MICROSENS

User Manual v1.1.1

10G Micro Switch

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany

Tel.: +49 2381 9452-0
Fax: +49 2381 9452-100
E-Mail: info@microsens.de
Web: www.microsens.de

Table of Contents

Information available from the MICROSENS Website

Registered users can find the latest firmware versions as well as further information on our website:

- **Registration:** www.microsens.de > Login > Click on the link 'Not registered'
  - Fill out the e-mail form and send it to sales@microsens.com.
  - MICROSENS will send you an email containing a username and password.
- **Login:** www.microsens.com > Login > Enter your username and password > Click the button 'Login'.
  - Firmware images: Please navigate to your device and select the section 'Download'.
  - Further information is available by selecting the other tabs on the product page.

Note: Make sure the browser allows the execution of scripts.

1 Overview

1.1 Introduction

The new 10G Micro Switch provides an entry into the world of 10 Gigabit Ethernet networks at the workplace. The manageable switch meets the demand for network solutions with extremely high data throughput, such as the integration of high-speed WLAN access points or high-resolution video cameras.

Item	Description
Model Name	10G Micro Switch
MICROSENS Article Numbers	MS440507PM
10/100/1000T Port	4 Local Ports
10/100T/1000T/2.5G/5G Port	1 Downlink Port
10G SFP+ Port	2 Uplink Port
PoE+ Port	Port 1 to 4 (30W per port)
PoE++ Port	Port 7 (60W per port)
Console Port	1 Serial Port

1.2 Hardware Description

1.2.1 Ports, Notifications and Controls

① 7x port status LEDs “link”
5x port status LEDs “PoE” (ports 1 - 4, 7)

② 1x device status LED “on”
1x device status LED “sys”

③ 4x local ports (10/100/1000T)
PoE+ (30 W per port)

④ 1x downlink port (10/100T/1000T/2.5G/5G)
PoE++ (60W)

⑤ USB-C port (virtual COM port for console access).

⑥ 2x uplink ports (10G SFP+, no PoE)

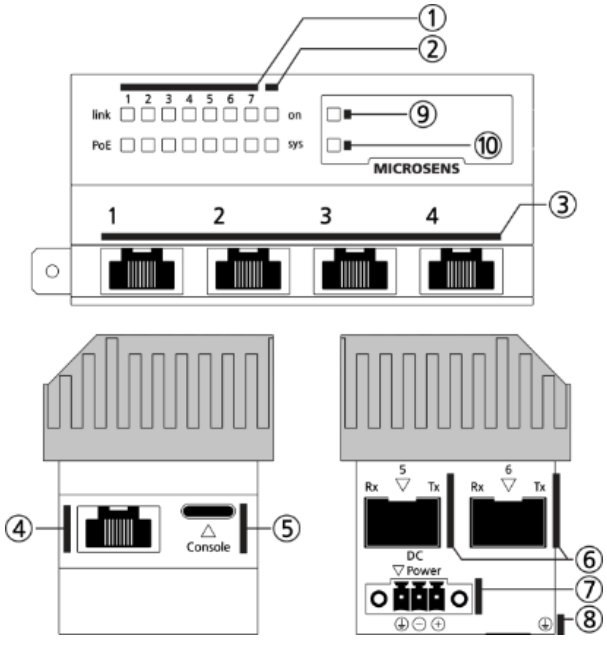
⑦ Power supply (50-57 VDC, 54 VDC typ.)

⑧ Earth lug

⑨ Hardware reset button

⑩ Factory default button

Note: Before use remove the protective plastic strip from the display!



2 Installation

This paragraph describes how to install the 10G Micro Switch to your corporate network.

1. Make sure to earth the device properly via the power supply ⑦ or the earth lug ⑧.
2. Optionally, connect a computer via the USB-C console port ⑤.
3. Connect the device to the network using either an SFP+ transceiver with one of the SFP+ uplink ports ⑥ or an Ethernet connector cable with one of the other local ports ③④.
4. Connect the power supply ⑦.

   Note: When connecting the power supply ⑦ observe the correct polarity (GND/+/-)!

After connecting the power supply the device boots from its internal memory.

3 Login

3.1 IP Address

By default, the 10G Micro Switch is set to DHCP mode, retrieving its IP parameters (IP address, subnet mask, and default gateway) from the DHCP server of the corporate network.

To discover the assigned IP parameters of the device, use one of the following methods:

- Log on to the DHCP server and search for the device's entry. You will find the corresponding MAC address printed on the device's chassis.
- Discover the IP parameters either with **Switch IP Configuration Tool** or **Network Management Plattform (NMP)**.

  Note: Both applications are available on the MICROSENS website for download. For more information on how to use these applications please refer to the provided user manuals.
- Use the console connection with your computer (see step 2 in chapter 2) and execute the following commands

```
MS440507PM-48G7> enable
MS440507PM-48G7# show ip interface
Status:
  Dynamic Device IP: 192.168.11.61
  Dynamic Subnet Mask: 255.255.255.0
  Dynamic Gateway: 192.168.11.1
  Dynamic DNS Server 1: 192.168.11.1
  Dynamic DNS Server 2: N/A
  Dynamic DNS Server 3: N/A
  Dynamic DNS Server 4: N/A
  Outgoing Device IP: 192.168.11.61
  [...]

MS440507PM-48G7#
```

Note: Set the communication parameters properly (**115200-8N1**).

Note: The USB-C port ⑤ is a console port for local configuration or diagnostic purposes.

Note: Familiarity with configuration of serial connections and using console commands is highly recommended!

3.2 Login with Credentials

1. Start your web browser and enter the device's IP address in the browser's address bar.
2. In the opening login dialog enter one of the following predefined credentials:

User Name	Password	Access Permissions
admin	administrator	Read / Write / Execute
user	microsens	Read only

Note: It is strongly recommended to assign different passwords at least for users admin and user after first login to prevent unauthorized access to the device (via "Access > User Account")!

3. The device's web GUI starting page opens, showing the system information by default.

4 Web GUI

4.1 General Description

The web GUI contains the following elements:

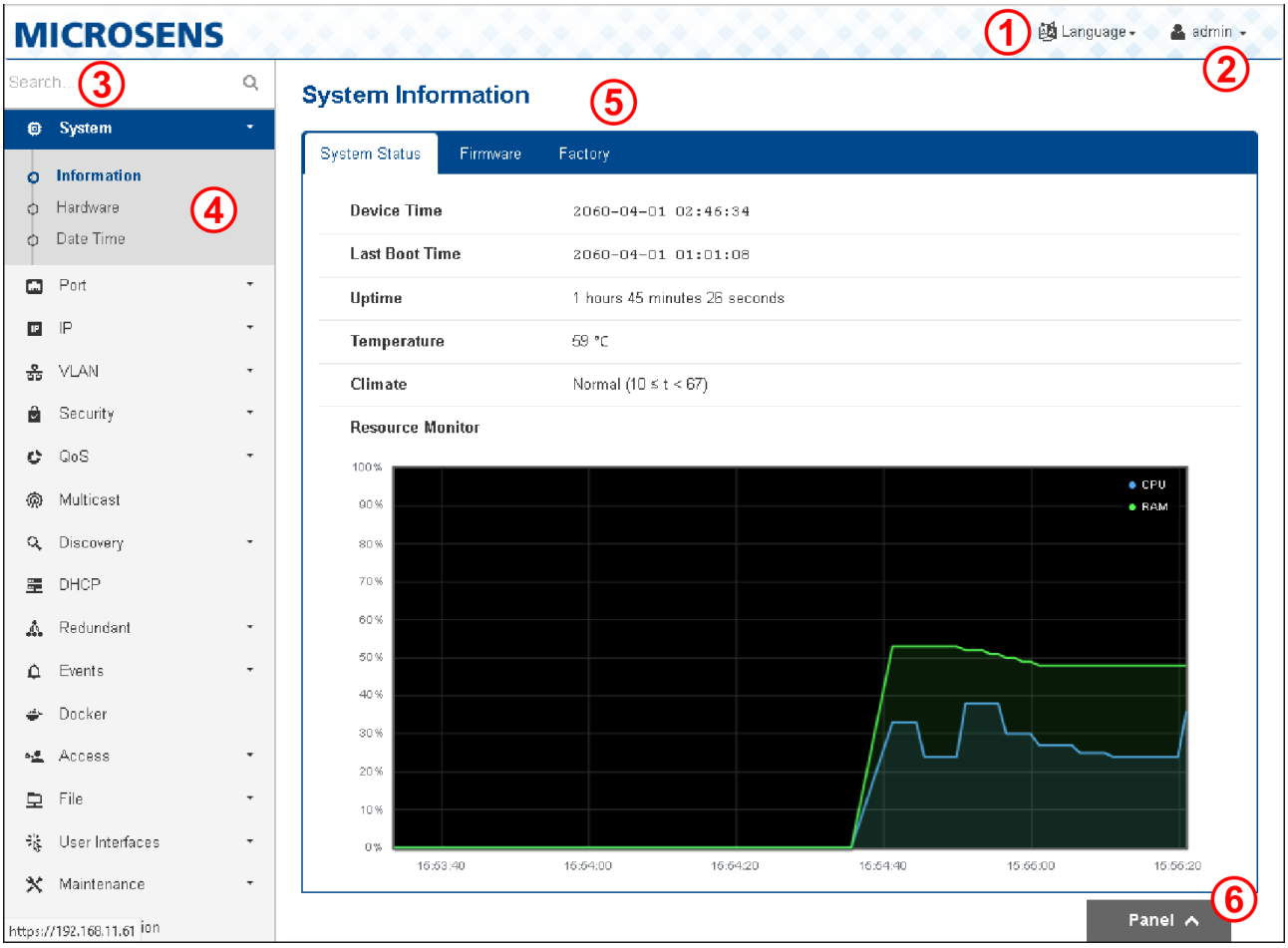


Fig. 1: Web GUI Description

① - Language selector: Select the available language from the drop-down list.

② - Admin area. To logout from the web GUI, select "Logout" from the drop-down list.

③ - Live search: Enter a non-casesensitive keyword. A drop-down list shows all available menu entries. Click on a search result to open the respective menu entry.

④ - Menu pane

⑤ - Main area

⑥ - Device information panel: Click on the panel area to open the information panel.

4.2 Device Information Panel

The device information panel gives a quick visual overview of all the device's ports and their respective connection status.

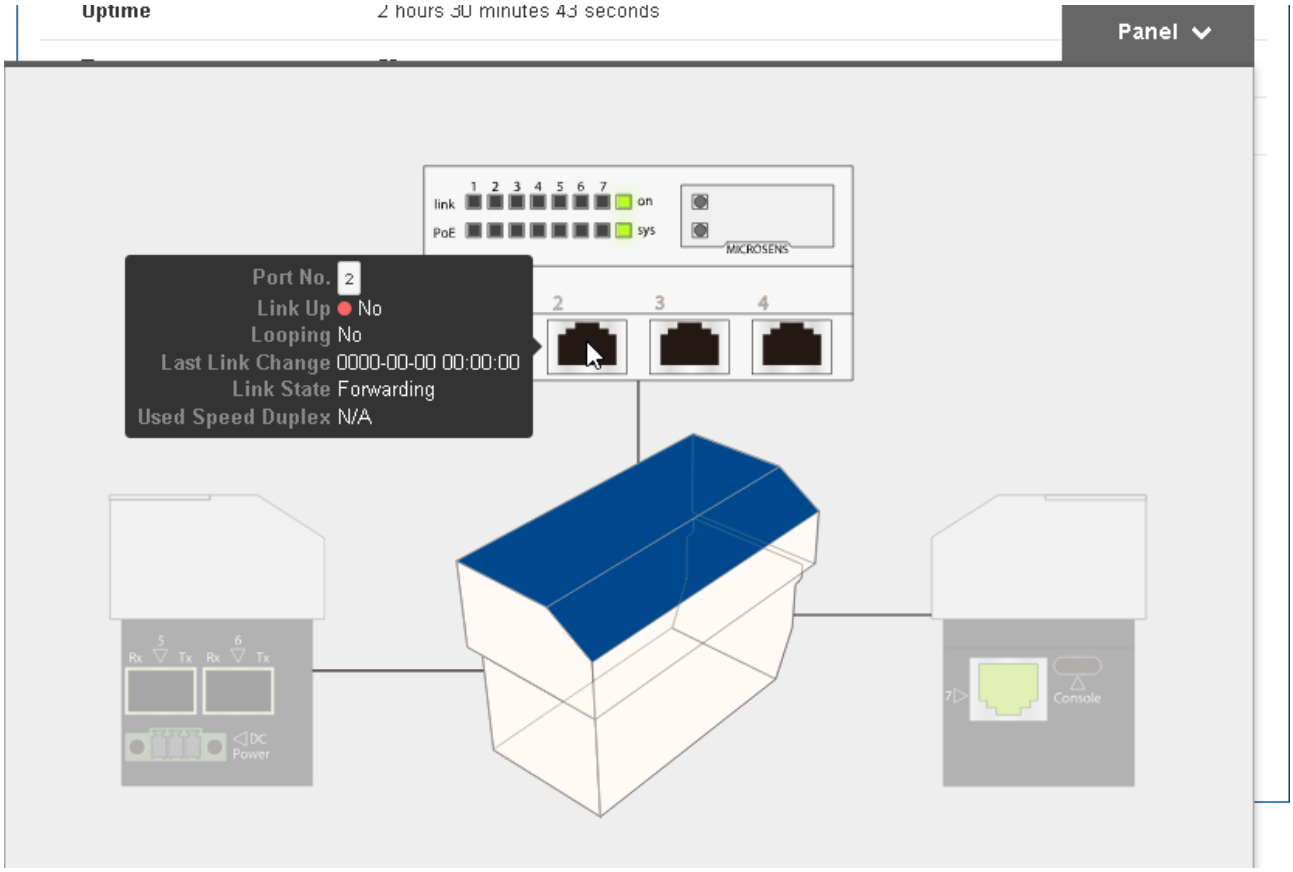


Fig. 2: Device Information Panel

When moving the cursor over the stylised image in the center, the specific housing side is activated.

When pointing the cursor to a port, a tooltip with its current status values opens.

Click on the panel area on the top right to close the information panel.

4.3 Tooltip Help

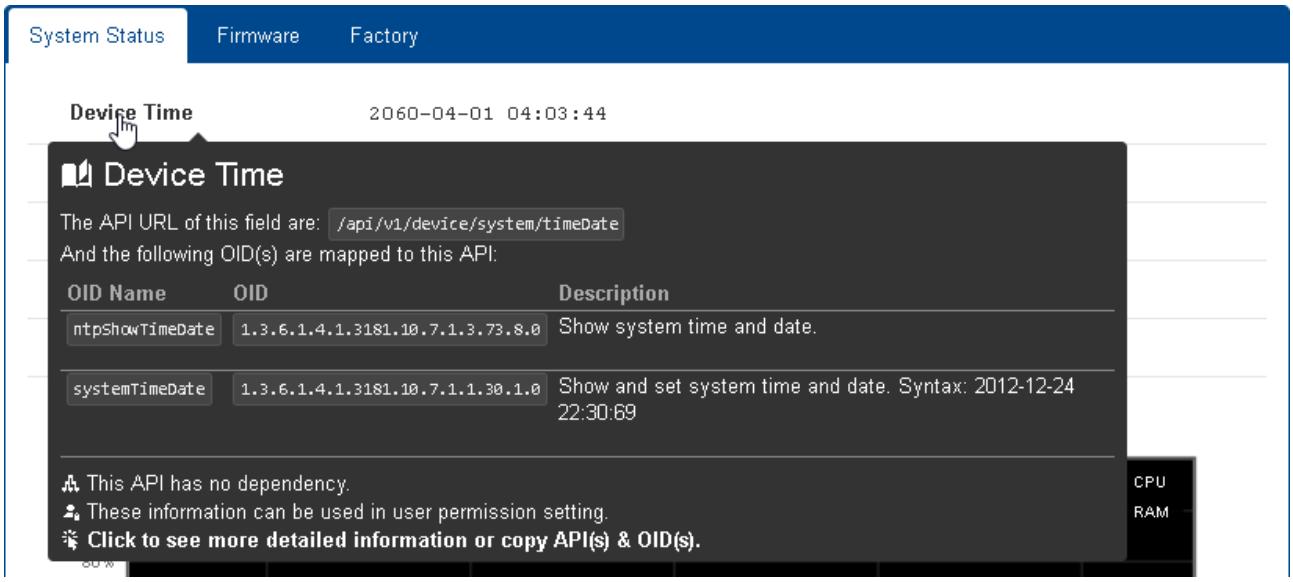


Fig. 3: Label Tooltip Help

When moving the cursor over a dialogue label, a tooltip opens containing information of associated OID and API values.

When clicking on a dialogue label, a pop-up window opens providing the opportunity to copy API or OID values to the clipboard.

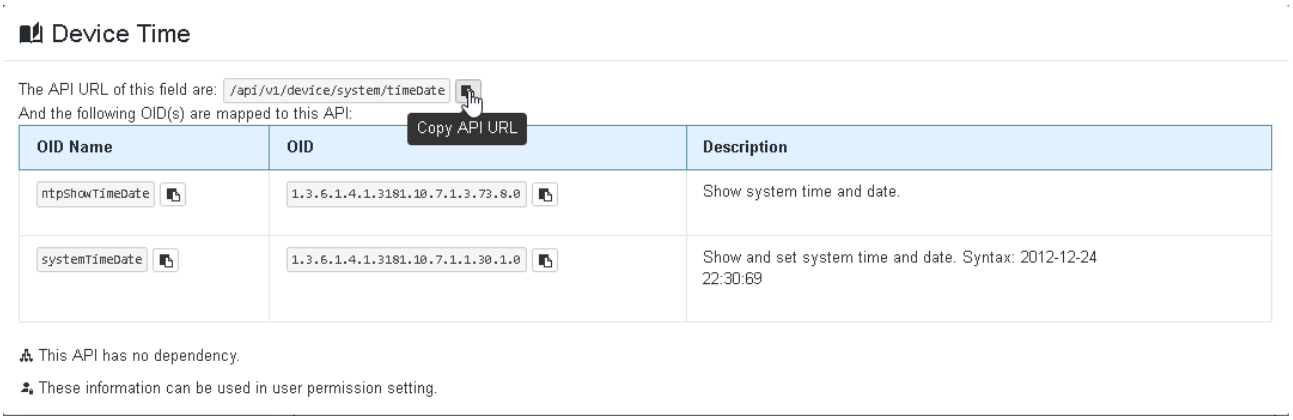


Fig. 4: Label Popup Window

Clicking anywhere else in the web GUI closes the popup window.

5 Main Menu

5.1 Overview

Set up the 10G Micro Switch by selecting one of the functions listed in the main menu.

Menu • Submenu	**Tabs and Sections**
System	
• Information	• System Status • Firmware • Factory
• Hardware	• Ports • LEDs • Configuration • LED Test • Wake On LAN • Cable Test Configuration • Cable Test Status
• Date Time	• Configuration • Status
IP	
• Basic	• Configuration
• V4	• Configuration • Status
• V6	• Configuration • Status
• Diagnosis	• Ping • Trace Route • DNS Lookup • ARP Table

Menu • Submenu	**Tabs and Sections**
Vlan	
• Basic	• Basic Configuration • Port Configuration • VLAN Table • Priority Override • Status
• MVRP	• Basic • Port Configuration • Port Status
Security	
• Mac Table	• Configuration • MAC Table • Authorized MAC Table
• PACC	• Basic Configuration • Port Configuration • Port Authentication • Locking Table • 802.1X Supplicant • Port Status • User Status • Supplicant Status
• ACL	• Basic • Ports • List • Rules
• Storm Control	• Configuration
Qos	
• Basic	• Mode • Priority Scheme
• Mapping	• CoS/802.1p to Queue • DSCP to Queue

Menu • Submenu	**Tabs and Sections**
• Interface	
• Rate Shaping	
Multicast	• Configuration • Static Group • Status • Statistics
Discovery	
• LLDP	• Configuration • Local Information • Neighbor Information • Statistics
• CDP	• Configuration • Local Information • Neighbor Information • Statistics
DHCP	• DHCP Relay • DHCP Snooping • PPPoE Snooping • ARP Inspection • Status
Redundant	
• STP	• Bridge Configuration • Ports Configuration • MSTP Groups • Status
• G.8032	• G.8032 Configuration • G.8032 Status
• MS Ring	• Configuration • Status • Statistics

Menu • Submenu	**Tabs and Sections**
Events	
• Actions	• Configuration
• Logs	• Configuration • Targets • Recent Logs • Logs • Statistics
Docker	• Overview • Image • Container • Archive
Access	
• Authentication	• Configuration
• Authentication Servers	• Configuration
• User Permission	• User • Group
• Restriction	• Configuration
• Status	
File	
• Server	• Configuration
• Certificate	• Configuration • Certificate Files
User Interfaces	
• CLI	• Configuration • Status
• Web	• Configuration • Timeout • Actions

Menu • Submenu	**Tabs and Sections**
• SNMP	• Configuration • Browser • Status • Actions
Maintenance	
• Configuration	• Save • Factory • Reset • Import & Export • Compare • Show
• CLI Script	• Run
• Firmware	• Current • Previous
• Snapshot	
• Reboot	• Basic
Documentation	
About	

5.2 System

5.2.1 Information - System Status

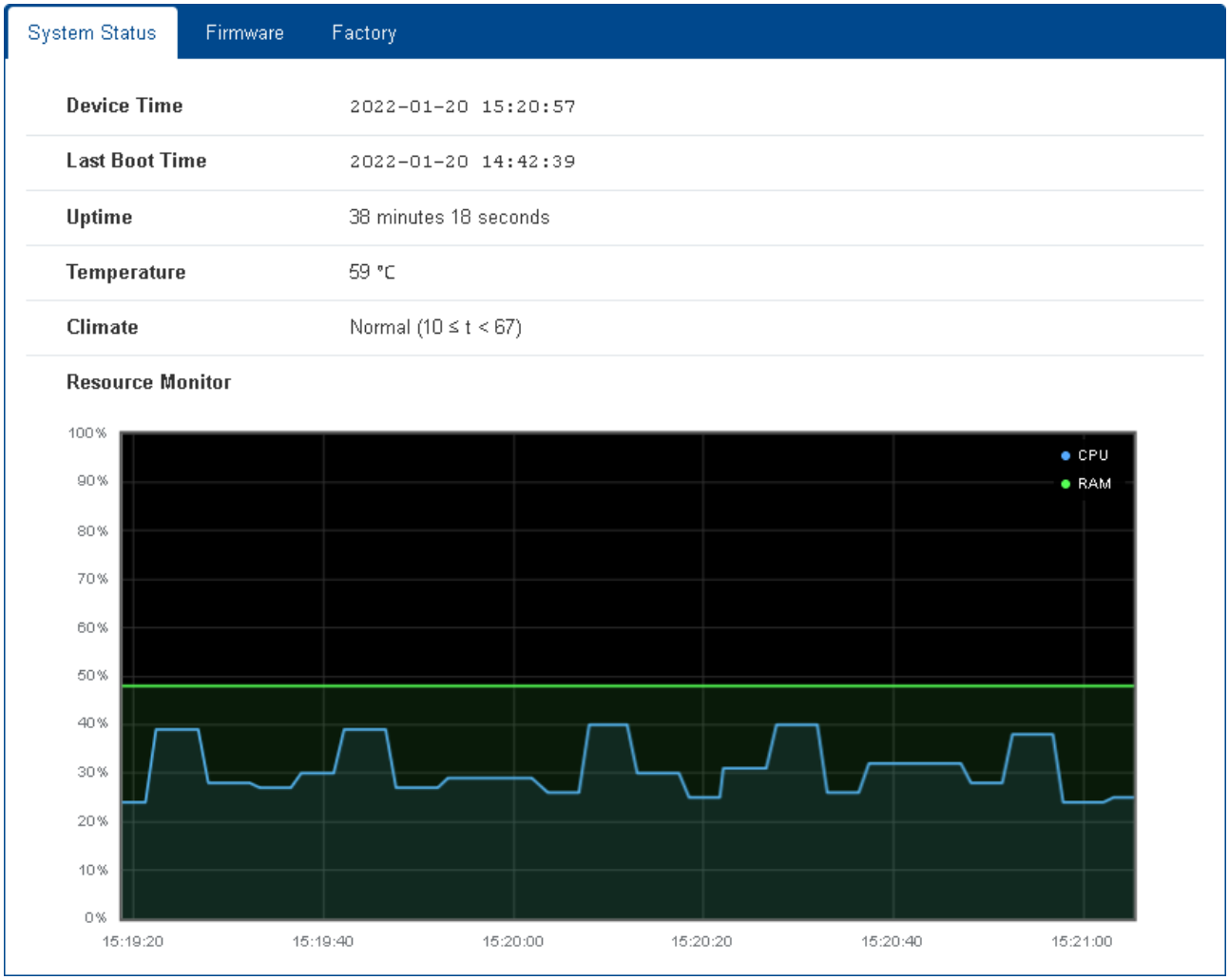


Fig. 5: System - Information - System Status

- **Device Time:** Current time setting of the device.

  For more information about setting time and date of the device please refer to section 5.2.11 on page 25.
- **Last Boot Time:** Date and time of the device's last boot.
- **Uptime:** The device's operating time since the last boot.
- **Temperature:** Current temperature inside the device's housing.
- **Climate:** Current annotated temperatur level of the device.
- **Resource Monitor:** Graphical overview of CPU and RAM load for the last 2 minutes

  Note:
  The timer restarts on reload of this dialogue.

5.2.2 Information - Firmware

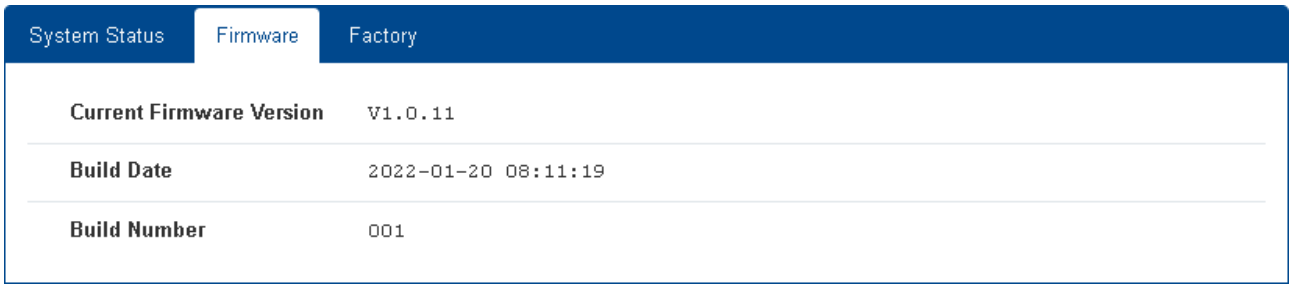


Fig. 6: System - Information - Firmware

- **Current Firmware Version:** The device can hold up to 2 firmware versions.

  This dialogue shows the currently active firmware version. For more information about managing the firmware please refer to section 5.17.8 on page 131.
- **Build Date:** Build date of the currently active firmware version.
- **Build Number:** Build number of the currently active firmware version.

Note:
When contacting our support in case of questions or problems, please keep these information at hand.

5.2.3 Information - Factory

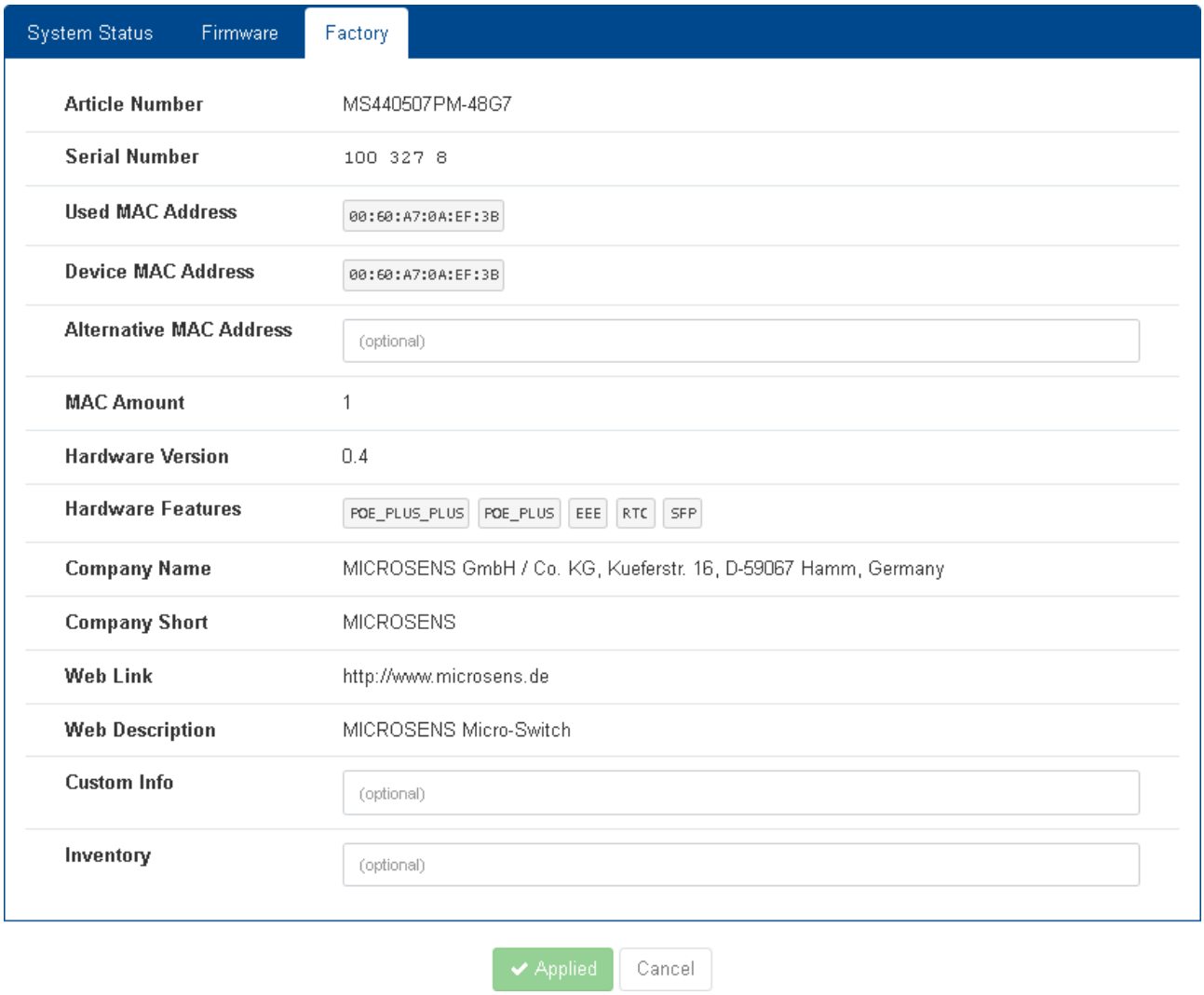


Fig. 7: System - Information - Factory

- **Article Number:** Article number of the device.
- **Serial Number:** Serial number of the device.
- **Used MAC Address:** MAC address used by this unit.

  Usually follows to device MAC address defined in the factory setting, but may be overwritten with the MAC address defined in the field **Alternative MAC Address**.
- **Device MAC Address:** Default MAC address.
- **Alternative MAC Address:** Enter a valid MAC address in the form "xx:xx:xx:xx:xx:xx" to override the factory setting.
- **MAC Amount:** Number of MAC addresses the device supports.
- **Hardware Version:** Hardware's revision number.
- **Hardware Features:** Hardware features available on this device.

- **Company Name/Company Short:** Complete and shorthand description of the manufacturer.
- **Web Link:** Web link to the manufacturers homepage.
- **Web Name:** Device's name as it is used in the web GUI.
- **Custom Info:** This field can be used to permanently store custom inventory or location data (up to 512 characters).

  This information is stored permanently within the device's non-volatile flash memory and thus will persist even when the SD card or the entire configuration is changed.
- **Inventory:** This field can be used to store an inventory string for customer use.

  This information is stored on the SD card and may change when config or SD card is exchanged.

  For an inventory information that is fixed to the hardware use the field **Custom Info**.

Note:
When contacting our support in case of questions or problems, please keep these information at hand.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.2.4 Hardware - Ports

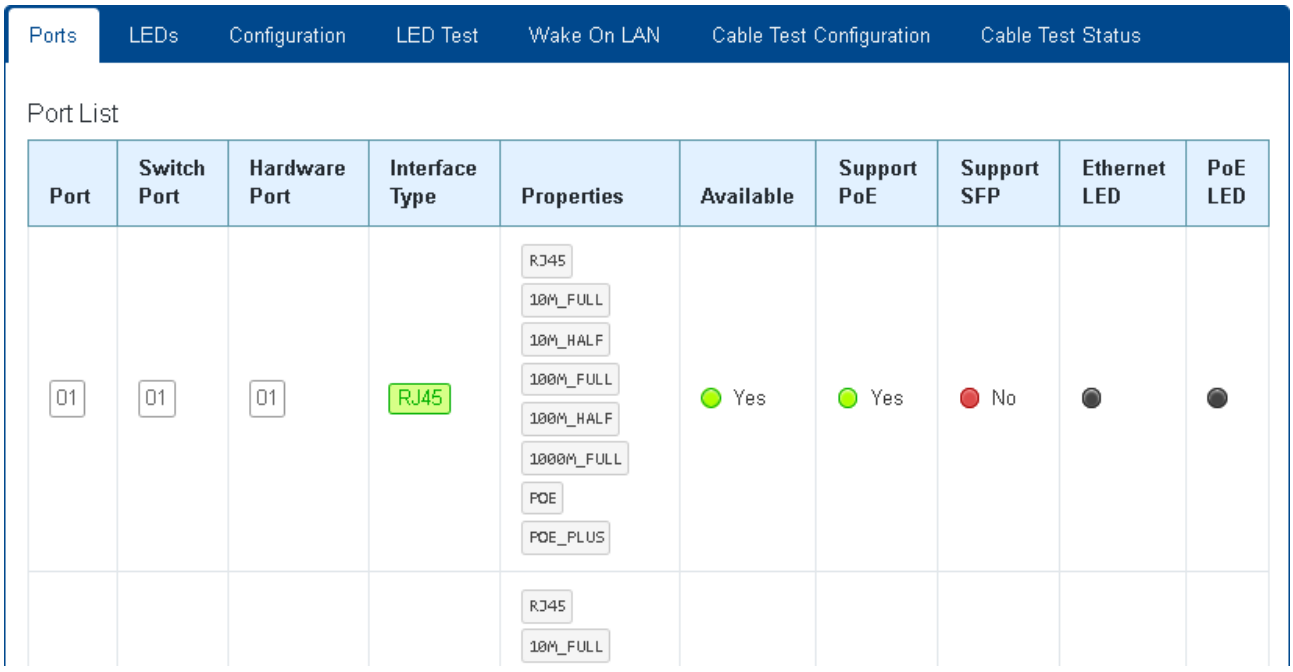


Fig. 8: System - Hardware – Ports

The port list gives a quick tabular overview of all physical and logical port settings.

5.2.5 Hardware - LEDs

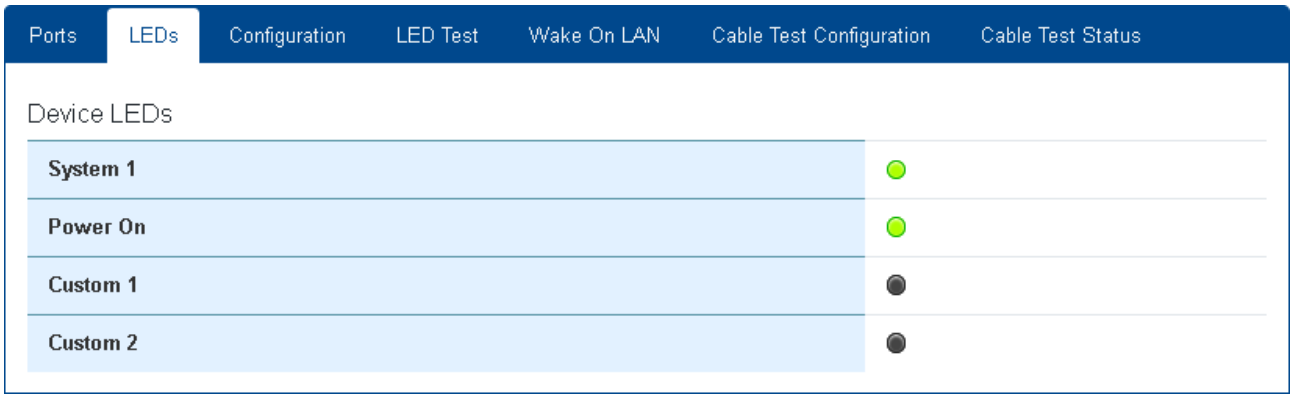


Fig. 9: System - Hardware – LEDs

The LED list gives a quick overview of the device's LED status (see section 1.2.1 on page 7).

5.2.6 Hardware - Configuration

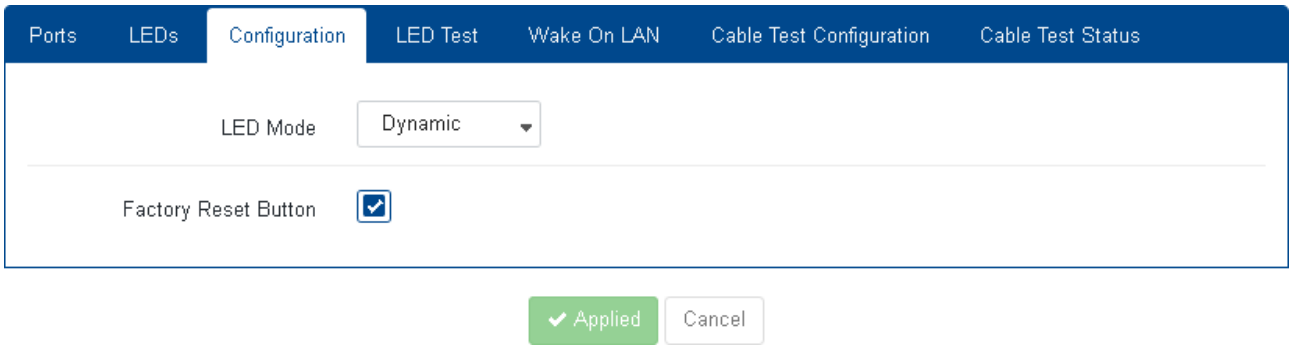


Fig. 10: System - Hardware – Configuration

- **LED Mode:** Select one of the following LED modes from the drop-down list:
  - **Static LED:** LEDs display static port states only, but do not blink on data flow.
  - **Dynamic:** LEDs display both static port states (light) and data flow (blink).
  - **Quiet Display:** All LEDs are off, except LEDs "on" and "sys".
  - **Dark all LED:** All LEDs are off, except LED "on".
  - **Lightsshow:** All LEDs light up in all available colors.
- **Factory Reset Button:** Enable or disable the device's factory reset button (see section 1.2.1 on page 7).

  Note:
  The IP discovery function with a short button click is not affected.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.2.7 Hardware - LED Test

Fig. 11: System - Hardware – LED Test

- **LED Self Test:** Click on the button **Start** to perform an LED test.

  All LEDs will light in different colors awhile.

  Tip: This may be helpfull to locate a device among others.

5.2.8 Hardware - Wake On LAN

It is possible to send a "Wake on LAN" data paket to one specific network device as follows:

Fig. 12: System - Hardware - Wake On LAN

- **Send Wake On LAN Packet:** Enter the MAC address of the specific network device in the field.
- **Send:** Click on this button to wake up the respective device.

  Note: Make sure that the connected network device has Wake on LAN function enabled.

5.2.9 Hardware - Cable Test Configuration

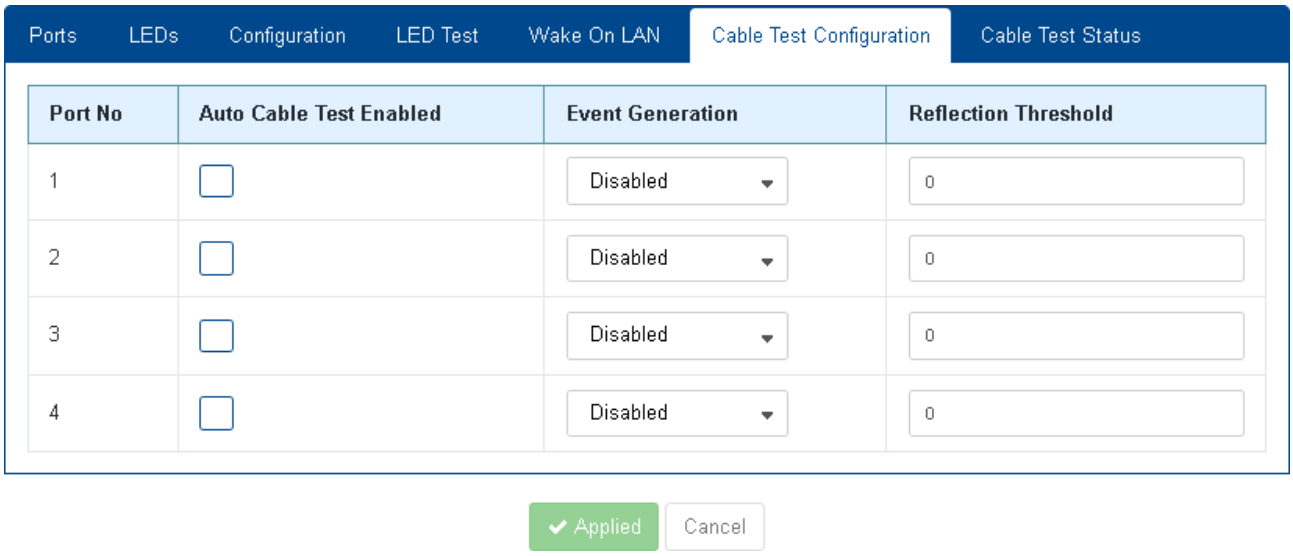


Fig. 13: System - Hardware - Cable Test Configuration

- **Port No:** Port number of the device.
- **Auto Cable Test Enabled:** When enabled the device executes a cable test on this port regularly.
- **Event Generation:** Enable or disable an event generation mode from the drop-down list:
  - Disabled: No event is generated in case of a cable failure.
  - Any change: Raise an event on any cable status change.
  - Connections only: Raise an event only on cable connection loss.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.2.10 Hardware - Cable Test Status

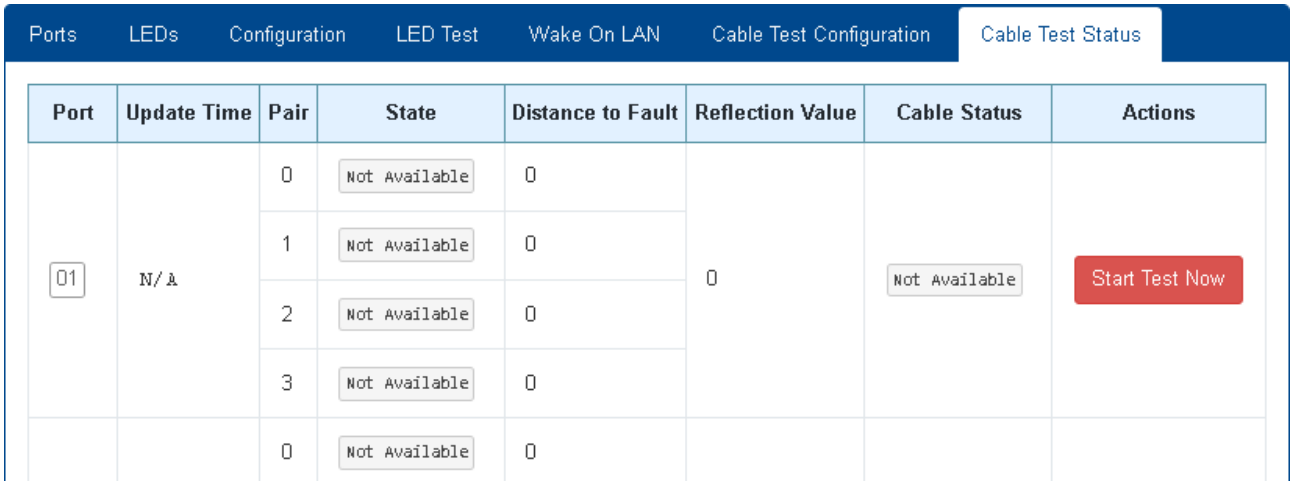


Fig. 14: System - Hardware - Cable Test Status

This tab offers to carry out a cable test on all ports.

- **Port:** Port number of device.
- **Update Time:** Latest time the cable test was executed for this port.
- **Pair:** Index number (0..3) of the twisted pair cables.
- **State:** Test result for every twisted pair cable of this specific port.
- **Distance to Fault:** Measured cable length to the port of the network communication partner or the occuring cable defect.
- **Reflection Value:** Reflection value in dB of the cable.
- **Cable Status:** Test result for the cable.

Click on the button **Start Test Now** to execute the cable test for the respective port. The table will show the test results:

The cable test highlights connection problems based on e.g. cable breakage (down to single twisted pair cables), unplugged cables or too expansive cable lengths.

5.2.11 Date & Time - Configuration

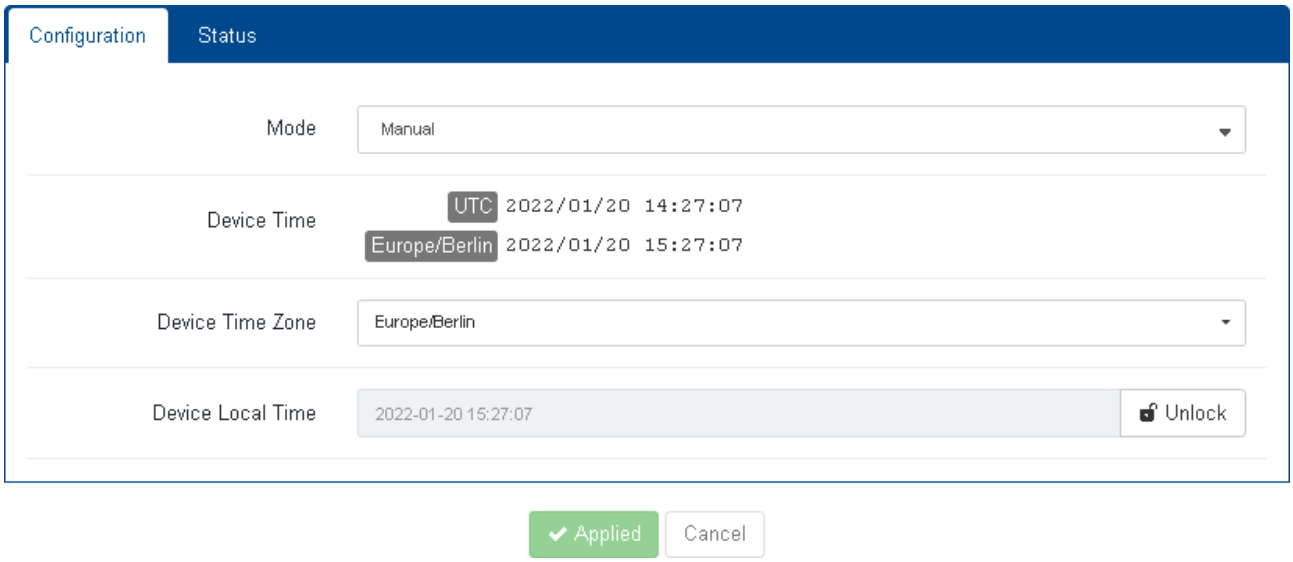


Fig. 15: System - Date & Time - Configuration

This tab offers the configuration of system time settings.

- **Mode:** Select one of both available time setting methods
  - **Manual:** Set time and date manually in the fields **TimeZone** and **Local Time**.
  - **Auto (Use NTP):** Enter the URL of an NTP server. This will synchronise the device's date and time regularly.
- **Device Time:** Shows current date and time setting of the device in UTC and selected time zone.
- **Device Time Zone:** With method "manual" enabled, select the time zone.
- **Device Local Time:** With method "manual" enabled, enter date and time manually.

  Click on the button **Unlock** to enable manual date and time setting.

  Click on the button **Get current browser time** to apply your browsers local time values to the device.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.2.12 Date & Time - Status

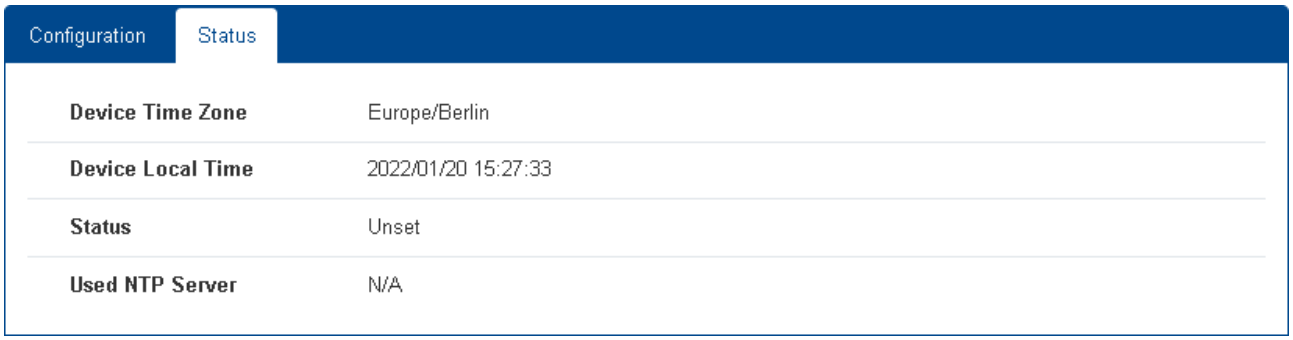


Fig. 16: System - Date & Time - Configuration

This tab shows the system's current time settings.

5.3 Port

5.3.1 Basic - Configuration

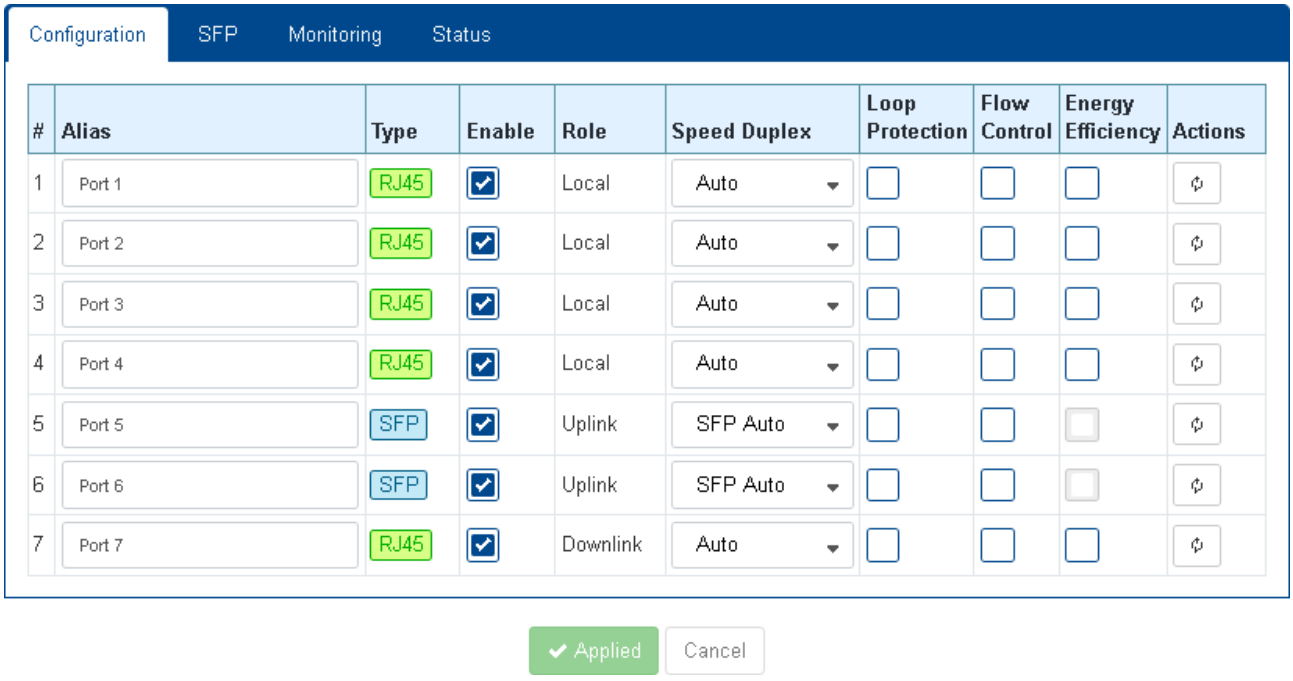


Fig. 17: Port - Basic - Configuration

This tab shows an editable tabular overview of the current ports configuration.

- **#:** Number of the specific hardware port.
- **Alias:** Descriptive name for this port.
- **Type:** Port connection type ("RJ45" or "SFP").
- **Enable:** Check or uncheck to enable or disable this port. If disabled, this port will not send or receive any data packets.
- **Role:** Dedicated port role ("Local", "Uplink", "Downlink").

- **Speed:** Select the port's speed setting from the drop-down list:
  - **Auto/SFP Auto:** The port will automatically negotiate the speed with the connected port.
  - **10Mbps / (Full/Half):** Sets the speed to 10 Mbit in full or half duplex mode.
  - **100Mbps / (Full/Half):** Sets the speed to 100 Mbit in full or half duplex mode.
  - **1Gbps / (Full/Half):** Sets the speed to 1000 Mbit in full or half duplex mode.
- **Flow Control:** Enable or disable flow control for this port.
- **EEE:** Enable or disable EEE (Energy Efficient Ethernet) function on this port.

  Note:
  EEE is not available for SFP ports.
- **Actions:** Click on the row-specific button to restart the respective port.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.3.2 Basic - SFP

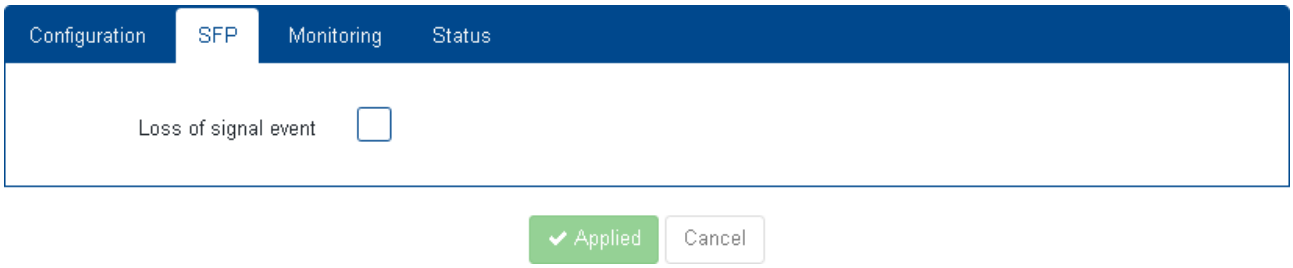


Fig. 18: Port - Basic - SFP

- **Loss of signal event:** Check or uncheck to enable or disable the device to generate an event in case of loss or comeback of an optical signal on one of the device's SFP ports.

5.3.3 Basic - Monitoring

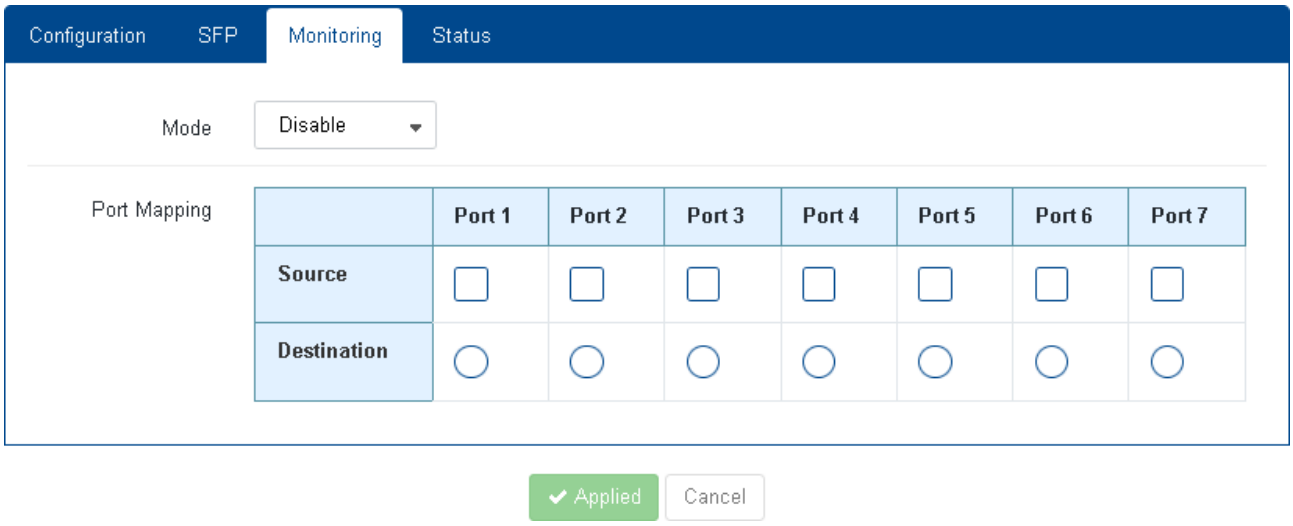


Fig. 19: Port - Basic - Monitoring

Port monitoring can help to analyse data traffic on specific ports by mirroring ingress or egress data communication to another port.

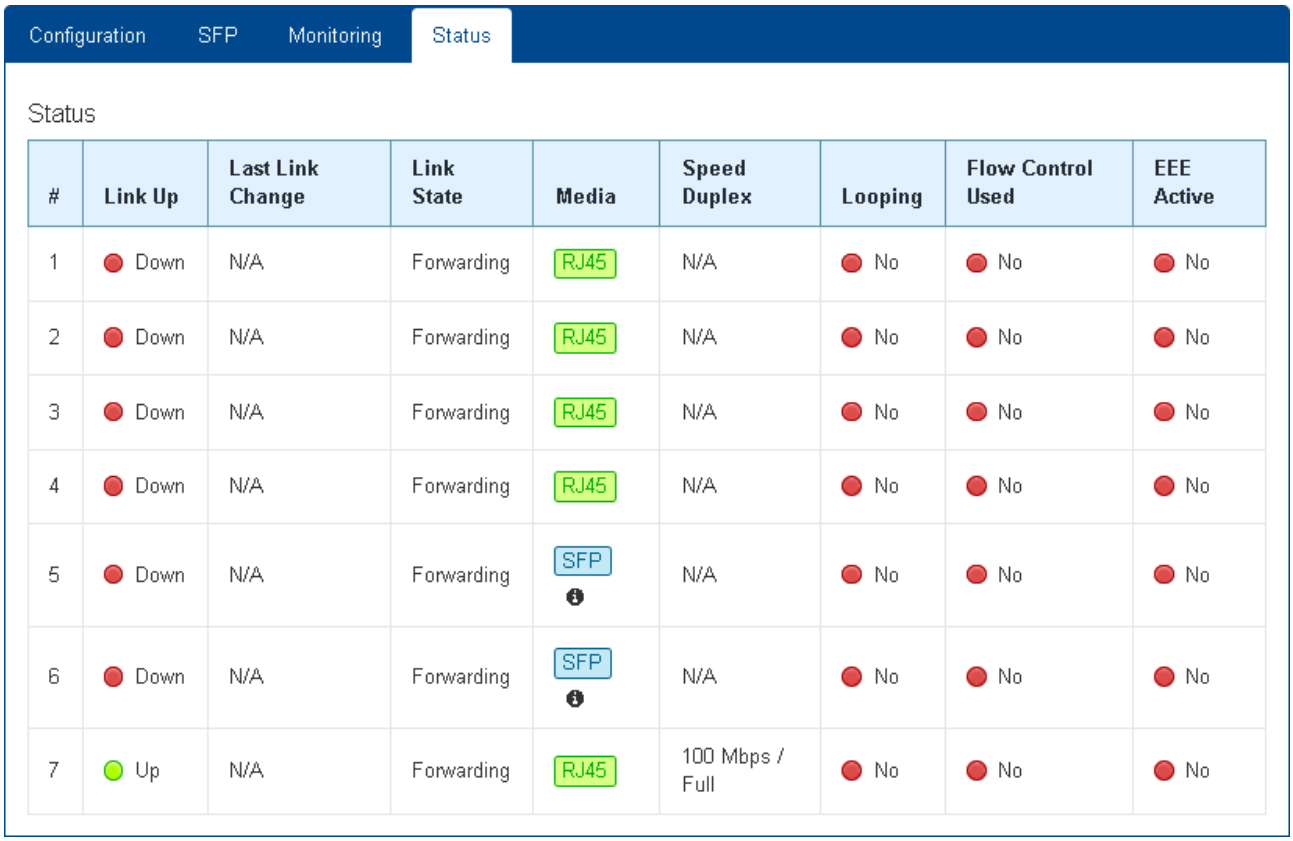
- **Mode:** Select one of the following modes from the drop-down list:
  - "Disable": No port monitoring. This is the default for normal operating.
  - "TX only": Monitor only transmitted data.
  - "RX only": Monitor only received data.
  - "Rx & TX": Monitor bit, transmitted and received data.
- **Port Mapping:**
  - Check the port you want to monitor as "Source" port.
  - Check the port you want to mirror the data to as "Destination" port.

  Note:
  It is not possible to mirror data of a port to itself.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Important: If the switch restarts, the port monitoring configuration is disabled!

5.3.4 Basic - Status



#	Link Up	Last Link Change	Link State	Media	Speed Duplex	Looping	Flow Control Used	EEE Active
1	Down	N/A	Forwarding	RJ45	N/A	No	No	No
2	Down	N/A	Forwarding	RJ45	N/A	No	No	No
3	Down	N/A	Forwarding	RJ45	N/A	No	No	No
4	Down	N/A	Forwarding	RJ45	N/A	No	No	No
5	Down	N/A	Forwarding	SFP	N/A	No	No	No
6	Down	N/A	Forwarding	SFP	N/A	No	No	No
7	Up	N/A	Forwarding	RJ45	100 Mbps / Full	No	No	No

Fig. 20: Port - Basic - Status

This tab gives a quick tabular overview of the current status of every port.

5.3.5 PoE - Configuration

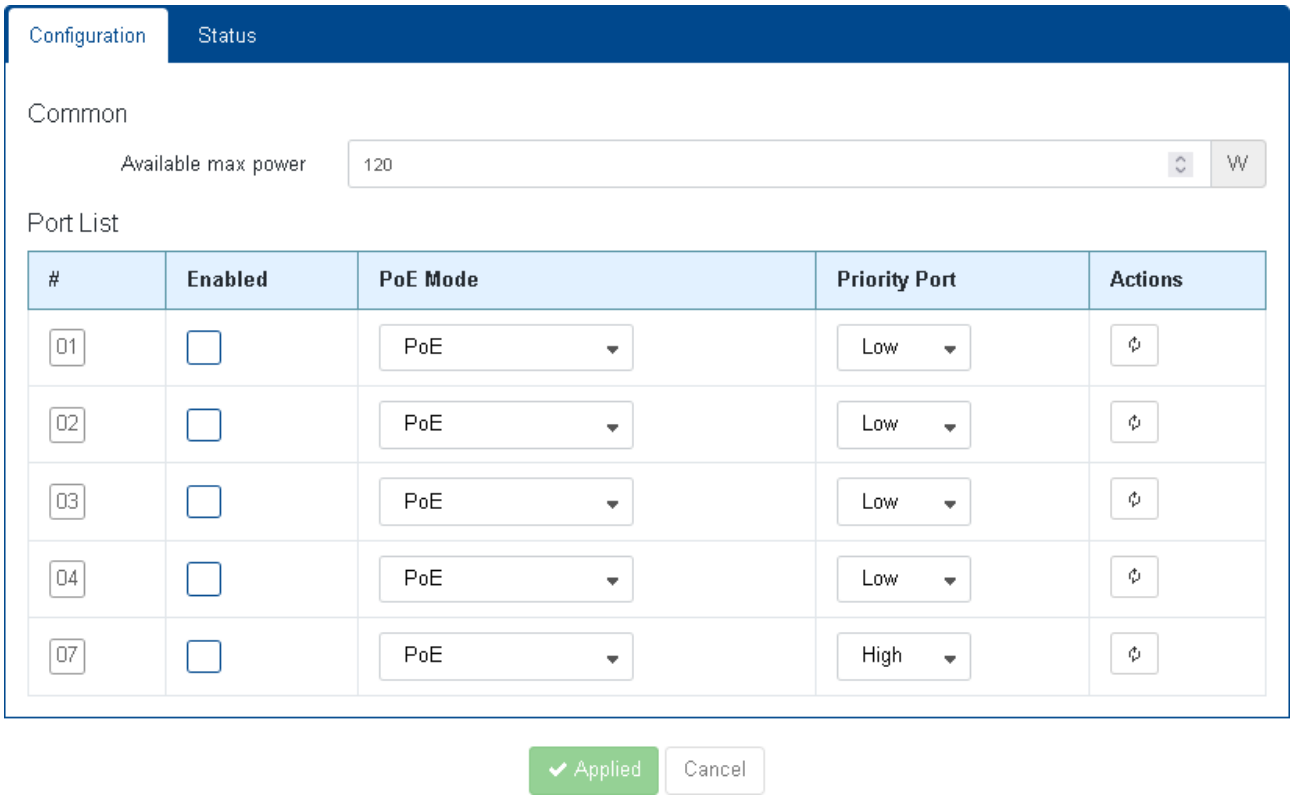


Fig. 21: Port - PoE - Configuration

This tab shows an editable tabular overview of the PoE settings of all ports.

- **Available max. Power:** Set the maximum power for all PoE ports combined in W (Watts).
- **#:** Index number of all ports of the device.
- **Enable:** Check or uncheck this option to enable or disable PoE for the respective port.
- **PoE Mode:** Select one of the following PoE modes from the drop-down list:
  - "PoE": PoE type 1 (IEEE 802.3af), max. port power: 15.4 W
  - "PoE+": PoE type 2 (IEEE 802.3at), max. port power: 30 W
  - "PoE++": PoE type 3 (IEEE 802.3bt), max. port power: 60 W
  - "LLDP Controlled": Enable automatic PoE configuration via LLDP.

  Note:
  Only port 7 supports PoE++!

  Note:
  LLDP has to enabled with "LLDP Controlled" selected!
- **Priority Port:** Choose the priority for the PoE port from the drop-down list:
  - "Low": When the combined power output of all PoE ports exceeds the assigned maximum power, a low priority port will be powered off first.

- "Medium": When the combined power output of all active PoE ports (without the powered off low priority ports) exceeds the assigned maximum power, a medium priority port will be powered off second.
- "High": A PoE port with high priority will be powered at last, if the power output of all remaining PoE port (without low and medium priority) will exceed the assigned maximum available power.
- **Actions:** Click on the row-specific button to restart the respective port.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.3.6 PoE - Status

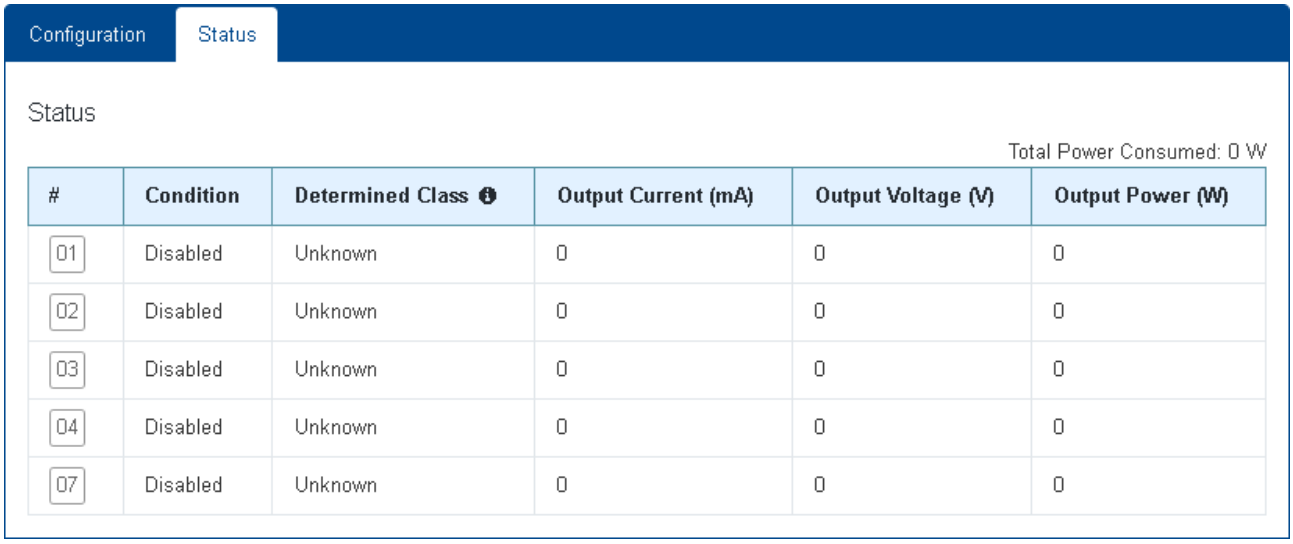


Fig. 22: Port - PoE - Status

This tab shows a tabular overview of the PoE status of all ports.

- **Total Power Consumed:** The power currently delivered to all PoE enabled ports.
- **#:** Index number of all ports of the device.
- **Condition:** PoE status of the specific port.
- **Determined Class:** The currently assigned PoE class (Class 1 to Class 6).
- **Output Current (mA)**: Shows the current in mA (Milliampere) the port provides, as soon as the port is connected to a powered device (PD).
- **Output Voltage (V)**: Shows the voltage in V (Volt) the port provides, as soon as the port is connected to a powered device (PD).
- **Output Power (W)**: Shows the power in W (Watt) the port provides, as soon as the port is connected to a powered device (PD).

5.3.7 Aggregation - Configuration

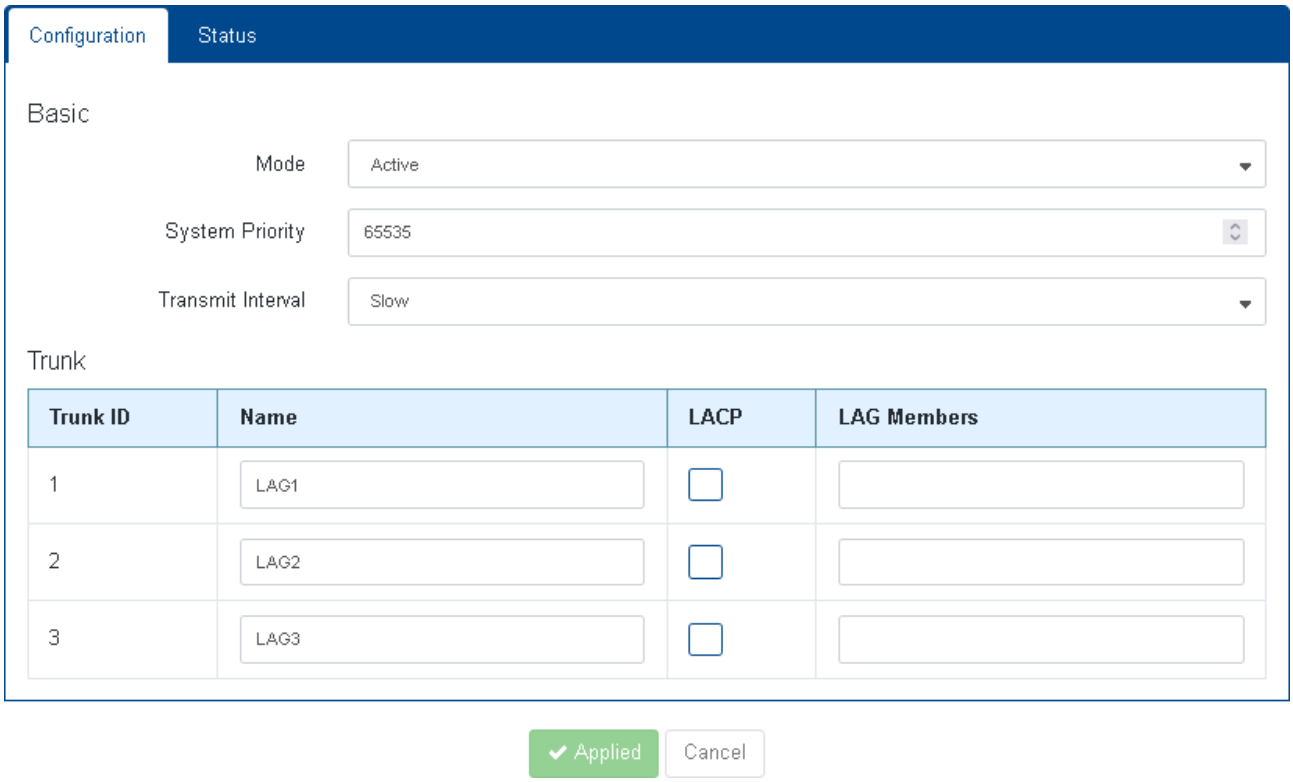


Fig. 23: Port - Aggregation - Configuration

It is possible to use Link Aggregation Control Protocol (LACP) to combine two or more ports for higher transfer rates or better availabilty of data transfer.

- **Mode:** Select the LACP mode from the drop-down list:
  - "Active": The device actively negotiates an LACP connection with a remote partner, no matter, whether the partner is configured in active or passive LACP mode.
  - "Passive": The device waits for the remote partner to negotiate an LACP connection.
- **System Priority:** The system priority determines which of the communicating LACP devices decides to use which LACP ports. The lower the priority value the highr the priority.
- **Transmit Interval:** Select one of the following values from the drop-down list:
  - "Slow": The device sends LACP control packets within longer periods.
  - "Fast": The device sends LACP control packets within a short period.
- **Trunk ID:** Index number of the link aggregation group (LAG).
- **Name:** Descriptive name for this group.
- **LACP:** Check or uncheck to enable or disable LACP for this group.
- **LAG Members:** Enter the port numbers (comma-separated) which should be part of the LAG.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.3.8 Aggregation - Status

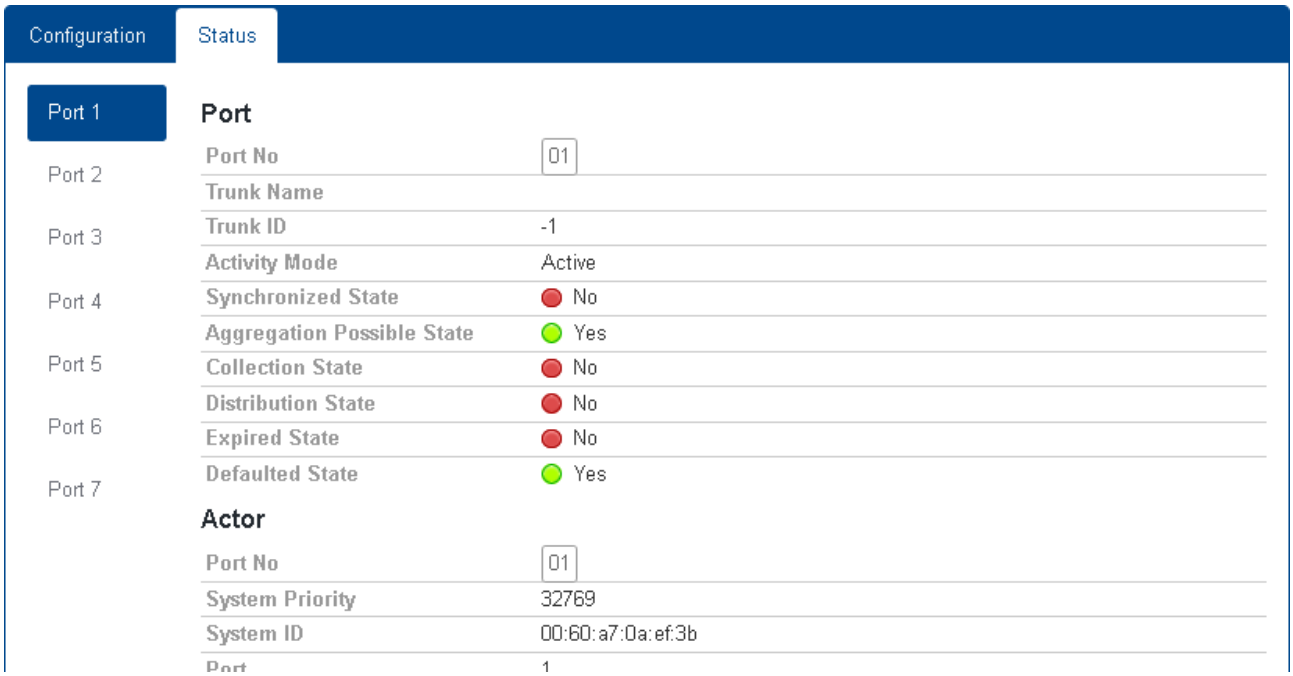


Fig. 24: Port - Aggregation - Status

This tab shows an overview of all LACP ports.

Select the respective port from the left-hand pane menu to view the LACP status of the specific port.

5.3.9 Counter

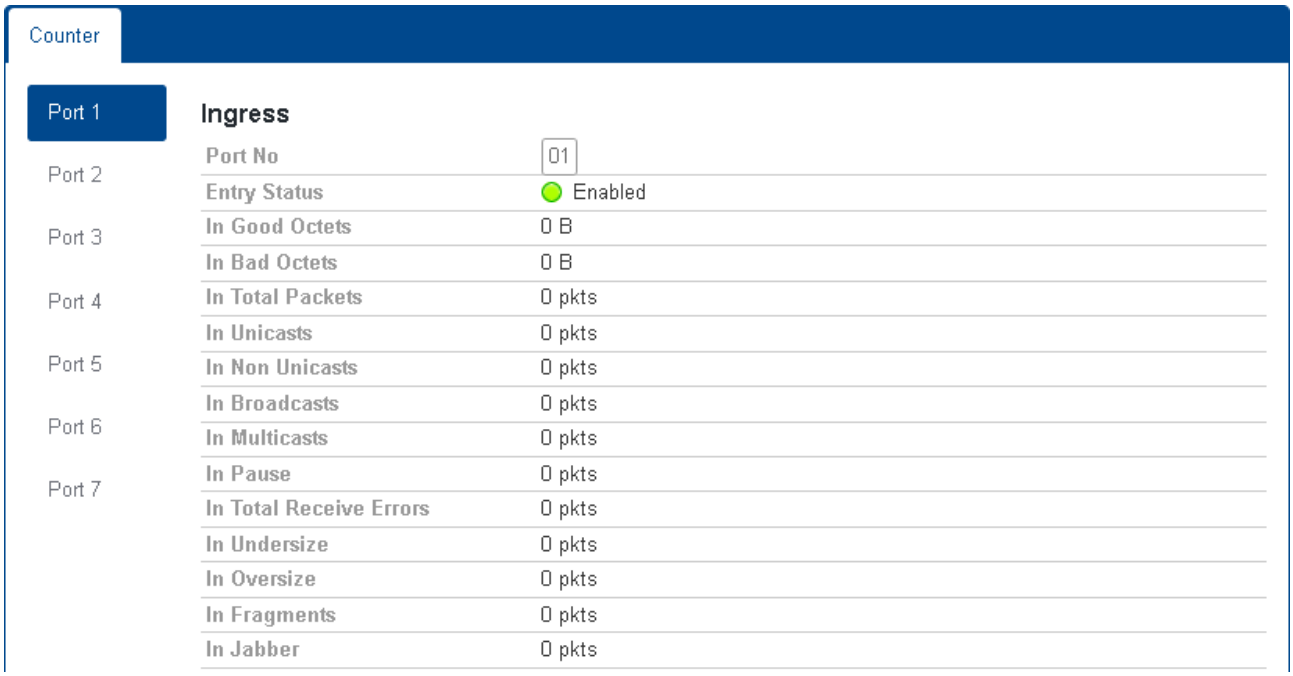


Fig. 25: Port - Counter

This tab shows detailed statistics for ingress and egress data transfer of all ports.

Click on the button **Clear All Counter** at the bottom of the tab to delete all statistics data and start collecting new data.

5.4 IP

5.4.1 Basic - Configuration

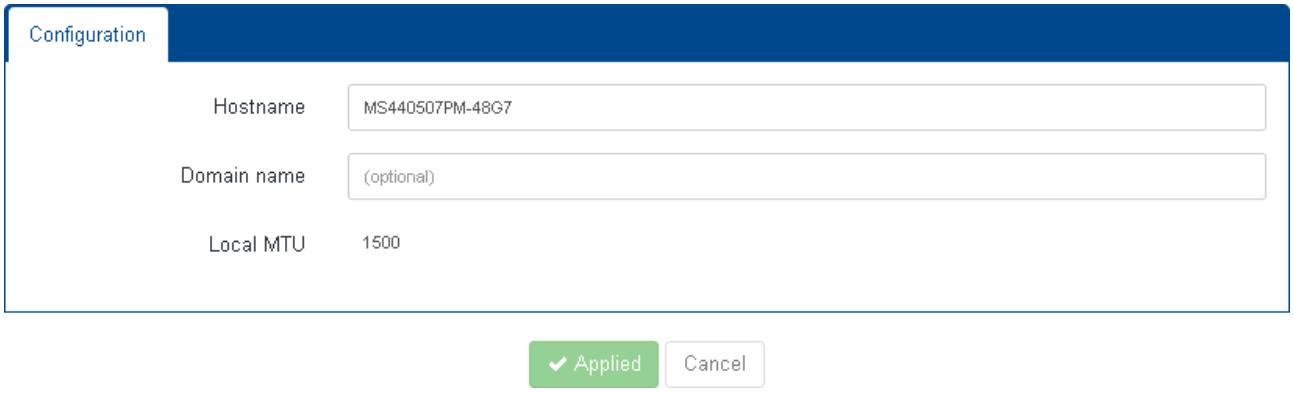


Fig. 26: IP - Basic - Configuration

- **Hostname:** Enter a descriptive hostname for this device. The hostname identifies the device, among others, on a network.
- **Domain name:** Defines an optional domain name used during name resolution (max length: 128 characters)

- **Local MTU:** The Maximum Transmission Unit (MTU) for locally generated data (1500 by default).

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.4.2 V4 - Configuration

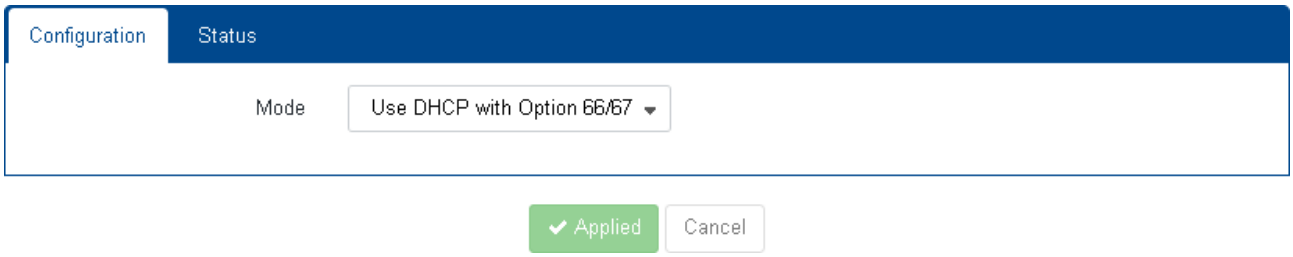


Fig. 27: IP - V4 - Configuration

- **Mode:** Select one of the following DHCP modes from the drop-down list:
  - "Static": Disables DHCP. The dialogue extends to enter the necessary static IP settings.

    Note:
    With DHCP enabled, DHCP overwrites existing static IP settings.
  - "Use DHCP": Enables DHCP.

    Note:
    A DHCP server has to be available in the network.
  - "Use DHCP with Option 66/67": Enables DHCP using the options 66 and 67 for retrieving a valid IPv4 configuration file.

    Note:
    Both, at least one DHCP server with options 66 and 67 enabled and at least on TFTP server providing the configuration file for download have to be available in the network
- **Primary IP:** Static primary IPv4 address of the device.
- **Primary Subnet Mask:** Static primary IPv4 subnet mask of the device.
- **Gateway:** Static gateway IPv4 address (optional).
- **DNS Server:** Static DNS server IPv4 address (optional).
- **Secondary IP:** Static secondary IPv4 address of the device (optional).
- **Secondary Subnet Mask:** Static secondary IPv4 subnet mask of the device.
- **Default Address Selection:** Select from the drop-down list, which IPv4 address should be used by the device.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.4.3 V4 - Status

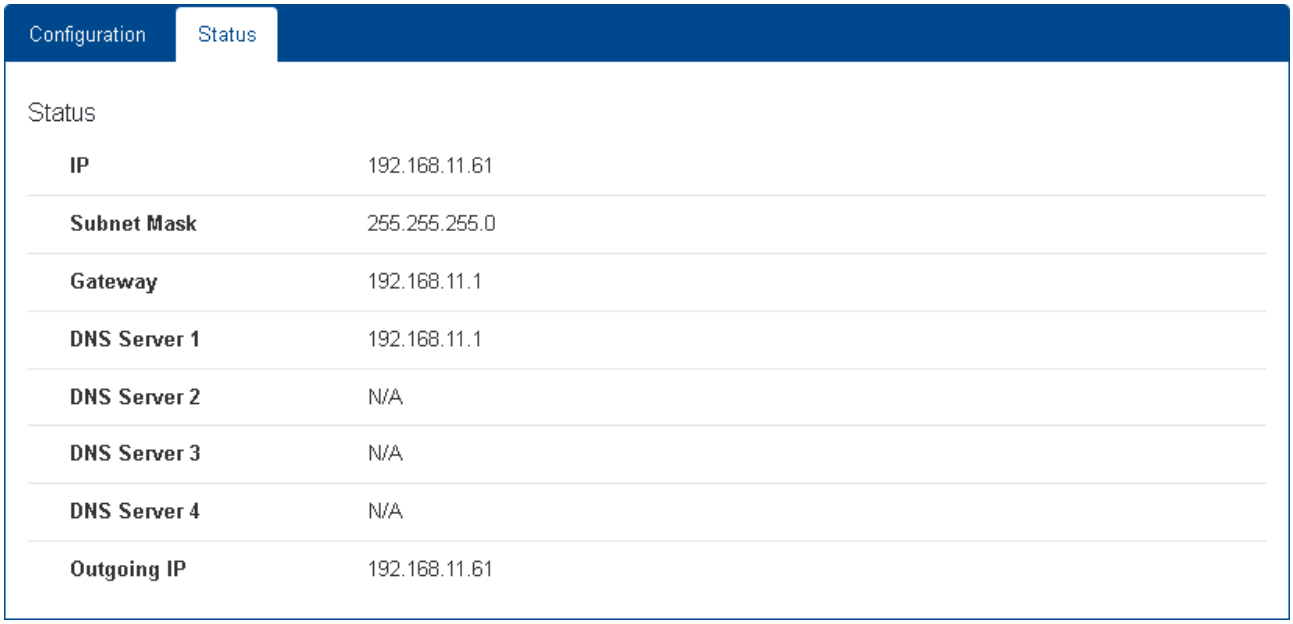


Fig. 28: IP - V4 - Status

This tab shows a tabular overview of the device's current IPv4 settings.

5.4.4 V6 - Configuration

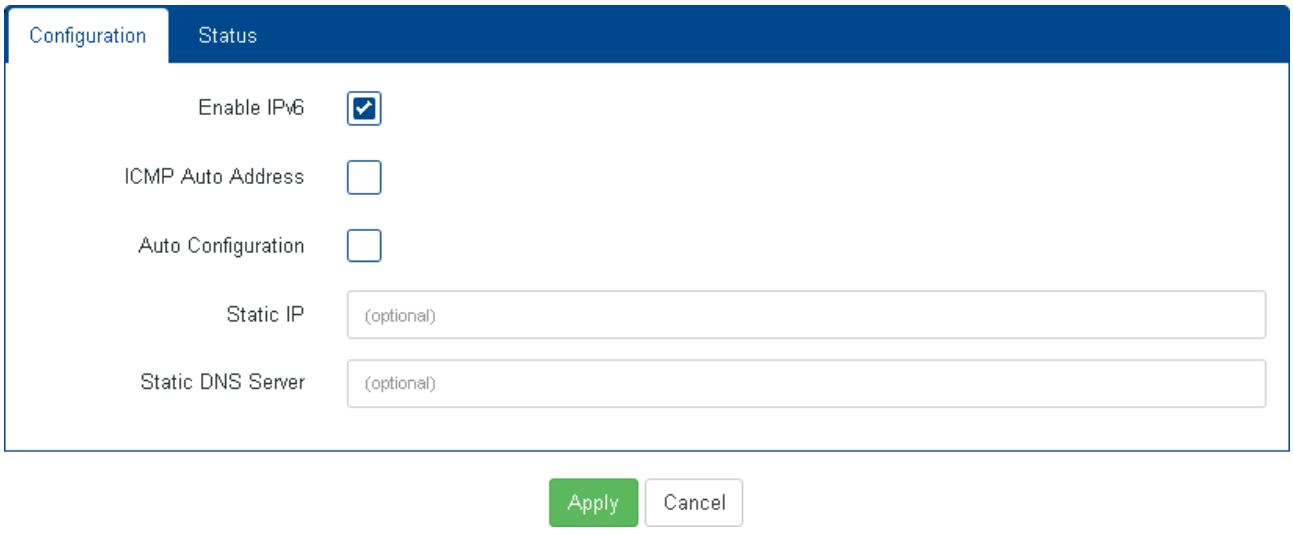


Fig. 29: IP - V6 - Configuration

- **Enable IPv6:** Check or uncheck this option to enable or disable IPv6, When enabled, all IPv6 settings become visible.
- **ICMP Auto Address:** Check or uncheck this option to enable or disable automatic address setting via ICMP.
- **Auto Configuration:** Check or uncheck to enable or disable automatic IPv6 address settings via DHCP.

- **Static IP:** Static IPv6 address (optional).
- **Static DNS Server:** Static DNS server IPv6 address (optional)

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.4.5 V6 - Status

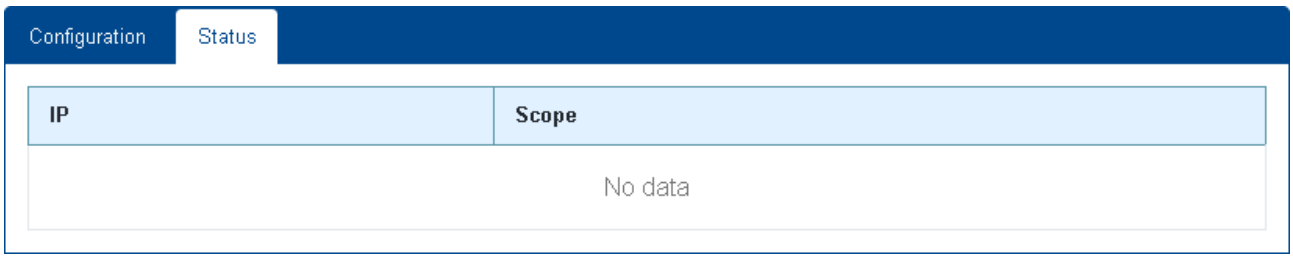


Fig. 30: IP - V6 - Status

This tab shows a tabular overview of the device's current IPv6 settings.

5.4.6 Diagnosis - Ping

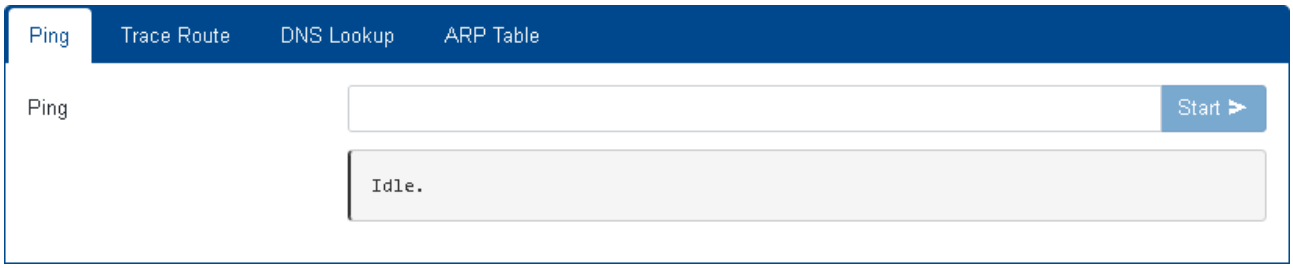


Fig. 31: IP - Diagnosis - Ping

This tab offers a ping function to test the availability of network devices.

- **Ping:** Enter a valid address and click on the button **Start**.
  After a short while the status dialogue below displays the resulting ping statistics.

After a short while the ping statistics appear below the button.

5.4.7 Diagnosis - Trace Route

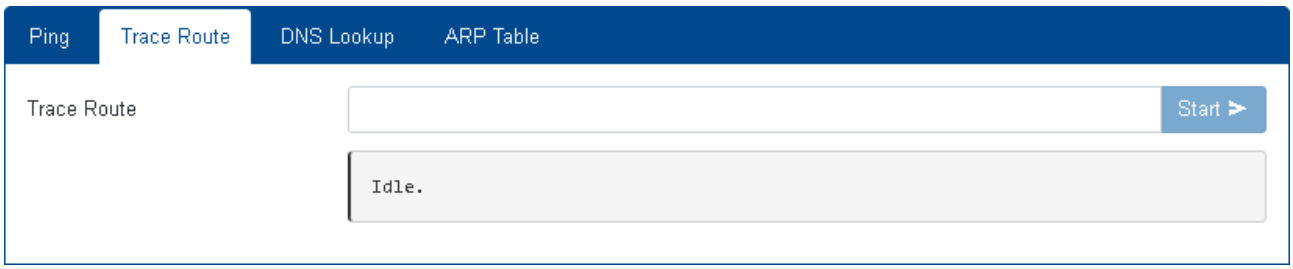


Fig. 32: IP - Diagnosis - Trace Route

5.4.8 Diagnosis - DNS Lookup

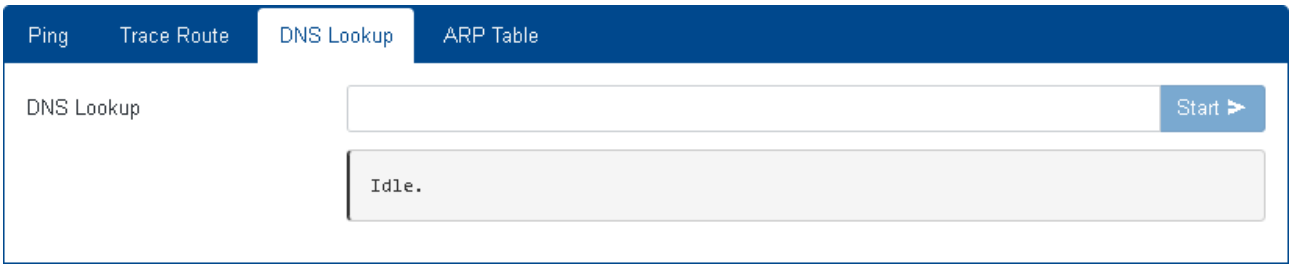


Fig. 33: IP - Diagnosis - DNS Lookup

5.4.9 Diagnosis - ARP Table

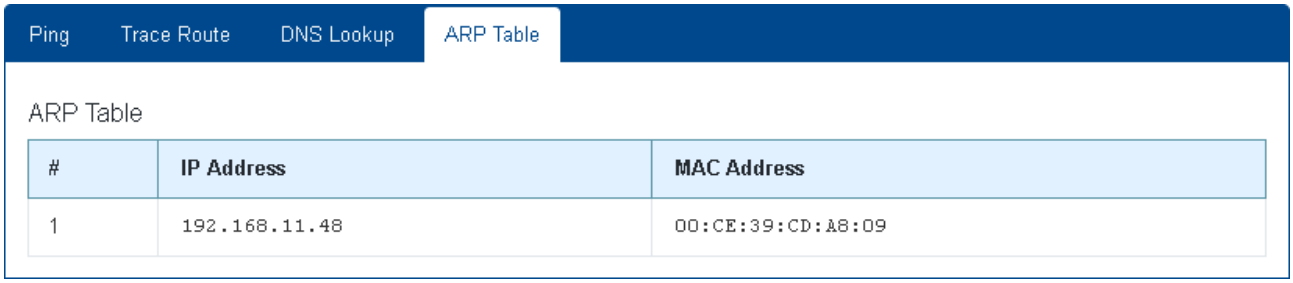


Fig. 34: IP - Diagnosis - ARP Table

This tab shows a tabular overview of MAC addresses and their corresponding IP addresses.

5.5 VLAN

5.5.1 Basic - Basic Configurations

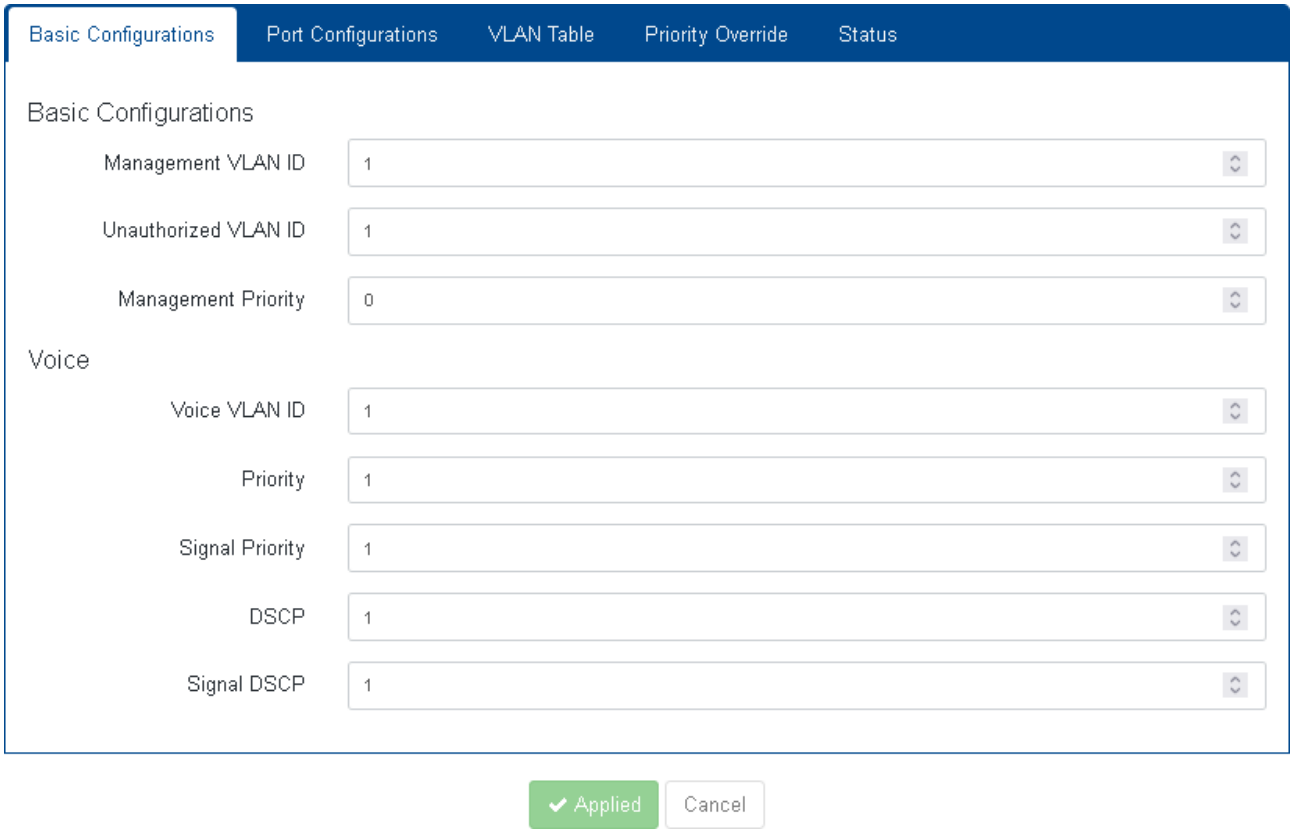


Fig. 35: VLAN - Basic - Basic Configuration

- **Management VLAN ID:** Enter the VLAN id for accessing the switch. If one port is in access mode and the default VLAN ID is identical to the management VLAN ID, then this port has management access to the switch.
- **Unauthorized VLAN ID:** When port authorization is enabled and authentication fails, the port can be set to this VLAN ID.
- **Management Priority:** Set the VLAN priority for internal management port.

  Packets sent by the internal management agent are tagged with this priority value.
- **Voice VLAN ID:** When connected e.g. to a Cisco VoIP phone, the switch can be auto configurated by the VoIP telephones using this VLAN ID.
- **Priority:** Assign the priority for the VoIP VLAN ID.
- **Signal Priority:** Set the signal priority for internal management port.

  Packets sent by the internal management agent are tagged with this priority value.
- **DSCP:** Assign the DSCP (Differentiated Services Code Point) for the VoIP VLAN ID.
- **Signal DSCP:** Assign the signal DSCP for the VoIP VLAN ID.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.2 Basic - Port Configurations

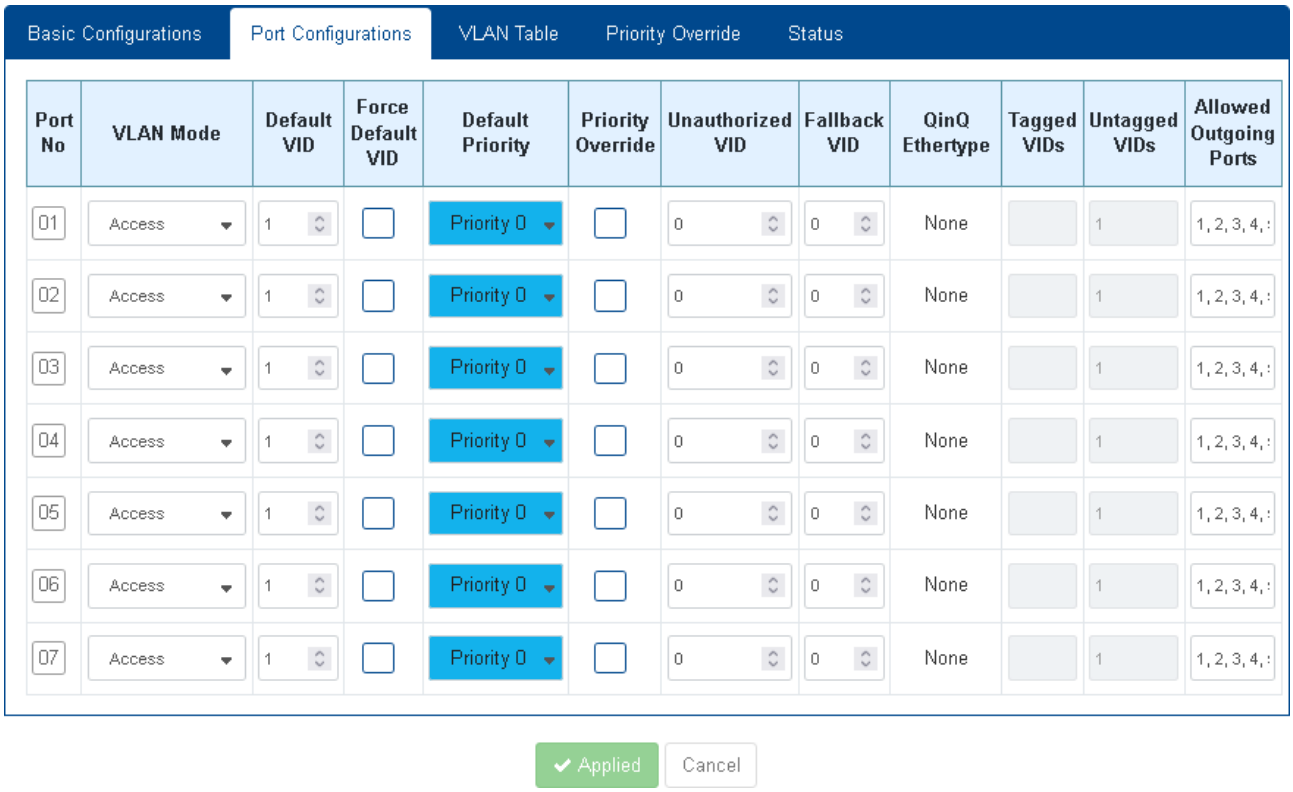


Fig. 36: VLAN - Basic - Port Configurations

This tab shows an editable tabular overview of the current configuration of all available VLAN IDs.

- **Port:** Lists all ports of the device.
- **VLAN Mode:** Select the VLAN mode of the specific port:
  - "Access": Only one VLAN ID is allowed on this port. Outgoing packets will not be tagged.
  - "Trunk": Multiple VLAN IDs are allowed on this port for sending and receiving multiple VLAN packets.
  - "Hybrid": Only one VLAN on this port is permitted to be untagged, the remaining VLANs must be tagged.
  - "QinQ Customer and QinQ Provider": Usually used in network environments that require double VLAN tags.
- **Default VID:** Sets the default VLAN ID when this port is in access mode. Untagged data packets will be tagged with this default VLAN ID.
- **Force Default VID:** The VLAN ID of all incoming data packets on that port is overwritten with the Port Default VLAN ID, even if they are tagged with a NULL value.
- **Default Priority:** Select the default priority value from the drop-down list for this port. Incoming packets without VLAN tag are automatically tagged using the default VLAN ID and default priority values.

- **Priority Override:** When enabled, incoming packets with existing VLAN tag are overwritten with the default priority value.
- **Unauthorized VID:** When using port access control with dynamic VLANs, unauthorized ports are attached to this VLAN.

  When set to "0" the global unauthorised VLAN ID parameter applies.

  Use this parameter to set an independent port specific unauthorized vlan.
- **Fallback VID:** When using port access control with dynamic VLANs and a RADIUS server, the fallback VLAN is assigned when the RADIUS server is unavailable.

  If this parameter is set to "0" the unauthorized VLAN is used instead.

  When set to "0" the global unauthorised VLAN ID parameter applies.
- **QinQ Ethertype:** When using QinQ mode, set the respective ethertype.
- **Taggged VID:** List of VLAN IDs used for tagged data packets on this port. These VLAN IDs will take effect in "Trunk" mode or "General" mode.

  The format must fit the following notation:

  - Single numbers ("1")
  - Multiple numbers, comma-separated ("1,2,3")
  - Several successive numbers, linked by hyphen ("1-5")

  Example: VLAN ID "1,2,5-7" corresponds to "1,2,5,6,7".
- **Untagged VID:** List of VLAN IDs used for untagged data packets on this port. These VLAN IDs will take effect in "Trunk" mode or "General" mode.

  The format corresponds to the VLAN IDs for tagged data packets.
- **Allowed Outgoing Ports:** Comma-separated list of egress ports for incoming data packets tagged with the respective VLAN IDs on this port.

  This function depends on port VLAN mode configured on tab **VLAN Basic Configuration** (see section 5.5.1 on page 39).

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.3 Basic - VLAN Table

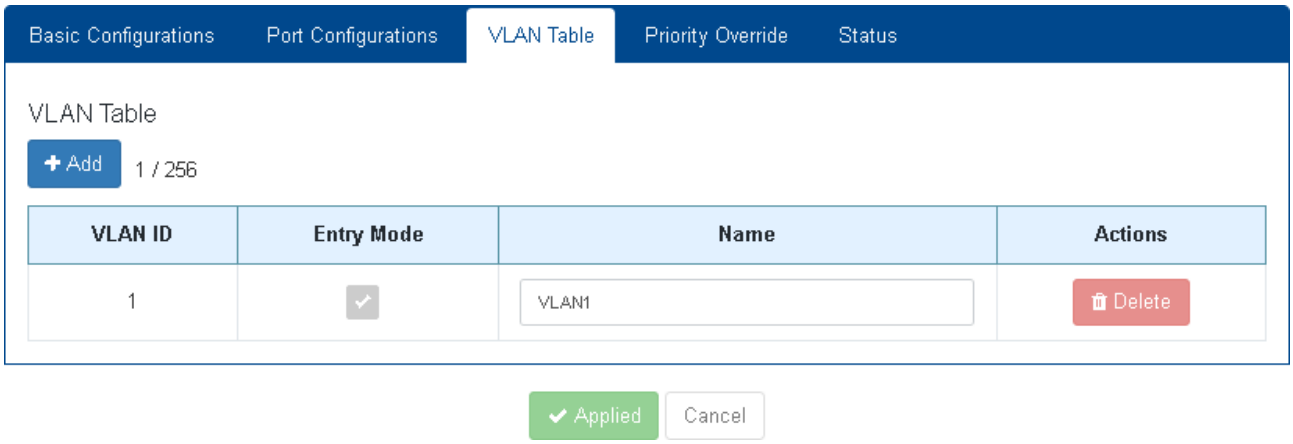


Fig. 37: VLAN - Basic - VLAN Table

This tab shows a tabular overview of all available VLAN Ids.

- **Add:** Opens the dialogue for adding a new VLAN ID.

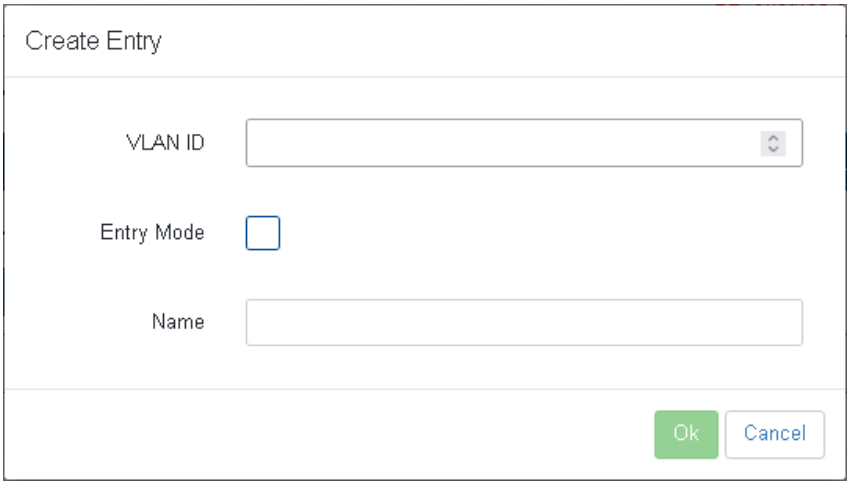


Fig. 38: VLAN - Basic - VLAN Table - Add

- **VLAN ID:** Contains a unique VLAN ID in ascending order (from 2 to 4094).

  Note: VLAN ID "1" is the default inband VLAN ID.
- **Entry Mode:** Check or uncheck to enable or disable entry mode for this VLAN.
- **Name:** Descriptive name for this entry.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.4 Basic - Priority Override

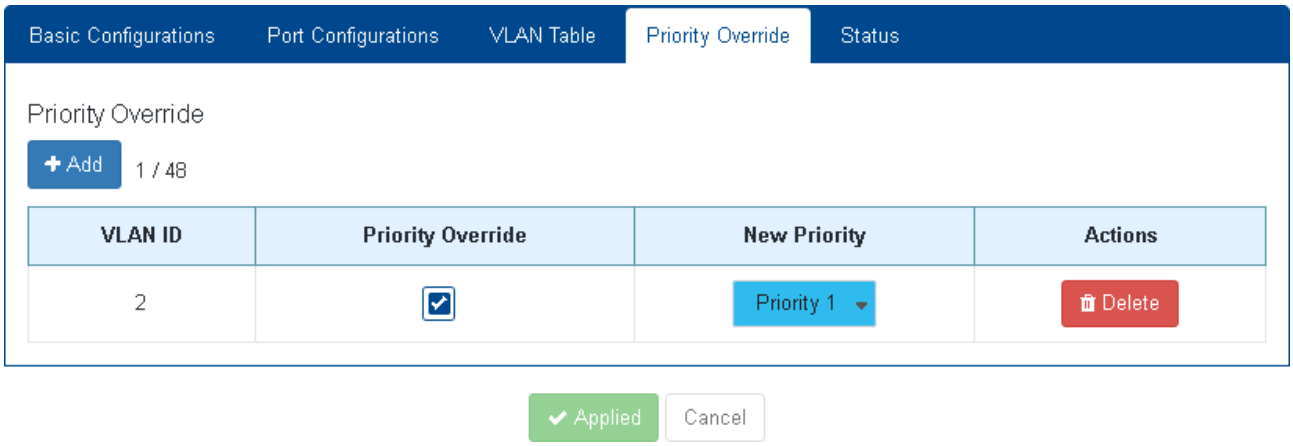


Fig. 39: VLAN - Basic - Priority Override

This tab allows the configuration of priority overrides for VLANs.

- **Add:** Opens the dialogue for adding a new entry.

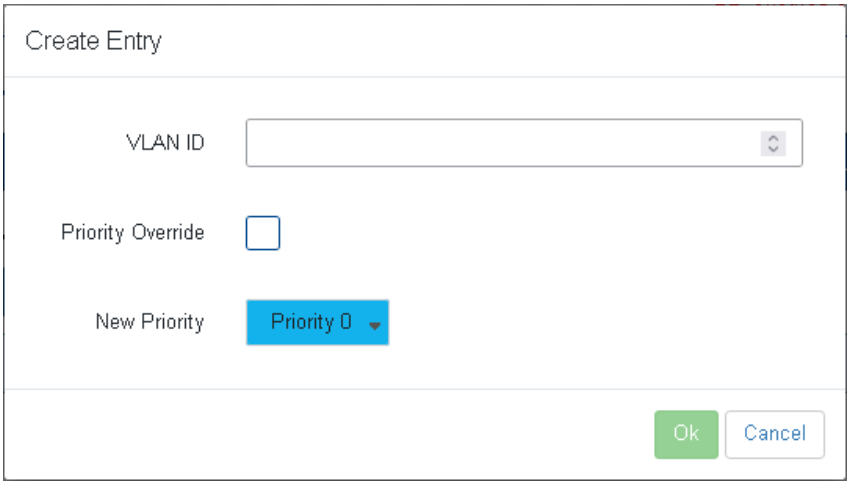


Fig. 40: VLAN - Basic - VLAN Table - Add

- **VLAN ID:** Contains a unique VLAN ID in ascending order (from 2 to 4094).

  Note: VLAN ID "1" is the default inband VLAN ID.
- **Priority Override:** Check or uncheck to enable or disable priority override for this VLAN.
- **New Priority:** Select the priority from the drop-down list.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.5 Basic - Status

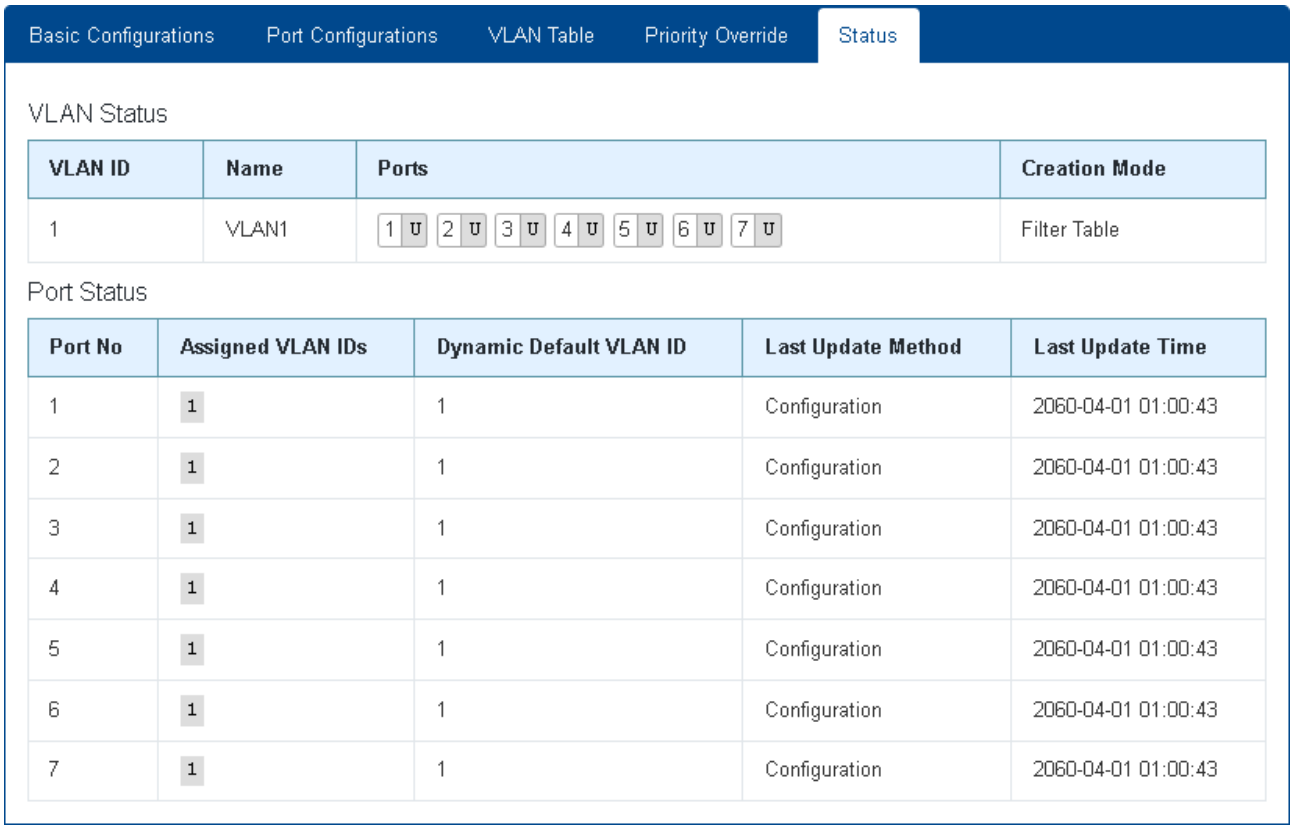


Fig. 41: VLAN - Basic - Status

This tab shows a tabular overview of the VLAN status.

5.5.6 MVRP - Basic

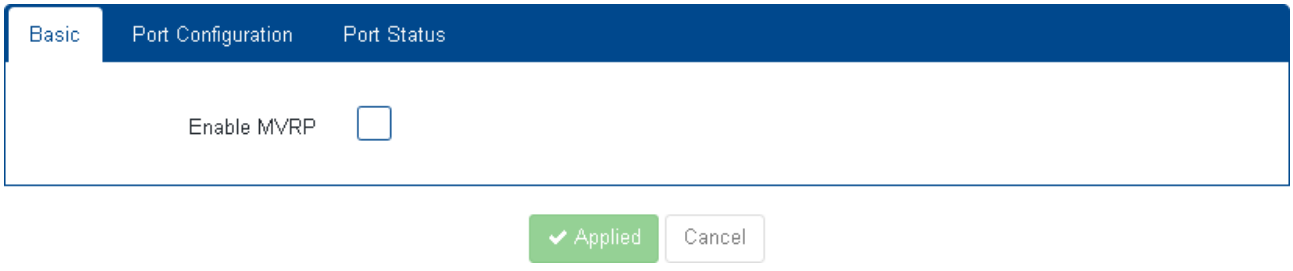


Fig. 42: VLAN - MVRP - Basic

- **Enable MVRP:** Check or uncheck this option to enable or disable MVRP (Multiple VLAN Reservation Protocol) globally.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.7 MVRP - Port Configuration

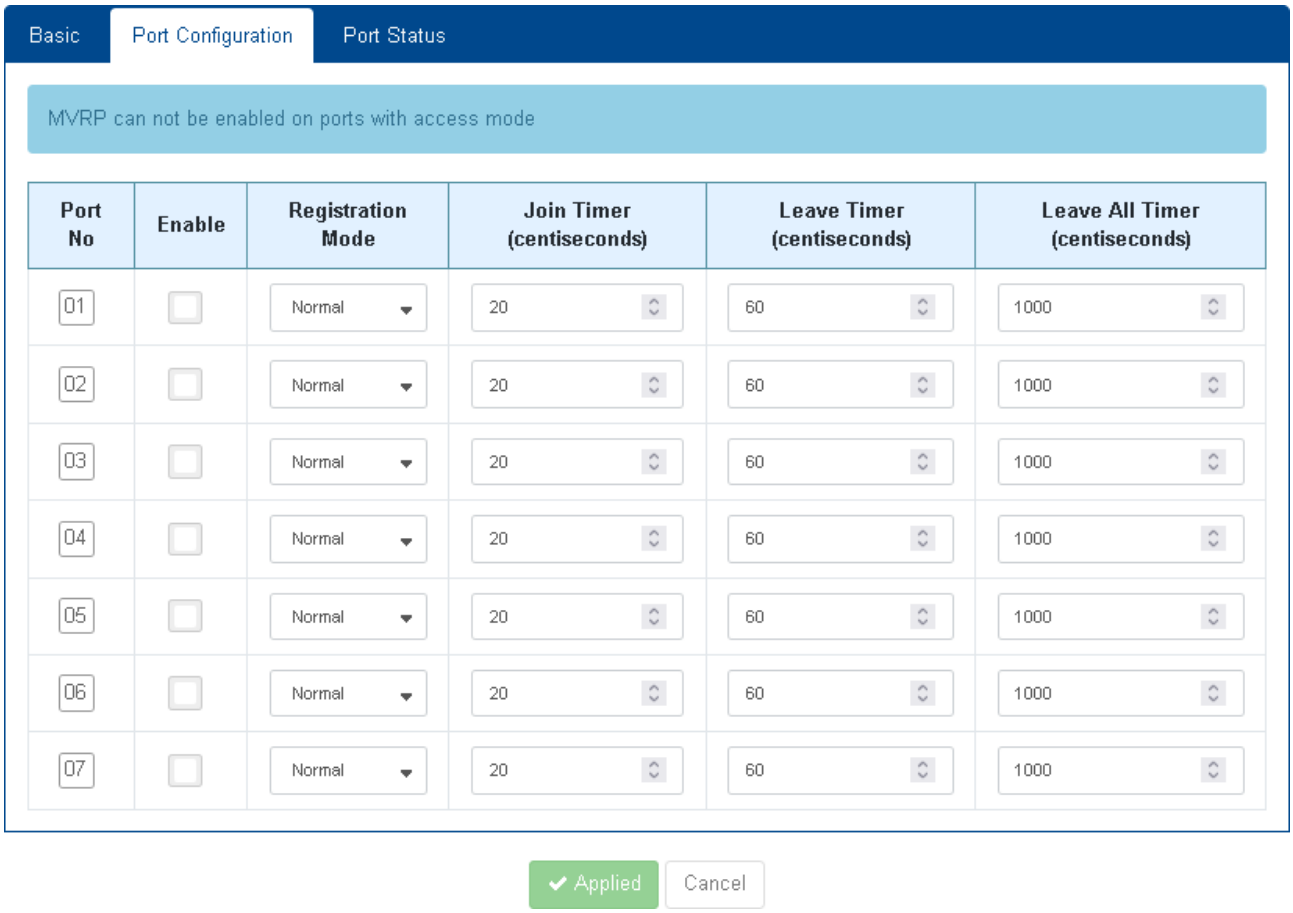


Fig. 43: VLAN - MVRP - Port Configuration

This tab shows an editable tabular overview of the MVRP configuration of all ports.

- **Port No:** List of all ports.
- **Enable:** Check or uncheck this option to enable or disable MVRP for this port.
- **Registration Mode:** Select the registration mode from the drop-down list:
  - "Normal": Dynamic registration of VLANs on this port, VLAN information propagation into the network.
  - "Fixed": No dynamic deregistration of VLANs on this port. Received MVRP frames are dropped. The device's port does not deregister dynamic VLANs or register new dynamic VLANs.
  - "Forbidden": No dynamic registration of VLANs on this port. Received MVRP frames are dropped. The ports MVRP participant does not register new dynamic VLANs or re-register a deregistered dynamic VLANs.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.5.8 MVRP - Port Status

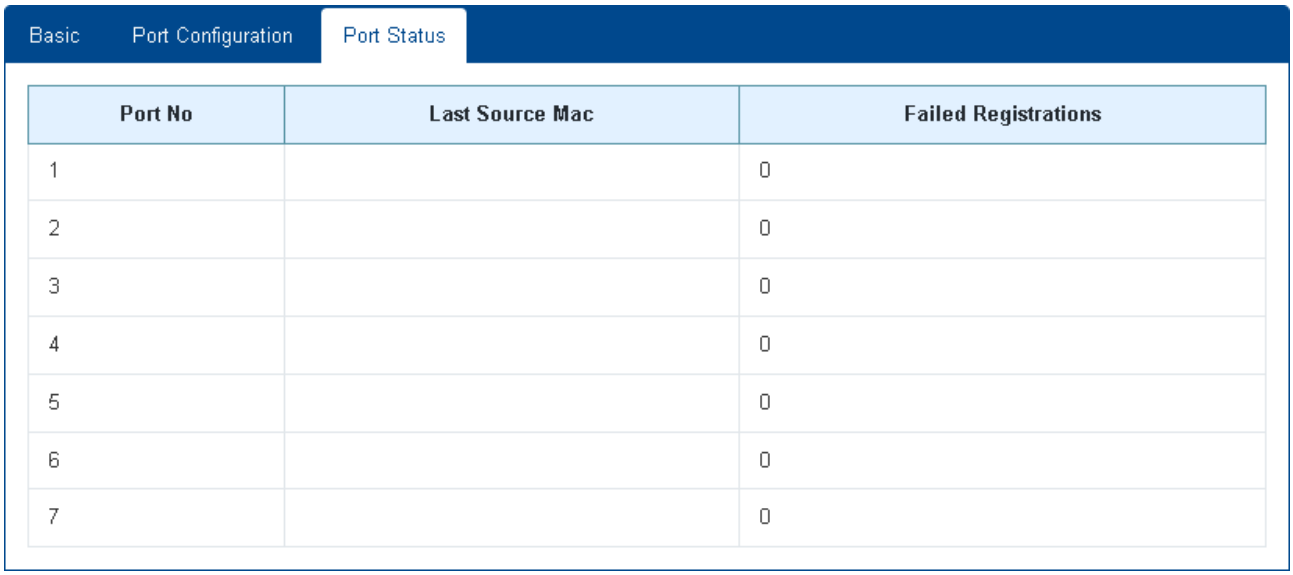


Fig. 44: VLAN - MVRP - Port Status

This tab shows a tabular overview of the current port status.

5.6 Security

5.6.1 MAC Table - Configuration

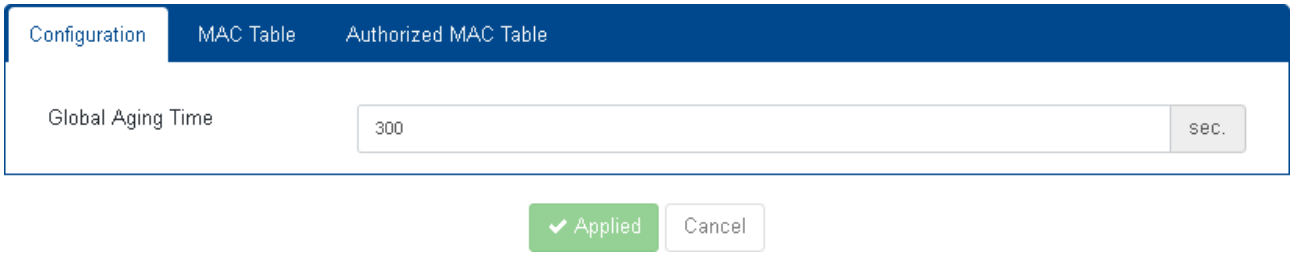


Fig. 45: Security - MAC Table - Basic

- **Global Aging Time:** Set the time period in seconds in which a MAC table entry for accessing a port becomes invalid.

  Note: The default aging time is 300 seconds. It can be set in 7 second increments to a maximum time of 10,000 minutes.

  If set to a value less than 7 seconds, the system resets it to a value of 7 seconds automatically.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.2 MAC Table - MAC Table

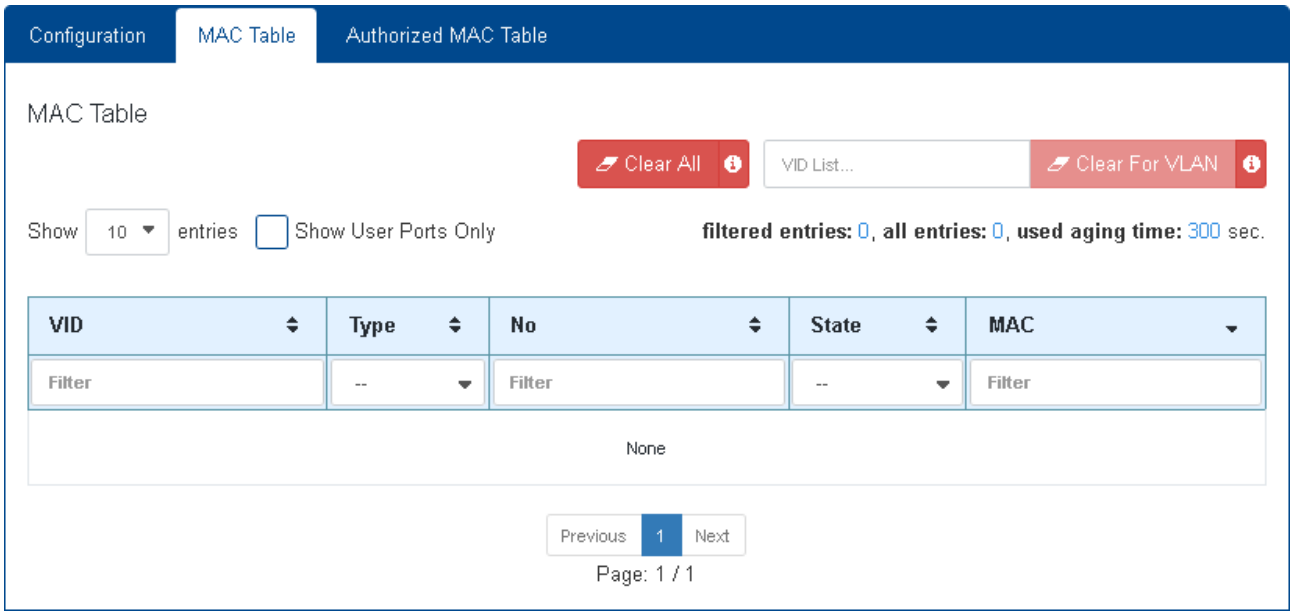


Fig. 46: Security - MAC Table - MAC Table

The tab shows a tabular overview of all MAC addresses currently known to the system (up to 2048 entries):

- **Show xx entries:** Select the number of entries that are shown in the table below.
- **Show User Ports Only:** Check this option to hide all non user ports in the table.
- **Vid:** The VLAN id of this MAC address.

  Enter a VID to filter all entries for this value.
- **Type:** Shows whether the MAC address is learned via an access or a trunk port.
- **No:** The systems port number this MAC address was recognized.

  Enter a port number to filter all entries for this value.
- **State:** The status of the MAC address.
- **MAC:** The MAC address.

  Enter a MAC address to filter all entries for this value.
- A click on the button **Clear All** deletes all table entries.
- A click on the button **Clear For VLAN** deletes all table entries associated with the given VLAN IDs

  Note: The system has to relearn all MAC addresses first before processing them.

5.6.3 MAC Table - Authorized MAC Table

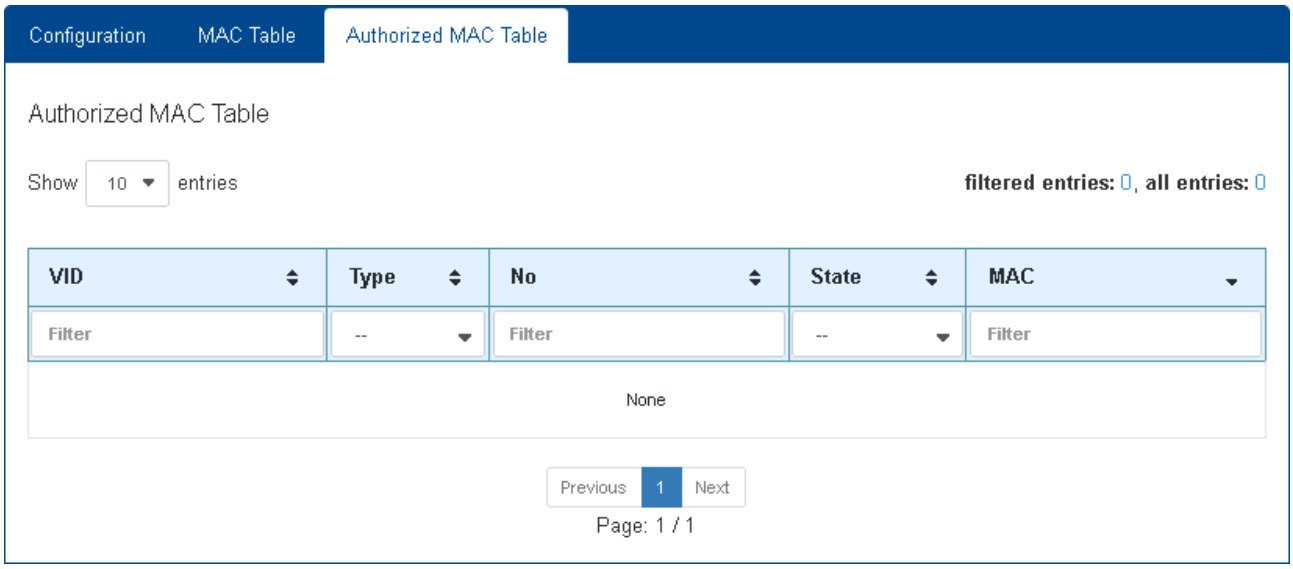


Fig. 47: Security - MAC Table - Authorized MAC Table

The tab shows a tabular overview of all authorised MAC addresses (up to 2048 entries):

- **Show xx entries:** Select the number of entries that are shown in the table below.
- **Vid:** The VLAN id of this MAC address.
  Enter a VID to filter all entries for this value.
- **Type:** Shows whether the MAC address is learned via an access or a trunk port.
- **No:** The systems port number this MAC address was recognized.
  Enter a port number to filter all entries for this value.
- **State:** The status of the MAC address.
- **MAC:** The MAC address.
  Enter a MAC address to filter all entries for this value.

5.6.4 PACC - Basic Configuration

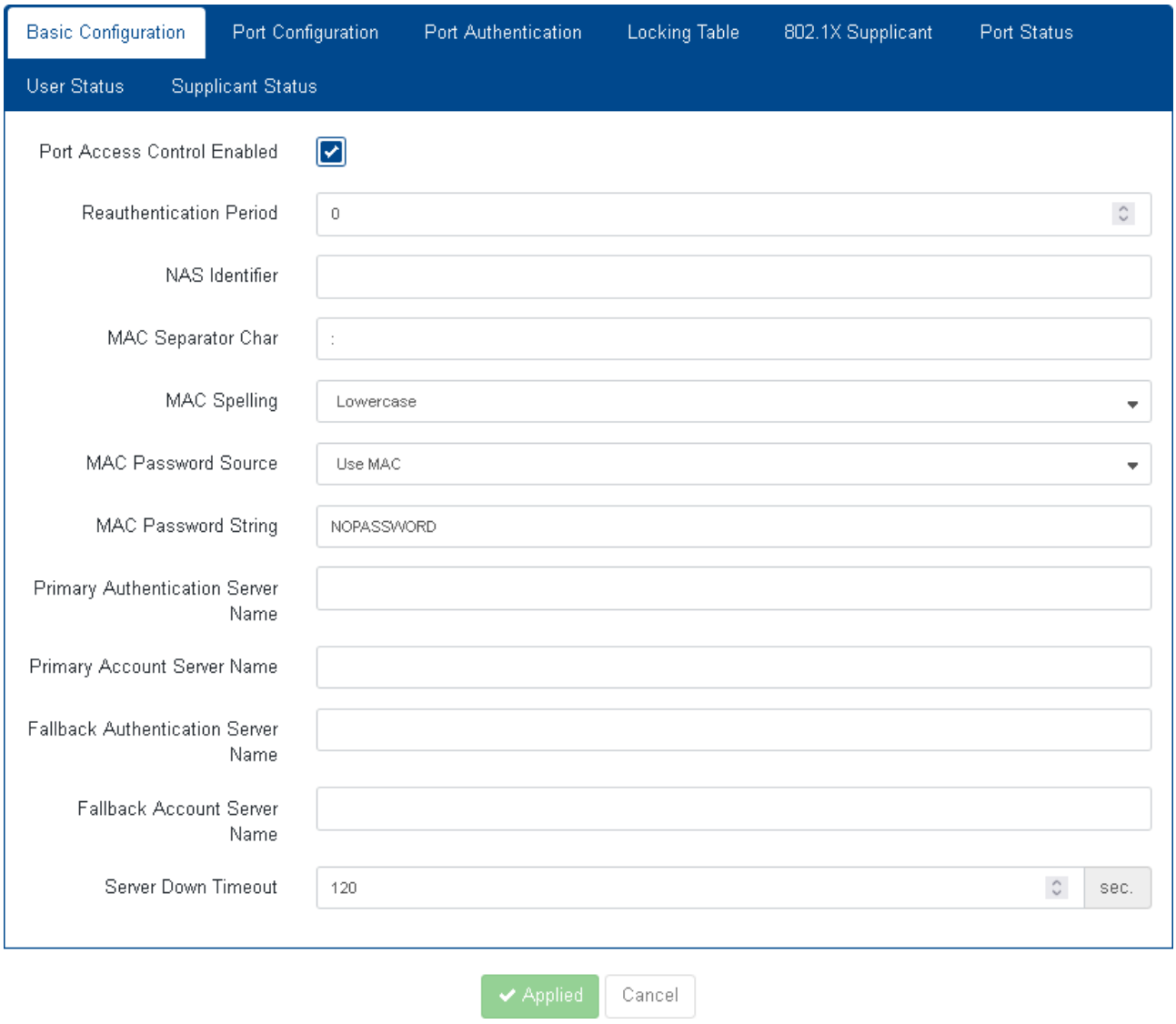


Fig. 48: Security - PACC - Basic Configuration

- **Port Access Control Enabled:** Check or uncheck this option to enable or disable PACC.
- **Reauthentication Period:** Set the EAP reauthentication period in seconds.

  To disable reauthentication set value to "0".
- **NAS Identifier:** Define the Network Access Service (NAS) Identtifier.
- **MAC Separator Char:** Define the character which separates the bytes of a MAC address.
- **MAC Spelling:** Select from the drop-down list, whether the notation of the hexadecimal characters is set to uppercase or lowercase.
- **MAC Password Source:** Define whether MAC or password is used for authentication.

- **MAC Password String:** If password source is set to "Password" enter a password string.
- **Primary Authentication Server Name:** Enter the available authentication server.

  For more information on managing authentication servers see section 5.14.2 on page 112.
- **Primary Account Server Name:** Enter the available accounting server.

  For more information on managing accounting servers see section 5.14.2 on page 112.
- **Fallback Authentication Server Name:** Enter an alternative server.
- **Fallback Accounting Server Name:** Enter an alternative server.
- **Server Down Timeout:** Set the retry interval in seconds for trying to return to the primary RADIUS server.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.5 PACC - Port Configuration

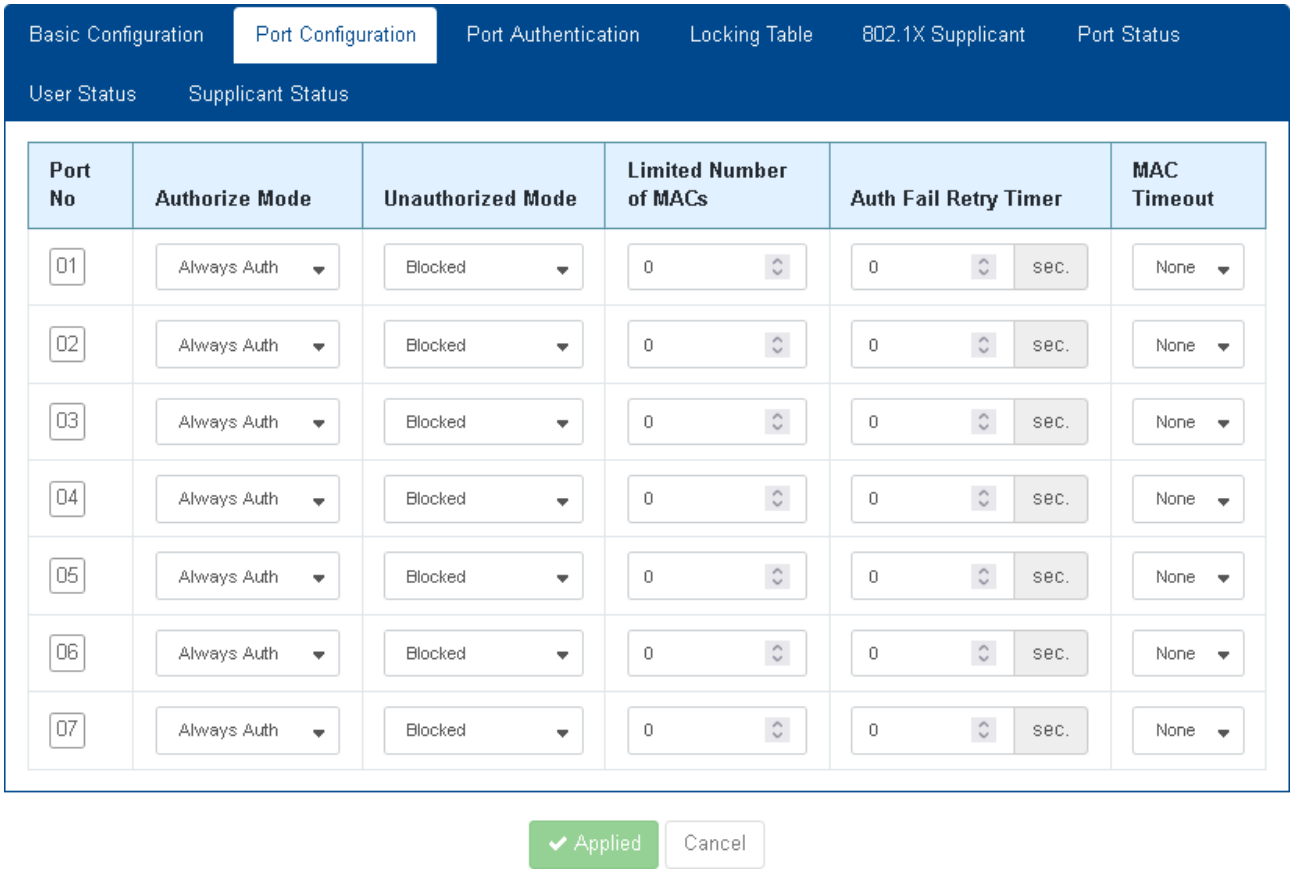


Fig. 49: Security - PACC - Port Configuration

The tab shows a tabular overview of the port access settings for all device's ports. Change the settings as needed.

- **Port No.:** Port number of the specific port.
- **Authorize Mode:** Select one of the following modes from the drop-down list:
  - "Always Auth": Disables Port Access Control for this port. The port is always in forwarding state, the access is authorised by default.
  - "Force Unauth": Forces the port to unauthorised mode, acting as defined in column Unauthorised Mode.
  - "Via MAC table": The device compares the MAC address with the entries in its internal MAC locking table. If the locking table contains the MAC address, the device grants port access.
  - "MAC via RADIUS": Authorisation on this port happens via MAC address of the connected network partner on this port. The assigned authentication server (primary or fallback) authenticates the MAC address requested by the device.

    Note: When the device learns a new MAC address on this port it uses this MAC address as username and password string in the form "xx:xx:xx:xx:xx:xx" in hexadecimal notation.
  - "802.1X via RADIUS": Authorisation on this port happens via secure 802.1X protocol. The assigned authentication server (primary or fallback) authenticates the certificate requested by the device.
  - "MAC 802.1X via RADIUS": Authorisation happens via both MAC address and 802.1X. The assigned authentication server checks both methods (MAC first, 802.1X second). At least one of both methods is sufficient for setting the port into forwarding state.
  - "802.1X MAC via RADIUS": Authorisation happens via both MAC address and 802.1X. The assigned authentication server checks both methods (802.1X first, MAC second). At least one of both methods is sufficient for setting the port into forwarding state.
  - "MAC Event only": Disables the Port Access Control for this port. The access is always authorized by default. When an unknown MAC address (no MAC table entry) occurs on this port, it will generate an authorization event.
  - "Edge 802.1X via RADIUS": The network edge authentication mode is used to authenticate a "supplicant switch" connected to a downlink port of the device. After successful authentication the port is open for any traffic from the downstream switch.
  - This feature authenticates an authentication switch placed outside a wiring closet with an authentication switch placed in the wiring closet.
- **Unauthorized Mode:** If the port is forced to unauthorised mode, select the operation the port has to perform:
  - "Blocked": If forced to unauthorised mode, the port will be blocked.
  - "Use Unauthorised VLAN": If forced to unauthorised mode, the port will be set to unauthorized VLAN (see section 5.5.1 on page 39).
  - "Incoming Blocked": If forced to unauthorised mode, the port will be blocked for incoming data traffic..
- **Limited Number of MACs:** Set the maximum number of MAC addresses allowed for port access.

- **Auth Fail retry Time:** Set the time interval in seconds after which a previously faild port access attempt is allowed again.
- **MAC Timeout:** Select how long authorized MACs remain authorized after inactivity of the MAC.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.6 PACC - Port Authentication

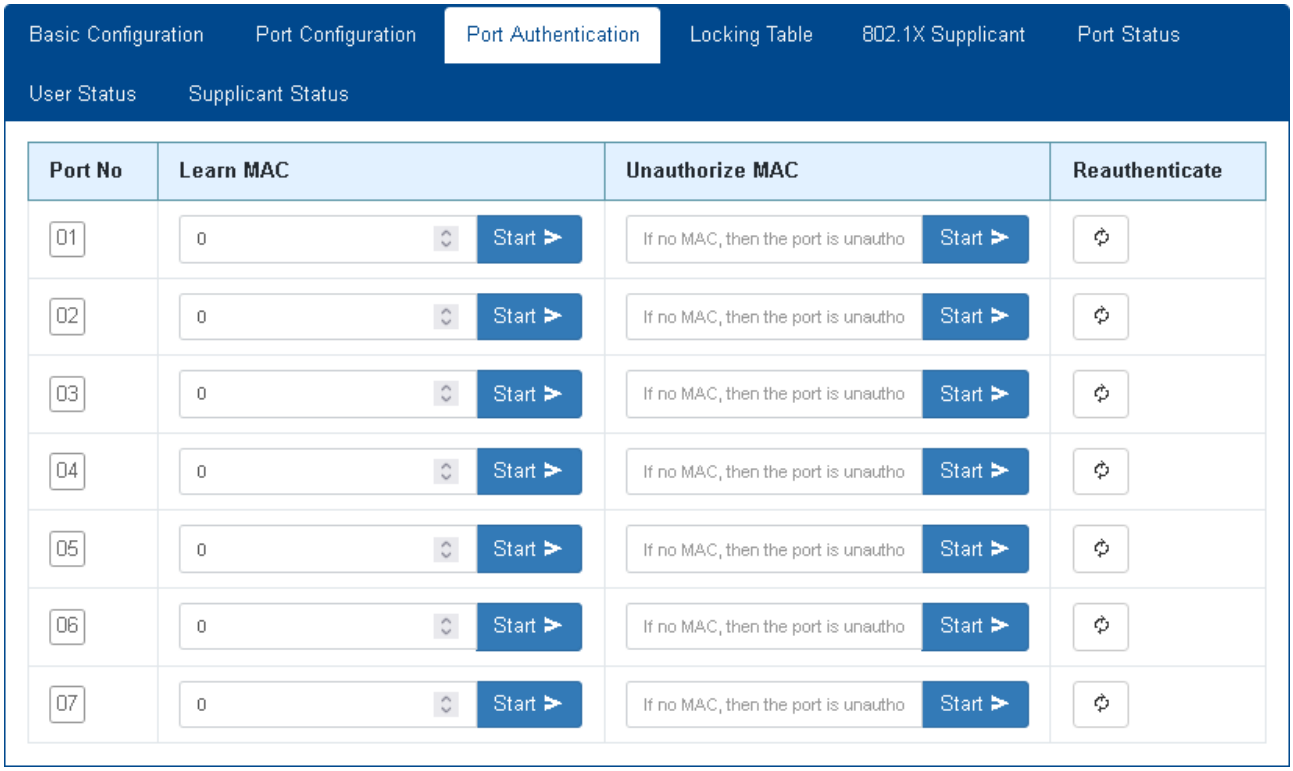


Fig. 50: Security - PACC - Port Authentication

This tab alloes to manage authentication of specific ports.

- **Port No:** Number of the port.
- **Learn MAC:** Enter a value and click on the button **Start** to learn the next incoming MAC(s) of this port (corresponding to the entered value) and enter them into the MAC table.
- **Unauthorize MAC:** Enter a specific MAC address and click on the button Start to unauthorize a this specific MAC address.

  When no MAC address is specified, the entire port is unauthorized.
- **Reauthenticate:** Click on this button to reauthenticate the respective port.

5.6.7 PACC - Locking Table

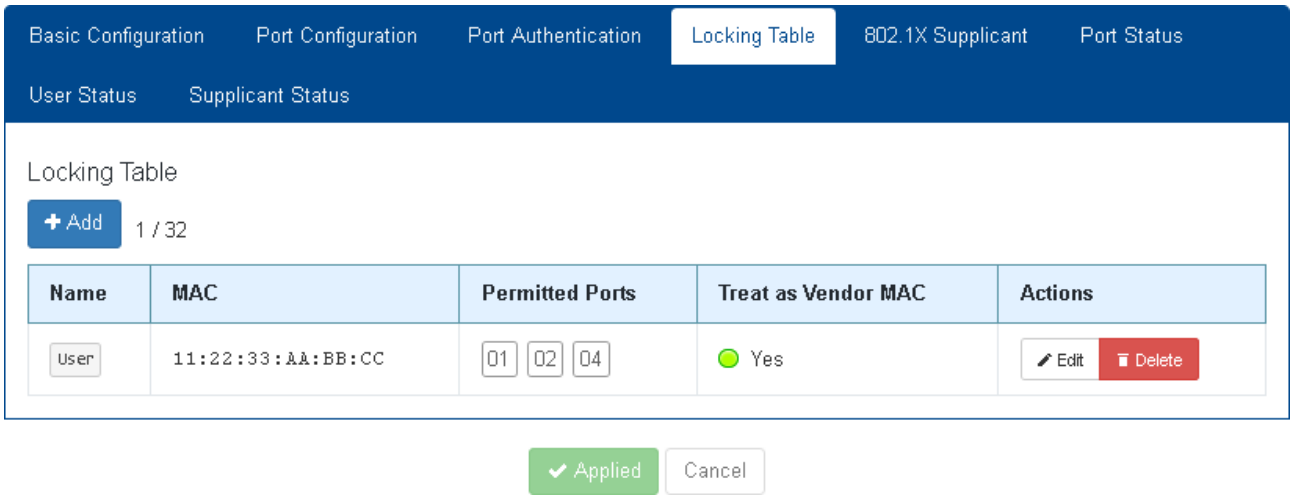


Fig. 51: Security - PACC - Locking Table

The MAC locking table is used when authorisation mode "Via MAC table" is enabled for a port.

The tab shows all previously learned MAC addresses from devices previously requested access on every port.

- **Edit:** Opens the edit dialogue of the respective entry. Change the entries as needed.
- **Add:** Opens the dialogue for adding a new MAC address entry.

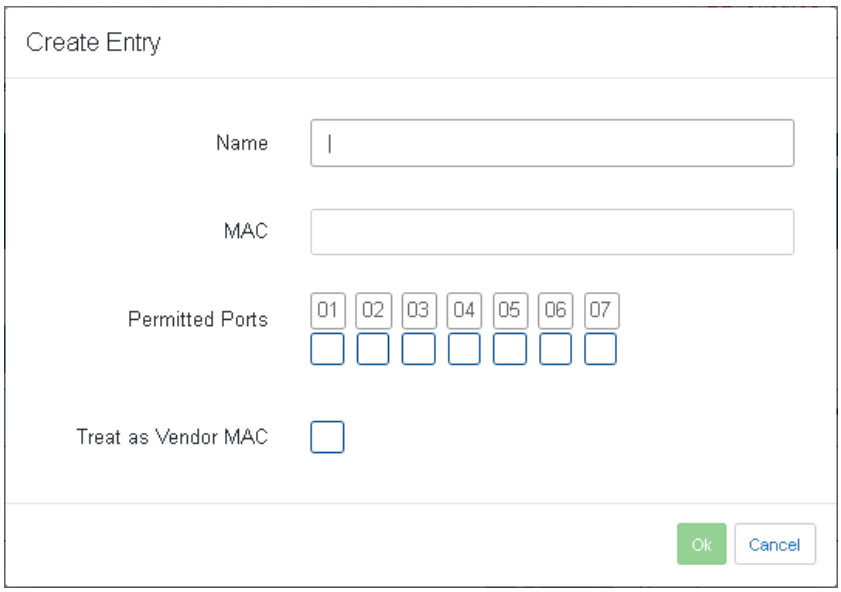


Fig. 52: Security - PACC - Locking Table - Add

- **Name:** Enter a descriptive name for this entry.
- **MAC:** Enter the MAC address in the form "xx:xx:xx:xx:xx:xx" in hexadecimal notation.

- **Permitted Ports:** Check or uncheck the ports to grant or reject access for this MAC address.
- **Treat as Vendor MAC:** Check this option to accept this MAC address as vendor MAC.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.8 PACC - 802.1X Supplicant

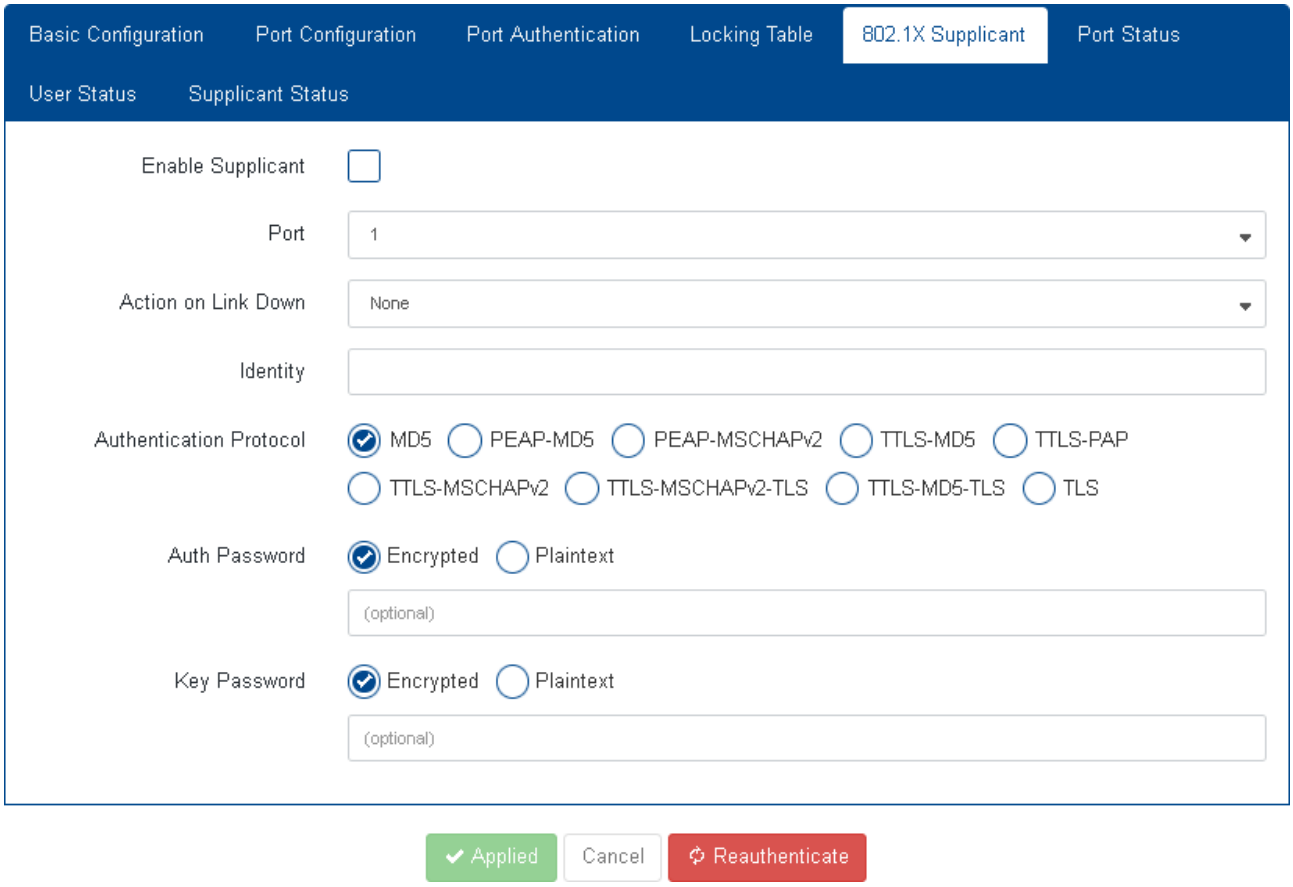


Fig. 53: Security - PACC - 802.1X Supplicant

- **Enable Supplicant:** Check or uncheck this option to enable or disable the supplicant option.

  When enabled, the device acts as supplicant for another switch connected to its port. This switch - if configured properly for 802.1X authentication - grants or rejects port access for this device on this port.

- **Port:** Select the port through which the authorizing authority is reached.

  Usually this is the link port.

- **Action on Link Down:** Select whether the local authenticated user ports should be deauthenticated, as soon as the supplicant link goes down.
- **Identity:** Enter the supplicant identity string for this device.
- **Authentication Protocol:** Check or uncheck the specific protocol to be used.
- **Auth Password:** Enter the encrypted EAP password.
- **Key Password:** Enter the encrypted private key password.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Reauthenticate** to reauthenticate the supplicant connection.

5.6.9 PACC - Port Status

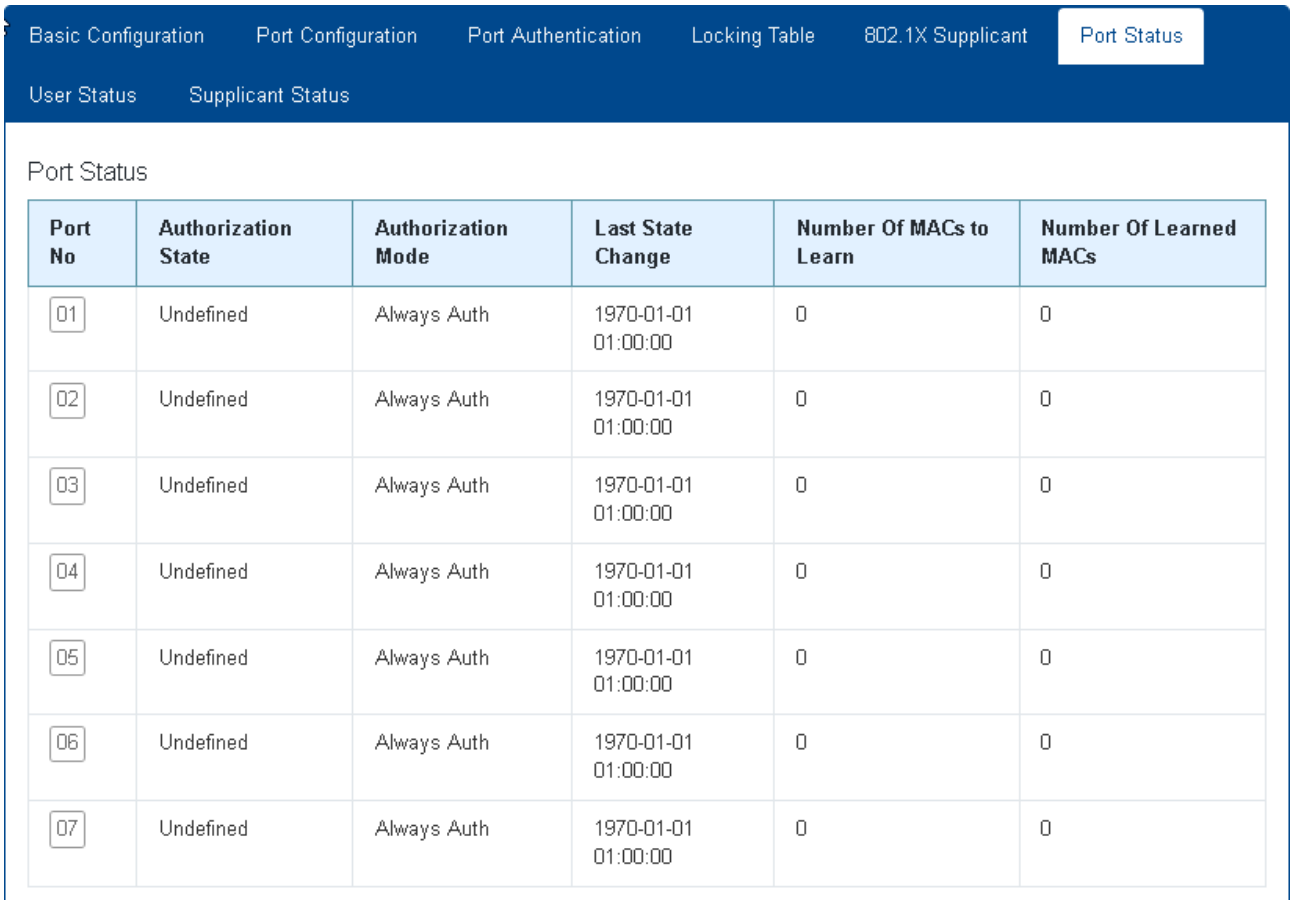


Fig. 54: Security - PACC - Port Status

This tab shows a tabular overview of the authorisation status of all ports.

5.6.10 PACC - User Status

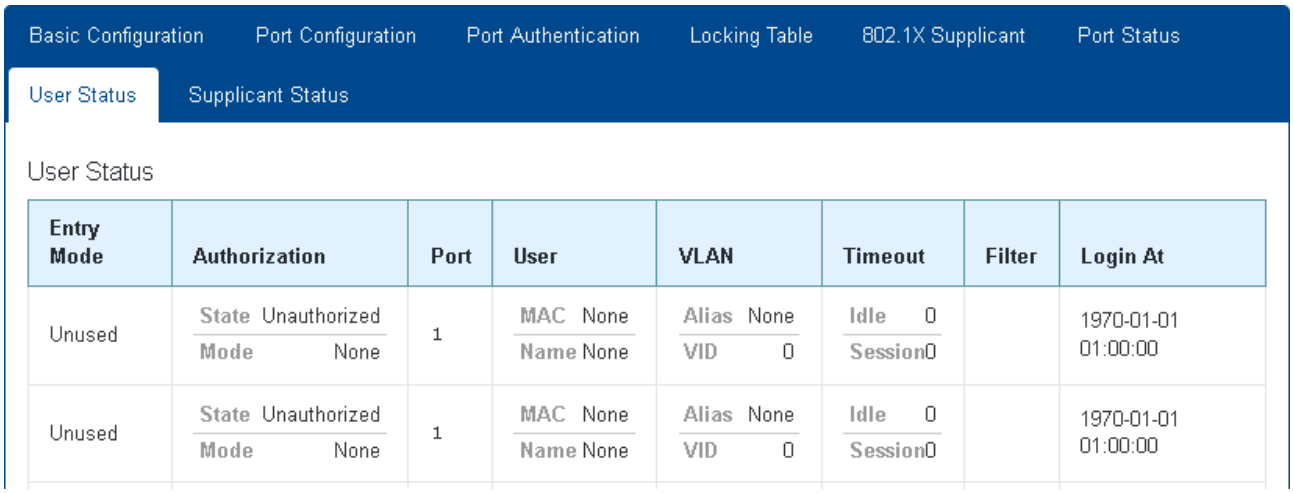


Fig. 55: Security - PACC - User Status

This tab shows a tabular overview of the authorisation status of all users

5.6.11 PACC - Supplicant Status

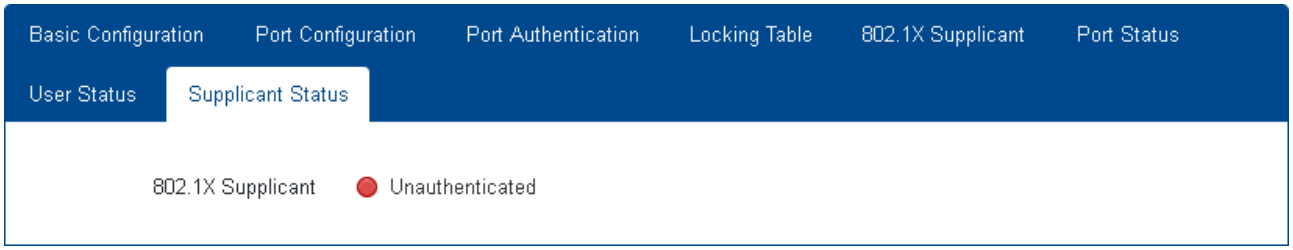


Fig. 56: Security - PACC - Supplicant Status

- **802.1X Supplicant:** Shows the currently active supplicant status
  - "Authenticated" (green indicator)
  - "Unauthenticated" (red indicator)

5.6.12 ACL - Basic

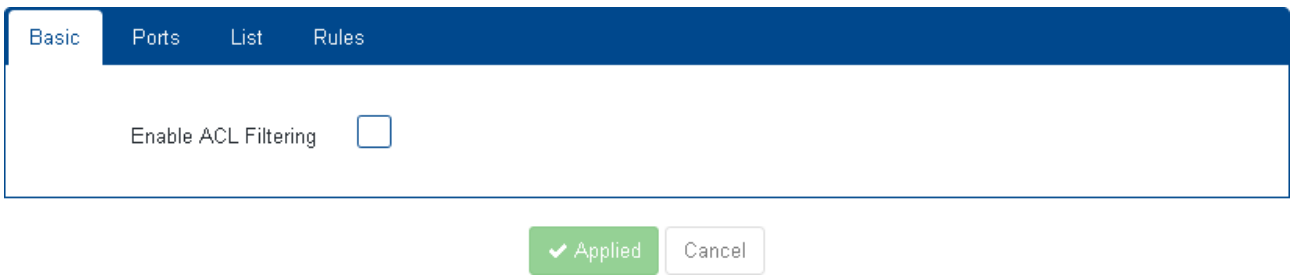


Fig. 57: Security - ACL - Basic

- **Enable ACL Filtering:** Check or uncheck this option to enable or disable ACL filtering generally.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.13 ACL - Ports

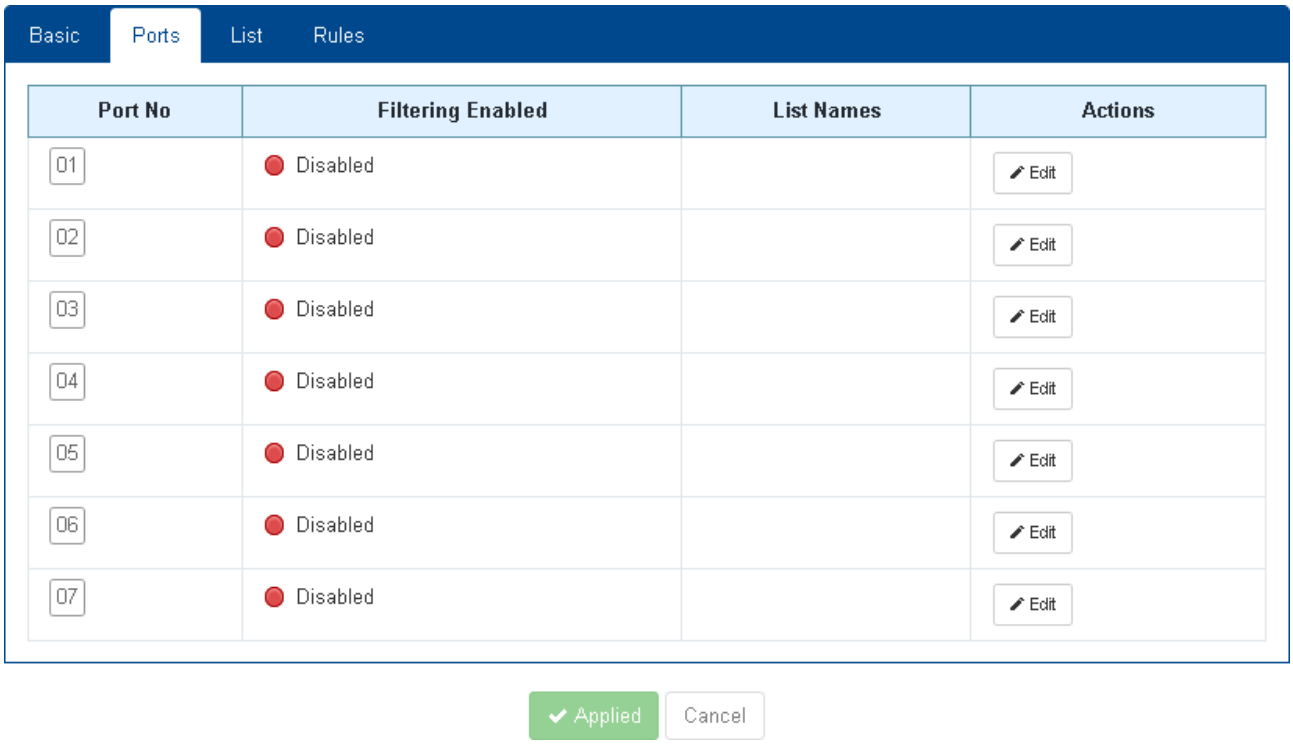


Fig. 58: Security - ACL - Ports

This tab allows the configuration of ACL filtering for specific ports.

- **Edit:** Opens the edit dialogue of the respective entry. Change the entries as needed.

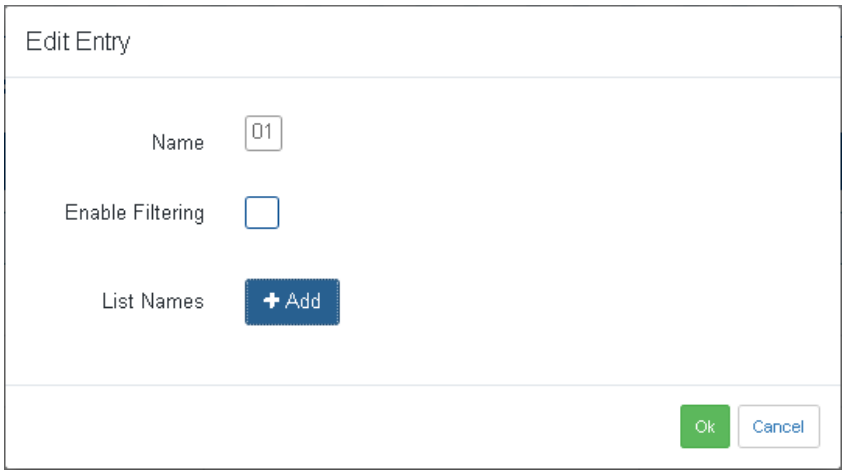


Fig. 59: Multicast - Static Group - Add

- **Name:** Port number.

- **Enable Filtering:** Check or uncheck this option to enable or disable ACL filtering for this port.
- **List Names:** Click on the button **Add** and select one or more available lists.

  Click on the button **Delete** to delete an associated list.

Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.14 ACL - List

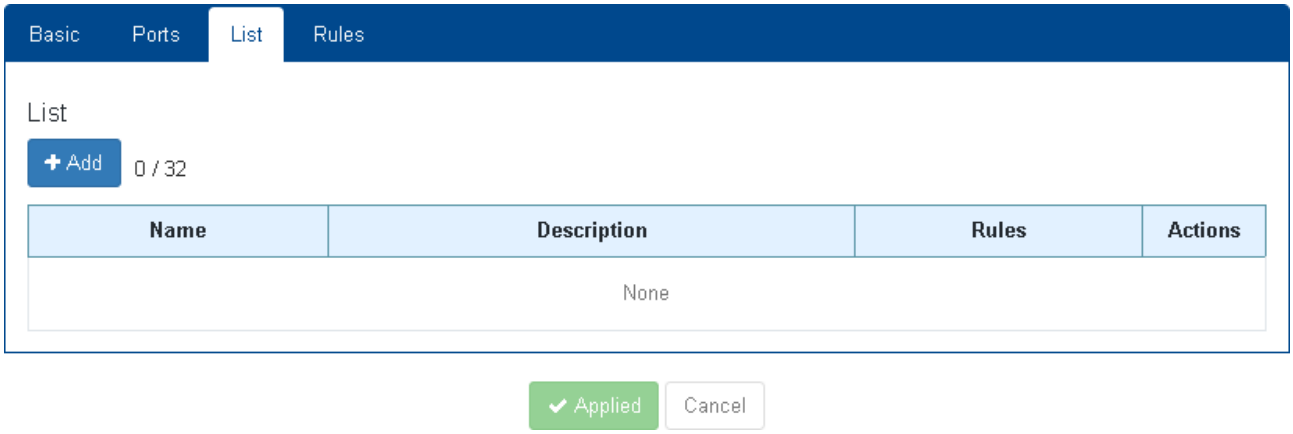


Fig. 60: Security - ACL - List

This tab allows to manage ACL lists.

- **Edit:** Opens the edit dialogue of the respective entry. Change the entries as needed.
- **Add:** Opens the dialogue for adding a new list entry.

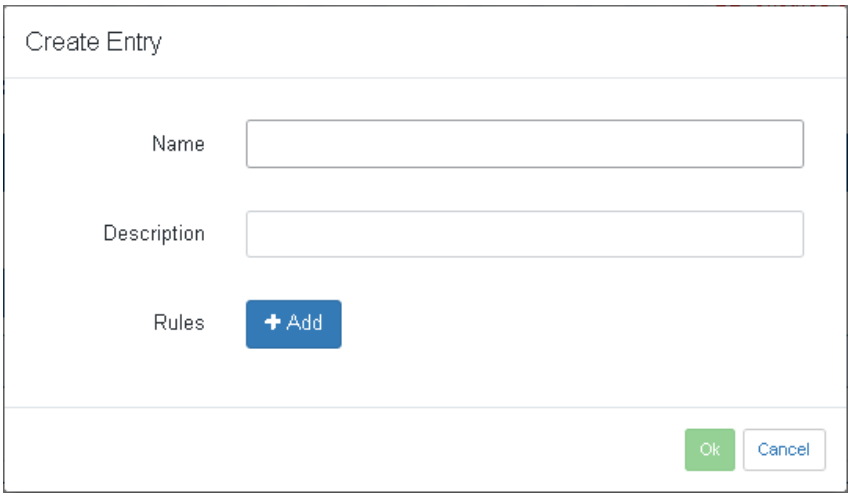


Fig. 61: Security - ACL - List - Add

- **Name:** Enter a descriptive name for this entry.
- **Description:** Enter a description for this entry.
- **Rules:** Click on the button **Add** and select one or more available rules.

Click on the button **Delete** to delete an associated rule.

Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.15 ACL - Rules

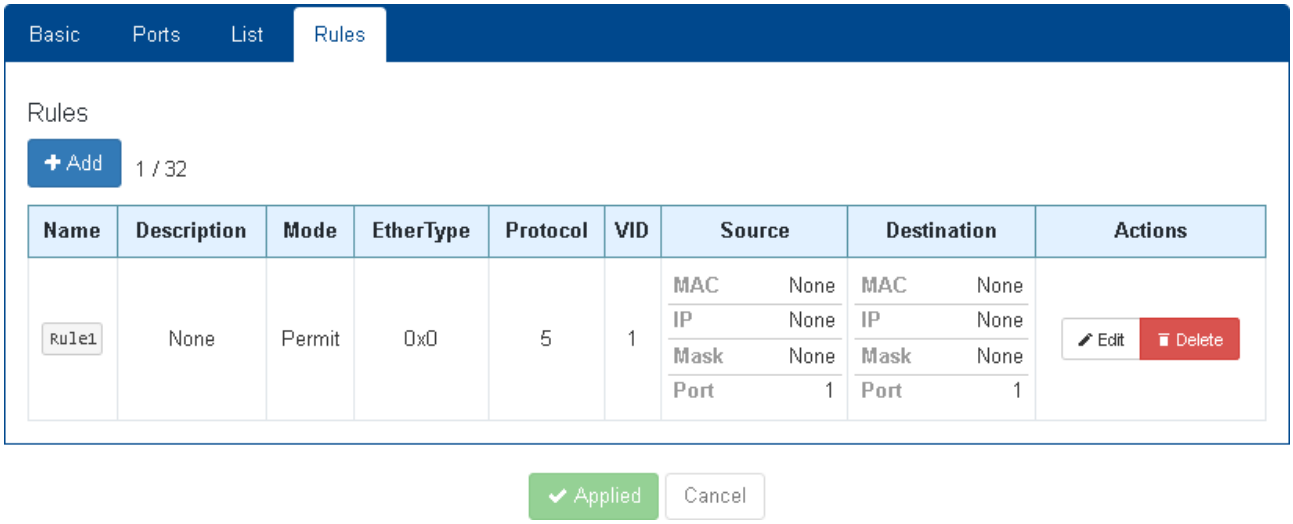


Fig. 62: Security - ACL - Rules

This section shows a tabular overview of the ACL rules.

- **Edit:** Opens the edit dialogue of the respective entry. Change the entries as needed.

- **Add:** Opens the dialogue for adding a new ACL rule.

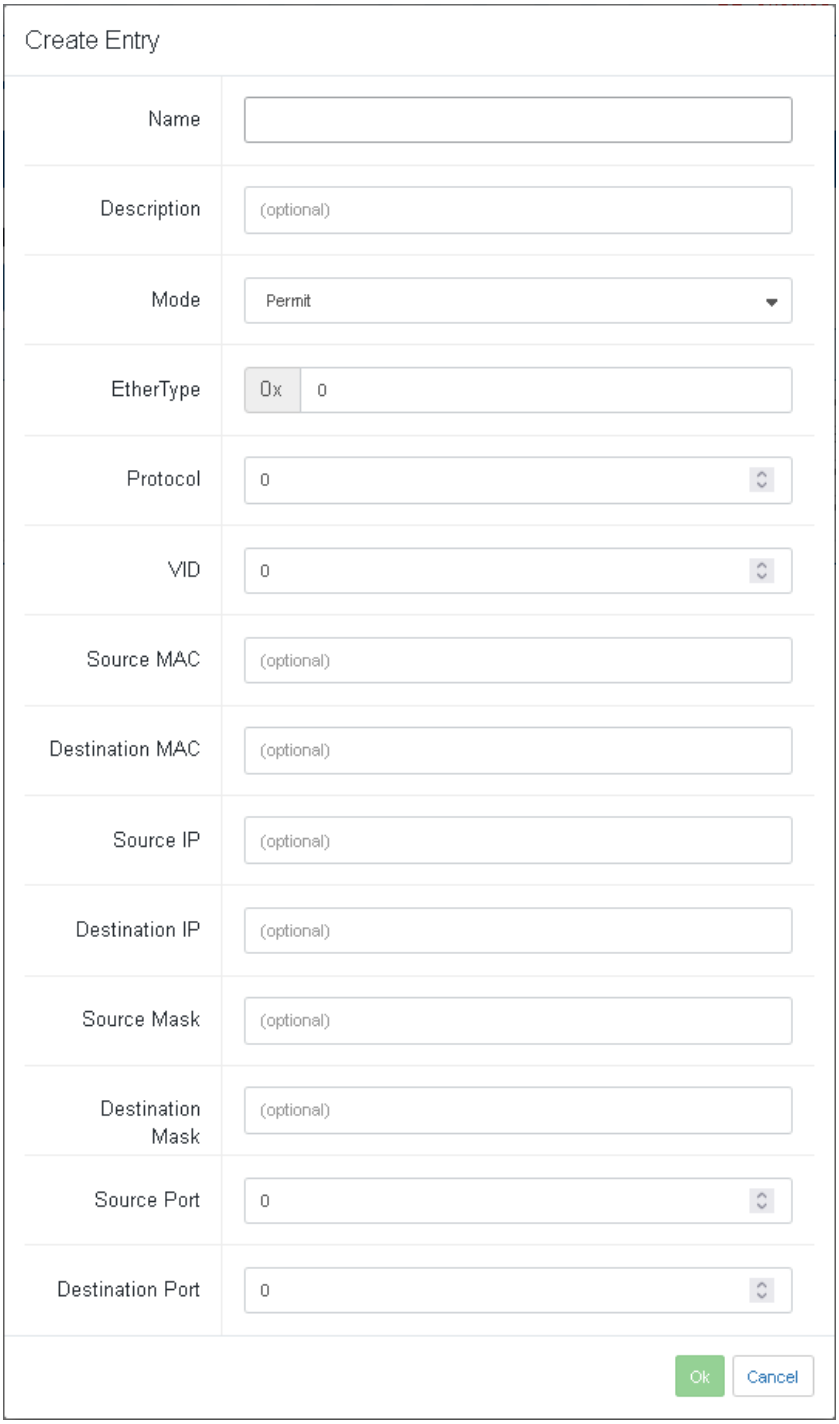


Fig. 63: Security - ACL - Rules - Add

- **Name:** Descriptive name of the ACL rule.
- **Description:** Enter a description for this entry.
- **Mode:** Filter action for data communication.

- "Deny": Data communication matching this rule will be denied.
- "Permit": Data communication matching this rule will be permitted.

- **Protocol:** Enter a value for the protocol used as protocol number in the IPv4 header, e.g.:
  - "6": TCP
  - "17": UDP
  - Use "0" (default value) to ignore the protocol field.
- **VID:** Enter the VLAN ID to which the rule applies.
- **Source MAC:** Source MAC of the data communication.
- **Destination MAC:** Destination MAC address of the data communication.
- **Source IP:** Source IP address of the data communication.
- **Destination IP:** Destination IP address of the data communication.
- **Source mask:** Source mask of the data communication.
- **Destination mask:** Destination mask of the data communication.
- **Source port:** Enter the source port.
- **Destination port:** Enter the source port.

The permit or deny mechanism works as follows:

- Each bit of the source or destination address (IP or MAC) is analysed in view of the respective source or destination mask.
- When a bit of the mask is set, the corresponding bit in the address is set as well, and vice versa.

Configuration		Source address	Result	Description
Source address	**Source mask**			
192.168.0.1	255.255.255.0 (Address must match the first three octets)	192.168.1.1	No match	Mismatch in the third octet
		192.168.0.11	Match	First three octets matching
		192.168.0.120	Match	First three octets matching
00:50:56:C0:00:01	ff:ff:ff:ff:00:00 (Address must match the first four hexadecimal digit groups)	00:50:56:C0:0a:01	Match	First four hexadecimal digit groups matching
		00:50:56:C0:0a:21	Match	First four hexadecimal digit groups matching
		00:50:56:D0:00:01	No match	Mismatch in the fourth hexadecimal digit group

Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.6.16 Storm Control - Configuration

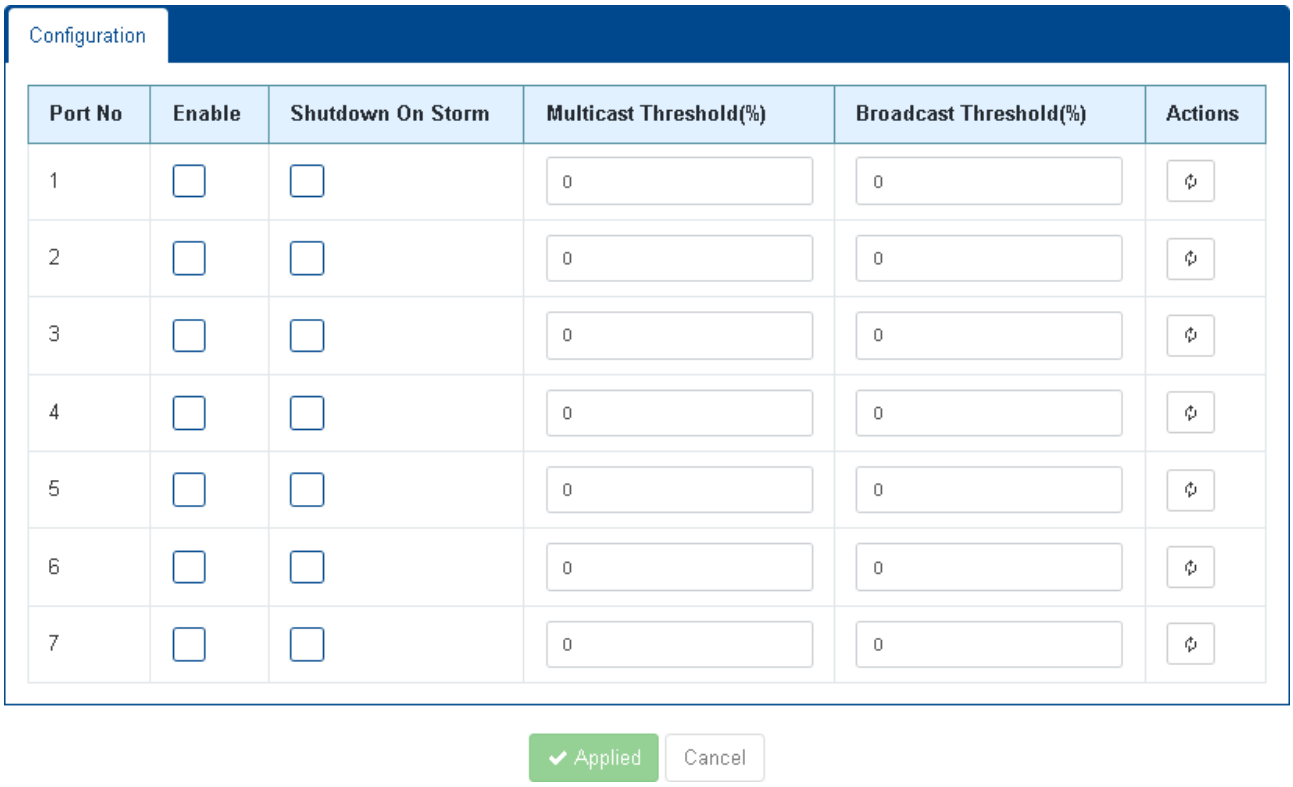


Fig. 64: Security - Storm Control - Configuration

This tab allows the configuration of storm control for specific ports.

- **Port No:** Number of the port.
- **Enable:** Check or uncheck this option to enable or disable storm control for this port.
- **Shutdown On Storm:** Check this option if the port is shut down when it is flooded by multicast and broadcast data packets beyond the assigned thresholds.
- **Multicast Threshold:** Enter the maximum rate at which multicast packets can be forwarded.
- **Broadcast Threshold:** Enter the maximum rate at which broadcast packets can be forwarded.
- **Actions:** Click this button of the respective port to unlock it manually after shutdown.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7 QoS

5.7.1 Basic - Mode

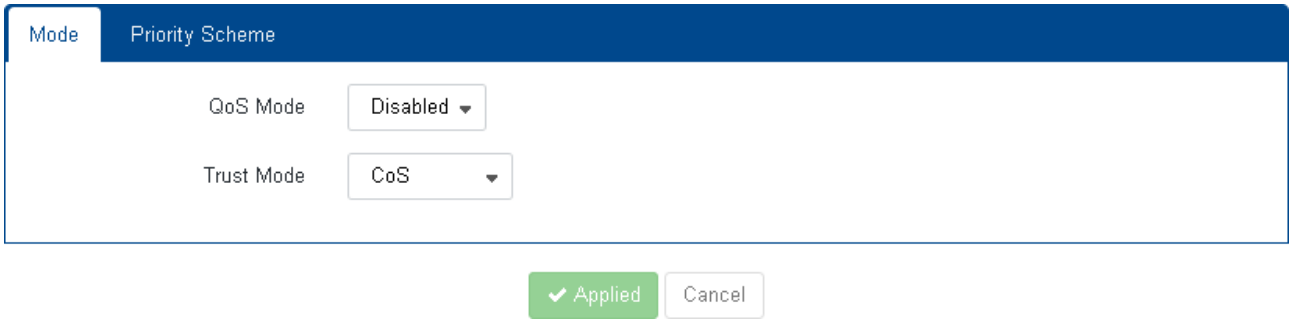


Fig. 65: QoS - Basic - Mode

This tab allows configuration of basic QoS mechanisms.

- **QoS Mode:** Select the QoS mode from the drop-down list:
  - "Disabled": Disables QoS
  - "Basic": Enables QoS generally.
- **Trust Mode:** Select the QoS trust mode from the drop-down list:
  - "CoS": Activate Class of Service
  - "DSCP Only": Activate DSCP as only method.
  - "DSCP First": Activate DSCP as first method.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7.2 Basic - Priority Scheme

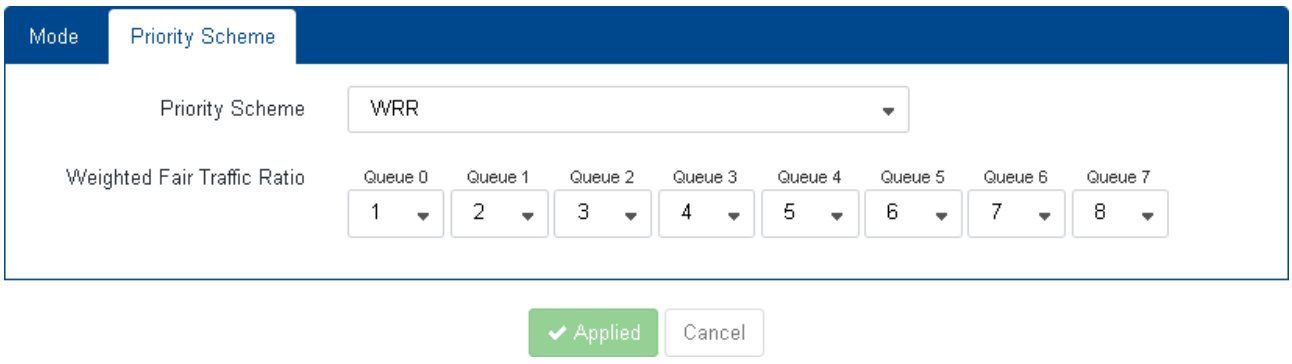


Fig. 66: QoS - Basic - Priority Scheme

This tab allows configuration of QoS priotity schemes.

- **Priority Scheme:** Select the priority scheme from the drop-down list
- **Weighted For Traffic Ratio:** Assign the traffic ratio for the respective priority queue.

  Traffic flow will follow this ratio so that the minimum bandwidth for traffic from lower-priority queues is guaranteed.

Note:
This option is only enabled with priority scheme set to "WRR".

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7.3 Mapping - CoS/802.1p to Queue

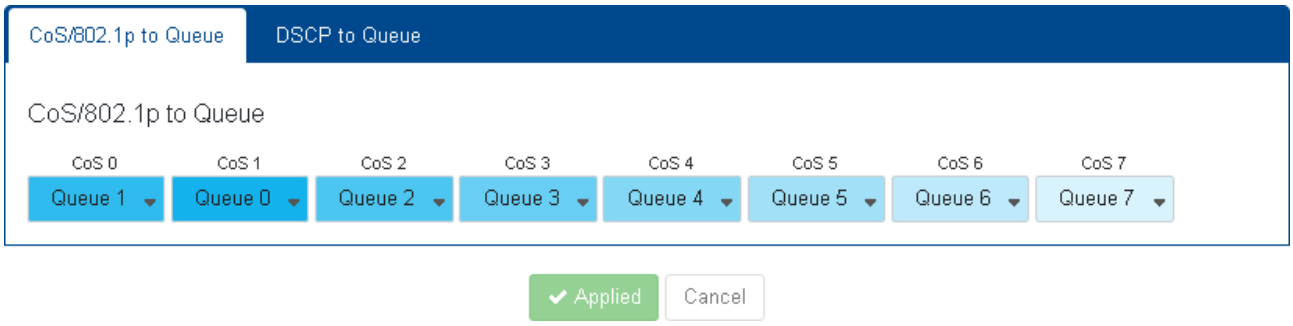


Fig. 67: QoS - Mapping - CoS/802.1p to Queue

Set the internal CoS/802.1p priority queue by selecting a queue number for every priority (0 to 7) from the drop-down list.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7.4 Mapping - DSCP to Queue

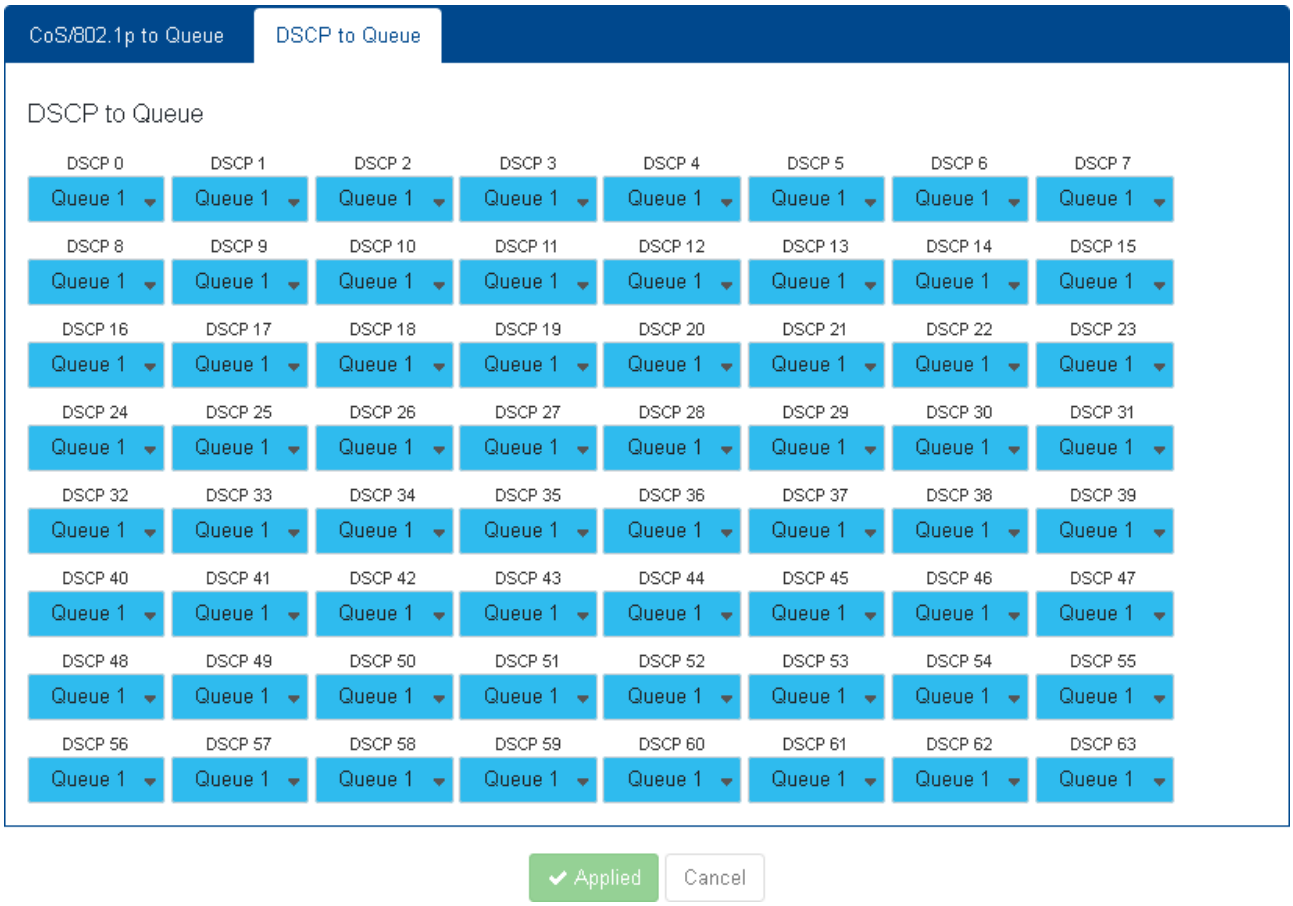


Fig. 68: QoS - Mapping - DSCP to Queue

Set the internal DSCP priority queue by selecting a queue number for every priority (0 to 7) from the drop-down list.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7.5 Interface - Interface Settings

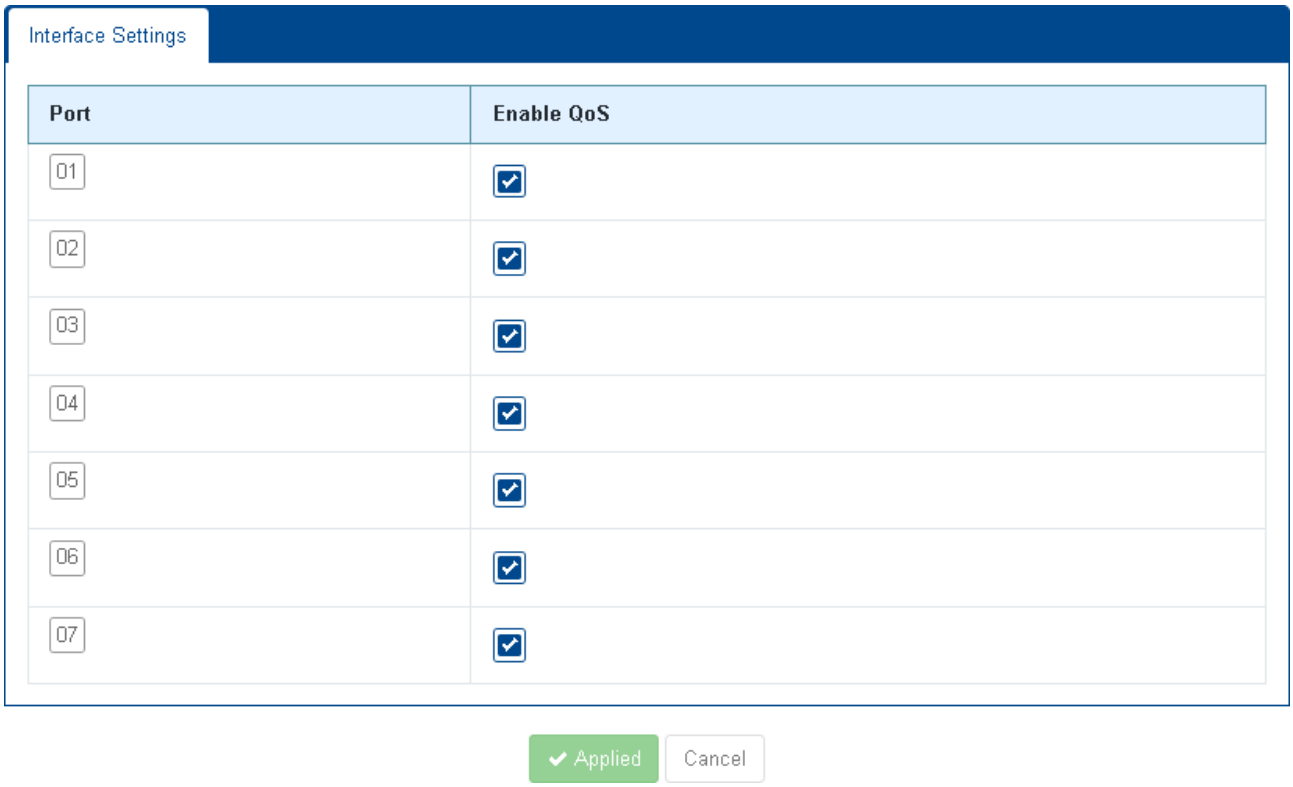


Fig. 69: QoS - Interface - Interface Settings

- **Port:** Port number
- **Enable QoS:** Check or uncheck this option to enable or disable QoS for specific ports.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.7.6 Rate Shaping - Rate Shaping

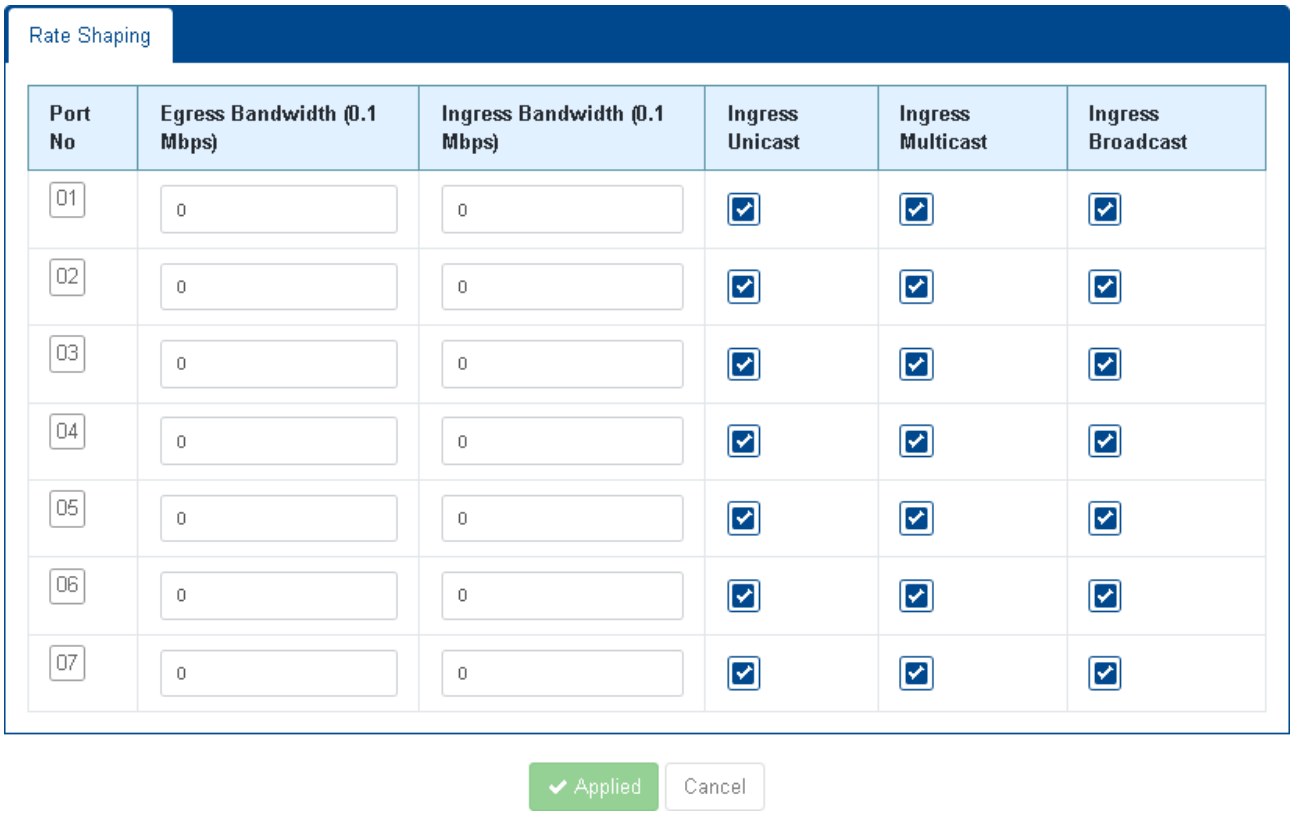


Fig. 70: QoS - Rate Shaping - Rate Shaping

This tab allows the configuration of QoS rate shaping for specific ports.

- **Port:** Port number
- **Egress Bandwidth (0.1 Mbps):** Set the limit for the the outgoing frame rate by extending the interframe gap.

  Egress rate shaping is independent of the frame type. Provide a value of the selected port data rate.

  Set to "0" to disable.
- **Ingress Bandwidth (0.1 Mbps):** Limits the incoming frame rate. Excess frames are dropped and lead to port flow control frames. Provide a value of the selected port data rate. Set 0 to disable or MaxPortSpeed with unit 0.1 Mbps.
- **Ingress Unicast:** Check or uncheck this option to enable or disable ingress unicast frames.
- **Ingress Multicast:** Check or uncheck this option to enable or disable ingress multicast frames.
- **Ingress Broadcast:** Check or uncheck this option to enable or disable ingress broadcast frames.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.8 Multicast

5.8.1 Multicast - Configuration

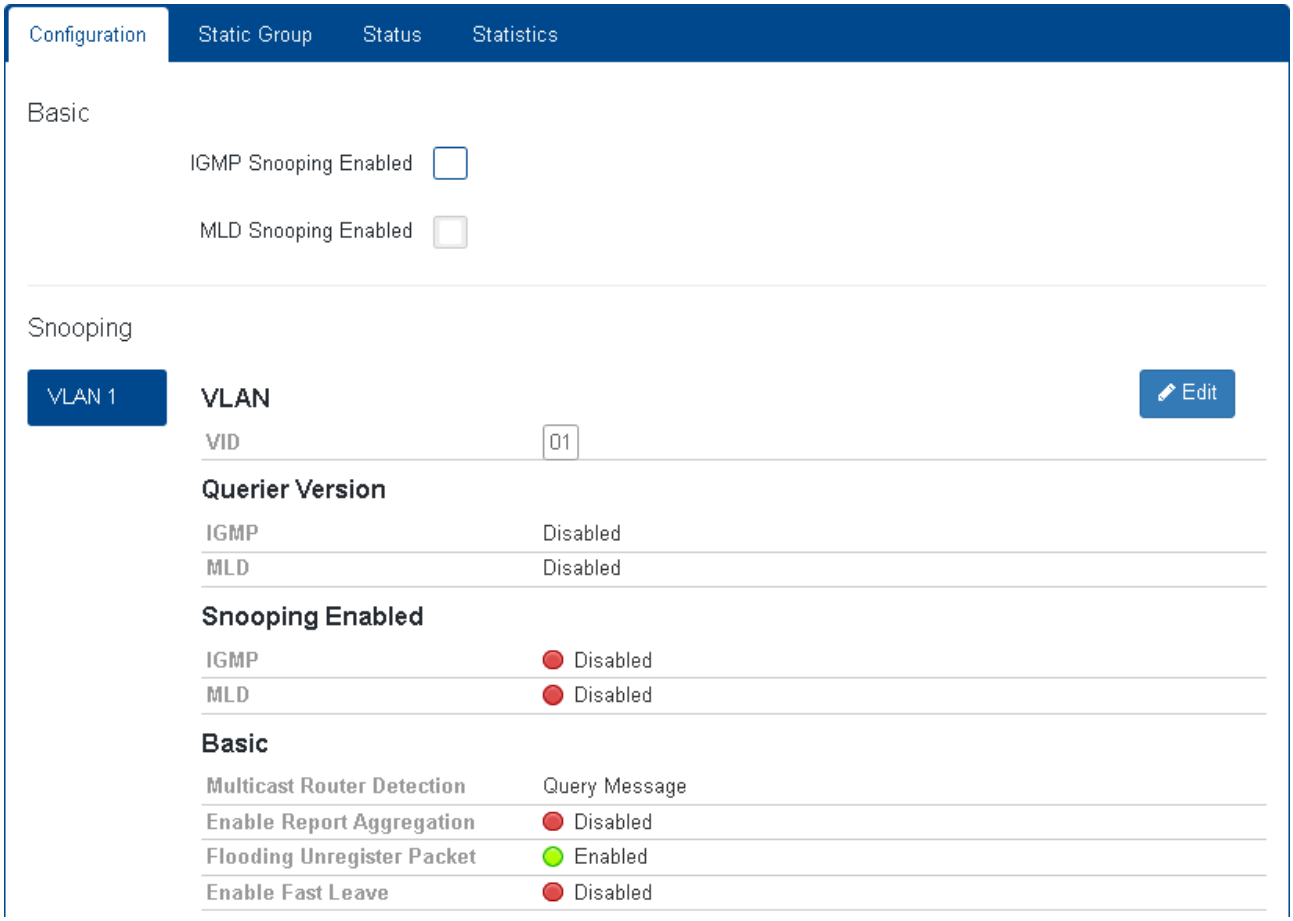


Fig. 71: Multicast - Configuration

This tab allows configuration of snooping mechanisms for handling multicast data transfer.

- **IGMP Snooping enabled:** Check this option to enable IGMP Snooping generally.

  Note: The device only supports one VLAN for IGMP.
- **MLD Snooping enabled:** Check this option to enable MLD Snooping generally.

- **Edit:** Opens the edit dialog for configuration of the IGMP settings.

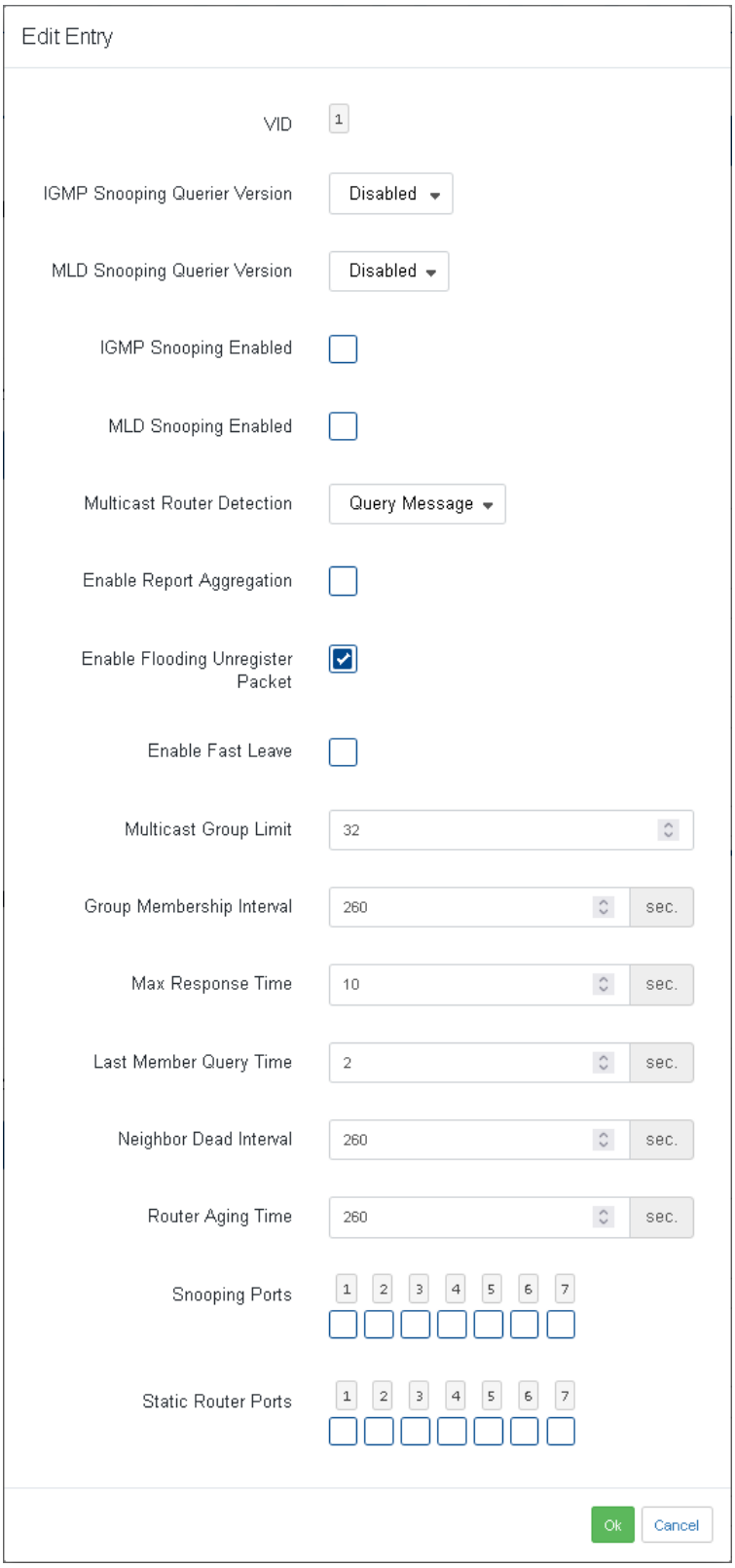


Fig. 72: Multicast - Configuration - Edit Entry

- **VID:** Set the VLAN ID for IGMP data packets.
- **IGMP Snooping Querier Version:** Select the IGMP version from the drop-down list.
- **MLD Snooping Querier Version:** Select the MLD version from the drop-down list.
- **IGMP Snooping Enabled:** Check this option to enable IGMP Snooping for this VLAN ID.
- **MLD Snooping Enabled:** Check this option to enable MLD Snooping for this VLAN ID.
- **Multicast Router Detection:** Select the message type from the drop-down list.
- **Enable Report Aggregation:** Check this option to enable report aggregation.
- **Enable Flooding Unregister Packet:** Check this option to enable forwarding unregistered multicast data packets to all IGMP ports.
- **Enable Fast Leave:** Check this option to activate fast blocking of unnecessary IGMP traffic.
- **Multicast Group Limit:** Set the maximum number of available IGMP groups (1 to 32).
- **Group Membership Interval:** Set the group membership interval in seconds.
- **Max Response Time:** Set the maximum response time in seconds.
- **Last Member Query Time:** Set the last member query interval in seconds.
- **Neighbor Dead Interval:** Set the neighbor dead interval in seconds.
- **Router Aging Time:** Set the aging time in seconds.
- **Snooping Ports:** Check the respective ports that should act as IGMP ports.
- **Static Router Ports:** Check the respective ports that should act as static ports.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.8.2 Multicast - Static Group

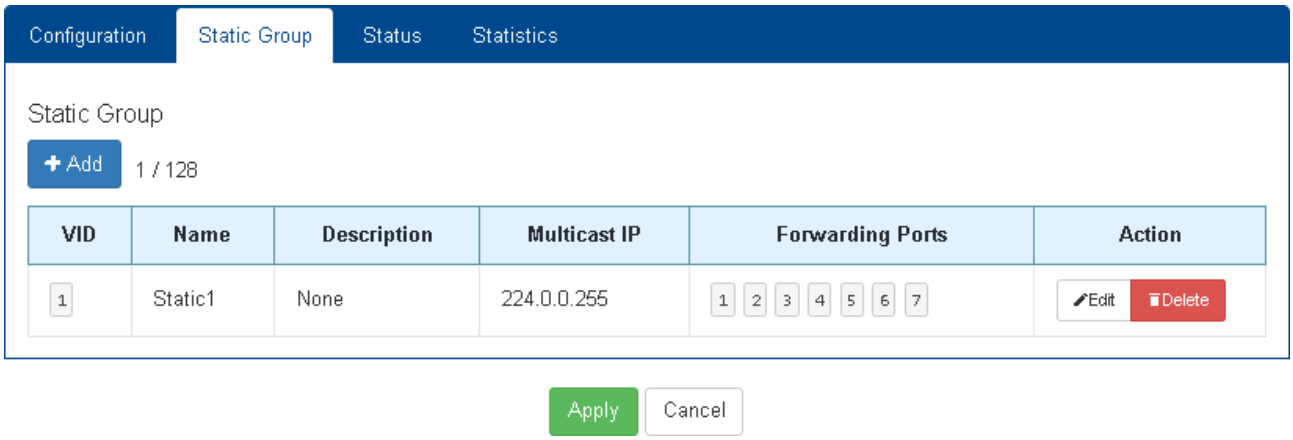


Fig. 73: Multicast - Static Group

This tab allows the configuration of static multicast groups.

- **Edit:** Opens the edit dialogue of the respective group entry. Change the entries as needed.
- **Add:** Opens the dialogue for adding a new group.

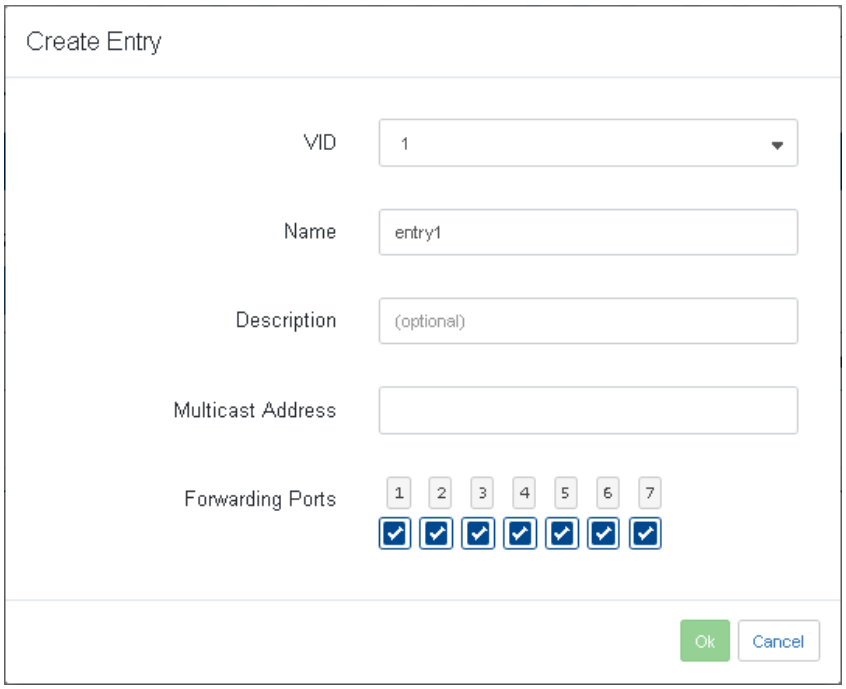


Fig. 74: Multicast - Static Group - Add

- **VID:** Select the VLAN ID from the drop-down list.
- **Name:** Enter a descriptive name for this entry.
- **Description:** Enter a description for this entry.
- **Multicast Address:** Enter the multicast IP address of this entry.

Valid IPv4 range is 224.0.0.255 to 239.255.255.255.

IPv6 is supported. Other addresses ares reserved.

- **Forwarding Ports:** Check or uncheck the forwarding ports.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.8.3 Multicast - Status

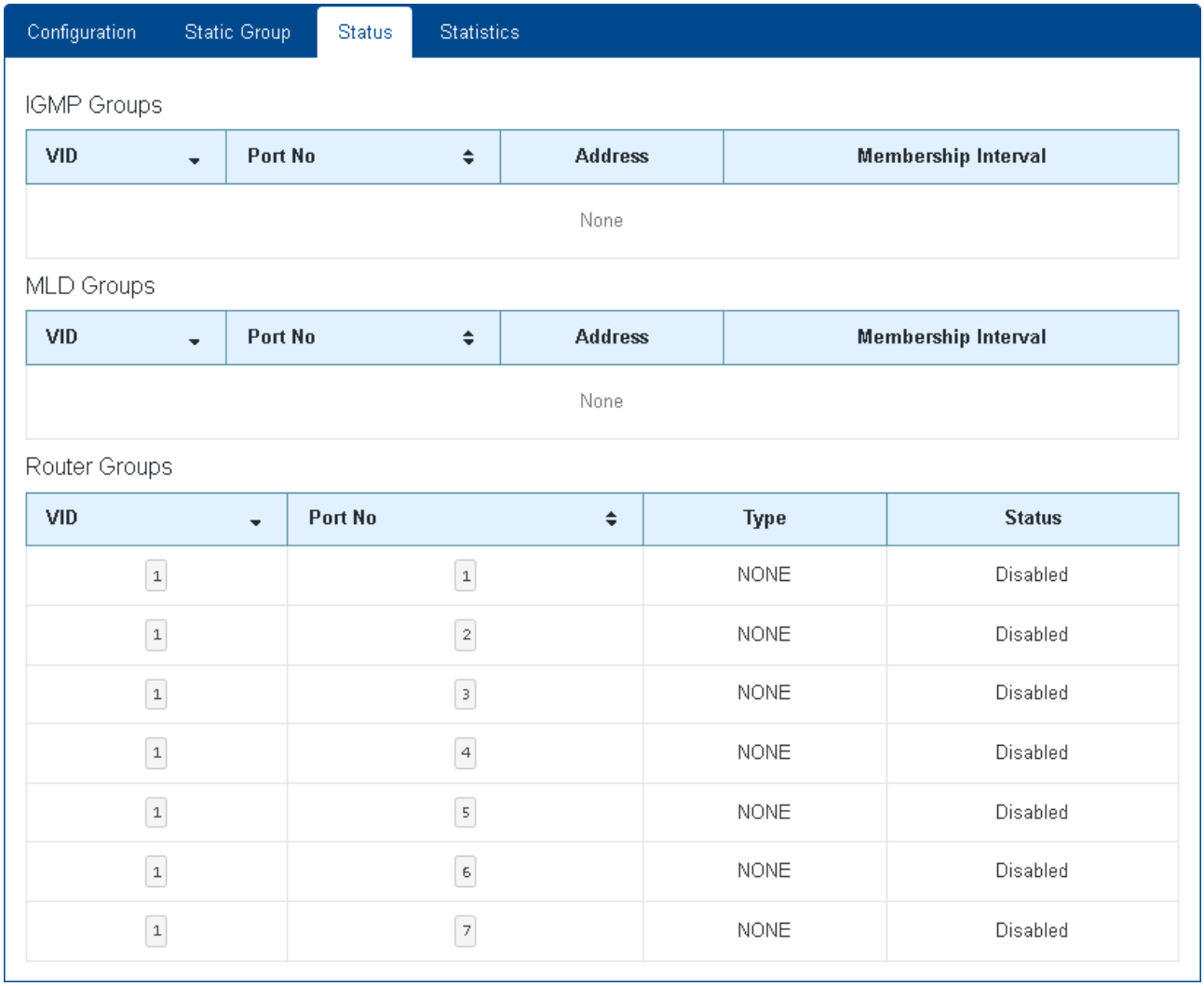


Fig. 75: Multicast - Status

This tab shows a tabular overview of the status of all available IGMP groups.

5.8.4 Multicast - Statistics

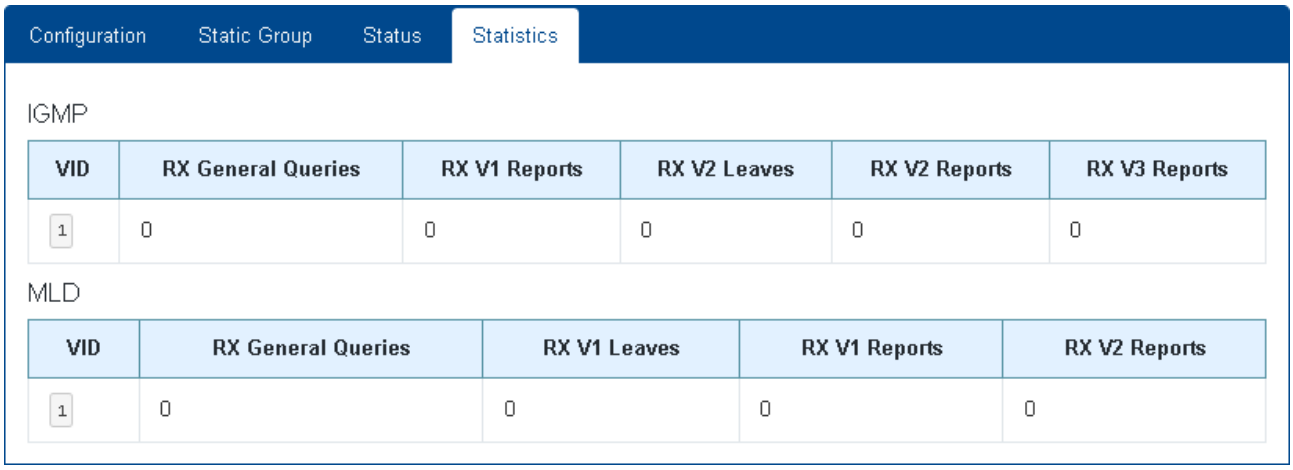


Fig. 76: Multicast - Statistics

This tab shows a tabular overview of all IGMP data packet statistics.

5.9 Discovery

5.9.1 LLDP - Configuration

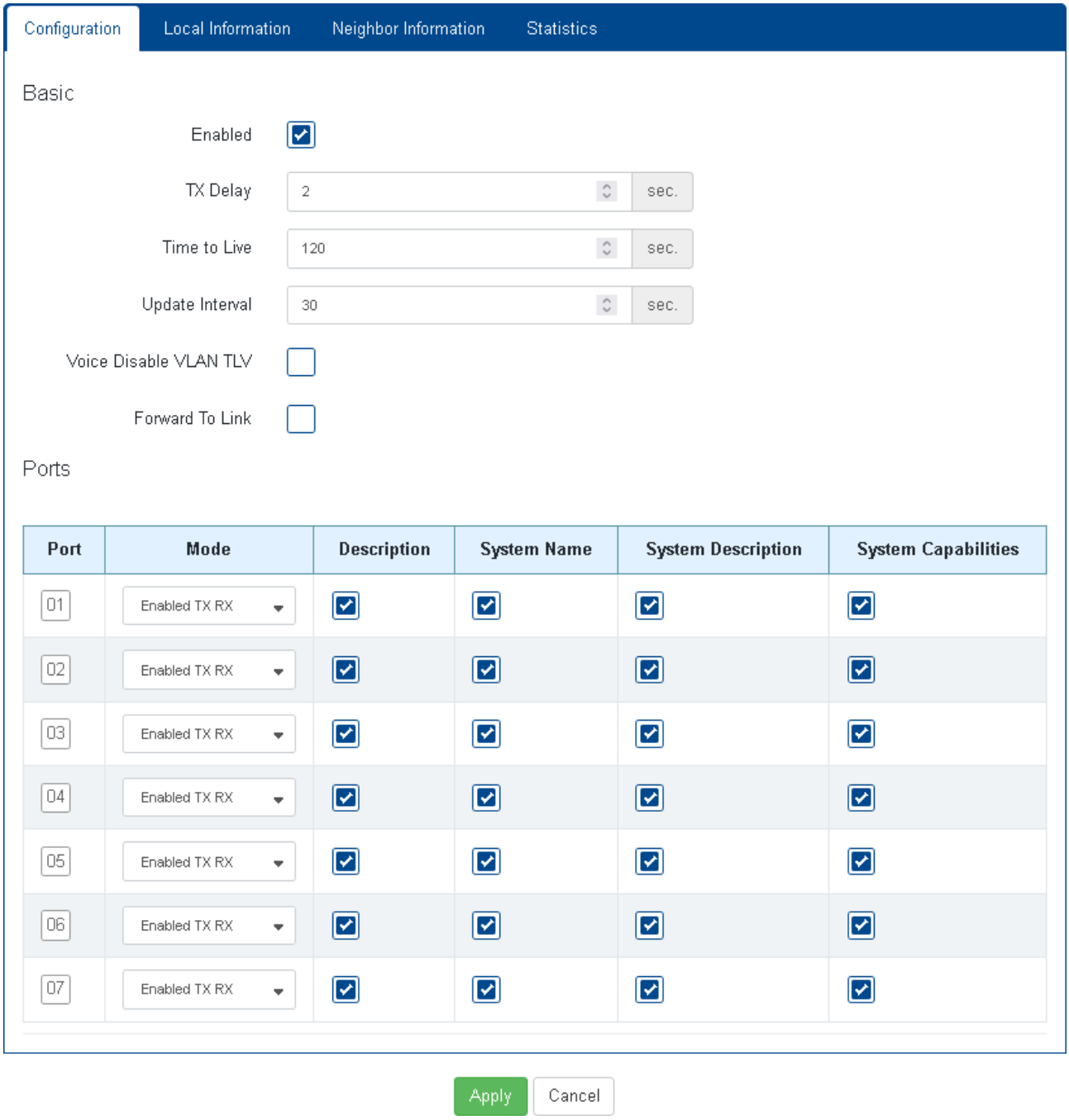


Fig. 77: Discovery - LLDP - Configuration

This tab allows the configuration of LLDP.

- **Enabled:** Check or uncheck this option to enable or disable LLDP.
  If enabled, all other options will appear.

- **TX Delay:** Set the transmission delay in seconds between successive LLDP frame transmissions initiated by changes in the LLDP local configuration.
- **Time to Live:** Set the TTL in seconds.

  The time to live value defines the time for which the LLDP transmitted details are valid and can be displayed in the status.

  Note: When the port is operating in TXRX or RX mode, the device will check the validity of the LLDP packet received and the TLV carried by it.

  After the check, the neighbor information is saved to the local device, and the aging time of the neighbor information on the local device is set according to the TTL value in TTL (Time To Live, Life Time) TLV.

  If this value is zero, the neighbor information is immediately removed.
- **Update Interval:** Set the update interval in seconds, at which LLDP frames are transmitted on behalf of this LLDP agent.
- **Voice Disable VLAN TLV:** Check or uncheck this option to enable or disable Voice VLAN indication TLV transmission.
- **Forward to Link:** Check or uncheck this option to enable or disable forwarding all received LLDP packets to the uplink port.

  In combination with port mode "Enabled RX Only" this unit keeps quiet and all LLDP handling should be taken care off by the upstream device.
- **Port:** Port number of the specific port.
- **Mode:** Select the mode from the drop-down list.
  - Disabled
  - Enabled Tx Rx
  - Enabled Tx Only
  - Enabled Rx Only
- **Description / System Name / System Description / System Capabilities:** Check or uncheck the specific option to enable or disable sending the respective information in LLDP.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.9.2 LLDP - Local Information

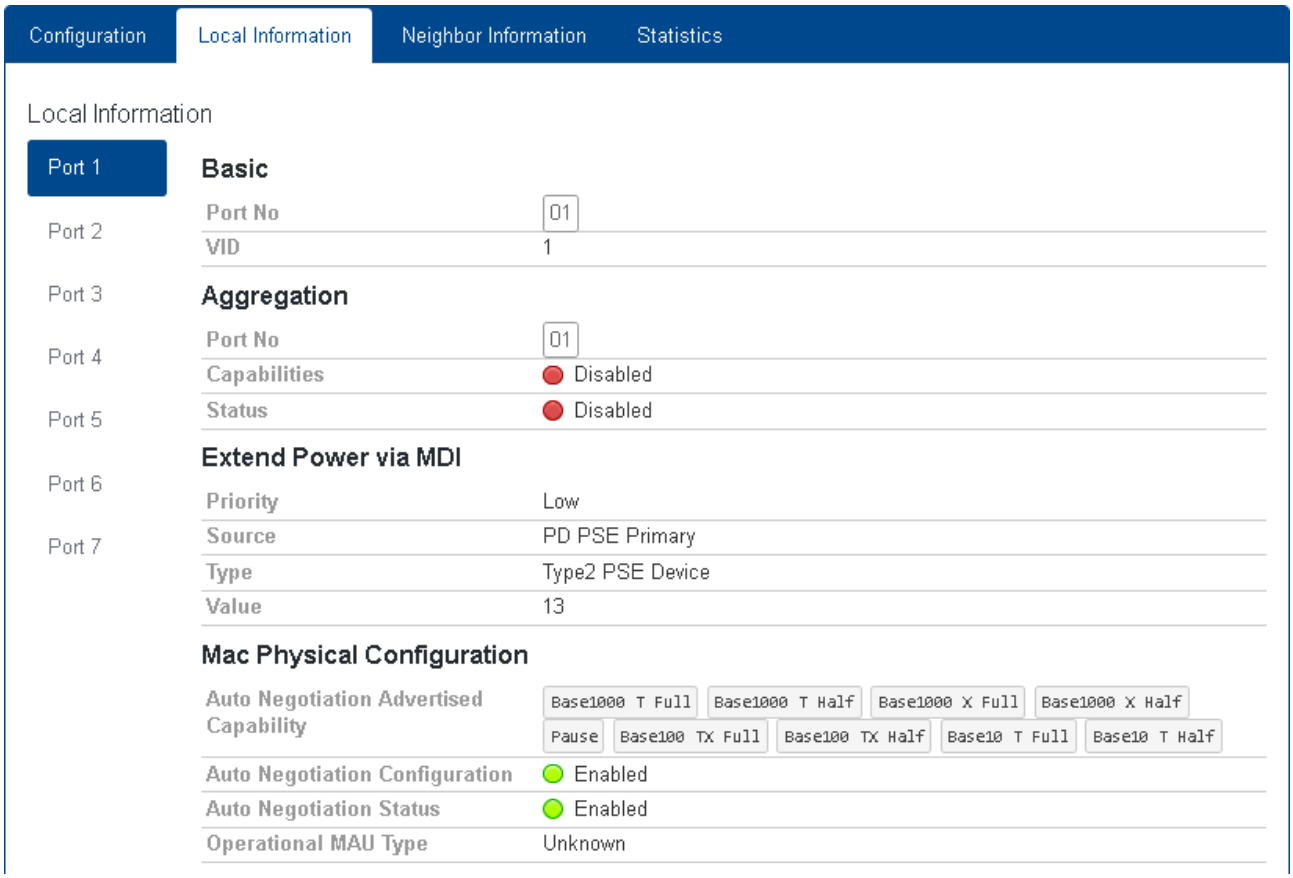


Fig. 78: Discovery - LLDP - Local Information

This tab shows the information the device publishes in its LLDP advertisements, depending on the selected port on the left hand pane.

5.9.3 LLDP - Neighbor Information

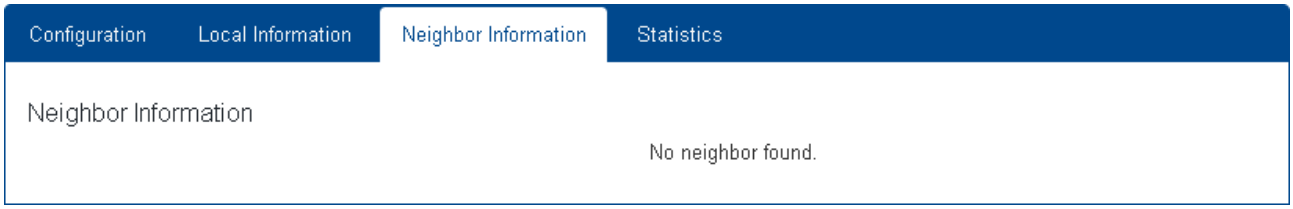


Fig. 79: Discovery - LLDP - Neighbor Information

This tab shows all LLDP advertisements the device have received from its LLDP neighbors.

Click on a radio button on top of the dialogue to select LLDP neighbor information from this port.

5.9.4 LLDP - Statistics

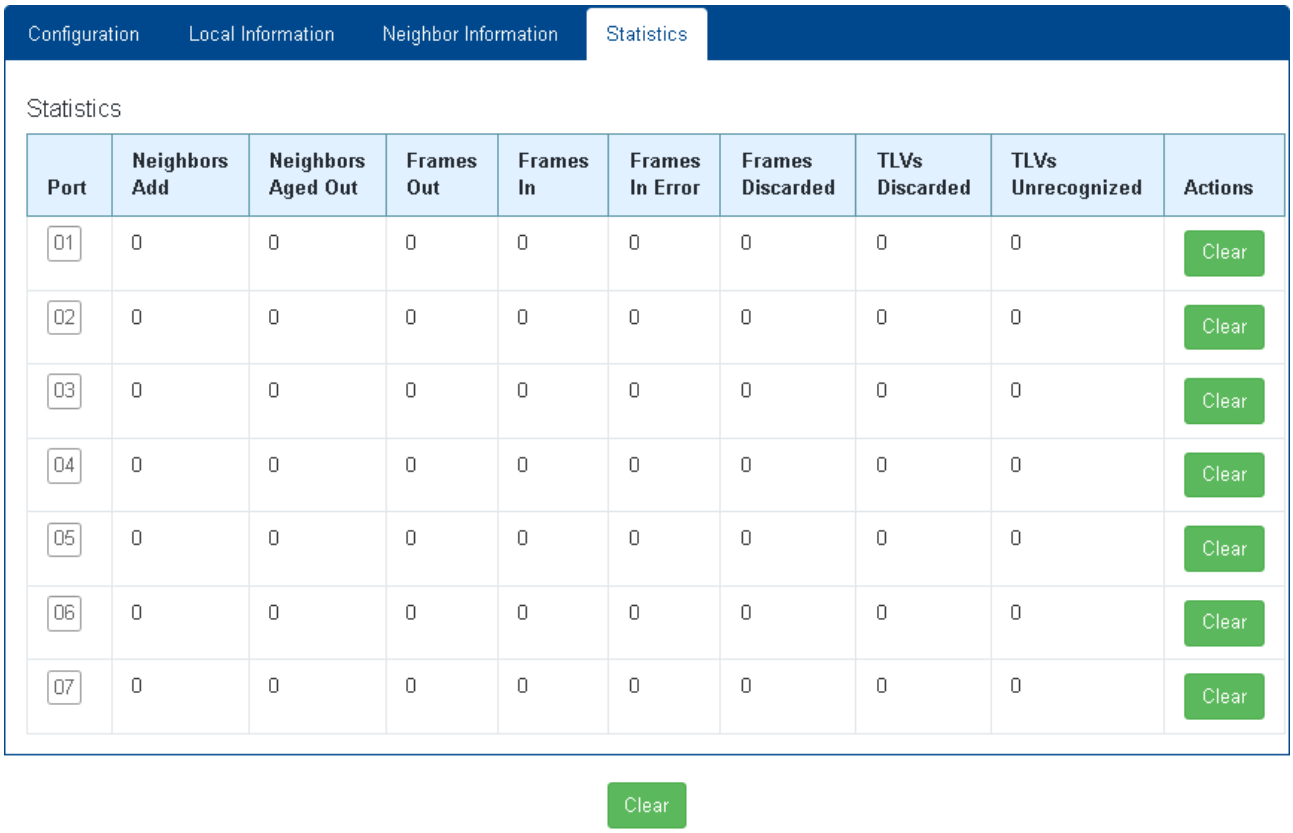


Fig. 80: Discovery - LLDP - Statistics

This tab shows a tabular overview of LLDP statistics.

- Click on the button **Clear** in the right-hand table column to flush the statistics of the respective port.
- Click the button **Clear** below the table to flush all statistics of all ports.

5.9.5 CDP - Configuration

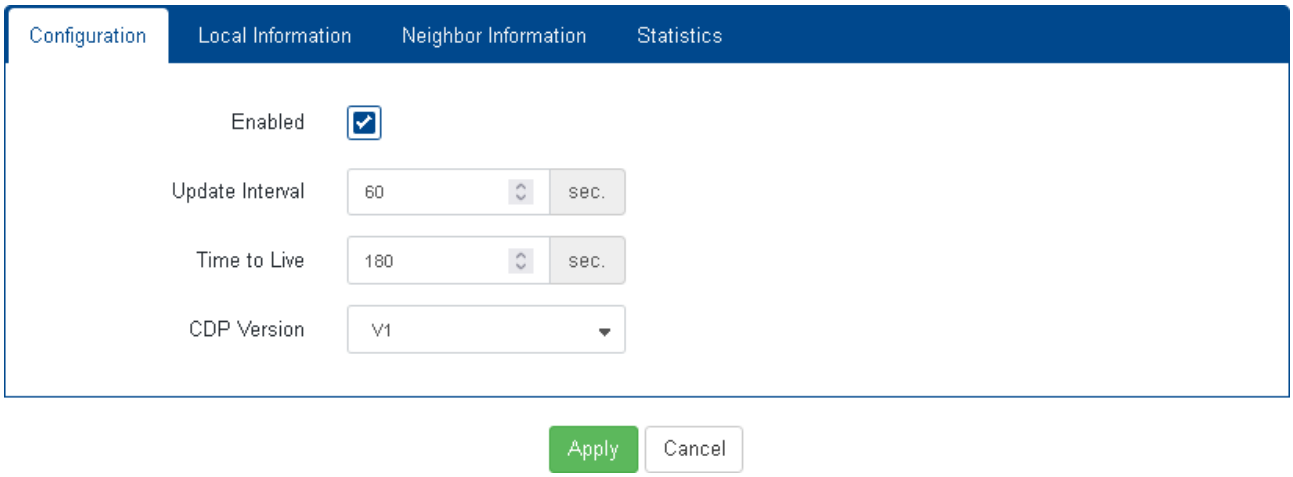


Fig. 81: Discovery - CDP - Configuration

This tab allows the configuration of CDP (Cisco Discovery Protocol).

- **Enabled:** Check or uncheck this option to enable or disable CDP.

  If enabled, all other options will appear.
- **Update Interval:** Set the time status to live in seconds while the CDP transmitted details are valid and can be displayed in the status.
- **Time to Live:** Set the interval status in seconds at which CDP frames are transmitted on behalf of this CDP agent.
- **CDP Version:** Select from the drop-down list, which CDP version should be used.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.9.6 CDP - Local Information

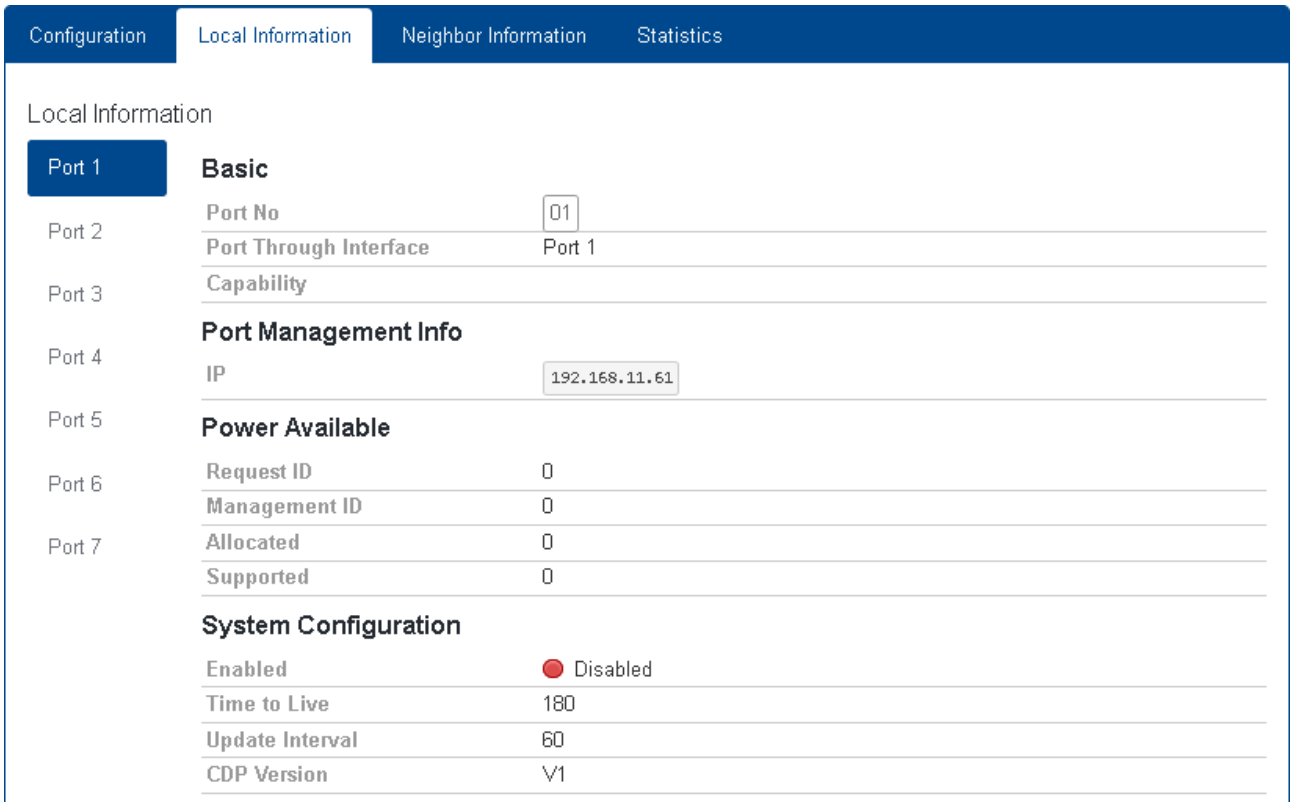


Fig. 82: Discovery - CDP - Local Information

This tab shows the information the device publishes in its CDP advertisements, depending on the selected port on the left hand pane.

5.9.7 CDP - Neighbor Information

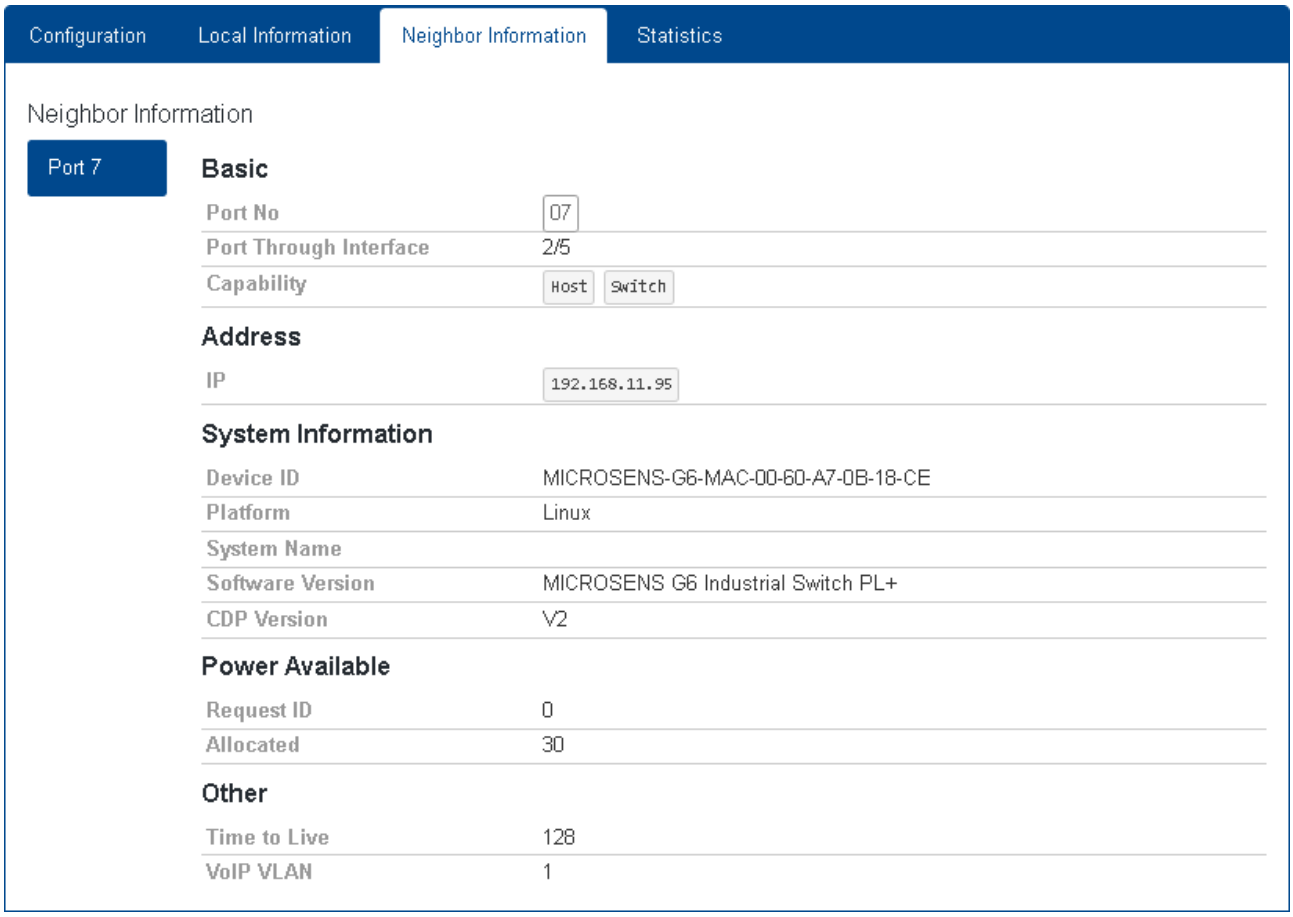


Fig. 83: Discovery - CDP - Neighbor Information

This tab shows all CDP information the device have received from its CDP neighbors.

5.9.8 CDP - Statistics

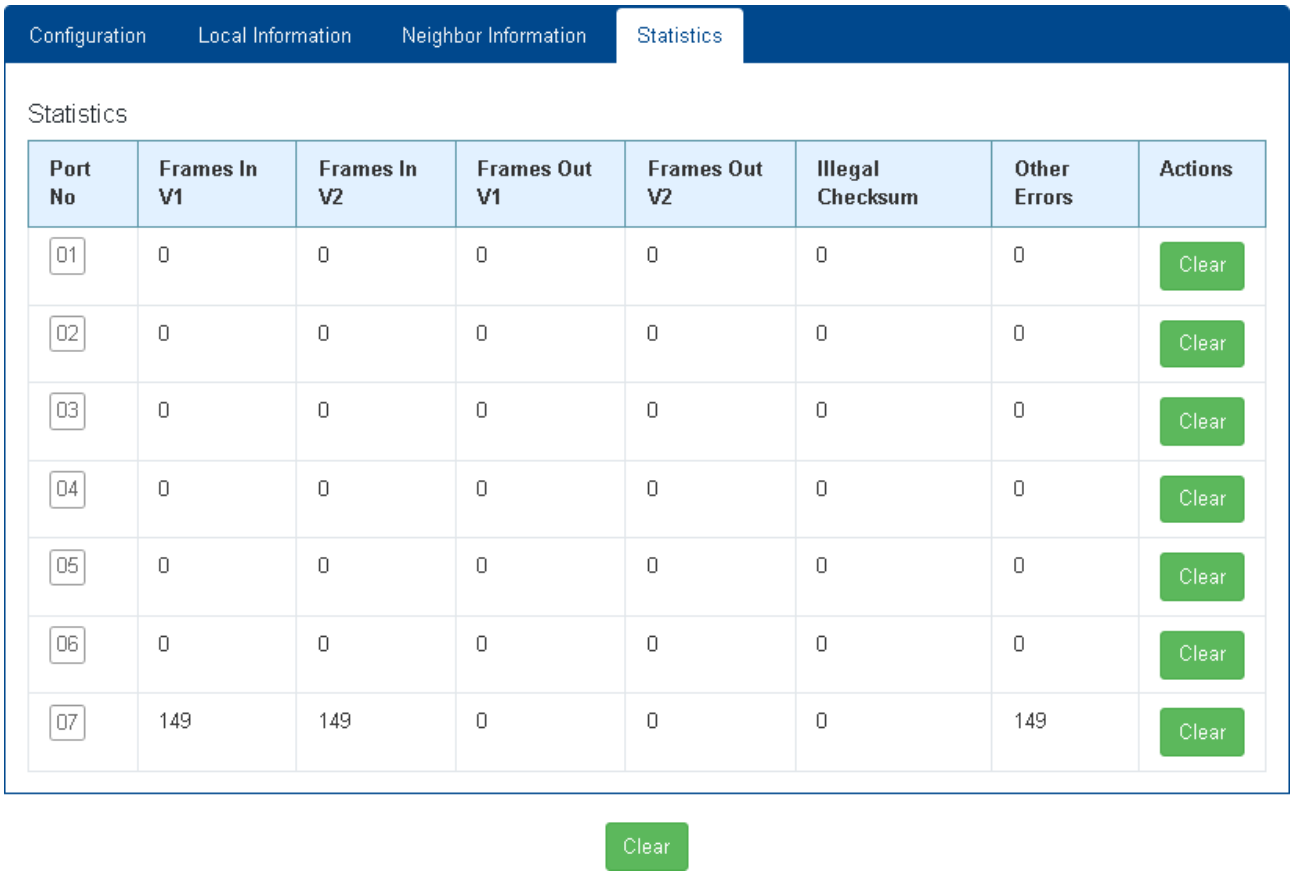


Fig. 84: Discovery - CDP - Statistics

This tab shows a tabular overview of CDP statistics.

- Click on the button **Clear** in the right-hand table column to flush the statistics of the respective port.
- Click the button **Clear** below the table to flush all statistics of all ports.

5.10 DHCP

5.10.1 DHCP - DHCP Relay

The DHCP Relay Agent eliminates the need to use a DHCP server on each physical segment. It can deliver messages to DHCP servers in remote physical subnets, and can also send messages from the DHCP server back to DHCP clients that are in remote physical subnets.

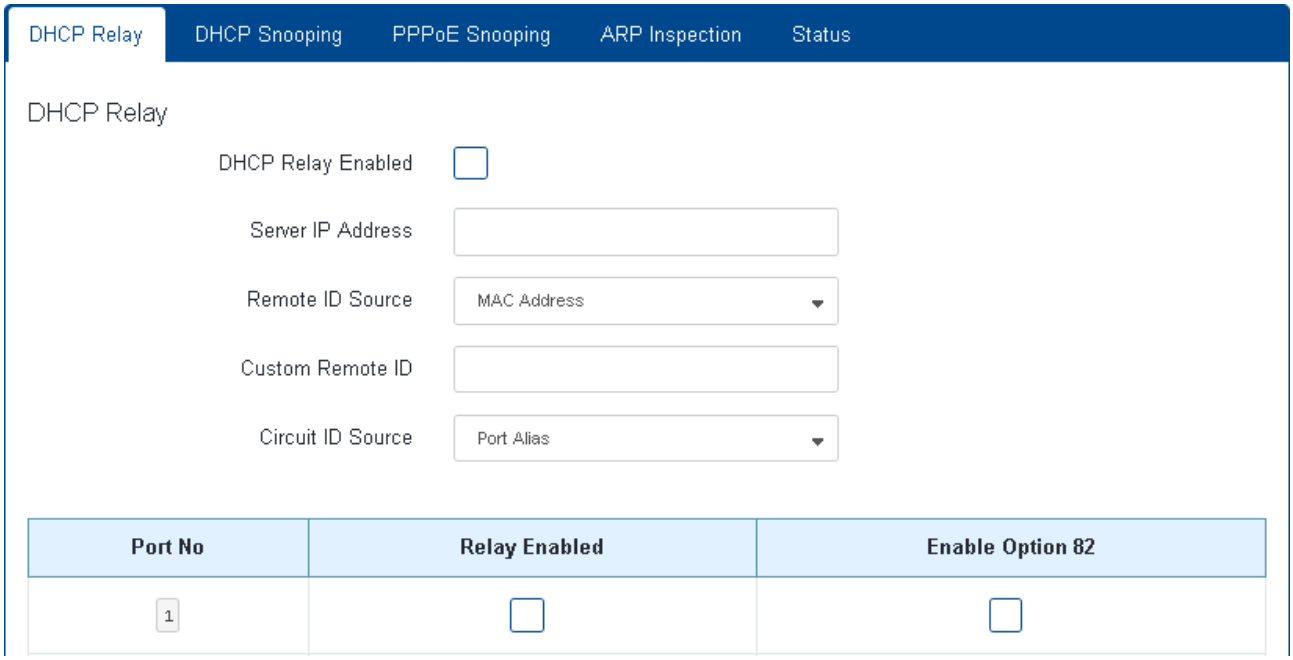


Fig. 85: DHCP - DHCP Relay

This tab allows the configuration of DHCP Relay settings.

- **DHCP Relay Enabled:** Check or uncheck this option to enable or disable the DHCP Relay.
- **Server IP Address:** Enter the DHCP server's IP address.
- **Remote ID Source:** Select the remote ID source from the drop-down list.
- **Custom Remote ID:** With "User Defined" selected as **Remote ID Source** enter the custom ID.
- **Circuit ID Source:** Select the port identification mode from the drop-down list:
  - "Port Alias": The port alias is used.
  - "IP Port VLAN": The port's VLAN ID is used.
- **Port No:** Lists all ports of the device.
- **Relay Enabled:** Check or uncheck this option to enable or disable DHCP Relay for the respective port.
- **Enable Option 82:** Check or uncheck this option to enable or disable DHCP Option 82.

  This option (Relay Agent Information Option) is part of the option content of the DHCP packet.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.10.2 DHCP - DHCP Snooping

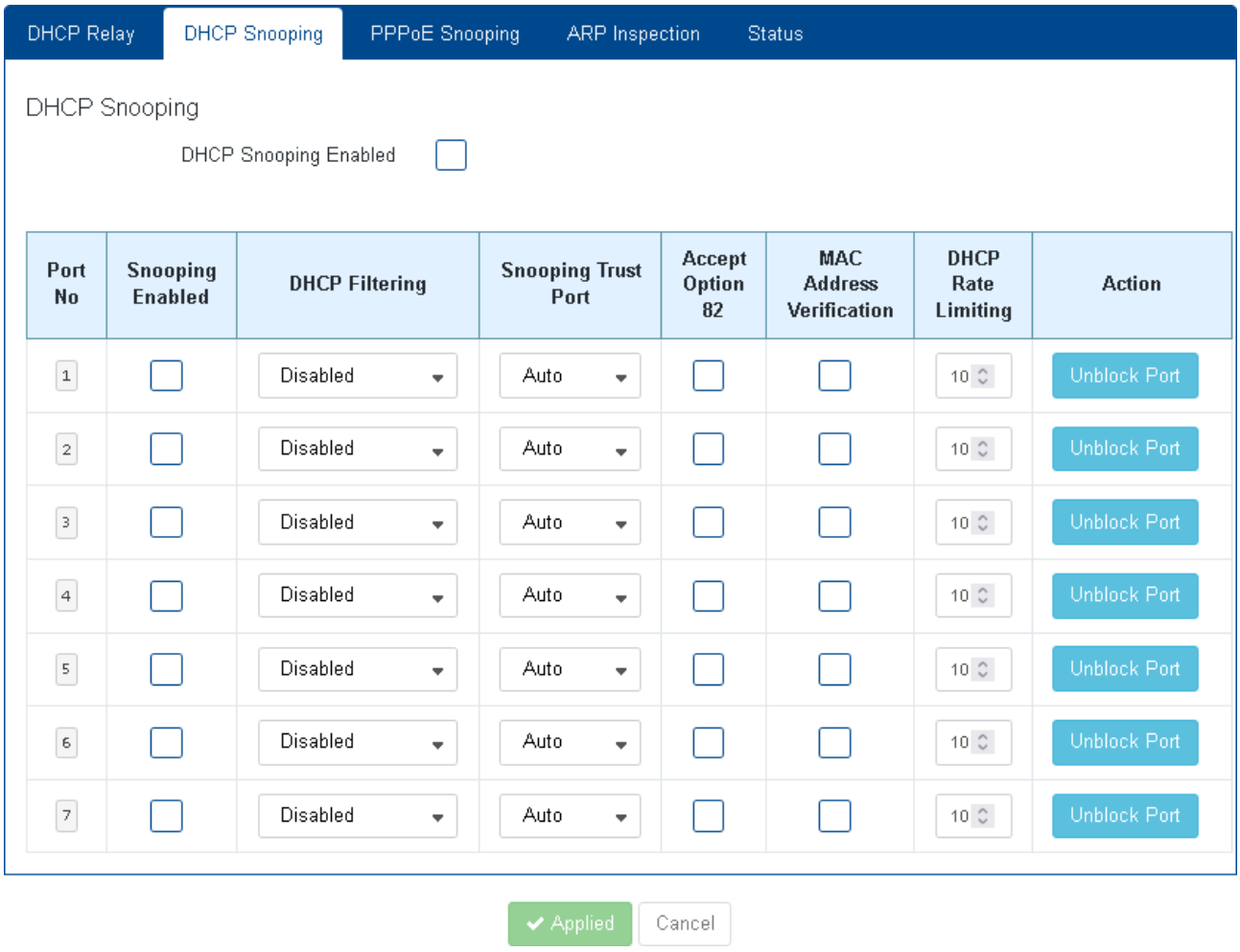


Fig. 86: DHCP - DHCP Snooping

This tab shows an editable tabular overview of the DHCP Snooping settings.

- **DHCP Snooping Enabled:** Check or uncheck this option to enable or disable DHCP Snooping.
- **Port No:** Lists all ports of the device.
- **Snooping Enabled:** Check or uncheck this option to enable or disable DHCP Snooping for the respective port.
- **DHCP Filtering:** Check or uncheck this option to enable or disable DHCP filtering for this port.
- **Snooping Trust Port:** Select the port's trust setting from the drop-down list.
  - "Auto": Uses the port role and declares all up or downlink ports as trusted.
  - "Trusted": If DHCP Snooping is enabled for this port, the device will forward the incoming DHCP messages "OFFER", "ACK" and "NAK" on this port.

- "untrusted": If DHCP is enabled for this port, the device will discard the incoming DHCP messages "OFFER", "ACK" and "NAK" on this port to block untrusted DHCP server messages.

- **Accept Option 82:** Check or uncheck this option to let this port accept or decline DHCP Option 82 packets.
- **MAC Address Verification:** Check or uncheck this option to enable or disable MAC address verification for this port.

  With MAC address verification enabled, the device compares the MAC address contained in the DHCP header ("CHADDR") of the received DHCP message to the destination MAC address. If these addresse do not match, the DHCP message is dropped.
- **DHCP Rate Limiting:** Defines how many DHCP request are accepted per second. When the limit is reached, DHCP flooding is assumed and the port is blocked.

  The value 0 disables the rate limit check.
- **Unblock Port:** Click this button to manually unblock a blocked port.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.10.3 DHCP - PPPoE Snooping

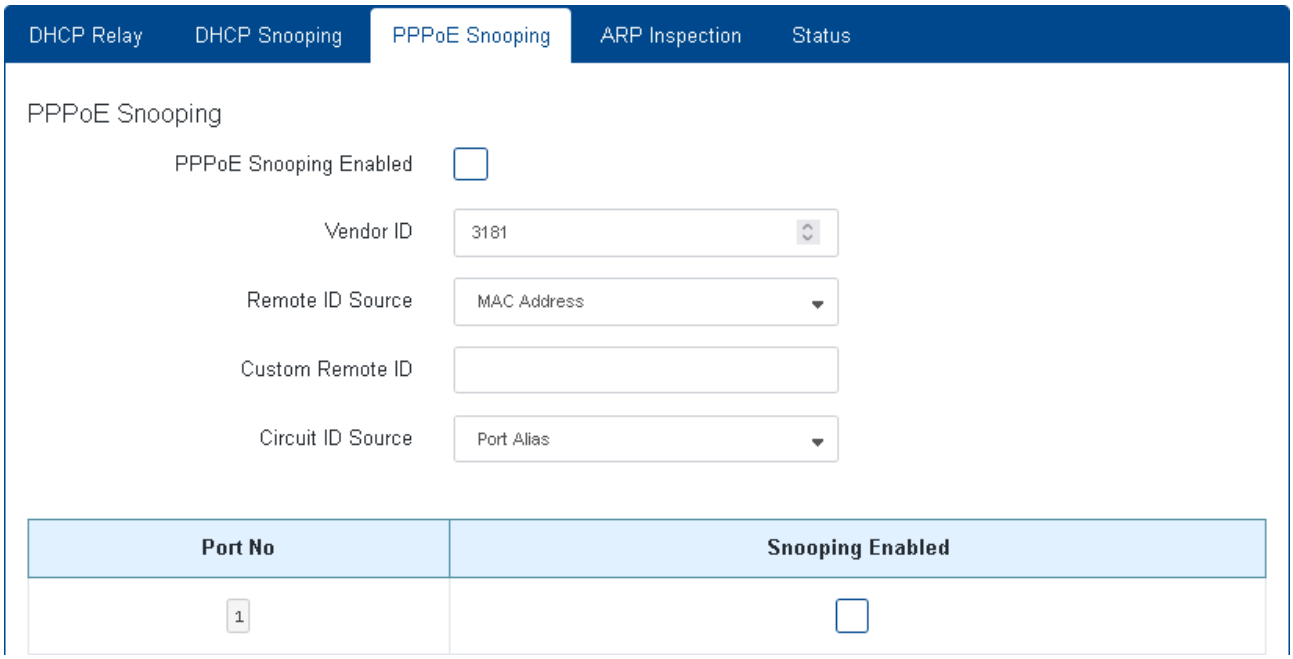


Fig. 87: DHCP - PPPoE Snooping

This tab shows an editable tabular overview of the PPPoE Snooping settings.

- **PPPoE Snooping Enabled:** Check or uncheck this option to enable or disable PPPoE Snooping.
- **Vendor ID:** Select the remote ID from the drop-down list as identification that this device adds to a PPPoE request before forwarding it to the server.

- **Remote ID Source:** The remote id identifies the client that requests a PPPoE connection.
- **Custom Remote ID:** With "User Defined" selected as **Remote ID Source** enter the custom ID.
- **Circuit ID Source:** Select the ID source of the port on which a PPPoE request comes in:
  - "Port Alias": The port alias is used.
  - "IP Port VLAN": The port's VLAN ID is used.
- **Port No:** Lists all ports of the device.
- **Snooping Enabled:** Check or uncheck this option to enable or disable PPPoE snooping for the respective port.
- Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.10.4 DHCP - ARP Inspection

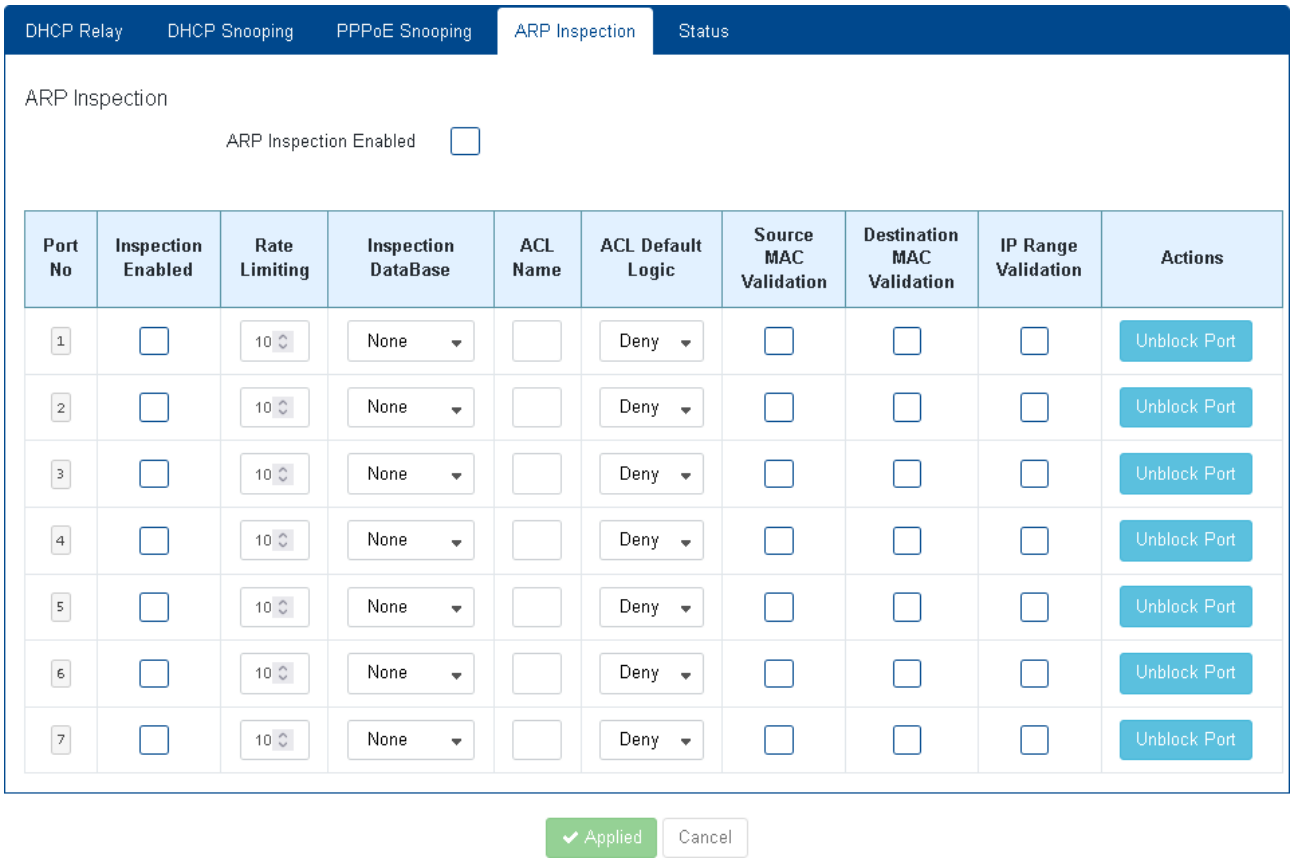


Fig. 88: DHCP - ARP Inspection

This tab shows an editable tabular overview of the ARP Inspection settings.

- **ARP Inspection Enabled:** check or uncheck this option to enable or disable DHCP Snooping.
- **Port No:** Lists all ports of the device.

- **Inspection Enabled:** Check or uncheck this option to enable or disable ARP Inspection for the respective port.
- **Rate Limiting:** Defines how many ARP request are accepted per second. When the limit is reached, a DDOS attack is assumed and the port is shut down.

  The value 0 disables the rate limit check.
- **Inspection Database:** When set to another value than "NONE", the MAC-IP relationship of the incoming ARPs is verified against the selected table.

  This ensures that only valid MACs enter the network.
- **ACL Name:** Enter the name of an existing ACL which declares which IP/MAC relations are acceptable. Several ACLs may be specified with a comma separated list.

  Note:
  For more information about managing ACLs refer to section 5.6.12 on page 56.
- **ACL Default Logic:** Defines which action is taken when none of the ACL records matches.

  Default is "deny" which blocks the ARP.
- **Source MAC Validation:** Check or uncheck this option to enable or disable source MAC validation for the respective port.
- **Destination MAC Validation:** Check or uncheck this option to enable or disable destination MAC validation for the respective port.
- **IP Range Validation:** Check or uncheck this option to enable or disable IP range validation for the respective port.

  Checks ARP for invalid addresses. Invalid addresses include "0.0.0.0", "255.255.255.255" and all IP multicast and loopback addresses.

  Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.
- **Unblock Port:** Click this button to manually unblock a blocked port.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.10.5 DHCP - Status

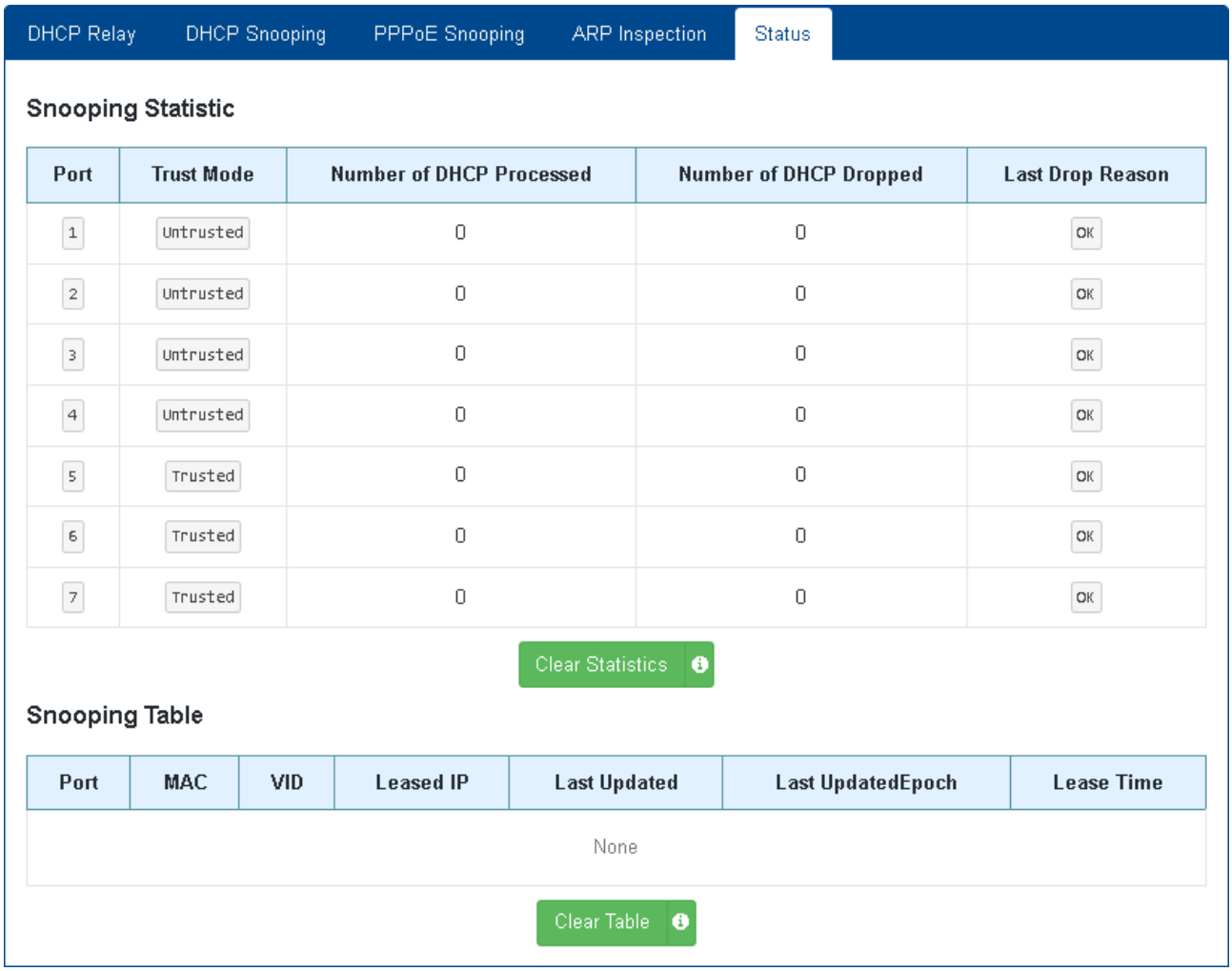


Fig. 89: DHCP - Status

This tab shows a tabular overview of the DHCP status of all ports.

- **Clear Statistics:** Click this button to clear all DHCP Snooping statistics.
- **Clear Table:** Click this button to clear the DHCP Snooping table.

5.11 Redundant

5.11.1 STP - Bridge Configuration

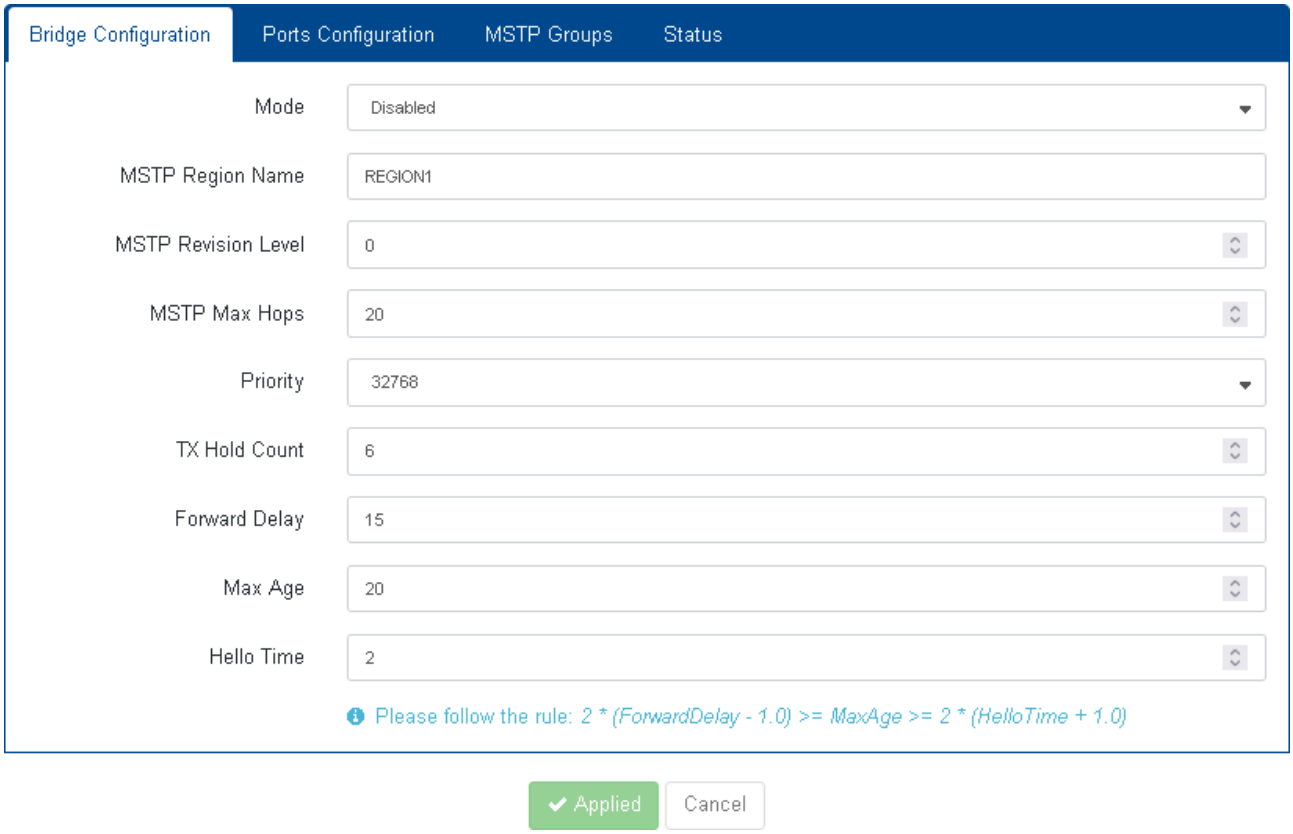


Fig. 90: Redundant - STP - Bridge Configuration

This tab allows the bridge configuration of the devices STP settings for redundant network topology.

- **Mode:** Select the redundant mode from the drop-down list
  - "Disabled": Disables redundant ring functionality.

    Otherwise (i.e., a Spanning Tree Protocol is selected), when a network loop is detected, both affected ports will be blocked.
  - "STP": Selects Spanning Tree Protocol.
  - "RSTP": Selects Rapid Spanning Tree Protocol.
  - "MSTP": Selects Multiple Spanning Tree Protocol.
- **MSTP Region Name:** Assign the MSTP region name.
- **MSTP Revision Level:** Assign the MSTP revision level.
- **MSTP Max Hops:** Set the maximum hops for the BPDU packets of MSTP.
- **Priority:** Set the root priority from values "0" to "32768".

  The smaller the value, the higher the priority.

The higher the bridge priority of a switch, the more likely the switch will become a root bridge.

- **TX Hold Count:** Set a limit value for BPDU transmissions.

  The internal counter is increased by 1, every time a BPDU is received.

  It is decreased by 1 every second.

  When the internal counter value reaches the RX Hold Count setting, sending a BPDU is delayed.
- **Forward Delay:** Set the time in seconds the device will remain in listening and learning state before sending a packet after a network topology change.
- **Max Age:** Set the STP timer for the BPDU survival time in seconds.
- **Hello Time:** Set the time period in seconds the root bridge will send BPDUs.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.11.2 STP - Ports Configuration

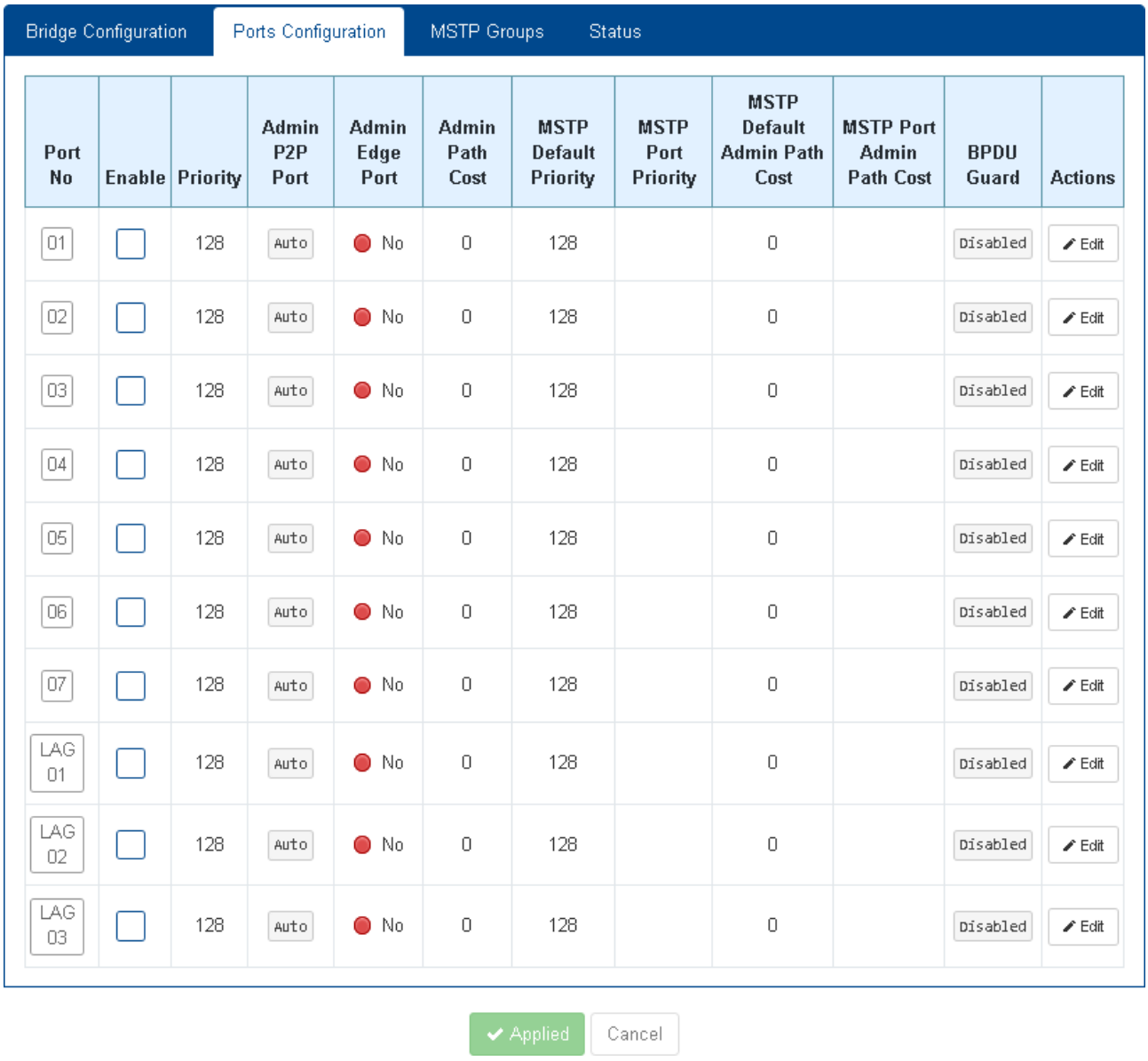


Fig. 91: Redundant - STP - Ports Configuration

This tab shows an editable tabular overview of the STP port settings.

Click on the button **Edit** to modify the respective port's STP settings.

- **Port No:** Lists all ports of the device.
- **Enable:** Check or uncheck this option to enable or disable STP for this port.
- **Priority:** Select the STP priority for this port from the drop-down list.
- **Admin P2P Port:** Select the point-to-point link type for this port from the drop-down list.
- **Admin Edge Port:** Check or uncheck this option to enable or disable the edge port function for this port.

If a device's port is directly connected to a terminal device, this port is called "edge port". With this option enabled this port does not participate in RSTP operations (e.g. receive or process BPDU packets).

This port can be switched directly from "Disabled" to "Forwarding" state.

- **Admin Path Cost:** Set the path cost of the root bridge.
- **MSTP Default Priority:** Set the priority used in all MSTP instances unless otherwise configured in **MSTP Port Priority**.

  Note:
  Value has to be a multiple of 16.
- **MSTP Port Priotity:** The port priotity used in all specific MSTP instances.

  Note:
  Value has to be a multiple of 16.
- **MSTP Default Admin Path Cost:** The port path cost used in all MSTP instances unless otherwise configured in **MSTP Port Admin Path Cost**.
- **MSTP Port Admin Path Cost:** The port path cost used in specific MSTP instances.
- **BPDU Guard:** Check or uncheck this option to enable or disable the BPDU guard for this port.

  If enabled, this port switches to "blocked" state as soon as it receives a BPDU.

  The event "BPDU_GUARD_EVENT" is generated.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.11.3 STP - MSTP Groups

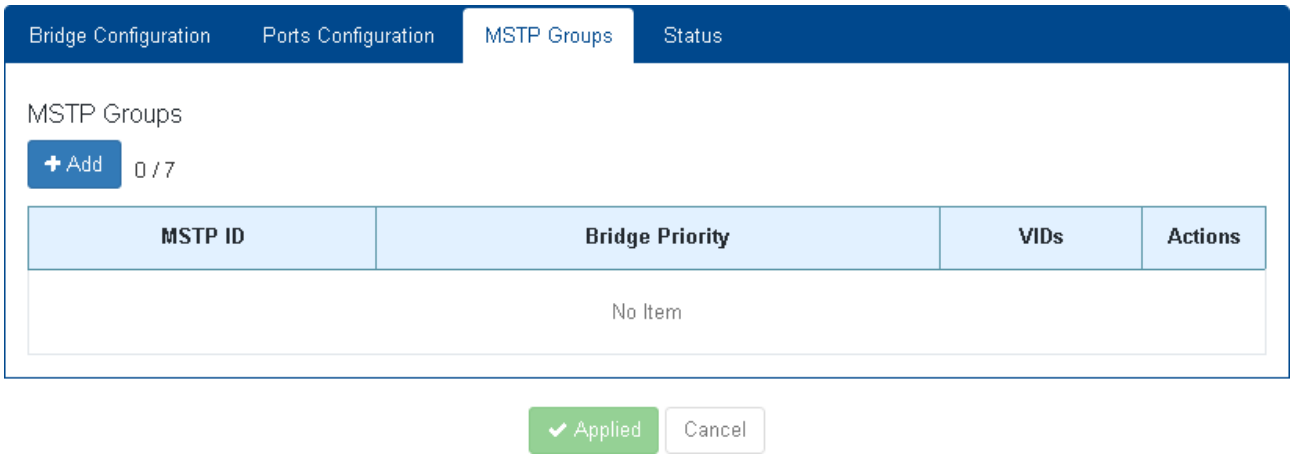


Fig. 92: Redundant - STP - MSTP Groups

The tab allows the configuration of MSTP groups.

Note:
This table defines MSTP parameters that may differ between instances. Several VLANs may share the same MSTP group. If needed up to 63 table entries can be created.

- **Edit:** Opens the edit dialogue of the respective group entry. Change the entries as needed.

- **Add:** Opens the dialogue for adding a new group.

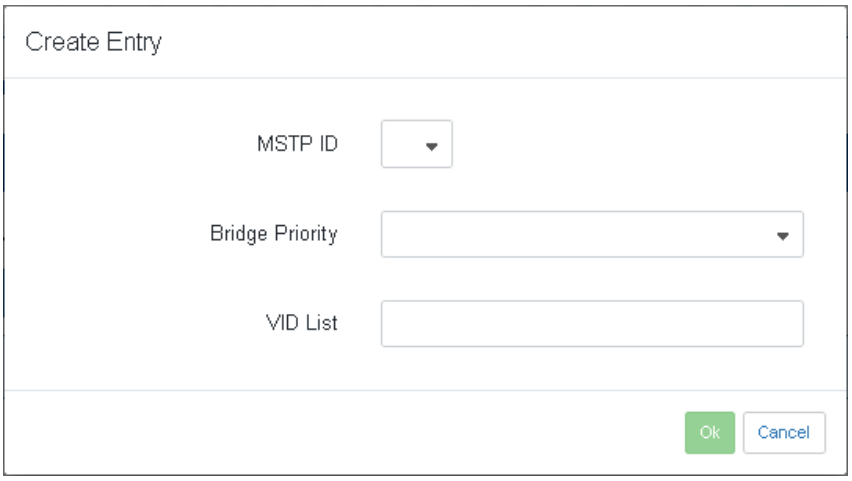


Fig. 93: Event & Log - Targets - Add

- **MSTP ID:** Select the ID from the drop-down list.
- **Bridge Priority:** Select the bridge priority from the drop-down list.
- **VID List:** Enter the VLAN IDs that should take part in the MSTP group.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.11.4 STP - Status

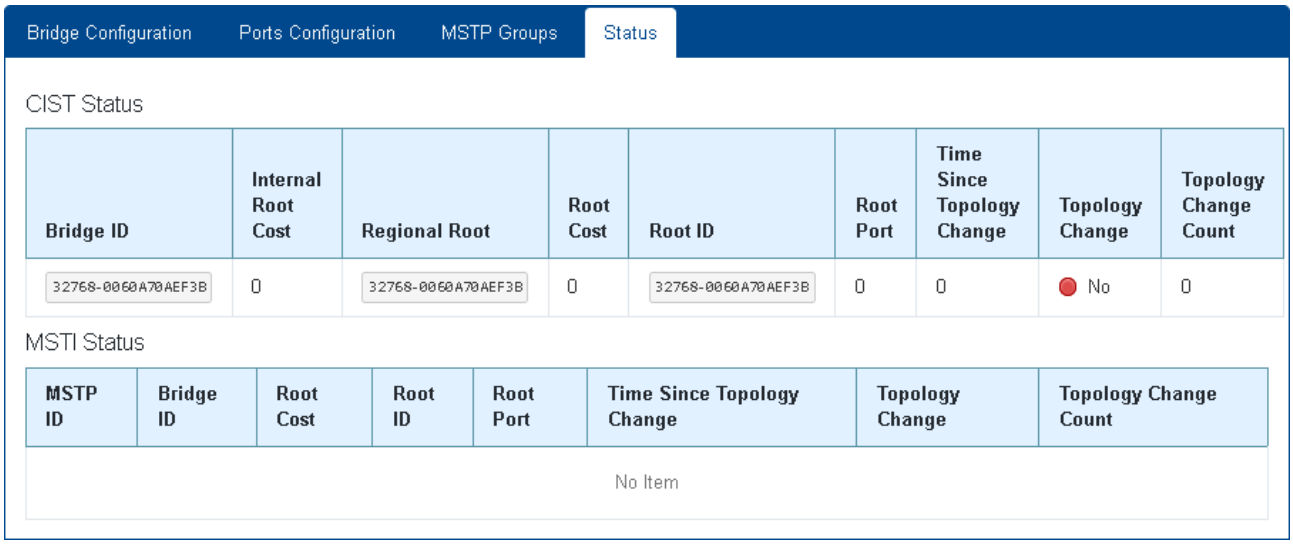


Fig. 94: Redundant - STP - Status

This tab shows a detailed tabular overview of the devices STP status.

5.11.5 G.8032 - G8032 Configuration

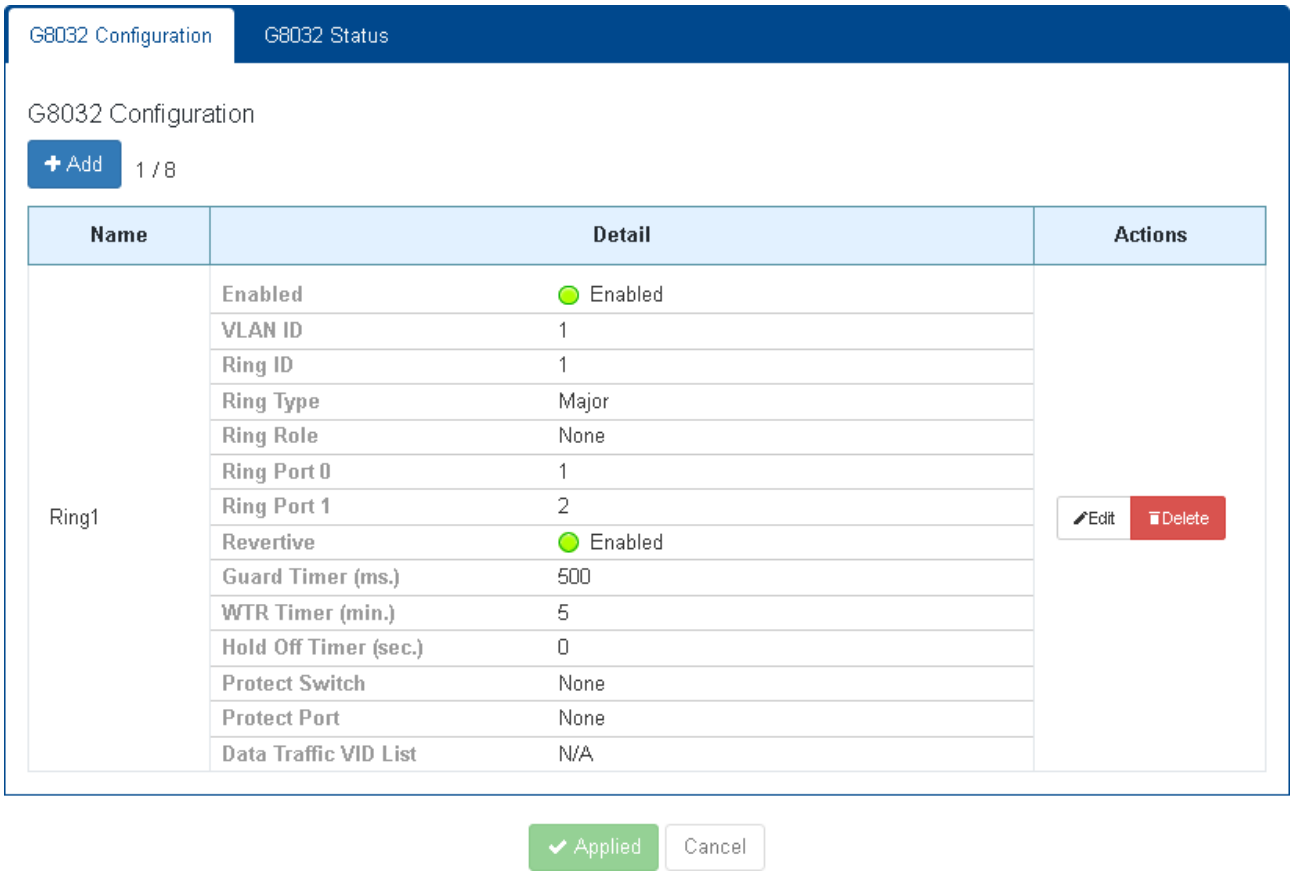


Fig. 95: Redundant - G.8032 - G8032 Configuration

This tab shows a tabular overview of availabe G.8032 rings.

- **Edit:** This button opens the edit dialogue to edit the respective ring entry.

- **Add:** Opens the dialogue for adding a new ring entry.

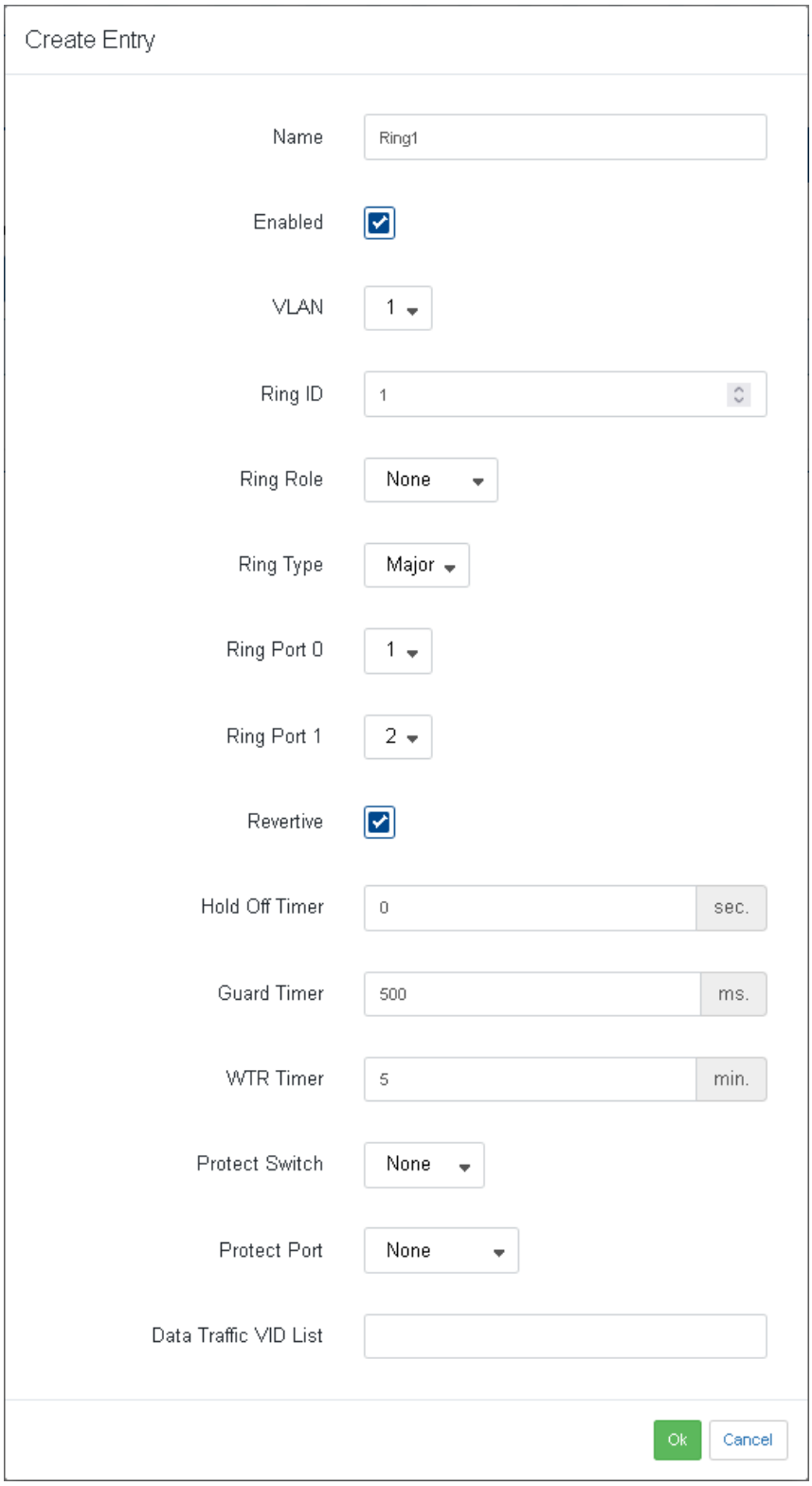


Fig. 96: Redundant - G.8032 - G8032 Configuration - Add

- **Name:** Descriptive name for this entry.
- **Enabled:** check or uncheck this option to enable or disable this entry.

  - Red indicator: Entry is disabled.

  - Green indicator: Entry is enabled.
- **VLAN ID:** The VLAN ID of the ring packets.
- **Ring ID:** The ID of this ring.
- **Ring Role:** Select one of the following entries:

  - Owner

  - Neighbor

  - None
- **Ring Type:** Shows the ring type:

  - Major

  - Sub
- **Ring Port 0:** Select the port that acts as Ring Protection Link (RPL).

  The ring protection link is the ring link that under normal conditions, i.e., without any failure or request, is blocked (at one or both ends) for data traffic, to prevent a loop.
- **Ring Port 1:** Select the port that is connected to the ring under normal conditions.

  This port is set to "forwarding" state.
- **Revertive:** Check this option to enable revertive switching.
- **Holf Off Timer:** Set the time in seconds for the hold-off timer in seconds.

  The hold-off timer delays a notification about a ring error for the assigned time. In case of the error persists after this duration, it will be reported.
- **Guard Timer:** Set the time in milliseconds for the ring guard timer.

  The guard timer is used to prevent Ethernet ring nodes from acting upon outdated R-APS messages and prevents the possibility of forming a closed loop.
- **WTR Timer:** Set the time in minutes for the WTR timer.
- **Protect Switch:** Select the port blocking mode from the drop-down list:

  - "None"

  - "Manual"

  - "Force"
- **Protect Port:** Select the ring port from the drop-down list.
- **Data Traffic VID List:** Enter a comma-separated list of VLAN IDs.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.11.6 G.8032 - Status

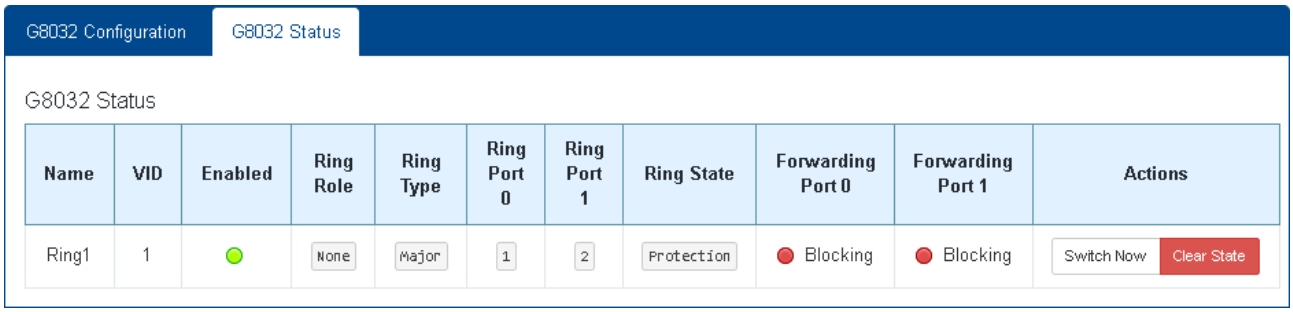


Fig. 97: Redundant - G.8032 - Status

This tab shows a tabular overview of the status of all enabled G.8031 rings.

- **Switch Now:** Click on this button to switch the respective ring entry.
- **Clear State:** Click on this button to clear the ring's state.

5.11.7 MS Ring - Configuration

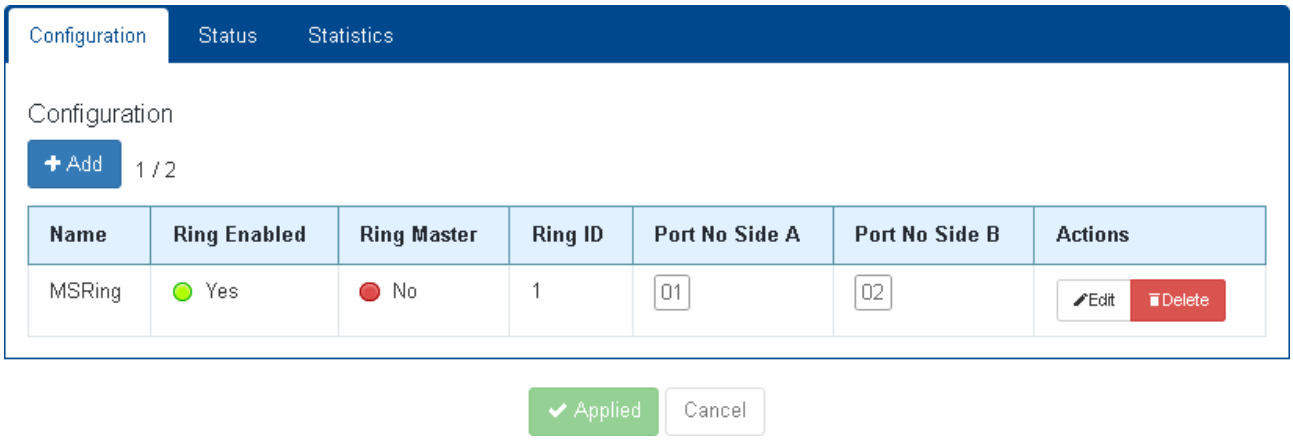


Fig. 98: Redundant - MS Ring - Configuration

This tab shows a tabular overview of availabe MS rings.

- **Edit:** This button opens the edit dialogue to edit the respective ring entry.

- **Add:** Opens the dialogue for adding a new ring entry.

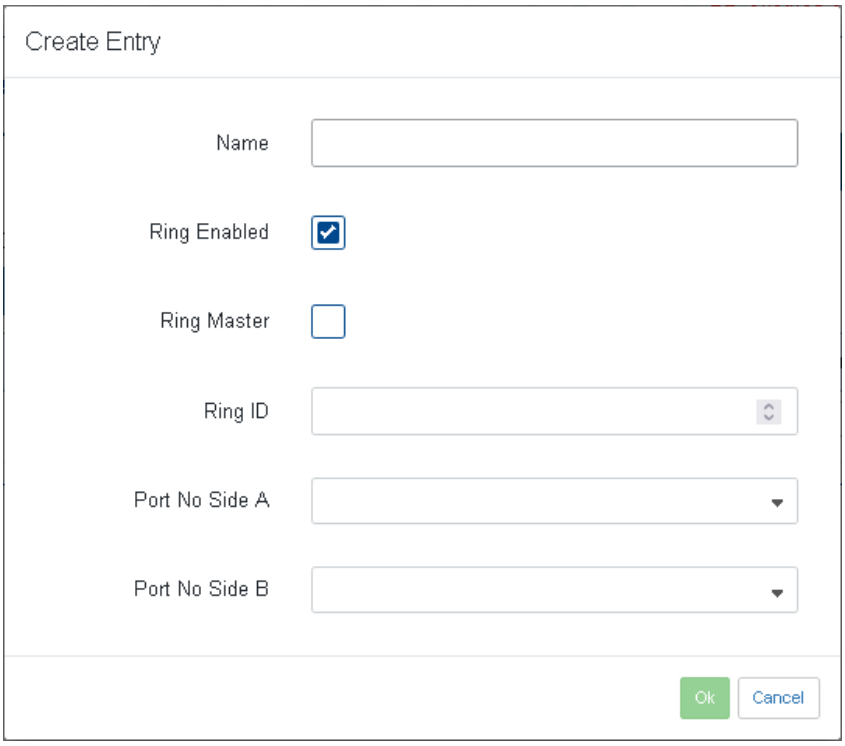


Fig. 99: Redundant - MS Ring - Configuration - Add

- **Name:** Enter a descriptive name for this entry.
- **Ring Enable:** Check or uncheck this option to enable or disable this ring.
- **Ring Master:** Check or uncheck this option to enable or disable this ring as ring master.
- **Ring ID:** Set the ring ID for this entry.
- **Port No Side A:** Select the port number from the drop-down list.
- **Port No Side B:** Select the port number from the drop-down list.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.11.8 MS Ring - Status

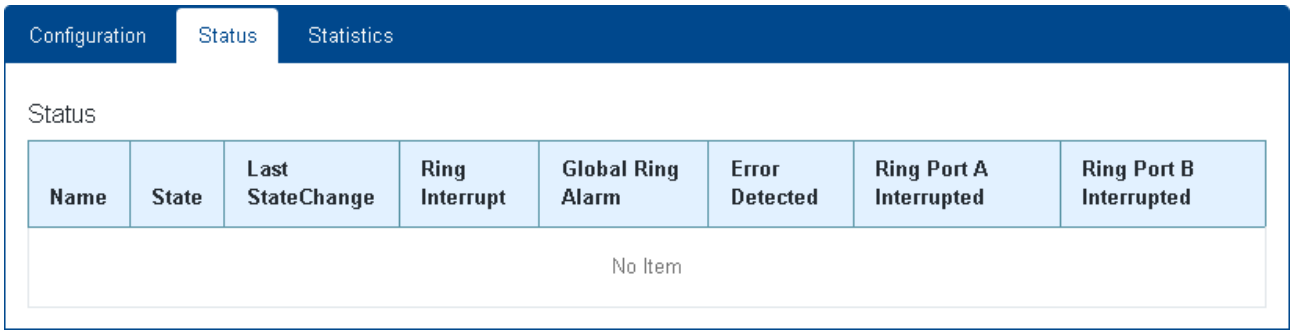


Fig. 100: Redundant - MS Ring - Status

This tab shows a tabular overview of the status of all available MS rings.

5.11.9 MS Ring - Statistics

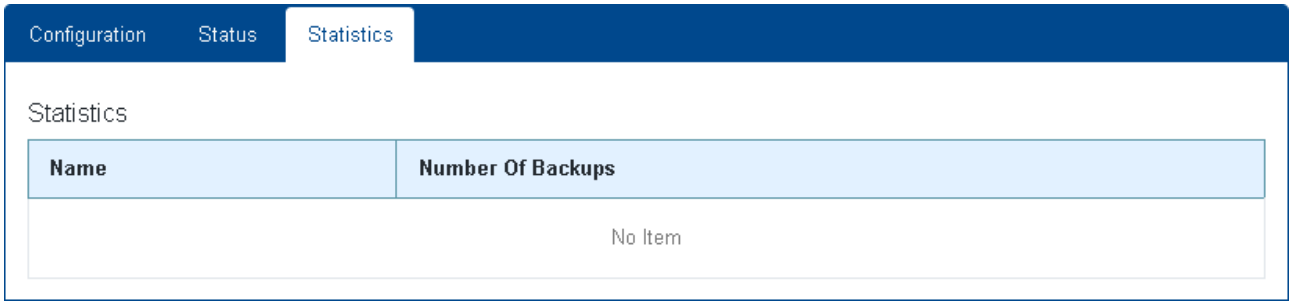


Fig. 101: Redundant - MS Ring - Statistics

This tab shows a tabular overview of the statistics of all available MS rings.

5.12 Events

5.12.1 Actions - Configuration

Fig. 102: Events - Actions - Configuration

This tab offers to assign severity levels to actions. The different severity levels are:

- Disabled: Syslog output to this target is disabled.
- Debug: Internal system debugging information.
- Info: Information without important consquences.
- Notice: Notification about normal occurence.
- Warning: Warning about a normal problem.
- Error: Unexpected error has occured.
- Critical: Critical error which compromises data traffic or stability.
- Alert: Very important error condition.
- Emergency: Highest possible error condition.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.12.2 Logs - Configuration

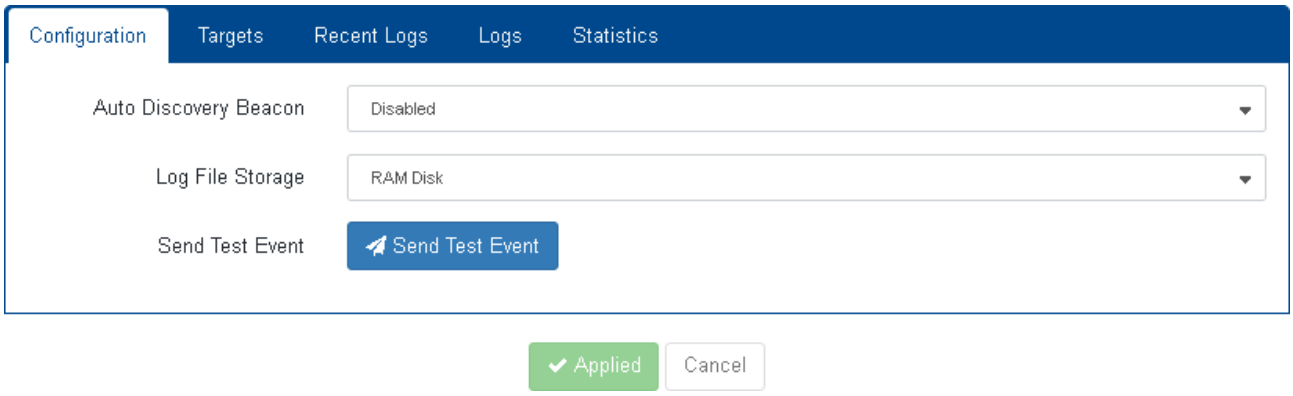


Fig. 103: Events - Logs - Configuration

This tab allows the management of event and logs.

- **Auto Discovery Beacon:** Disable or select the interval of sending discovery beacons (alive test event) to the defined target from the drop-down list.
  - Disabled
  - Every 10 seconds
  - Every minute
  - Every 5 minutes
  - Every 15 minutes
  - Every hour
- **Log File Storage:** Select, where the system should store the log files.
  - **Flash:** The log files are stored within the device's non-volatile flash memory. They are accessible via FTP and are retained even after the device is switched off.
  - **RAM Disk:** The log files are stored within the device's RAM. When the device is switched off the log files will be removed.
- **Send Test Event:** Click on this button to manually send an alive test to the defined target.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.12.3 Logs - Targets

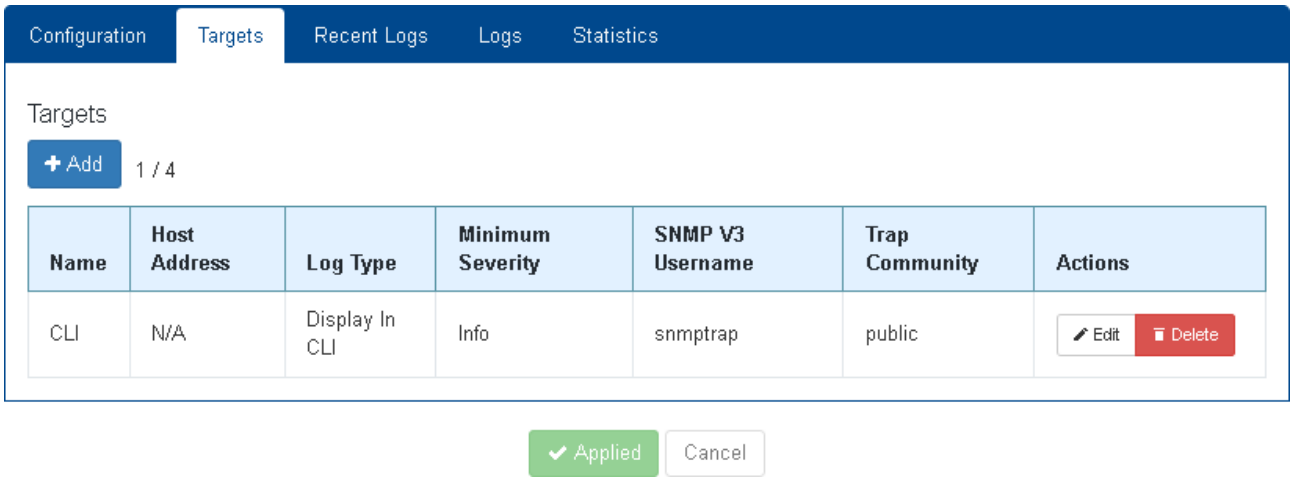


Fig. 104: Events - Logs - Targets

The tab allows the configuration of notification targets.

- **Edit:** Opens the edit dialogue of the respective target entry. Change the entries as needed.
- **Add:** Opens the dialogue for adding a new target.

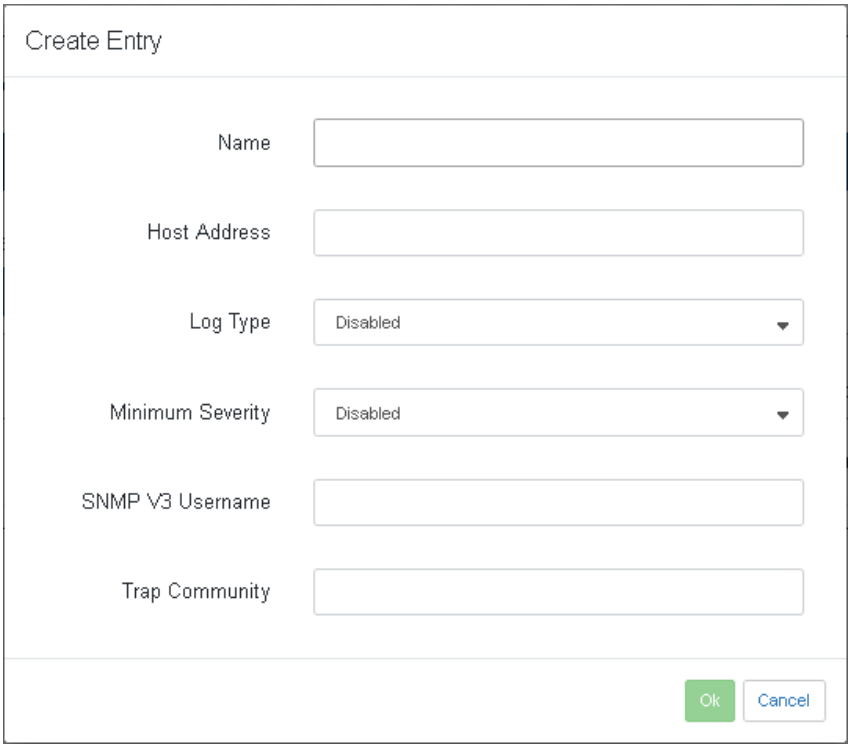


Fig. 105: Event & Log - Targets - Add Target

- **Name:** Enter a descriptive name of the target.
- **Host Address:** Enter the IP address of the target.

- **Log Type:** Select the target type from the drop-down list.
  - "disabled": Disables the target.
  - "syslog": UDP protocol, using standard port 514, complying to syslog format.
  - "SnmpTrapV1/V2c/V3": Using traps of the respective SNMP version.
  - "SnmpInformV2c/V3": Using notifications of the respective SNMP version.
  - "Display in CLI": Using CLI as target.
  - "Recent Logs": Using recent logs as target.
- **Trap Community:** When activating SNMP traps, this field appears. Enter the respective SNMP trap community string.
- **Minimum Severity:** Select the minimum event severity that is necessary for notification of the target.
- **SNMP V3 Username:** Assign the username for SNMP V3.
- **Trap Community:** Assign the trap community.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

- **Delete:** Deletes the respective entry.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.12.4 Logs - Recent Logs

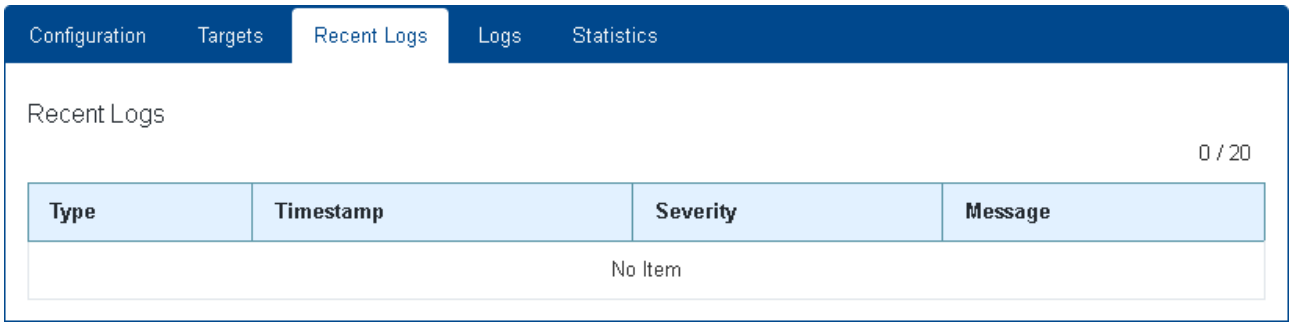


Fig. 106: Events - Logs - Recent Logs

This tab shows a tabular overview of recent events.

5.12.5 Logs - Logs

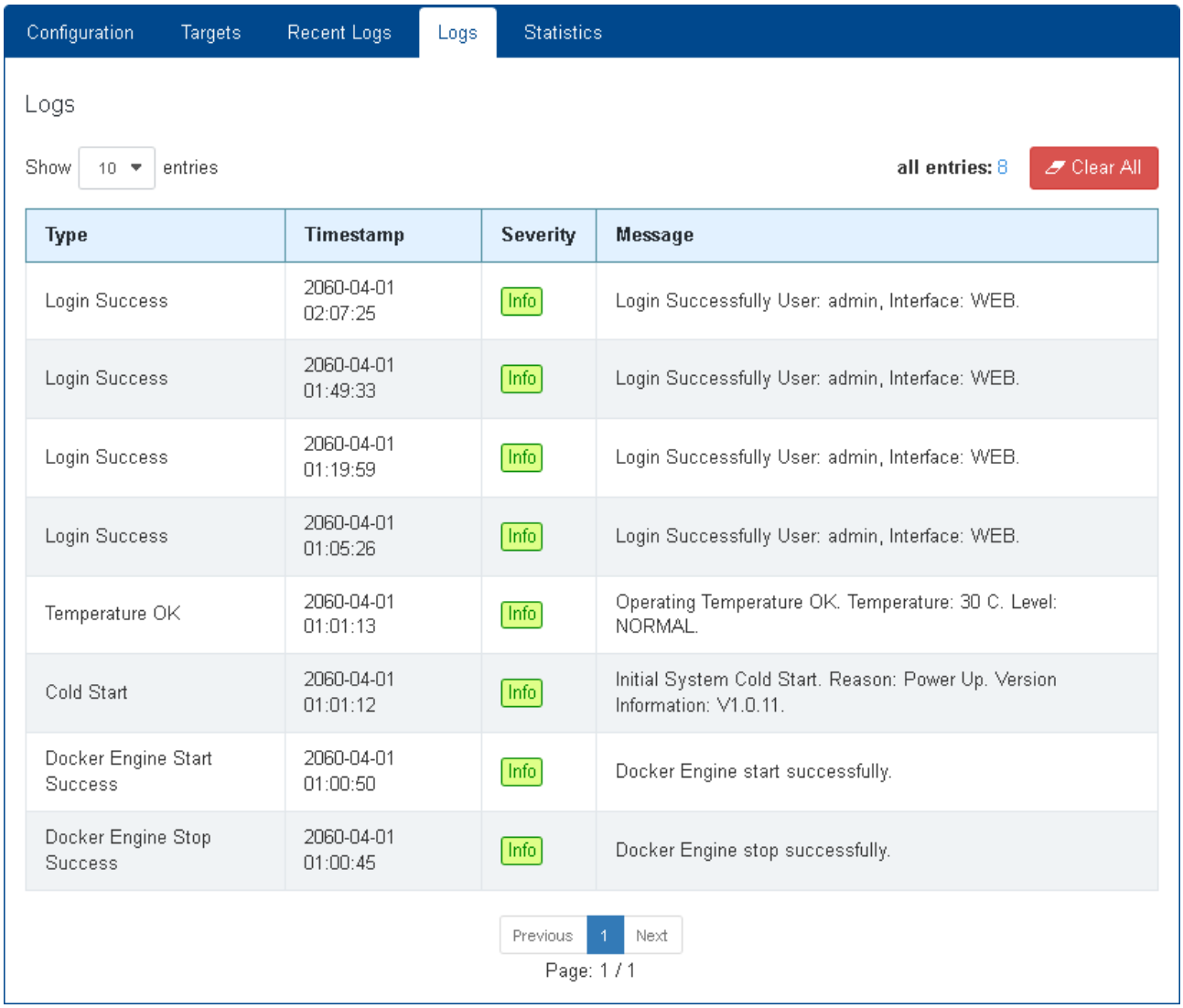


Fig. 107: Events - Logs - Logs

The tab shows a tabular overview of all events.

Note: The event list is stored in the volatile RAM. On system restart/reset all entries will be deleted.

- **Show xx entries:** Select the number of entries shown in the table.
- **Clear All:** Deletes all entries.
- **Previous / <No.> / Next:** Browse forward and backward through the entry pages or select a specific page.

5.12.6 Logs - Statistics

Fig. 108: Events - Logs - Statistics

This tab shows general log file statistics.

5.13 Docker

5.13.1 Docker - Overview

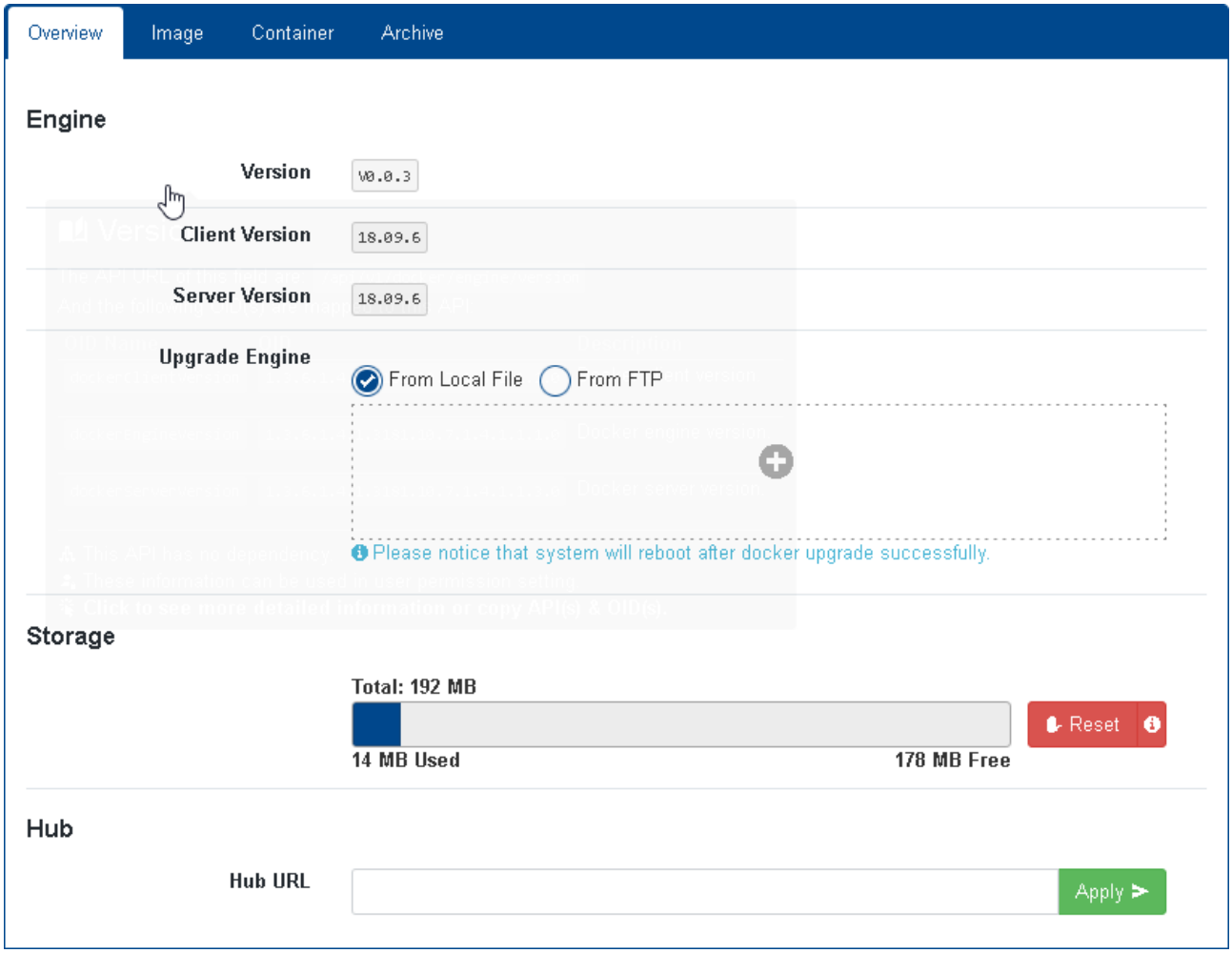


Fig. 109: Docker - Overview

This tab shows an overview of the docker statistics.

- **Engine:** Shows several version numbers of the docker engine.
- **Upgrade Engine:** Check one of the following options to assign the engine file source.
  - **From Local File:** After clicking the + icon the file manager dialogue of your web browser opens to select a local directory from where you want to load the docker engine file.
  - **From FTP:** When selecting the FTP option for import, enter the FTP address in the appearing address field and click on the button **Start**.
    The FTP address format reads as follows:

    `ftp://username:password@url/<Docker engine file>`
    (Example: `ftp://admin:adminstrator@192.168.0.101/<Docker engine file>`)

  After a docker update finished successfully, the device restarts automatically.

- **Storage:** Shows the actual memory usage of docker.
- **Hub URL:** Enter the hub URL (e.g. hub.docker.com).

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.13.2 Docker - Image

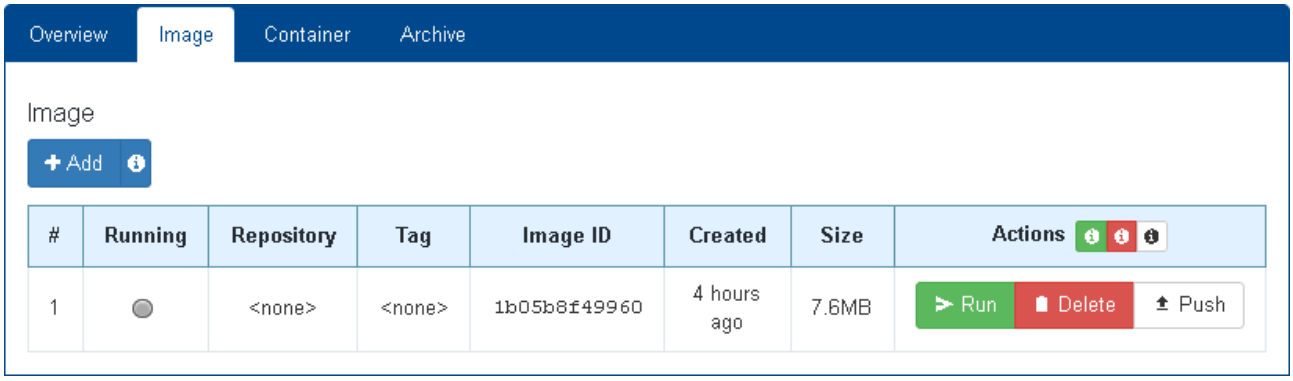


Fig. 110: Docker - Image

This tab shows a tabular overview of all executable Docker images.

Note: First you have to load the respective Docker image into the device, either by a determined Docker Hub or via loading a Docker image as local file or from an FTP server.

- **#:** Index number of the image.
- **Running:** Indicator, whether a Docker image is currently running.
  - Green: Image is active.
  - Grey: Image is not active.
- **Repository:** Shows the image's repository.
- **Tag:** Shows the tag of the image.
- **Image ID:** Shows the unique Docker image ID.
- **Created:** Shows the age of the image.
- **Size:** Shows the image's size.

- **Add:** Opens a dialogue to add a Docker image from the hub.

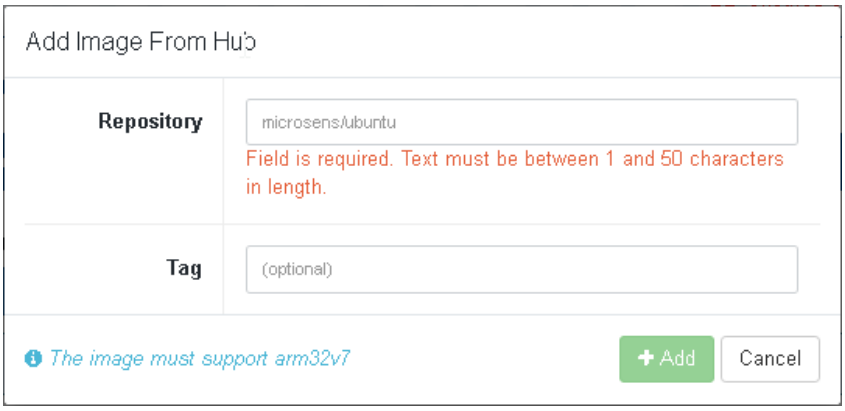


Fig. 111: Docker - Image - Add from Hub

- **Repository:** Enter a repository that is available from the assigned Docker hub URL (see page 105).
- **Tag:** Enter a tag for this image.

Click on the button **Add** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Important: The Docker image must support ARM architecture!

- **Run:** Executes the respective Docker image. To execute an image, enter the following additional information:

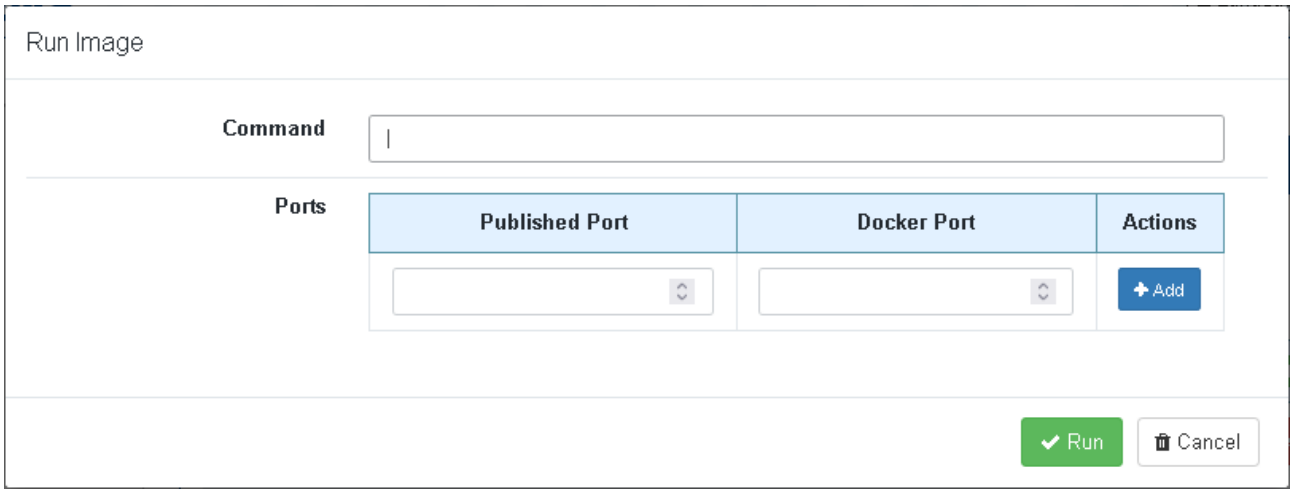


Fig. 112: Docker - Image - Run

- **Command:** Enter the Docker command.
- **Publish Port:** Set the container's publish port.
- **Docker Port:** Set the containers's Docker port.

Click on the button **Add** to assign the port settings to the Docker image.

Click on the button **Run** to execute the image. Otherwise, click on the button **Cancel** to abort.

- **Delete:** Deletes the specific Docker image.
- **Push:** Push the Docker image to the assigned Docker Hub.

5.13.3 Docker - Container

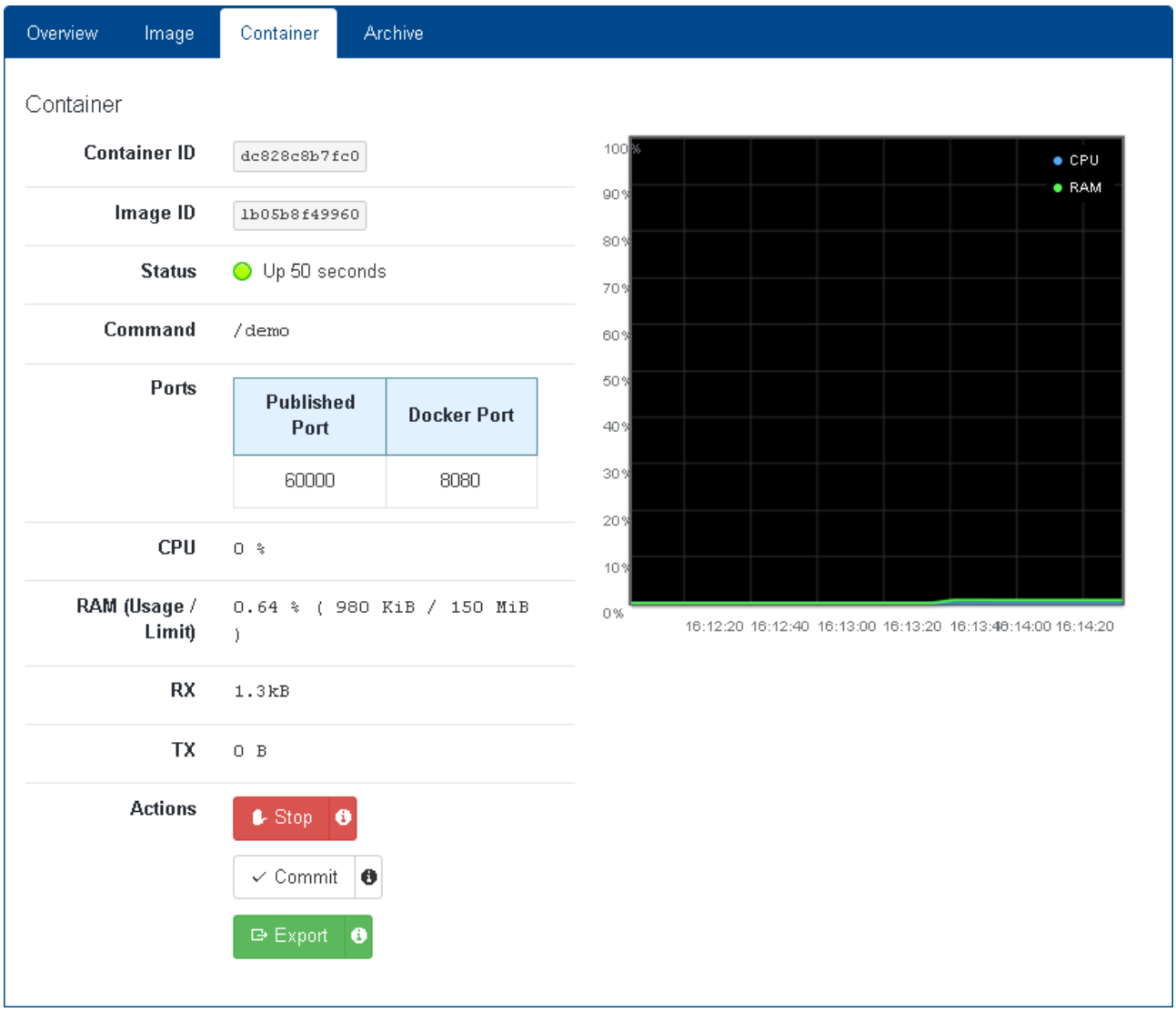


Fig. 113: Docker - Container

This tab shows the status of the last active Docker image.

- **Container ID:** Shows the unique container ID, automatically assigned by the system on image start.
- **Image ID:** Shows the unique Docker image ID.
- **Status:** Shows the operating time of the container.
- **Command:** Shows the respective Docker command.
- **Published Port:** Shows the container's published port (as assigned during container start).

- **Docker Port:** Shows the container's Docker port (as assigned during container start).
- **CPU:** Shows the current CPU load of the running container.
- **RAM (Usage/Limit):** Shows the current RAM usage and RAM limit of the running container in percentage and absolut values.
- **RX / TX:** Shows the network traffic of the running container.
- **Stop / Run:** Click on this button to stop or start the container.
- **Commit:** Click on this button to commit the container into a new image.
- **Export:** Click on this button to export the container.
- **Remove:** Click on this button to remove the container's information from this tab.

  Note: The Docker image remains in the list executable images!

5.13.4 Docker - Archive

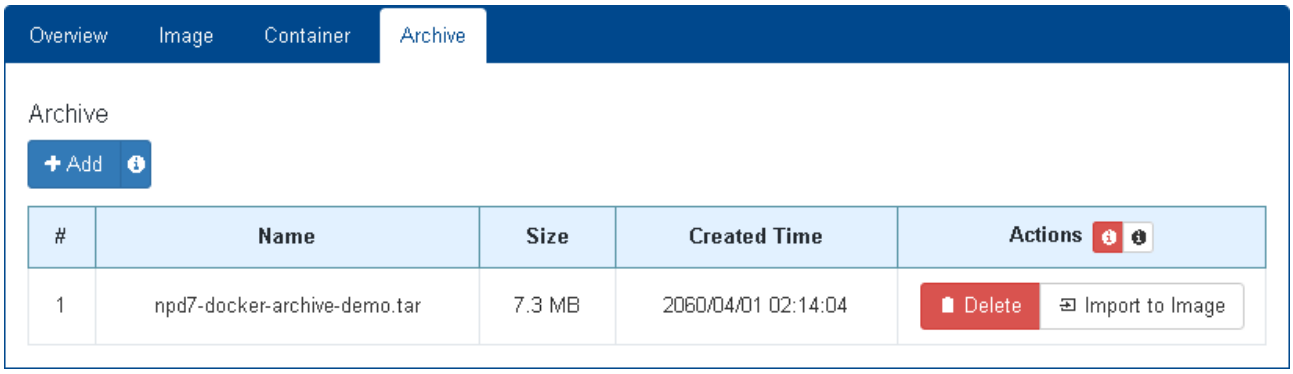


Fig. 114: Docker - Archive

This tab shows a tabular overview of available Docker images on the device.

Note: As long a Docker image is not "imported" to the image list (see page 106), it cannot be executed!

- **Add:** Opens the dialogue to load a docker image into the device.

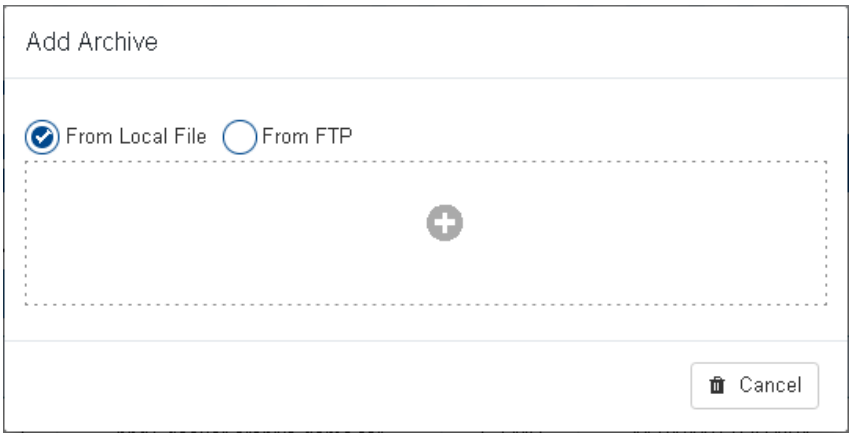


Fig. 115: Docker - Archive - Add

  - **From Local File:** After clicking the + icon the file manager dialogue of your web browser opens to select a local directory from where you want to load the Docker image file.
  - **From FTP:** When selecting the FTP option for import, enter the FTP address in the appearing address field and click on the button **Start**.
    The FTP address format reads as follows:

    `ftp://username:password@url/<Docker image file>`
    (Example: `ftp://admin:adminstrator@192.168.0.101/docker-image.zip`)

    Note: The Docker image is a `zip` or `tar` file that does not need to be unzipped.

    Click on the button **Start** to load the Docker image into the device. Otherwise, click on the button **Cancel** to abort.

    After successfully loading the Docker image into the device, it is listed in the tabular overview.

    Note: The Docker image is not ready for execution yet! Before you can run the Docker image you have to import it.
- **Import to Image:** Click on this button to import the respective Docker image into the list of executable images.

  The image is listed in the tabular overview of executable images (see page 106).
- **Delete:** Delete the respective image.

5.14 Access

5.14.1 Authentication - Configuration

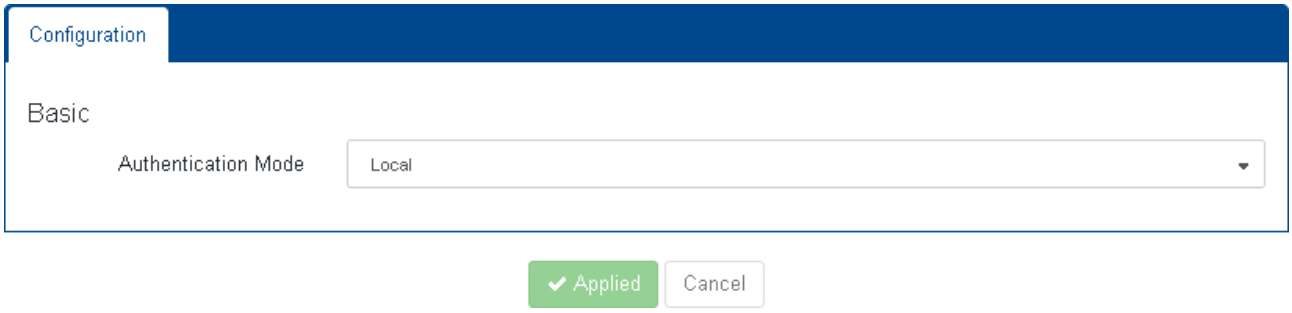


Fig. 116: Access - Authentication - Configuration

User management happens either via the device's local user database or an external server (RADIUS or TACACS+).

- **Authentication Mode:** Select the authentication mode from the drip-down list:
  - "Local": User's credentials have to be stored in the local database. If not found, the user gets no access.
  - "Local then RADIUS": If the user's credentials are not found in the local database, the device requests data from the RADIUS server. If the user is unknown to the RADIUS server, he gets no access.
  - "Local then TACACS+": If the user's credentials are not found in the local database, the device requests data from the TACACS+ server. If the user is unknown to the TACACS+ server, he gets no access.
  - "RADIUS then Local": The device requests data from the RADIUS server. If the user is unknown to the RADIUS server, the device searches the local database. If not found, the user gets no access.
  - "RADIUS": User's credentials have to be stored in the RADIUS server's database. If not found, the user gets no access.
  - "TACAS+ then Local": The device requests data from the TACACS+ server. If the user is unknown to the TACACS+ server, the device searches the local database. If not found, the user gets no access.
  - "TACACS+": User's credentials have to be stored in the TACACS+ server's database. If not found, the user gets no access.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.14.2 Authentication Servers - Configuration

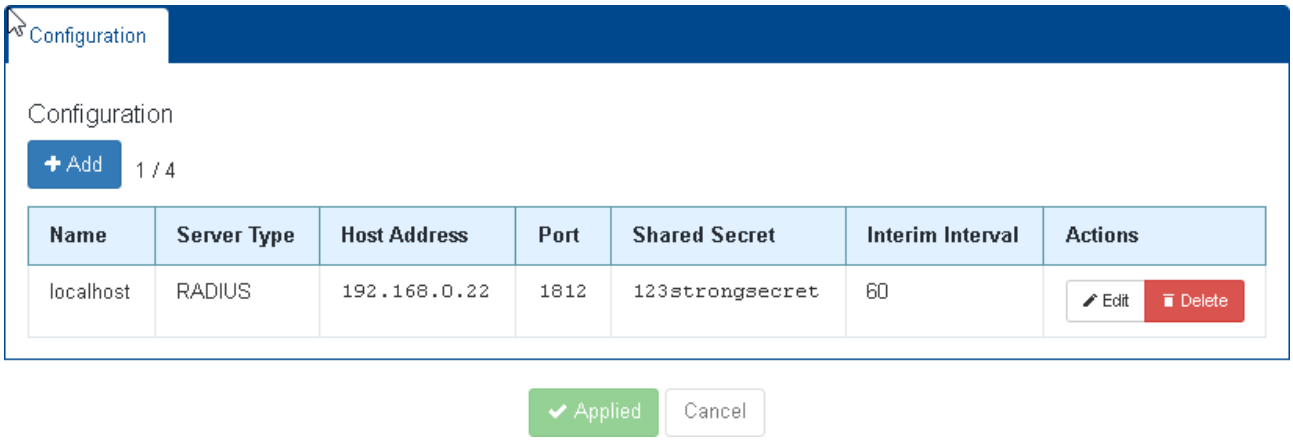


Fig. 117: Access - Authentication Servers - Configuration

This tab shows a tabular overview of currently exisiting authentication server entries.

- **Edit:** Opens the edit dialogue of the respective target entry. Change the entries as needed.

  Note: Make sure these changes fit the respective server settings!

- **Add:** Opens the dialogue for adding a new target.

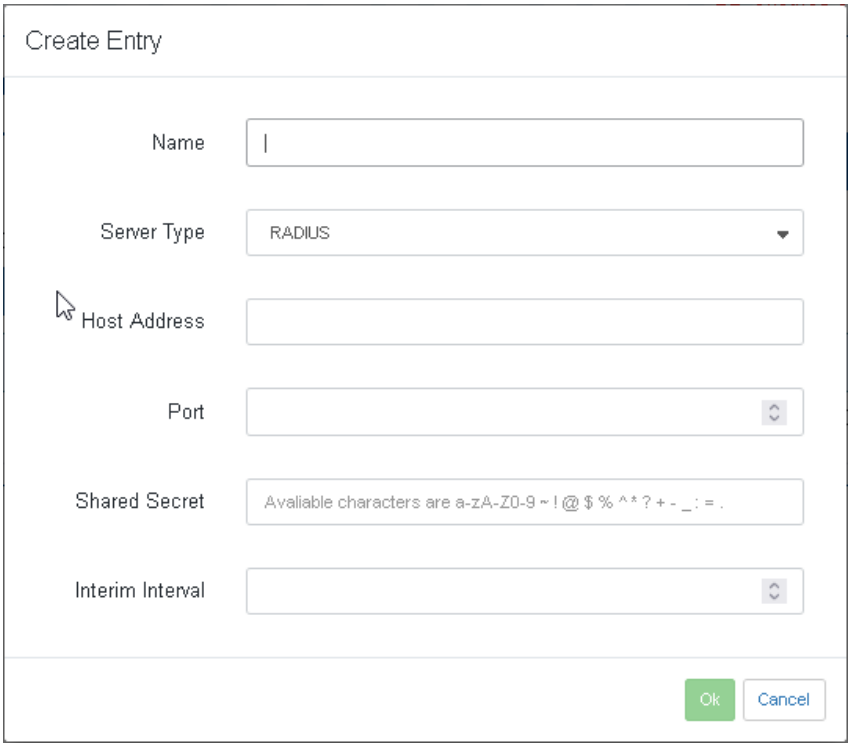


Fig. 118: Access - Authentication Servers - Configuration - Add

- **Name:** Enter a descriptive name of the server.
- **Server Type:** Select a server type (RADIUS, TACACS+) from the drop-down list

- **Auth Host Address:** Enter the authentication server's IP address.
- **Auth Port:** Enter the port number (default: 1812).

  Note: Unless necessary, leave the default setting as is.
- **Auth Shared Secret:** Enter the password for authentication with the authentication server.

  Available characters are: `a-z, 0-9, ~!@$%^*+-_?:=.`
- **Interim Interval:** Set the interval in seconds between accounting updates.

  Note: Set to "0" to disable updates.

Note: It is recommended to use at least two authentication servers for fallback issues.

- **Delete:** Deletes the respective entry.

  Note: It is not allowed to delete a RADIUS server that is determined as primary or fallback server!

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.14.3 User Permission - User

There are two predefined user accounts (see section 3.2 on page 9).

Note: Only users with administrator access rights can manage user accounts.

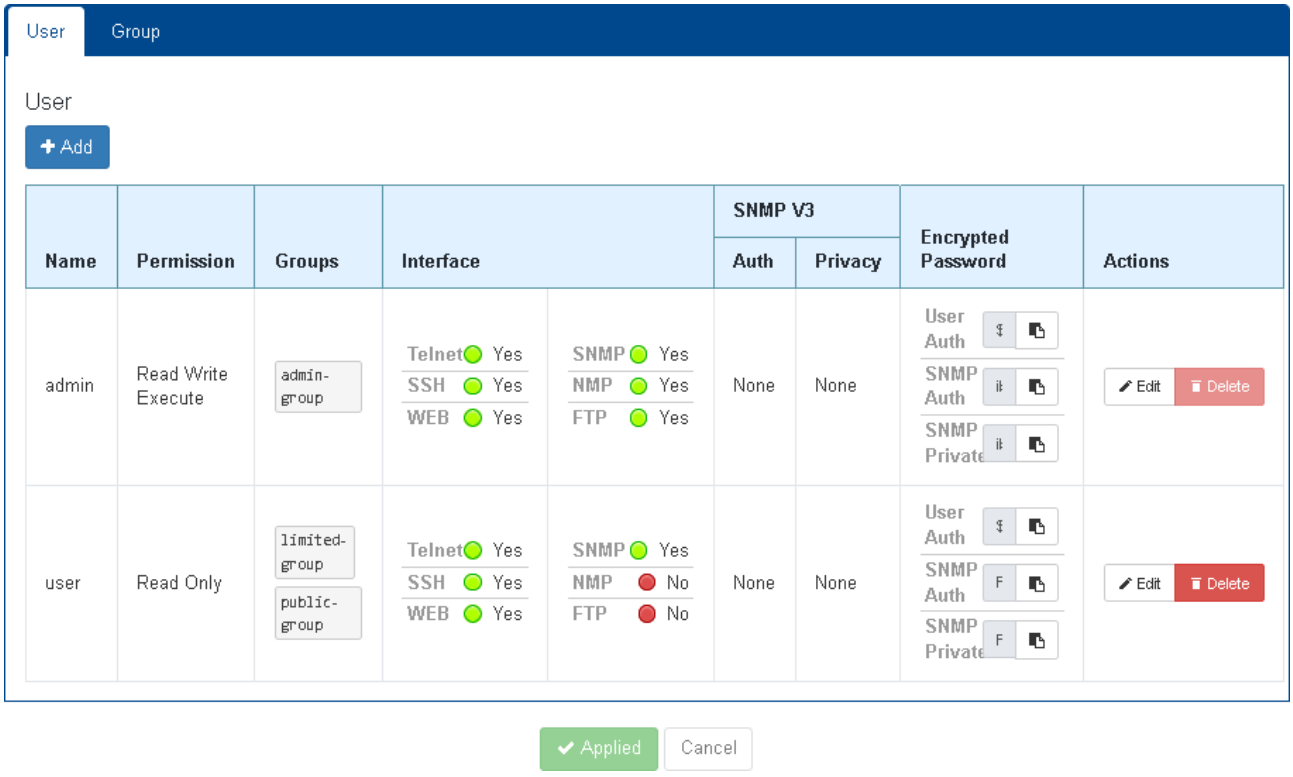


Fig. 119: Access - User Permission - User

Note: It is strongly recommended to assign different passwords at least for users "admin" and "user" after first login to prevent unauthorized access to the device!

This tab shows a tabular overview of all registered users.

- **Edit:** Opens the edit dialogue of the respective user entry. Change the entries as needed.
- **Add:** Opens the dialogue for adding a new user.

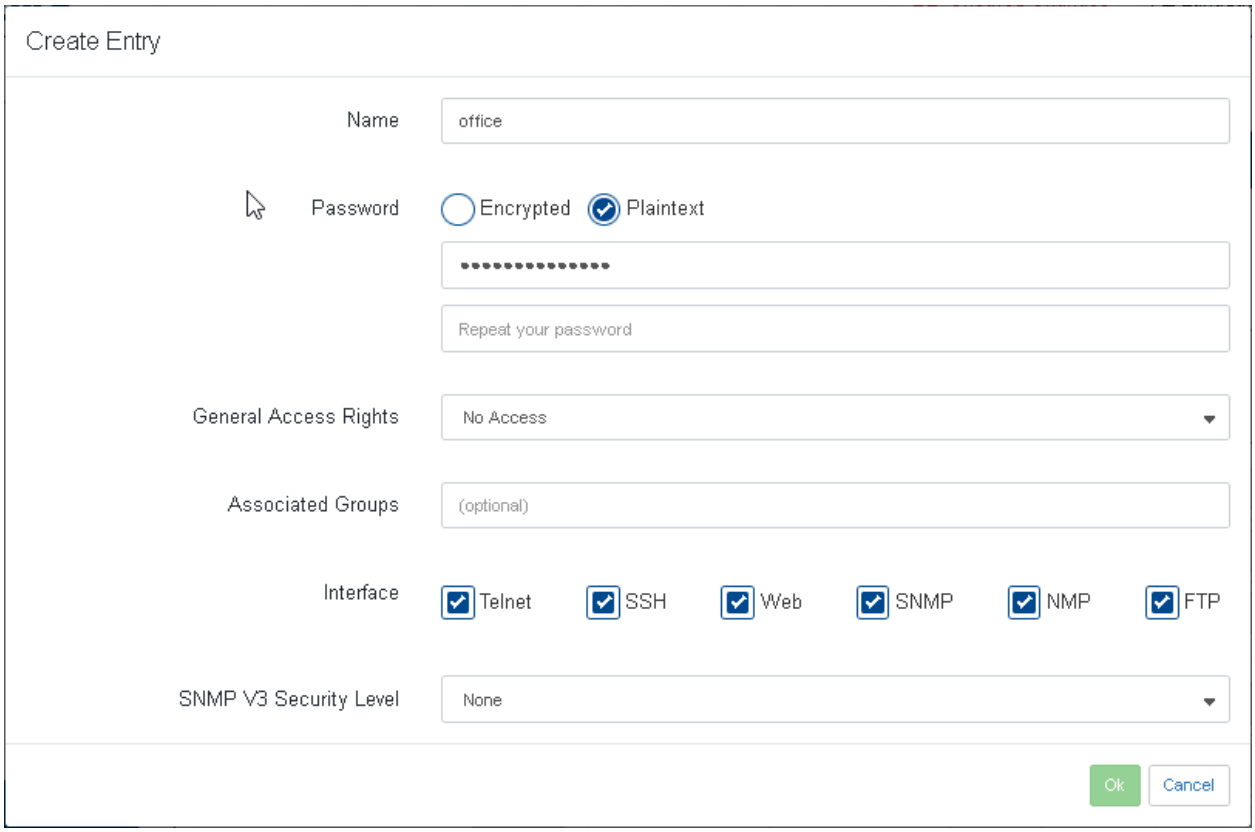


Fig. 120: Access - User Permission - User - Add

- **User Name:** Enter a unique and descriptive user name.
- **Password:** Enter a secure password. Select, wh
- **General Access Rights:** From the drop-down list, select the access rights for this user (No Access, Execute Only, Read Only, Read Write, Read Execute, Read Write Execute).
- **Associated Groups:** Enter the group name the user should be associated to.

  Note: It is possible to enter multiple groups, separated by comma.
- **Interface:** Select the access methods available for this user (Telnet, SSH, Web, SNMP, NMP, FTP).
- **SNMPv3 Security Level:** Select one of the following entries from the drop-down list (None, OnlyAuth, Auth & Privacy)

  Note: With security level "none" selected, the user account does not support SNMPv3.

- **Delete:** Delete the respective user.

  Note: At least one user with administrator access rights must exist. It is not possible to delete the only administrator account. The respective button is disabled.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.14.4 User Permission - Group

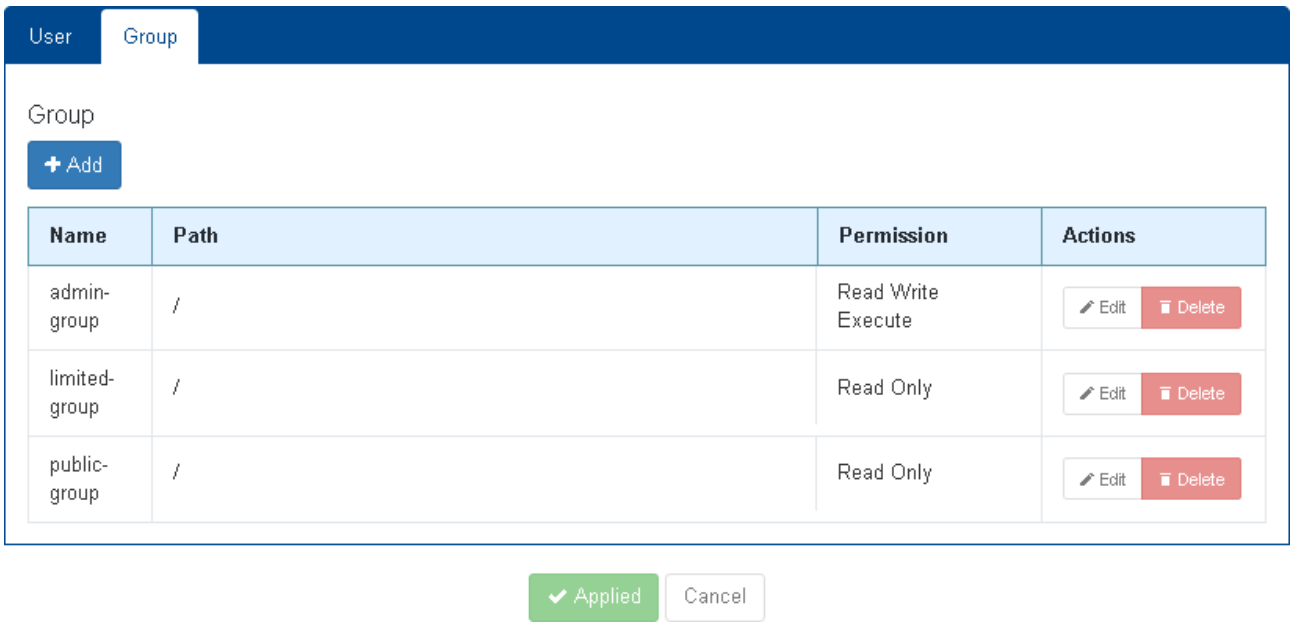


Fig. 121: Access - User Permission - Group

This tab offers to manage user groups. There are three predefined user groups.

- **Edit:** Opens the edit dialogue of the respective group entry. Change the entries as needed.

- **Add:** Opens the dialogue for adding a new user.

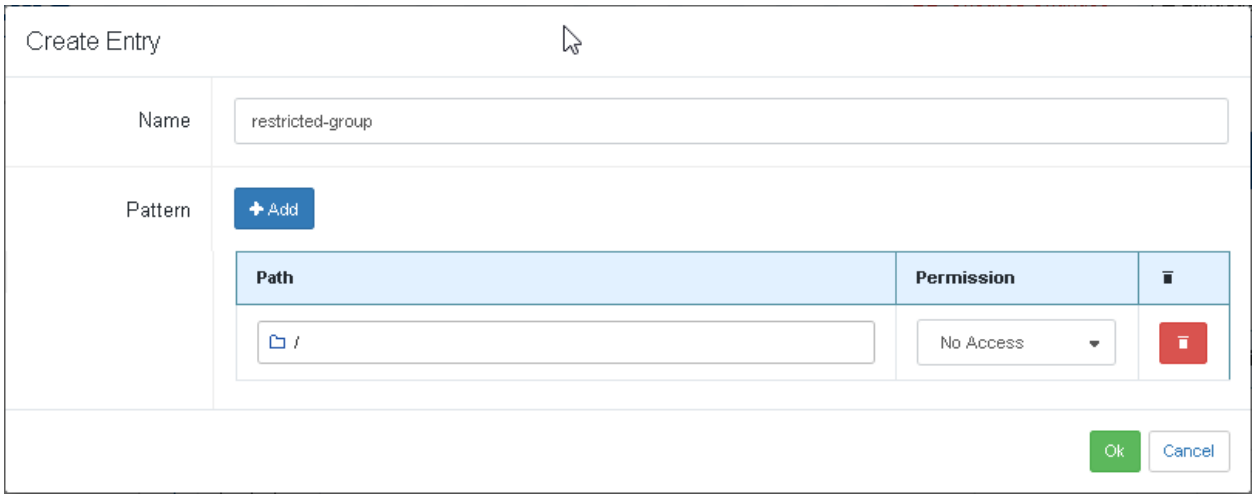


Fig. 122: Access - User Permission - Group - Add

- **Name:** Enter a unique and descriptive group name.
- **Add:** Click on this button to add a parh and a specific permission to access this path for group members.

  It is possible to add multiple paths with different access rights.
- **Path:** Select a specific path from the drop-down list.
- **Permission:** Select the respective access right from the drop-down list for the selected path.
- **Delete:** Click on this button to delete the specific entry.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.14.5 Restriction - Configuration

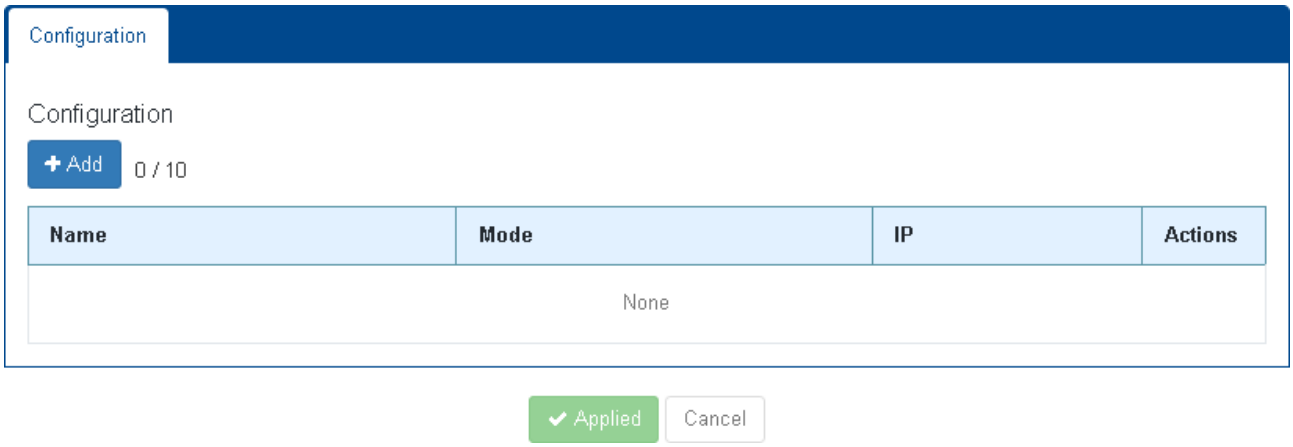


Fig. 123: Access - Restriction - Configuration

This tab offers the configuration of restriction settings to grant or reject user logins by means of their respective IP address.

- **Add:** Opens the dialogue for adding a new address entry.

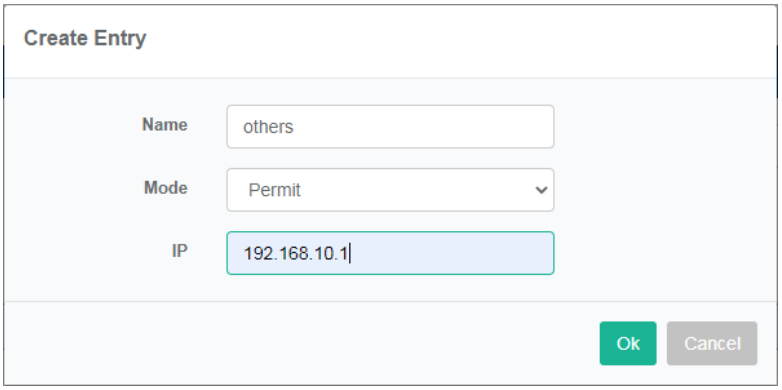


Fig. 124: Access - Restriction - Configuration - Add Entry

- **Name:** Enter a descriptive name for this entry.
- **Mode:** Select the mode (Permit, Deny, Unused) from the drop-down list.
- **IP:** Enter the IP address.

  Click on the button **OK** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.14.6 Status - Status

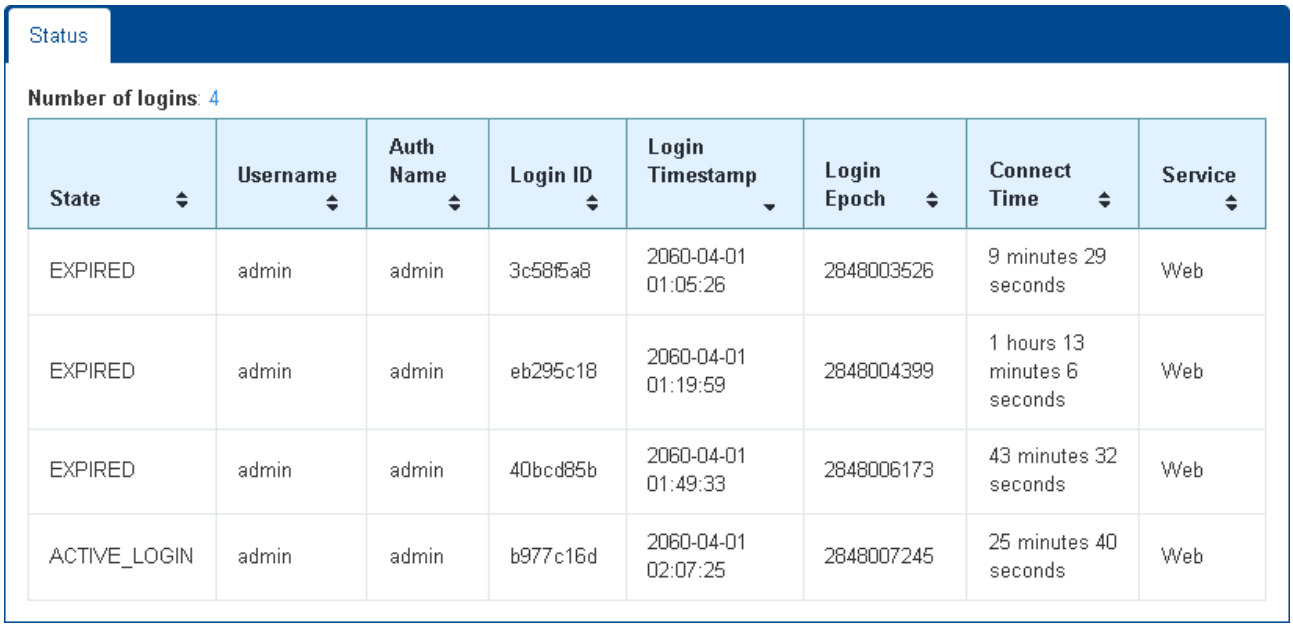


Fig. 125: Access - Status - Status

This tab offers a tabular overview of active and recent user logins.

5.15 File

5.15.1 Server - Configuration

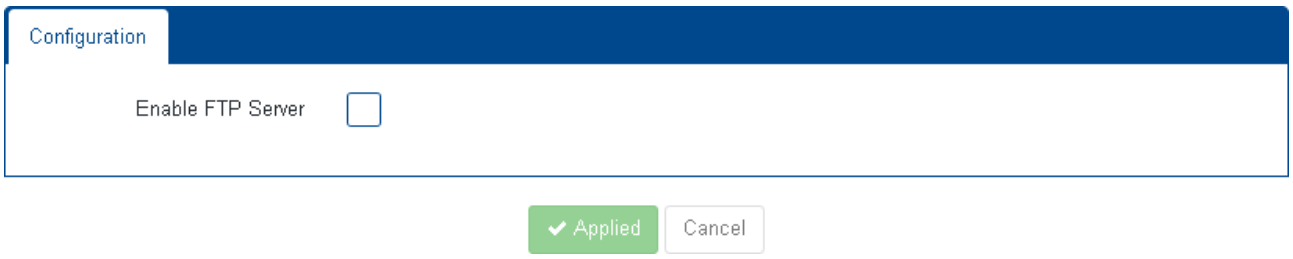


Fig. 126: File - Server - Configuration

- **Enable FTP Server:** Check or uncheck this option to enable or disable the internal FTP server of the device.

  With FTP server enabled, users can use an FTP client to login to the switch and e.g. transfer firmware images or configuration script files to the device.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.15.2 Certificate - Configuration

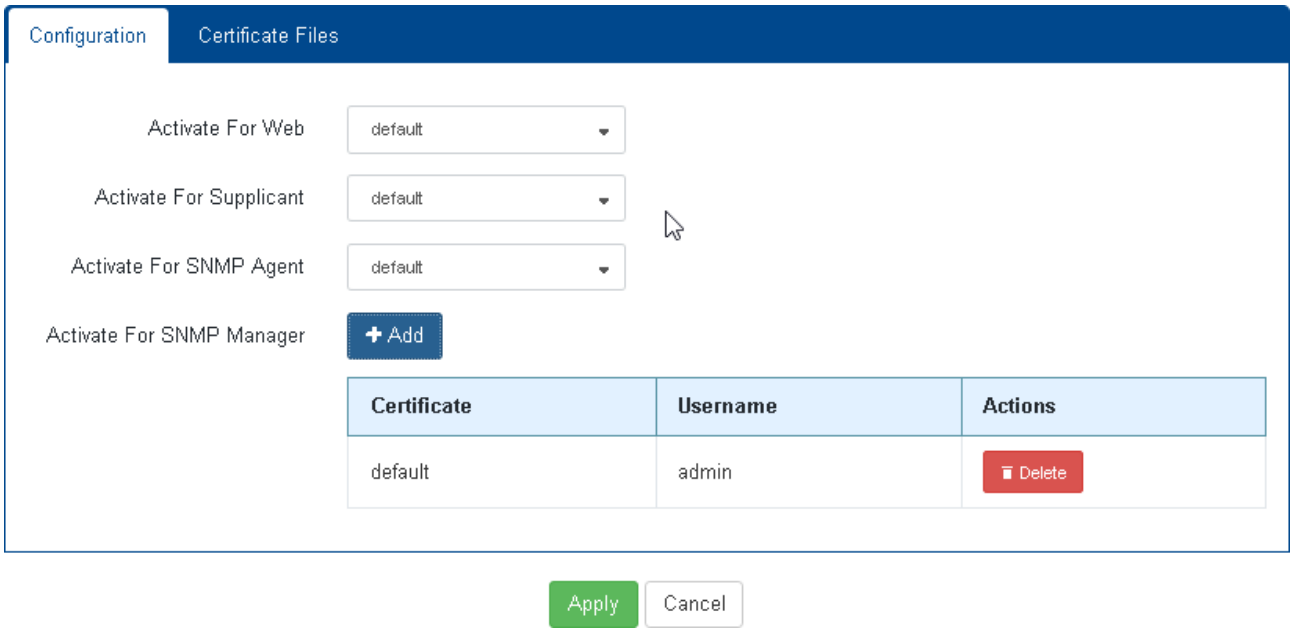


Fig. 127: File - Certificate - Configuration

This tab offers to select the existing certification files for their particular uses.

- **Activate For Web:** Select a certificate file from the drop-down list that applies for web access to the device.
- **Activate For Supplicant:** Select a certificate file from the drop-down list that applies for supplicant use.

  Note: Certificate files for supplicants are neccessary only when they use TLS authentication.
- **Activate For SNMP Agent:** Select a certificate file from the drop-down list that applies for the SNMP agent.
- **Activate For SNMP Manager:** The tabular overview shows already assigned certificates.

  To assign additional certificates, click on the button **+Add** and select a certificate and a registered user name.

  To delete an entry, click on the button **Delete**.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.15.3 Certificate - Certificate Files

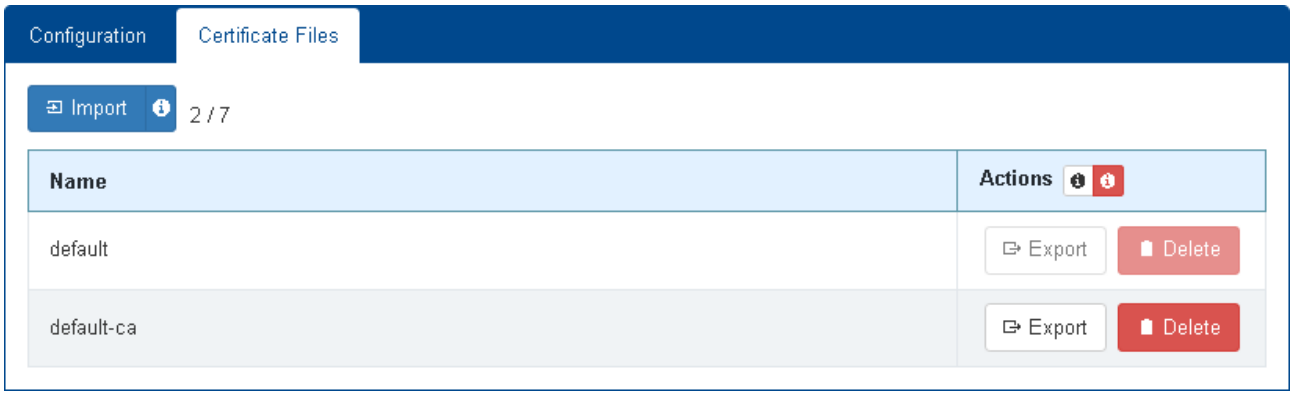


Fig. 128: File - Certificate - Certificate Files

This tab shows a tabular overview of all available certificate files.

- **Export:** Click this button to export the respective certificate file either as local file or as upload file for an FTP server.
- **Delete:** Click on this button to delete the respective certificate file.
- **Import:** Click on this button to import a new certificate file.

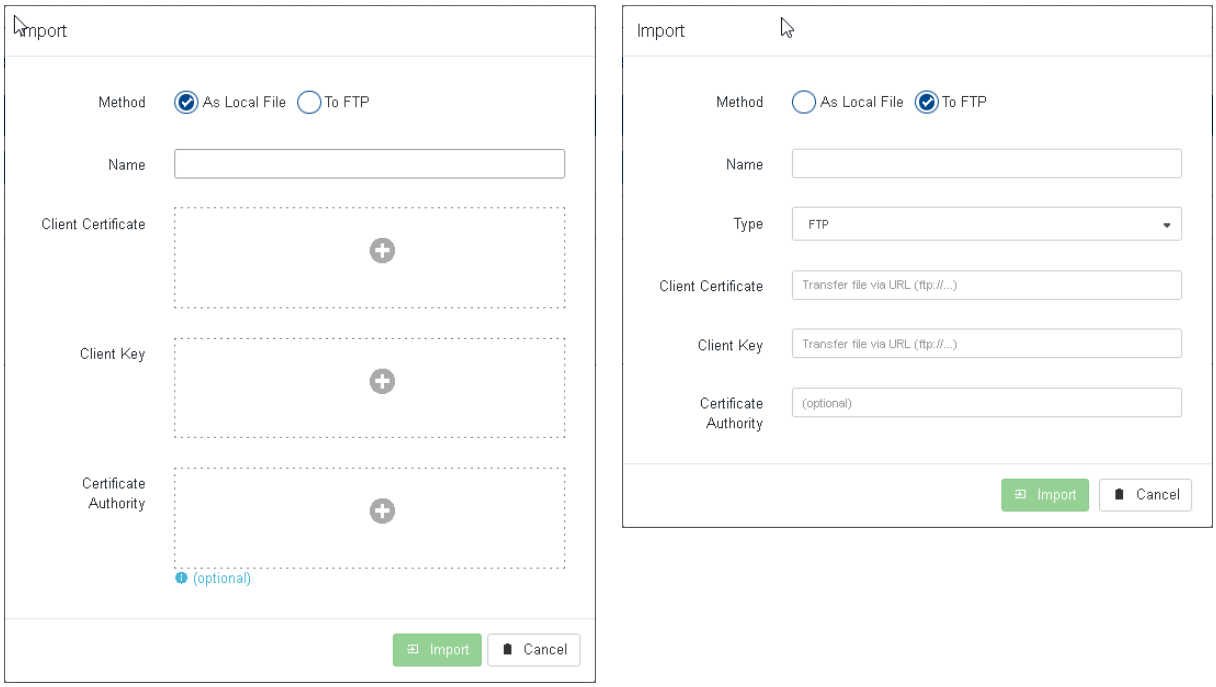


Fig. 129: File - Certificate - Certificate Files (Local File/FTP)

- **Method:** Select whether to use a local certificate file or to download a certificate file from a server.
- **Name:** Enter a descriptive name for the certificate.

- **Type:** When selecting the FTP option for import, select the server type from the drop-down list ("FTP", "FTPS", "SFTP").
- **Client Certificate:** Name of the client certificate file (mandatory).
- **Client Key:** Name of the client key file(mandatory)
- **Certificate Authority:** name of the certificate authority file (optional).

With local file selected, click on the **+** icon of the respective file area to open the file manager of your operation system and select the respective file.

With FTP selected, enter the server address, the login credentials and the respective file name.

Click on the button **Import** to start the file upload or **Cancel** to discard the changes.

5.16 User Interfaces

5.16.1 CLI - Configuration

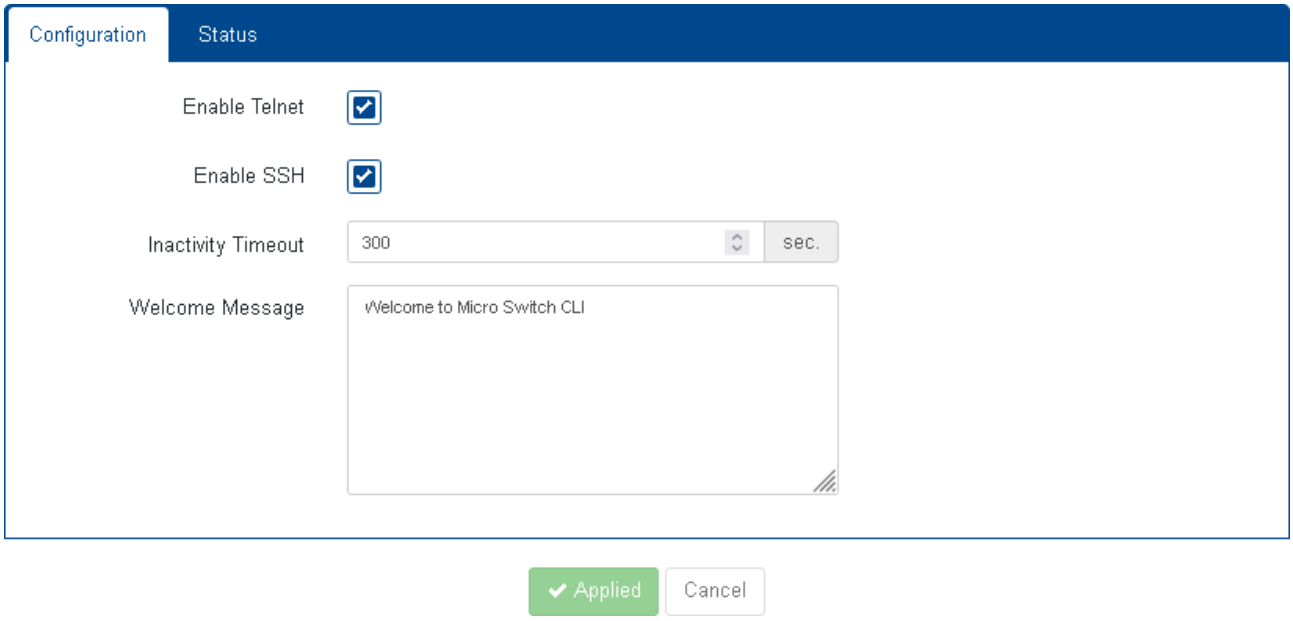


Fig. 130: User Interfaces - CLI - Configuration

- **Enable Telnet:** Enable or disable Telnet access for all users.
- **Enable SSH:** Enable or disable SSH acces for all users.

  Note: If both Telnet and SSH access are disabled, it's only possible to access the switch via web GUI.
- **Inactivity Timeout:** Set the idle time (no session activity) in seconds, before the users are logged out by the system.
- **Welcome Message:** Enter the message the device will show the users after successfully logged in via Telnet or SSH.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.16.2 CLI - Status

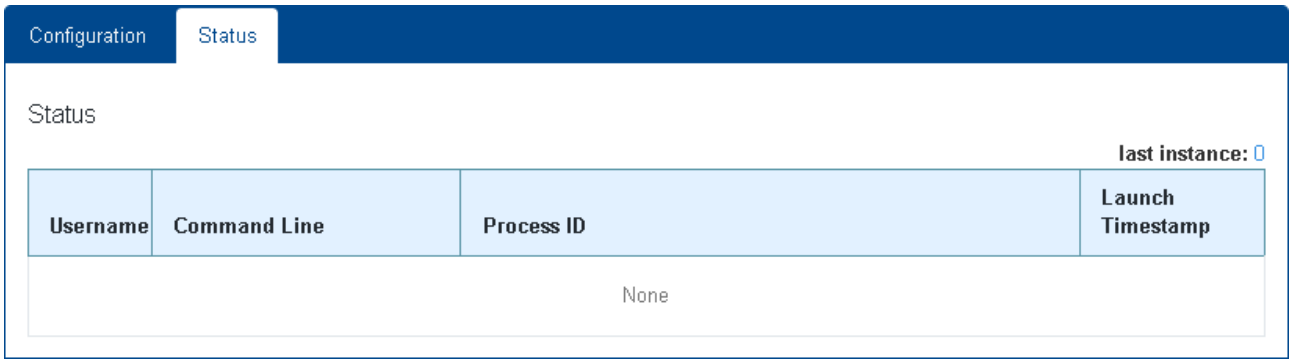


Fig. 131: User Interfaces - CLI - Status

This tab offers a tabular overview of all users recently and currently logged in.

5.16.3 Web - Configuration

Note:
Changes only become active after restarting the web server or the whole device.

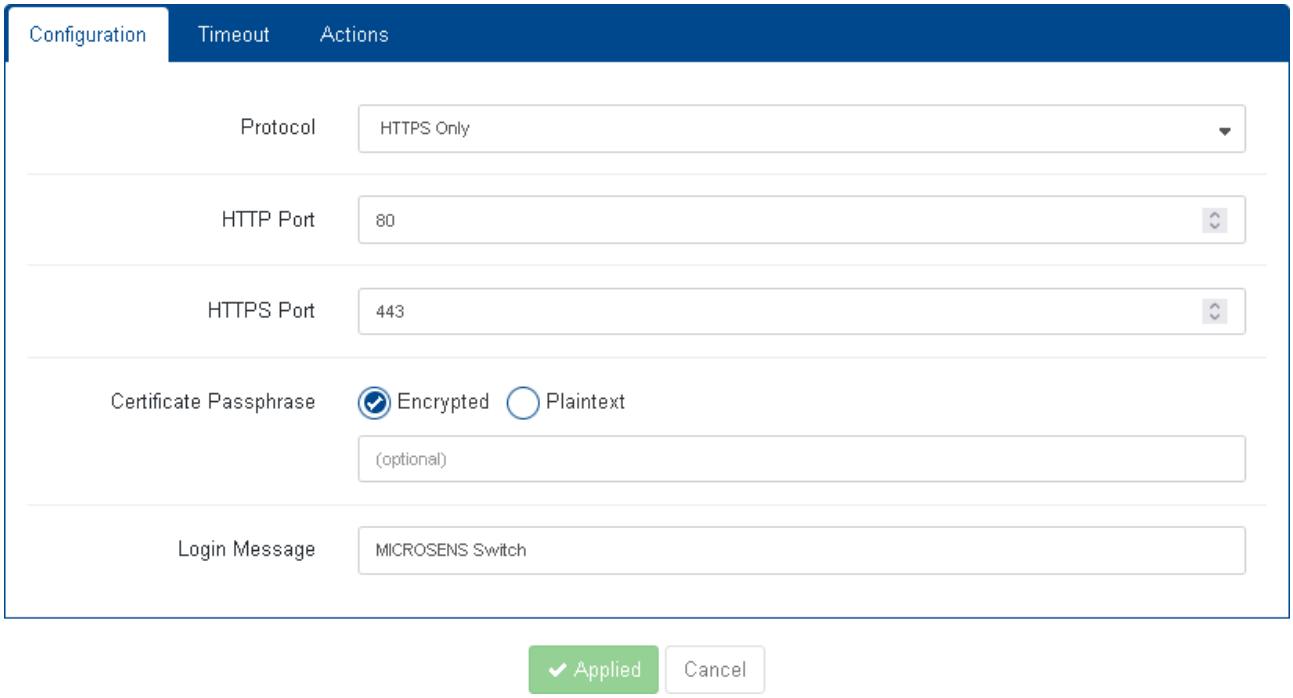


Fig. 132: User Interfaces - Web - Configuration

- **Protocol:** Select the transfer protocol from the drop-down list:
  - **Disabled:** No web access is allowed. Access is only possible via SSH and or Telnet.
  - **HTTP Only:** Web access is only allowed via unsecure HTTP.

    Note:
    This is strongly not recommended for security reasons!

- **HTTPS Only:** Web access is only allowed via secure HTTPS. Access via HTTP is not possible.
- **HTTP & HTTPS:** Both transfer protocols HTTP and HTTPS are allowed.

Note: For security reasons it is strongly recommended to use **HTTPS only**!

- **HTTP Port:** Enter the HTTP port (default: 80).
- **HTTPS Port:** Enter the HTTPS port (default: 443).

  Note: Unless it is strictly necessary, leave the default port settings as is.
- **Certificate Passphrase:** Select whether the certificate passphrase is encrypted or in plain text.
- **Login Message:** This message is displayed during login to the management web server.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.16.4 Web - Timeout

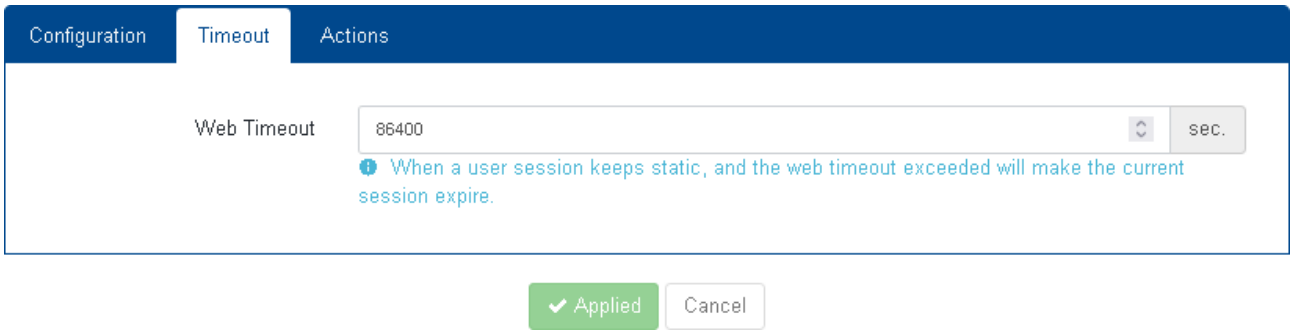


Fig. 133: User Interfaces - Web - Timeout

- **Web Timeout:** Set the idle time (no session activity) in seconds, before the users are logged out by the system.

  Note: The value "0" will prevent users from being disconnected automatically from the system after a period of inactivity.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.16.5 Web - Actions

Fig. 134: User Interfaces - Web - Actions

- **Restart Web Server:** Click on the button **Restart**, to restart the web server.

  Note: The restart will log-out all users, which are currently logged-in!

5.16.6 SNMP - Configuration (Device Information)

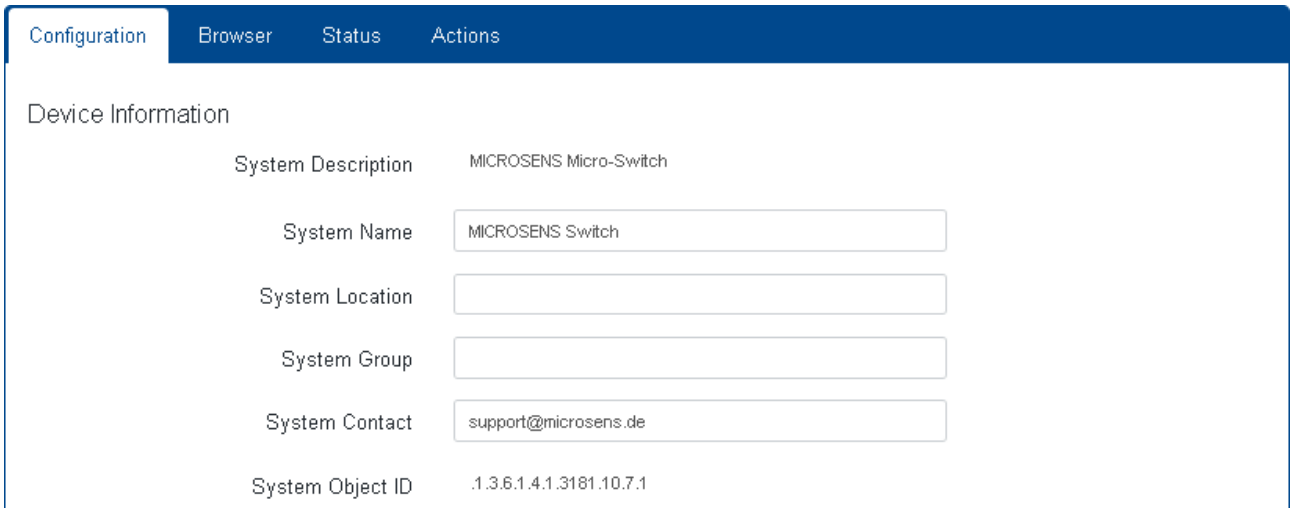


Fig. 135: User Interfaces - SNMP - Configuration (Device Information)

- **System Description:** System description used by SNMP.
- **System Name:** System name used by SNMP.
- **System Location:** System location used by SNMP.
- **System Group:** System group used by SNMP.
- **System Contact:** System contact used by SNMP.
- **System Object ID:** Response to SNMP sysObject requests.

5.16.7 SNMP - Configuration (V1/V2 Configuration)

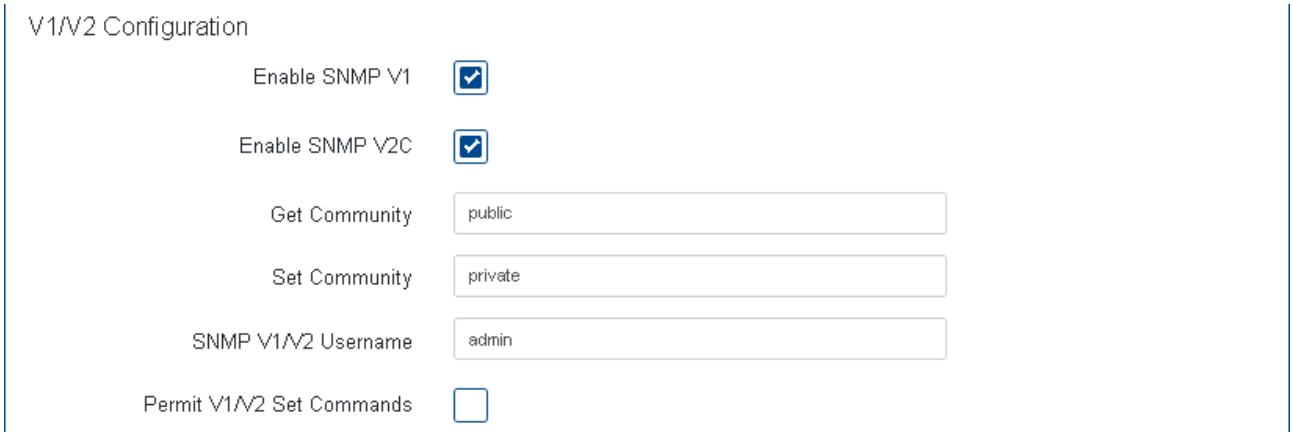


Fig. 136: User Interfaces - SNMP - Configuration (V1/V2 Configuration)

- **Enable SNMP v1:** Enable or disable SNMP v1 version. If disabled, the switch will not support SNMP v1.
- **Enable SNMP v2c:** Enable or disable SNMP v2c version. If disabled, the switch will not support SNMP v2c.
- **Get Community:** Set get community of SNMP.

- **Set Community:** Set set community of SNMP.
- **SNMP V1/V2 Username:** SNMP v1/v2 normally only provides light security by means of the community strings.

  Additional V3 like security can be applied by setting this field to any user name defined in the access section. The access restrictions defined for the selected user also apply to the SNMP V1/v2 access, when the user name is specified here.

  When no user name or an invalid user name is configured, SNMP access is blocked.
- **Permit V1/V2 Set Commands:** When disabled, SNMP sets (writes) are declined and no modifications to the system via unsecure SNMP V1/V2 can occur.

5.16.8 SNMP - Configuration (V3 Configuration)

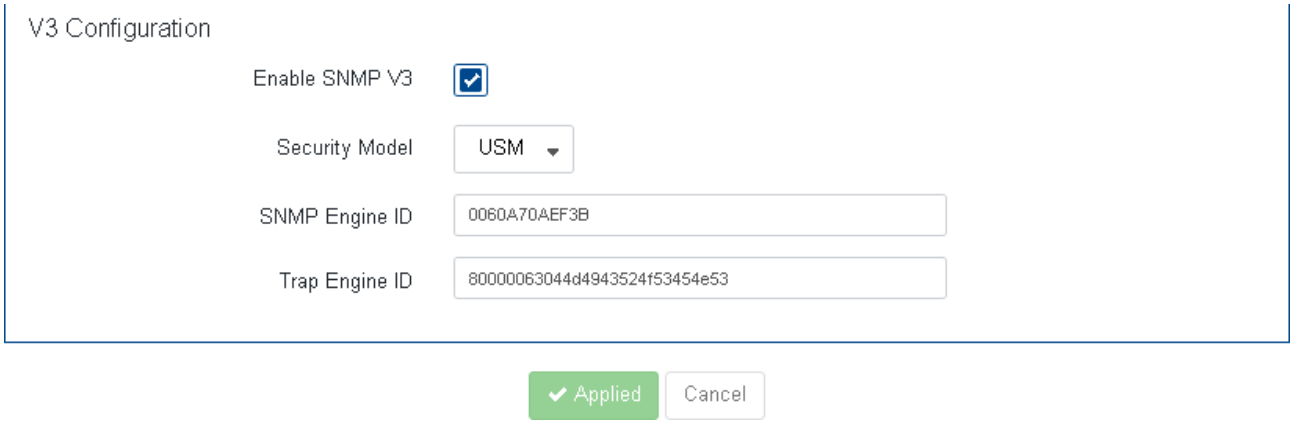


Fig. 137: User Interfaces - SNMP - Configuration (V3 Configuration)

- **Enable SNMP v3:** Enable or disable SNMP v3 version. If disabled, the switch will not support SNMP v3.
- **Security Model:** Set the security model of SNMP v3 by from the drop-down list. Use USM or VACM or TSM. Default is USM.

  Note: Current version only supports USM model.
- **SNMP Engine ID:** Display the engine ID that is created by the switch's SNMP module after first start.
- **Trap Engine ID:** This engine ID is used for outgoing SNMP v3 traps.

  The value is treated as hexadecimal characters. The associated trap receiver must match this sequence or may be setup to ignore the engine id altogether.

Click on the button **Apply** to confirm your choice. Otherwise, click on the button **Cancel** to discard the changes.

5.16.9 SNMP - Browser

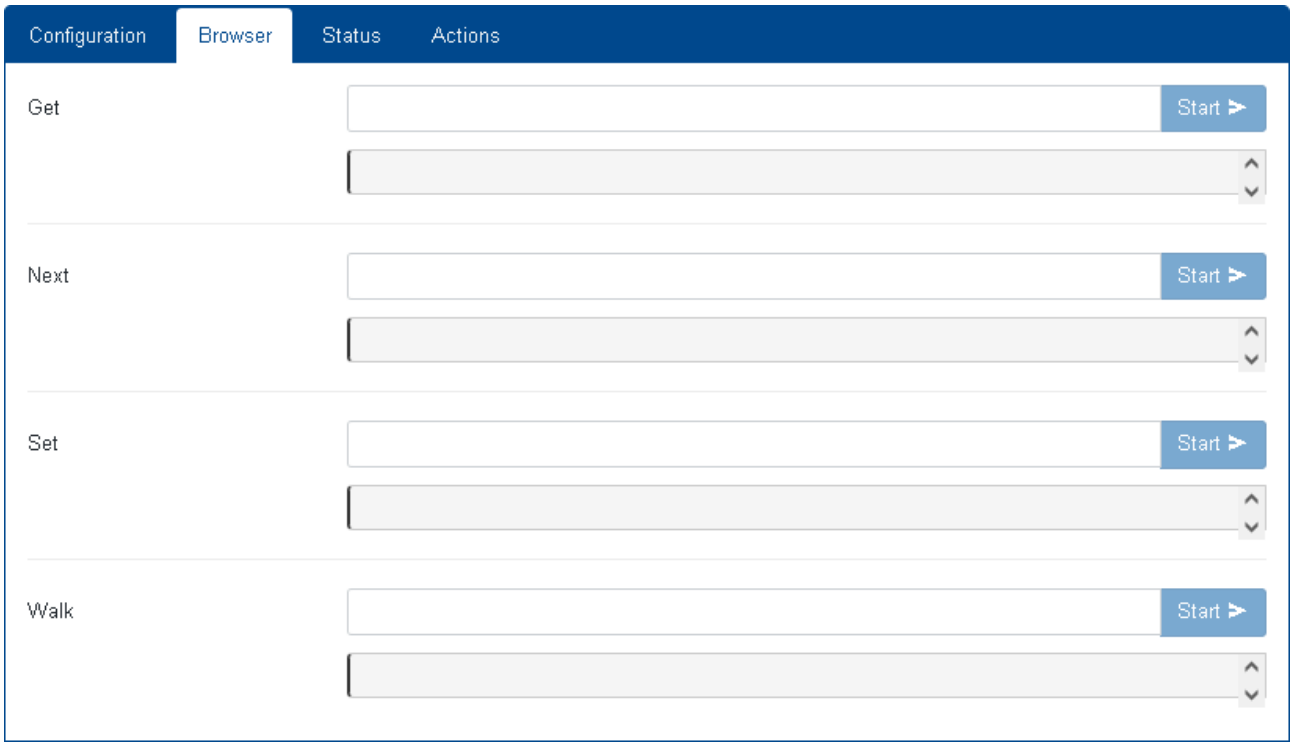


Fig. 138: User Interfaces - SNMP - Browser

This tab offers a basic SNMP browsing functionality by using the following CLI commands:

- **Get:** Corresponds to the SNMP command `snmpget`.
- **Next:** Corresponds to the SNMP command `snmpgetnext`.
- **Set:** Corresponds to the SNMP command `snmpset`.
- **Walk:** Corresponds to the SNMP command `snmpwalk`.

Click on the respective Button **Start** to execute the SNMP command.

The status field below shows the result of the command execution.

Note:
For more information about the specific command's options and parameters enter the command `-h` in the command field to show the help text.

5.16.10 SNMP - Status

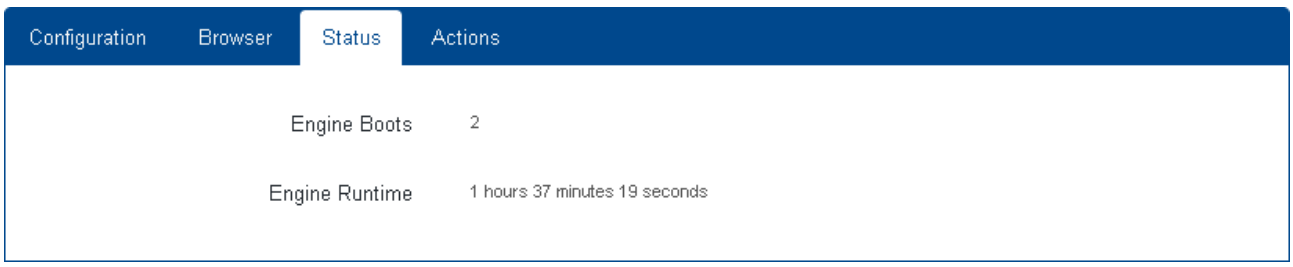


Fig. 139: User Interfaces - SNMP - Status

- **Engine Boots:** Indicates whether the device's SNMP engine is "running" or "not running".
- **Engine Runtime:** Shows the the duration since the SNMP engine was started last time.

5.16.11 SNMP - Actions

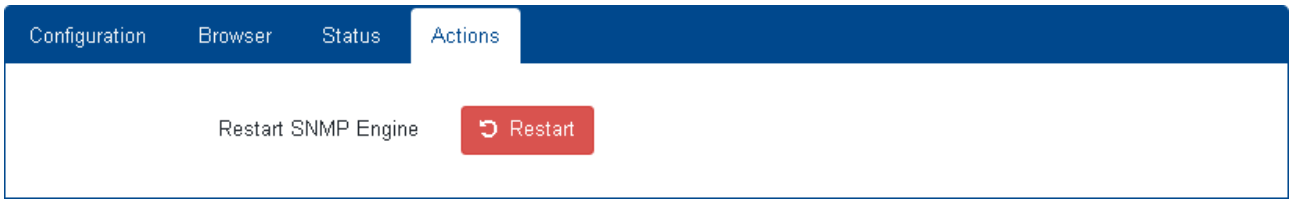


Fig. 140: User Interfaces - SNMP - Actions

- **Restart SNMP Engine:** Click on the button **Restart** to rerstart the SNMP engine.

  After restart, the SNMP engine runtime is reset.

5.17 Maintenance

5.17.1 Configuration - Save

Important: When changing the device's configuration by web GUI or CLI, the changes are stored in the volatile RAM of the device. After the device is powered off, the configuration changes are removed on next start-up, unless the changes are stored in the non-volatile Flash memory.

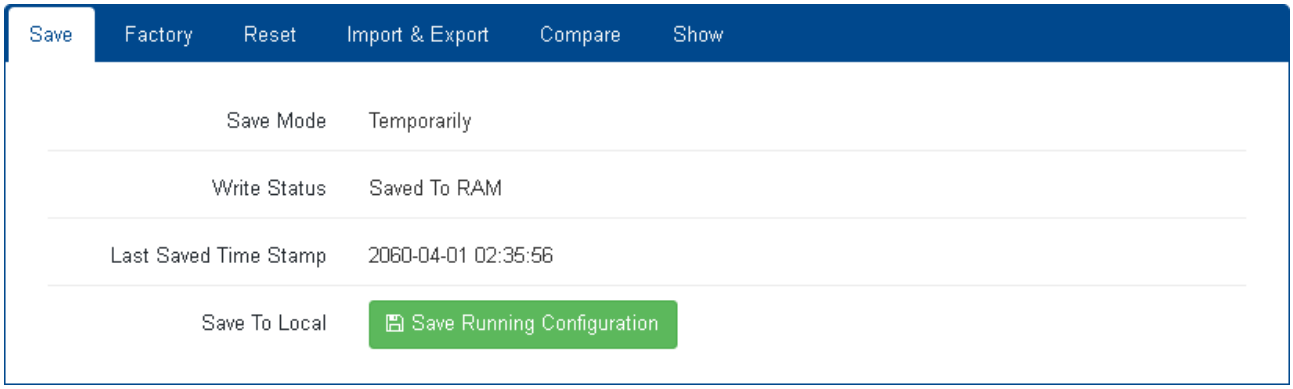


Fig. 141: Maintenance - Configuration - Save

This tab shows some statistics about the actual running configuration.

Note: If the **Safe Mode** shows "Temporarily" and the **Write Status** shows "Saved to RAM", it is strongly recommended to save the configuration, unless you want to discard the configuration changes for the next start-up.

Click on the button **Save Running Configuration** to store it to the device's Flash memory.

5.17.2 Configuration - Factory

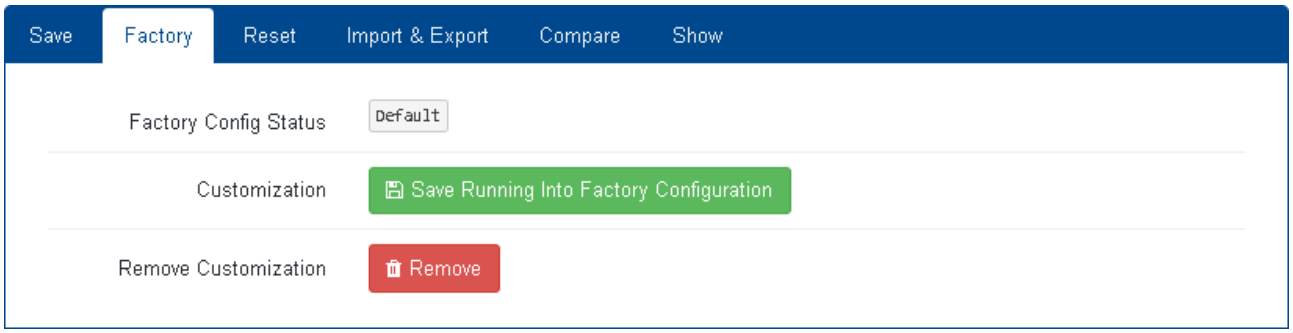


Fig. 142: Maintenance - Configuration - Factory

This tab offers to change the device's default configuration.

- **Factory Config Status:** Shows the current status of the default configuration.
- **Customization:** Click on the button **Save Running to Default Configuration** to take the running configuration as default configuration.

  From now on, when resetting the device (see section 5.17.3 on page 128) the current configuration is loaded instead of the factory configuration.
- **Remove Customization:** Click on the button **Remove** to restore the original factory configuration.

  From now on, when resetting the device the original factory configuration is loaded.

5.17.3 Configuration - Reset

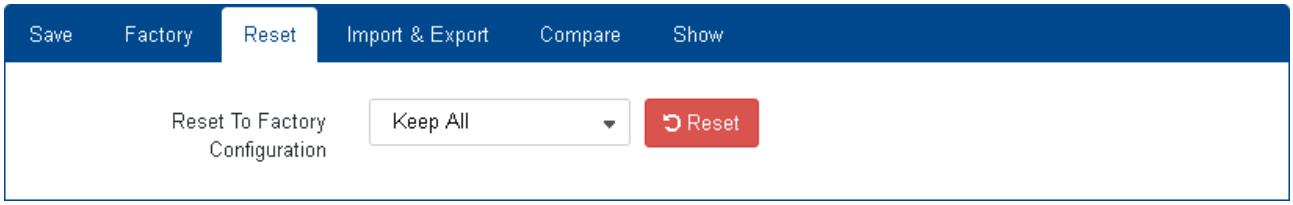


Fig. 143: Maintenance - Configuration - Reset

This tab offers to reset the device's configuration to factory default settings.

- **Reset to Factory Default:** Select the reset mode from the drop-down list.
  - **Keep All:** Reset configuration except user accounts and network settings.
  - **Keep User Accounts:** Reset configuration except user accounts. Network settings are reset to factory default!
  - **Keep Network Configs:** Reset configuration except network configuration. User accounts are reset to factory default!
  - **Reset All:** Reset configuration, including user accounts and network settings!

Click on the button **Reset** to restore the factory default settings.

5.17.4 Configuration - Import & Export (Local File/FTP)

Important: The system's import and export function refers to the start-up configuration, that is stored in the device's flash memory. The running configuration may not be identical to the start-up configuration due to unsafed changes!.

- If you want to export the device's running configuration, save it first before exporting it.
- After importing a configuration it will take effect after the device restarts.

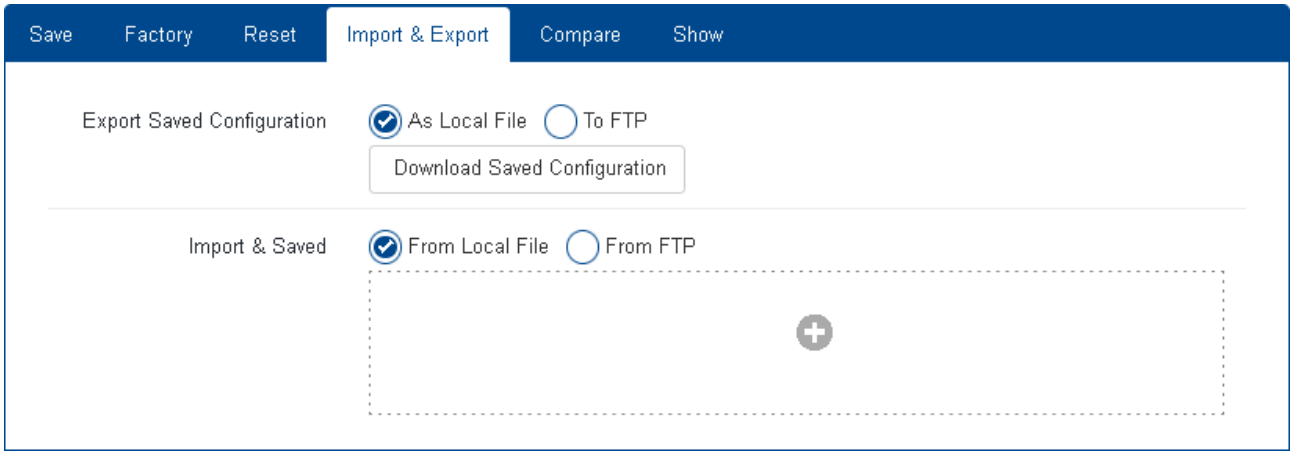


Fig. 144: Maintenance - Configuration - Import & Export (Local File/FTP)

This tab offers to import and export the device's configuration.

- **Export Saved Configuration:** Check one of the following options to assign the export destination:
  - **As Local File:** After clicking the button **Download Saved Configuration** the file manager dialogue of your web browser opens to select a local directory where you want to save the configuration file.
  - **To FTP:** When selecting the FTP option for export, enter the FTP address in the appearing address field and click on the button **Start**.

    The FTP address format reads as follows:

    `ftp://username:password@url/<filename>`
    (Example: `ftp://admin:adminstrator@192.168.0.101/`)

    The exported file name will be `startup-config` by default, if the filename is omitted.

    Note: Observe the trailing "/" in the FTP address when omitting the filename!
- **Import and Saved:** Check one of the following options to assign the import source.
  - **From Local File:** After clicking the + icon the file manager dialogue of your web browser opens to select a local directory from where you want to import the configuration file.
  - **From FTP:** When selecting the FTP option for import, enter the FTP address in the appearing address field and click on the button **Start**.
    The FTP address format reads as follows:

Import: `ftp://username:password@url/startup-config`
(Example: `ftp://admin:adminstrator@192.168.0.101/startup-config`)

After a configuration import is finished successfully, the device restarts automatically.

5.17.5 Configuration - Compare

Fig. 145: Maintenance - Configuration - Compare

This tab offers to compare all kinds of configuration settings against each other.

- **Compare:** Select the configurations you wish to compare from the drop-down list and click on the button **Start**.

  A pop-up window opens showing the results of the comparison.

  Click on the button **Close** to close the pop-up window.

5.17.6 Configuration - Show

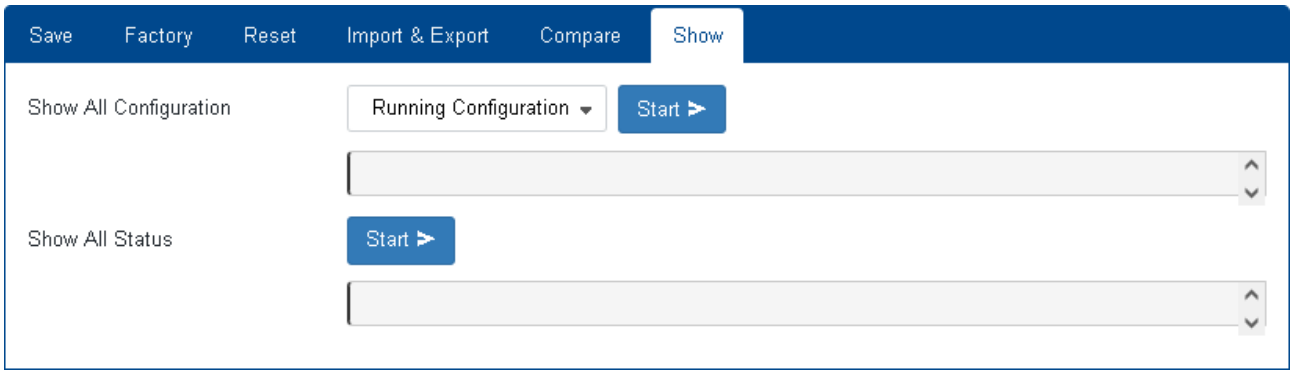


Fig. 146: Maintenance - Configuration - Show

This tab shows the different configuration types and the system's status as follows:

- **Show All Configuration:** Select the configuration type from the drop-down list.
  - **Factory Configuration:** The default configuration.
  - **Saved Configuration:** The startup configuration saved in the device's Flash memory.
  - **Running Configuration:** The currently running configuration containing all non-saved changes to the startup configuration.

  A click on the button **Start** shows the selected configuration.
- **Show All Status:** A click on the button **Start** displays all settings of the device, e.g. ports, PoE status and ACL data.

5.17.7 CLI Script - Run (Local File/FTP)

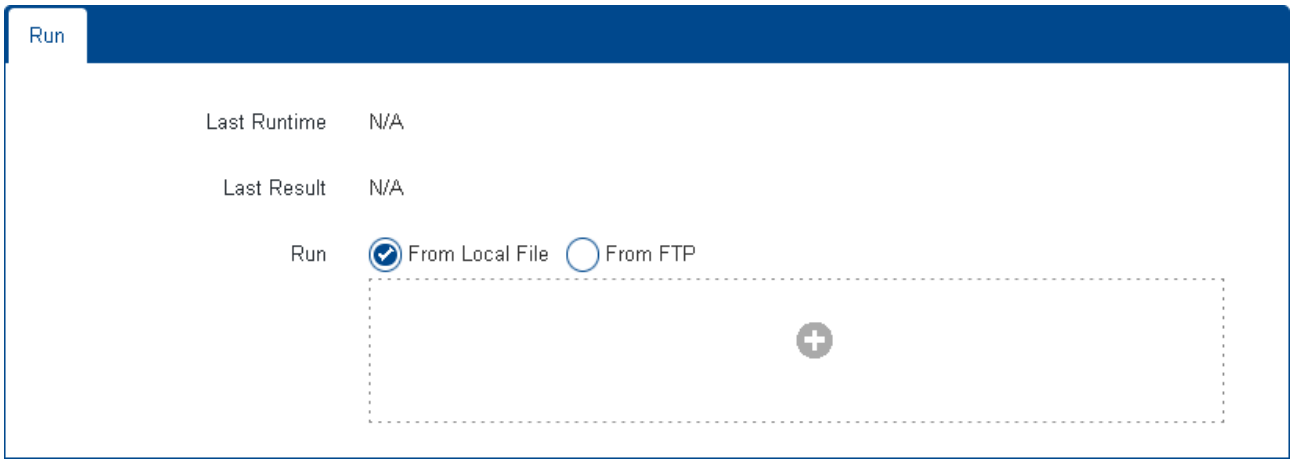


Fig. 147: Maintenance - CLI Script - Run (Local File/FTP)

This tab offers to run additional scripts on the device.

- **Last Runtime:** Shows the date a script was executed on this device recently.
- **Last Result:** Shows the result of the script run.
- **Run:** Check one of the following options to assign the script source:
  - **From Local File:** After clicking the + icon the file manager dialogue of your web browser opens to select a local directory from where you want to import the script file.
  - **From FTP:** When selecting the FTP option for import, select the server type from the drop-down list ("FTP", "FTPS", "SFTP"), enter the respective server address in the appearing address field and click on the button **Start**.

    The system will download and start the script file automatically.

5.17.8 Firmware - Current (Local File)

Note: For information about how to get the latest firmware for your device see page 6.

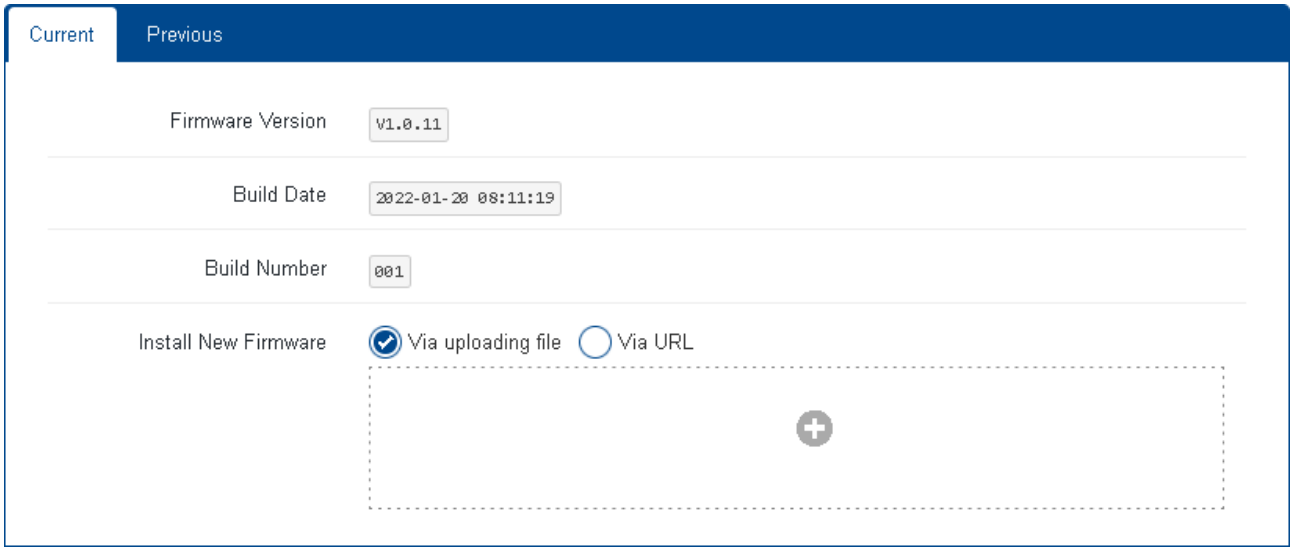


Fig. 148: Maintenance - Firmware - Current

- **System Version:** Shows the currently active firmware version of the device.
- **Build Date:** Shows the build date of the currently active firmware.
- **Build Number:** Shows the build number of the currently active firmware.
- **Install New Firmware:** Check the option "Via uploading file".

1. Click on the **+** icon of the area below to open the file manager of your operation system.
2. Navigate to the directory where you have downloaded the latest firmware file from the MICROSENS website.
3. Click on the button **Upload** to start the firmware upload.
4. The system shows a pop-up dialogue after verifying the uploaded firmware successfully.
5. In the pop-up dialogue click on the button **Sysupgrade** to start the upgrade.
6. After the upgrade has finished successfully, the system restarts automatically.

Note:
The device's configuration will stay unchanged when upgrading or downgrading the firmware.

5.17.9 Firmware - Current (URL)

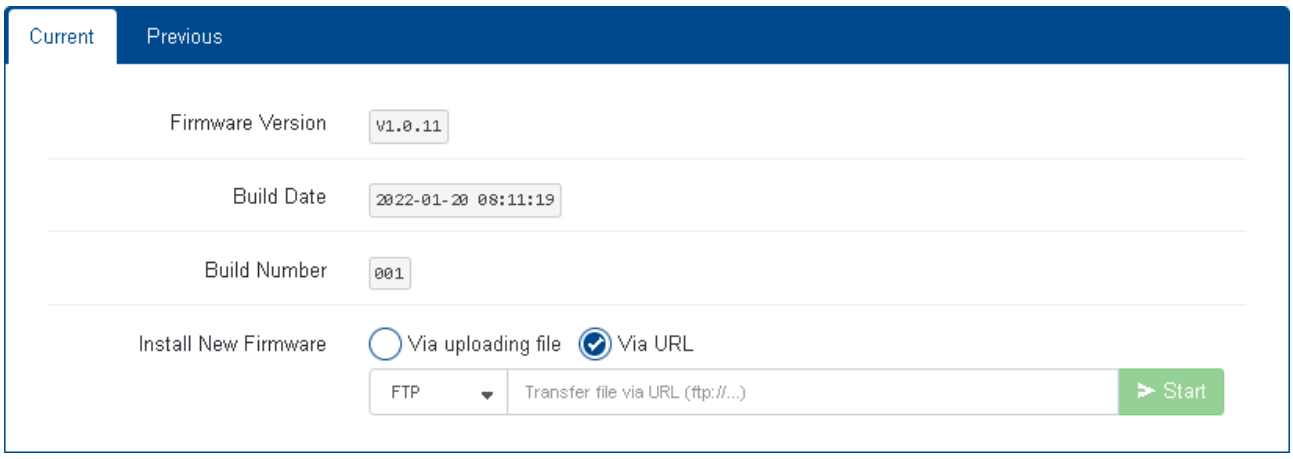


Fig. 149: Maintenance - Firmware - Current (URL)

- **Install New Firmware:** Check the option "Via URL".

1. Select the server type from the drop-down list ("FTP", "FTPS", "SFTP")
2. Enter the URL of the respective server.
3. Click on the button **Start** to start the firmware download.
4. The system shows a pop-up dialogue after verifying the uploaded firmware successfully.
5. In the pop-up dialogue click on the button **Sysupgrade** to start the upgrade.
6. After the upgrade has finished successfully, the system restarts automatically.

Note:
The device's configuration will stay unchanged when upgrading or downgrading the firmware.

5.17.10 Firmware - Previous

Fig. 150: Maintenance - Firmware - Previous

This tab gives information about a previous inactive firmware version. It is possible to activate this version with a click on the button **Go To Previous Firmware**.

5.17.11 Snapshot - Snapshot (Local File/FTP)

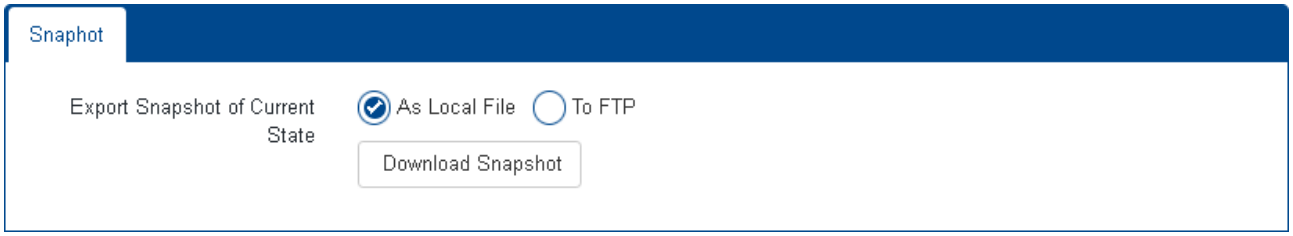


Fig. 151: Maintenance - Snapshot - Snapshot (Local File/FTP)

Note:
A system snapshot should be included e.g. for support requests!

This tab offers to take a snapshot of the current system configuration.

- **Export Snapshot of Current State:** Check one of the following options.
  - **As Local File:** After clicking the button **Download Snapshot** the file manager dialogue of your web browser opens to select a local directory where you want to save the snapshot `zip` file.
  - **To FTP:** When selecting the FTP option, enter the FTP address in the appearing address field and click on the button **Start**.

    The FTP address format reads as follows:

    `ftp://username:password@url/<filename>`
    (Example: `ftp://admin:adminstrator@192.168.0.101/yyyymmdd_snapshot`)

  The resulting `zip` file contains the `allinfo.log` file (`running config/status/allinfo.log`).

5.17.12 Reboot - Basic

Fig. 152: Maintenance - Reboot - Basic

Click on the button **Reboot now** to restart the device manually.

Important:
All unsaved changes will get lost!

5.18 Documentation

5.18.1 Documentation - Basic

Fig. 153: Documentation - Basic

This dialogue lists all documentation available on the device.

Click on one of the buttons **Download** to download the specific documentation as PDF file.

5.19 About

Fig. 154: About

This pop-up dialogue shows the vendor and article number of the device.

A click on **Open Source Software Licenses** opens a pop-up window showing all open source software licenses that are used by the device.

Click on the button **Ok** to close this dialogue.

6 Tutorials

This chapter assists you in performing specific tasks to obtain the full functionality of the device.

6.1 Docker

Note:
For more information about GUI settings for using Docker images please refer to section 5.13 on page 105.

6.1.1 Using Docker Image Files

The following example describes how to use a Docker image in form of a local file.

1. In the main menu, select **Docker**.
2. Click on the tab **Archive**.
3. Click on the button **Add** to open the loading dialogue.
4. Check the option **From Local File** and click on the **+** sign in the area below.
5. In the opening file management dialogue of your operating system navigate to the Docker image `docker-archive-demo.tar`.

   Note:
   In case you do not have this file at hand, please contact the MICROSENS support.
6. Click on the button **Start** to start the loading process.

   The process starts, showing a progress bar.
7. As soon as the Docker image is successfully loaded, it is listed in the **Archive** table.

   You will notice that the image is not yet listed in the tabular overview on the tab **Image**. As long as the Docker image only is "loaded" but not "imported", the image cannot be started.
8. On the tab **Archive** click on the button **Import to Image** of the specific image to make it an executable Docker image.

   Depending on the image size this may take a while.
9. As soon as the image is imported successfully, change to the tab **Image**.

   The new Docker image is listed in the image table.

10. Click on the button **Run** to open the starting image dialogue

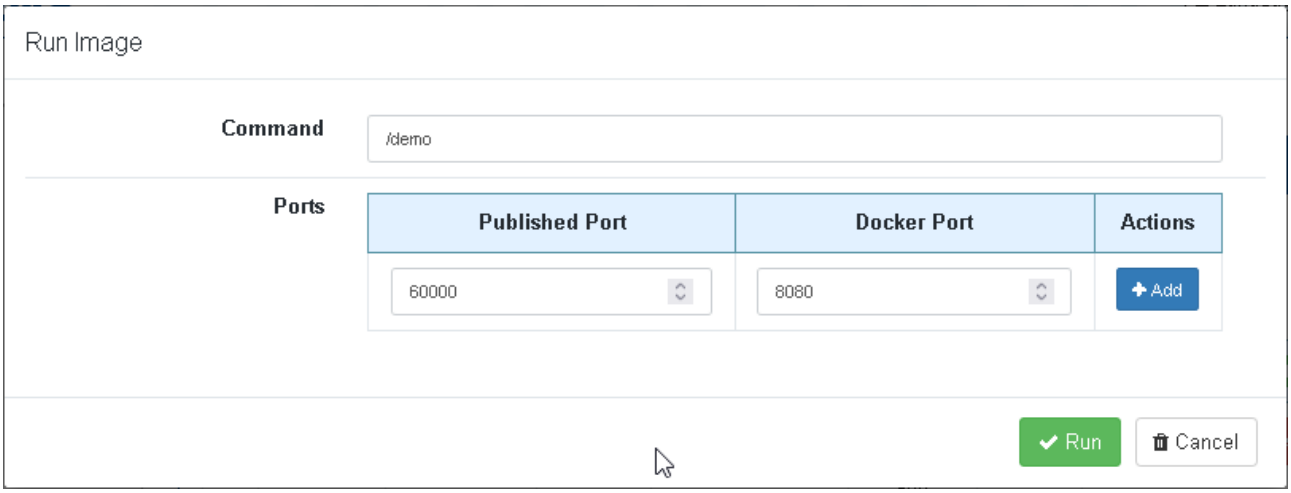


Fig. 155: Docker - Image - Run (Example)

11. Enter the **Command** `/demo`.
12. Set **Publish Port** to "60000".
13. Set **Docker Port** to "8080".
14. Click on the button **Add** to assign the settings.
15. Click on the button **Run** to start the Docker image.
    Depending on the image size the startup may take a while.

16. Change to the tab **Container** to view Docker image statistics of the currently selected Docker image.

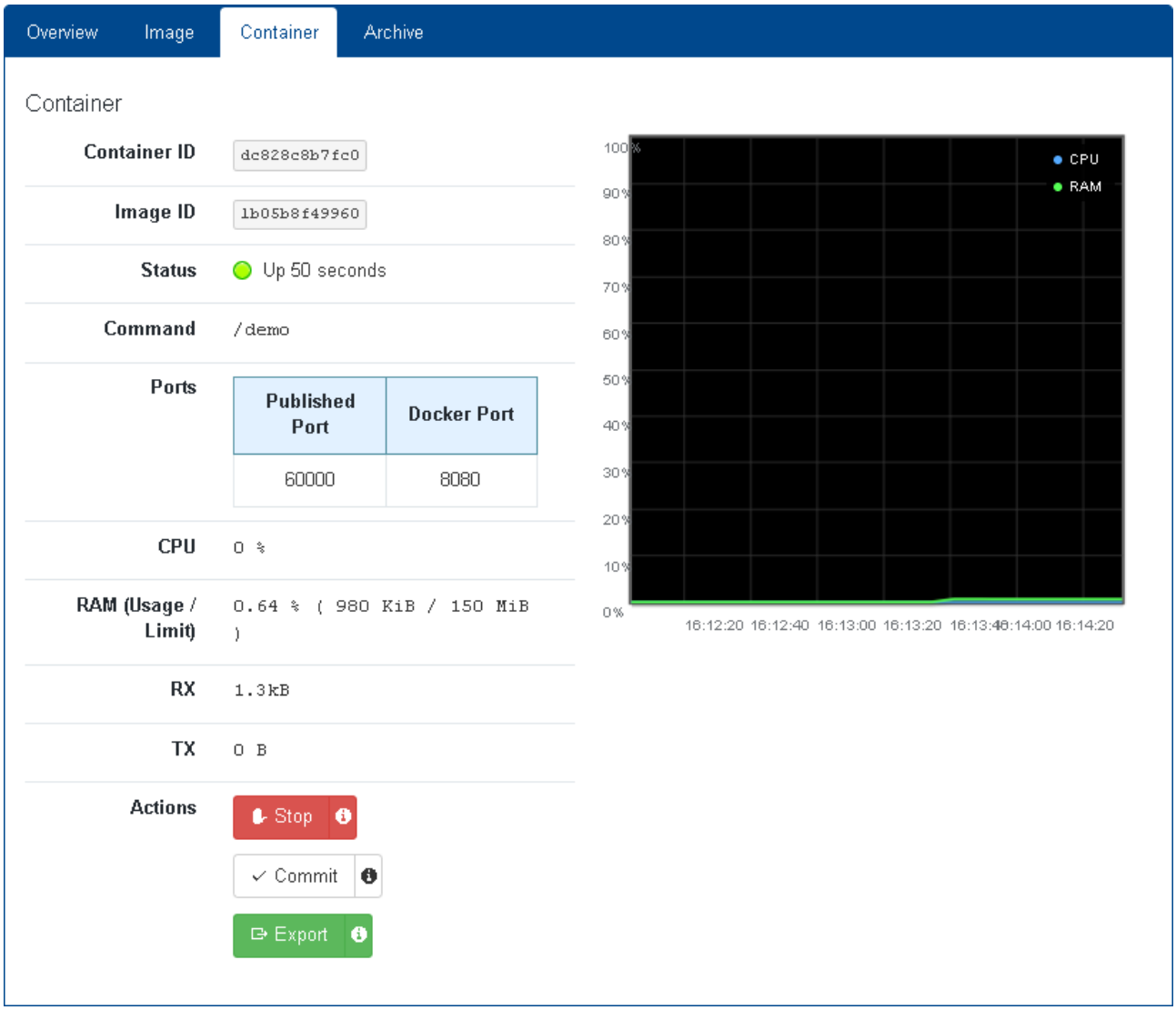


Fig. 156: Docker - Container (Example)

17. Open your web browser and navigate to the following address:

    `http://<device's IP address>:60000`

18. The browser shows the functional Docker website with extensive Docker and device related information.

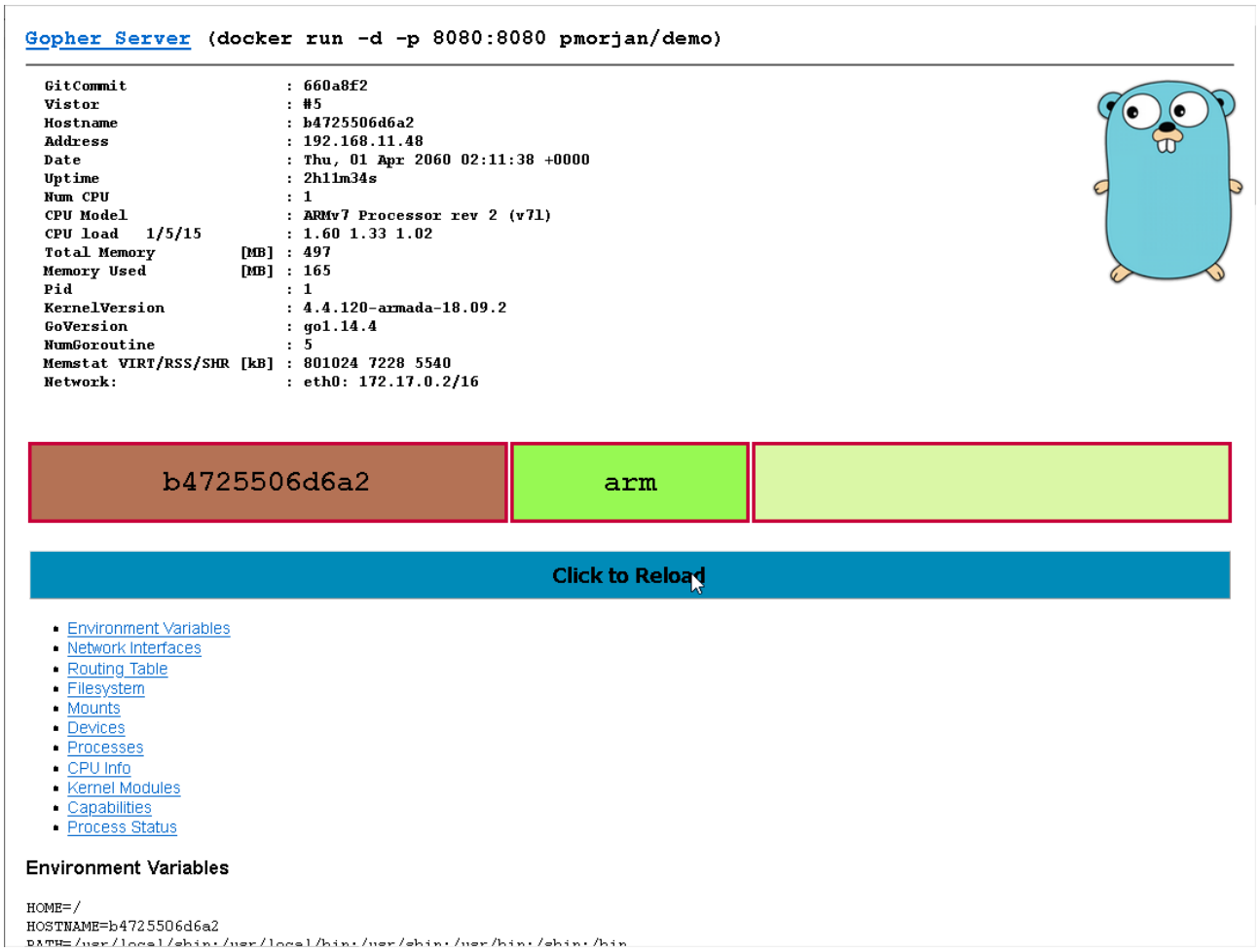


Fig. 157: Docker - Container - Website (Example)

6.1.2 Using Docker Image Hub

The Docker Image Hub URL may point to an image repository where useful Docker images are stored.

6.1.3 Update Docker Engine

The following example describes how to update a Docker engine.

Note:
In case you do not have the latest Docker engine file at hand, please contact the MICROSENS support.

1. In the main menu, select **Docker**.
2. Click on the tab **Overview**.
3. In the section **Upgrade Engine** check the option **From Local File** and click on the **+** sign in the area below.

4. In the opening file management dialogue of your operating system navigate to the Docker engine file `docker-engine-vx.x.x.tar`.
5. Click on the button **Start** to start the updating process.

   Note:
   The updating process will take a while! Do not refresh the browser window or switch of the device!
6. As soon as the Docker image is successfully updated, the device reboots.
7. After reboot, login to the device and select **Docker** in the main menu.
8. The tab **Overview** shows version information about the updated Docker engine.

Disclaimer

All information in this document is provided ‘as is’ and subject to change without notice.

MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or consecutive damage.

Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Document ID:PM-21005-2022-11-23