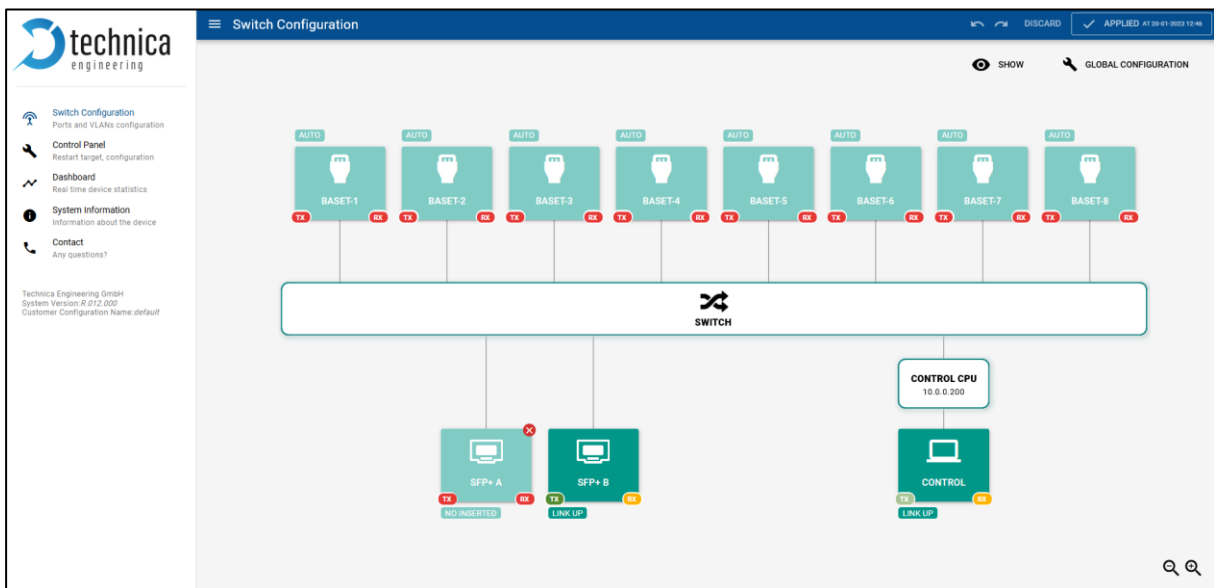


Figure 6-5 Home screen

➔ Finished

**i** If a newer version of a bootloader is present, then the same procedure has to be followed to update the bootloader.

## 7 Remote control API

The Enhanced Ethernet switch has a remote-control API based on HTTP protocol. Two types of methods are used for configuration.

- GET Methods: These allow retrieving the configuration and status using the .JSON format. They are used to read configuration and status information from the switch.
- Post Methods: These allow to setting and modification of the configuration coded and trigger actions

For detailed documentation of the remote API please contact Technica Engineering at [Support](#).

## 8 Appendix

This chapter describes the UDP discovery and configuration messages for the enhanced ethernet switch.

### 8.1 UDP Discovery messages

A mechanism to make it possible to detect and find all the Enhanced ethernet switches present in a network has been implemented. This discovery mechanism is based on UDP messages, comprising a multicast discovery request and a unicast discovery response.

This makes it possible to discover all Enhanced ethernet switches connected and retrieved for each of the basic information such as TECMP ID, firmware version, hardware version, etc.

#### 8.1.1 Broadcast discovery request

This message is a UDP broadcast message with the following parameters:

- Destination MAC address: FF-FF-FF-FF-FF-FF
- Destination IP address: 10.104.3.255
- UDP Src Port = UDP Dst Port = 9999

The following values are used for the UDP payload:

| Field name     | Data type | Value      |
|----------------|-----------|------------|
| Version        | UINT16    | 0x0001     |
| Operation      | UINT16    | 0x0000     |
| Length options | UINT32    | 0x00000000 |
| Options        | Variable  | None       |
| Reserved       | UINT32    | 0x00000000 |

##### 8.1.1.1 Unicast discovery response

The Enhanced Ethernet switch responds to a multicast discovery request with a unicast response within a maximum time interval of 2 seconds. The response is only sent to the port of the Enhanced Ethernet switch to which the request was addressed.

- Source MAC address: MAC address of the switch
- Destination MAC address: MAC address of the endpoint
- Destination IP address: IP address of the endpoint
- Source IP address: configured IP address of the switch

- UDP Src Port = UDP Dst Port = 9999

The following values are used for the UDP payload:

| Field name     | Data type | Value                                                                                                                                                                                                                                                                                                                                   |
|----------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version        | UINT16    | 0x0001                                                                                                                                                                                                                                                                                                                                  |
| Operation      | UINT16    | 0x0001                                                                                                                                                                                                                                                                                                                                  |
| Length options | UINT32    | 0x0000001C                                                                                                                                                                                                                                                                                                                              |
| Options        | Variable  | parameter1 [6B]: Current MAC address<br>parameter2 [4B]: Current source IP address (default 192.168.0.49):<br>parameter3 [6B ]: Destination multicast address (default 01-00-5E-00-00-00)<br>parameter4 [4B]: Current destination IP address<br>parameter5 [4B]: TECMP ID<br>parameter6 [4B]: Enhanced Ethernet switch firmware version |
| Reserved       | UINT32    | 0x00000000                                                                                                                                                                                                                                                                                                                              |

Example for options:

0xC47D46155922 C0A80031 01005E000000 C0A800FF.0001 000A

The switch has:

- MAC address C4:7D:46:15:59:22
- Source IP address 192.168.0.49
- Destination multicast address 01005E000000
- Destination IP address 192.168.0.255
- TECMP ID 1
- Enhanced Ethernet switch firmware version 10.00

## 8.2 UDP Configuration messages

The Enhanced Ethernet switch provides a specific mode for remote device configuration, without the need to access the built-in webserver.

Enhanced Ethernet switch switches to remote configuration mode when it receives on the configuration port a UDP message with a specific layout and content that enables this mode.

The configuration mode is not enabled persistently. To keep the Enhanced Ethernet switch in this mode, the UDP message for mode activation must be sent cyclically from the endpoint every 20 seconds. While the device is in configuration mode, it is ready to receive and process configuration requests, transmitted via UDP messages.

As soon as the UDP messages for mode activation disappear, and after a short timeout, the Enhanced Ethernet switch goes back into normal mode.

Details about how exactly this remote configuration mode can be found below.

All configuration messages, including the one used for mode activation, are based on the IP/UDP protocol (EtherType: 0x0800) and share the same header data:

- Source MAC address: MAC address of the DLM
- Destination MAC address: MAC address of the switch
- Source IP address: IP address of the DLM
- Destination IP address: IP address of the switch
- UDP src port = UDP dst port = 9998

And the same layout for the UDP payload:

| Config Message |   |           |   |
|----------------|---|-----------|---|
| 4 bytes        |   |           |   |
| 0              | 1 | 2         | 3 |
| Version        |   | Operation |   |
| Length Options |   |           |   |
| Options        |   |           |   |
| ...            |   |           |   |
| Reserved       |   |           |   |

The meaning of each field is described in the table below:

| Field name     | Data type | Description                                                                                                                                |
|----------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Version        | UINT16    | Indicates the version of the control API                                                                                                   |
| Operation      | UINT16    | Indicates the operation to be performed                                                                                                    |
| Length options | UINT32    | Specifies the number of bytes to be read after this field to register and analyze all of the options required for the preceding operation. |
| Options        | Variable  | Options or parameters required for a particular operation.                                                                                 |
| Reserved       | UINT32    | Reserved for future use. If not used, it must be set to 0x00000000                                                                         |

## 8.2.1 Set Configuration mode

As explained at the beginning of this section, to set the Enhanced Ethernet switch in configuration mode, an instance in the system (usually the endpoint) must send cyclically a UDP message containing the command for mode activation.

This command is expected to be received every 20 seconds. If this message fails to arrive, the switch goes back to its normal state on its own after 25 seconds.

In this configuration mode, the switch deactivates its features and enables other functions that allow the device configuration.

**i** Most of the configuration settings are only possible in this special configuration mode.

The following values are used for the mode activation command:

| Field name     | Data type | Value                                                                      |
|----------------|-----------|----------------------------------------------------------------------------|
| Version        | UINT16    | 0x0001                                                                     |
| Operation      | UINT16    | 0x0002                                                                     |
| Length options | UINT32    | 0x00000001                                                                 |
| Options        | UINT8     | 0x00 = Deactivate configuration mode<br>0x01 = Activate configuration mode |
| Reserved       | UINT32    | 0x00000000                                                                 |

## 8.2.2 Restart device

It simply restarts the switch.

| Restart                     |   |                   |   |
|-----------------------------|---|-------------------|---|
| 4 bytes                     |   |                   |   |
| 0                           | 1 | 2                 | 3 |
| Version                     |   | Operation= 0x0103 |   |
| Length Options = 0x00000001 |   |                   |   |
| Restart=0x01                |   | Reserved          |   |

| Field name     | Data type | Description                                                                                                                                             |
|----------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restart        | UINT8     | <ul style="list-style-type: none"> <li>➤ 0x01 to perform a restart</li> <li>➤ With any other value, the message will not trigger the restart</li> </ul> |
| Length Options | UINT32    | <ul style="list-style-type: none"> <li>➤ 0x01</li> <li>➤ With any other value, the message will not trigger the restart</li> </ul>                      |



### 8.2.3 Mute/Unmute PHY

This instruction is meant to be used in a testing environment. These changes are applied immediately, no reset is needed.

If transparency mode is active for a pair, this message will not be considered for the pair. A negative acknowledge (NACK) message can be sent so that the user will know that the remote-controlling action was not executed. The PHY is to be muted given its Interface ID is muted immediately.

| Mute PHY             |   |                   |   |
|----------------------|---|-------------------|---|
| 4 bytes              |   |                   |   |
| 0                    | 1 | 2                 | 3 |
| Version              |   | Operation= 0x0104 |   |
| Length Options = 0x5 |   |                   |   |
| Channel ID           |   |                   |   |
| Mute                 |   | Reserved          |   |

| Field name | Data type | Description                                                                            |
|------------|-----------|----------------------------------------------------------------------------------------|
| Mute       | UINT8     | <ul style="list-style-type: none"> <li>↻ 0: False</li> <li>↻ 1: true_normal</li> </ul> |

### 8.2.4 Import configuration

In configuration mode only.

It imports any .cfg file exported by the switch.

| Import Config               |              |                   |   |
|-----------------------------|--------------|-------------------|---|
| 4 bytes                     |              |                   |   |
| 0                           | 1            | 2                 | 3 |
| Version                     |              | Operation= 0x0101 |   |
| Length Options              |              |                   |   |
| Seq. number                 | Total number | Length total      |   |
| Serialized config (n bytes) |              |                   |   |

| Field name   | Data type | Description                                                      |
|--------------|-----------|------------------------------------------------------------------|
| Seq. Number  | UINT8     | Eth. Frame sequence out of the total number of frames (1 based)  |
| Total Number | UINT8     | Total Number of Eth. Frames needed to send the whole information |

|                |        |                                                                                                                                                                               |
|----------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Length options | UINT32 | Length of the payload of the current frame.<br>Length options = 1 byte (seq.number) + 1 byte (TotalNumber) + 2Bytes (Length total) + nBytes (serialized config in this frame) |
| Length total   | UINT16 | total length in Bytes of the serialized config                                                                                                                                |

## 8.2.5 Export configuration

In configuration mode only.

It pulls the current configuration from the switch. Note that the configuration may be split into more than one ethernet frame.

| Export Config Request     |   |                  |   |
|---------------------------|---|------------------|---|
| 4 bytes                   |   |                  |   |
| 0                         | 1 | 2                | 3 |
| Version                   |   | Operation=0x0102 |   |
| Length Options=0x00000001 |   |                  |   |
| Action=0x01               |   | Reserved         |   |

| Field name     | Data type | Description                                                                                                   |
|----------------|-----------|---------------------------------------------------------------------------------------------------------------|
| Action         | UINT8     | Action 0x01 to pull (with any other the message will not trigger the export of the config)                    |
| Length Options | UINT32    | The value of this field has to be 0x01 (with any other the message will not trigger the export of the config) |

| Export Config Response      |              |                  |   |
|-----------------------------|--------------|------------------|---|
| 4 bytes                     |              |                  |   |
| 0                           | 1            | 2                | 3 |
| Version                     |              | Operation=0x0102 |   |
| Length Options              |              |                  |   |
| Seq. number                 | Total number | Length total     |   |
| Serialized config (n bytes) |              |                  |   |

| Field name     | Data type | Description                                |
|----------------|-----------|--------------------------------------------|
| Length Options | UINT32    | Length of the payload of the current frame |

|              |       |                                                                                                                                    |
|--------------|-------|------------------------------------------------------------------------------------------------------------------------------------|
|              |       | Length options = 1 byte (seq. number) + 1 byte (total number) + 2 bytes (length total) + n bytes (serialized config in this frame) |
| Seq. Number  | UINT8 | Ethernet frame sequence out of the total number of frames (1-based)                                                                |
| Total Number | UINT8 | Total number of Ethernet frames needed to send the whole information                                                               |
| Length total | UINT8 | Total length in bytes of the serialized config                                                                                     |

## 9 Contact

If you have any questions regarding this product, please feel free to contact us:

Technica Engineering GmbH  
Leopoldstr. 236  
80807 München  
Germany

Technical support:  
[support@technica-engineering.de](mailto:support@technica-engineering.de)

General information:  
[Info@technica-engineering.de](mailto:Info@technica-engineering.de)

Most current user manuals and product information:  
<https://technica-engineering.de/en/>

## 10 Declaration of conformity (EES RJ-45 variant)

### Български

С настоящото Technica Engineering GmbH декларира, че продуктът Модул за улавяне Enhanced Ethernet Switch RJ-45 (TE-2002), е в съответствие с Директива 2014/30/ЕС. Цялостният текст на ЕС декларацията за съответствие може да се намери на следния интернет адрес:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Čeština

Tímto Technica Engineering GmbH prohlašuje, že produkt Enhanced Ethernet Switch RJ-45 (TE-2002), je v souladu se směrnicí 2014/30/EU. Úplné znění EU prohlášení o shodě je k dispozici na této internetové adrese:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Dansk

Hermed erklærer Technica Engineering GmbH, at produktet Enhanced Ethernet Switch RJ-45 (TE-2002), er i overensstemmelse med Direktiv 2014/30/EU. EU-overensstemmelseserklæringens fulde tekst kan findes på følgende internetadresse:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Deutsch

Hiermit erklärt Technica Engineering GmbH, dass das Produkt Enhanced Ethernet Switch RJ-45 (TE-2002), die Richtlinie 2014/30/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Eesti

Käesolevaga deklareerib Technica Engineering GmbH, et toode hõivamismoodul Enhanced Ethernet Switch RJ-45 (TE-2002), vastab direktiivi 2014/30/EL nõuetele. ELi vastavusdeklaratsiooni tselik tekst on kttesaadav jrgmisel internetiaadressil:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### English

Hereby, Technica Engineering GmbH declares that the product Enhanced Ethernet Switch RJ-45 (TE-2002), complies with Directive 2014/30/EU. The full text of the EU declaration of conformity is available at the following internet address:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Español

Por la presente, Technica Engineering GmbH declara que el producto Enhanced Ethernet Switch RJ-45 (TE-2002), es conforme con la Directiva 2014/30/UE. El texto completo de la declaración UE de conformidad está disponible en la página web siguiente:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Ελληνικά

Με την παρούσα ο/η Technica Engineering GmbH, ότι το προϊόν Enhanced Ethernet Switch RJ-45 (TE-2002), πληροί την οδηγία 2014/30/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης ΕΕ διατίθεται στην ακόλουθη ιστοσελίδα στο διαδίκτυο:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Français

Le soussigné, Technica Engineering GmbH, déclare que le produit Enhanced Ethernet Switch RJ-45 (TE-2002), est conforme la directive 2014/30/UE. Le texte complet de la déclaration UE de conformité est disponible l'adresse internet suivante:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Hrvatski

Technica Engineering GmbH ovime izjavljuje da je proizvod Enhanced Ethernet Switch RJ-45 (TE-2002), u skladu s Direktivom 2014/30/EU. Cjeloviti tekst EU izjave o sukladnosti dostupan je na sljedećoj internetskoj adresi:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

### Italiano

Il fabbricante, Technica Engineering GmbH, dichiara che il prodotto Enhanced Ethernet Switch RJ-45 (TE-2002), , conforme alla direttiva 2014/30/UE. Il testo completo della dichiarazione di conformità UE disponibile al seguente indirizzo Internet:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Latviešu

Ar šo Technica Engineering GmbH deklarē, ka produkts Enhanced Ethernet Switch RJ-45 (TE-2002), , atbilst Direktīvai 2014/30/ES. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā interneta vietnē:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Lietuvių

Aš, Technica Engineering GmbH, patvirtinu, kad produktas sugavimo modulis Enhanced Ethernet Switch RJ-45 (TE-2002), , atitinka Direktyvą 2014/30/ES. Visas ES atitikties deklaracijos tekstas prieinamas šiuo internet adresu:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Magyar

Technica Engineering GmbH igazolja, hogy a termék Enhanced Ethernet Switch RJ-45 (TE-2002), a 2014/30/EU irányelvnek. Az EU-megfelelőségi nyilatkozat teljes szövege elérhető a következő internetes címen:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Malti

B'dan, Technica Engineering GmbH, niddikjara li l-prodott Enhanced Ethernet Switch RJ-45 (TE-2002), , huwa konformi madDirettiva 2014/30/UE. It-test kollu tad-dikjarazzjoni ta' konformit ta'UE huwa disponibbli f'dan l-indirizz talInternet li ġej:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Nederlands

Hierbij verklaar ik, Technica Engineering GmbH, dat het Enhanced Ethernet Switch RJ-45 (TE-2002), product voldoet aan richtlijn 2014/30/EU. De volledige tekst van de EU-conformiteitsverklaring kan worden geraadpleegd op het volgende internetadres:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Polski

Technica Engineering GmbH niniejszym oświadcza, że produkt Enhanced Ethernet Switch RJ-45 (TE-2002), , jest zgodny z dyrektywą 2014/30/UE. Pełny tekst deklaracji zgodności I UE jest dostępny pod następującym adresem internetowym:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Português

O(a) abaixo assinado(a) Technica Engineering GmbH declara que o produto Enhanced Ethernet Switch RJ-45 (TE-2002), , está em conformidade com a Diretiva 2014/30/UE. O texto integral da declaração de conformidade está disponível no seguinte endereço de Internet:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Română

Prin prezenta Technica Engineering GmbH declară ca produsul Enhanced Ethernet Switch RJ-45 (TE-2002), , este în conformitate cu Directiva 2014/30/UE. Textul integral al declarației UE de conformitate este disponibil la următoarea adresă

internet:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Slovensko

Technica Engineering GmbH potrjuje, da je izdelek Enhanced Ethernet Switch RJ-45 (TE-2002), , skladen z irektivno 2014/30/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>

## Slovensky

Technica Engineering GmbH týmto vyhlasuje, že produkt Enhanced Ethernet Switch RJ-45 (TE-2002), , je v slade so smernicou 2014/30/EÚ. Úplné EÚ vyhlásenie o zhode je k dispozícii na tejto internetovej adrese:

<https://technica-engineering.de/wp-content/uploads/2021/05/eu-declaration-of-conformity-te-2002.pdf>