Operating Instructions

19"- RY-Switches of the L-series

- RY-LGS23-26
- RY-LGSO25-24
- RY-LGSO25-28
- RY-LGSP16-10
- RY-LGSP23-10G
- RY-LGSP23-26/xxx
- RY-LGSP23-28/xxx
- RY-LGSP23-52/xxx
- RY-LGSPTR23-26

RY Industrial-Switches of the L-series

- RY-LPIGE-602GBTME
- RY-LPIGE-804GBTME
- RY-LPITE-802GBTME
- RY-LPITE-804GBTME
- RY-804GBTME, without PoE

19"-Switches:
Firmware Release v6.54.3133
Hardware Version 1.01

Industrial-Switches:
Firmware Release v7.10.1972
Hardware Version v1.01

Liability
Information contained in this document may be changed without prior notice. barox Kommunikation reserves the right to modify the respective devices and/or this manual without prior notification.
Our products may contain unintentional technical and/or typographical errors.
Modifications are regularly carried out to improve our products.
The latest operating instructions are available on our website.
www.barox.ch

Published by:

barox Kommunikation AG
Im Grund 15
CH-5405 Baden-Daettwil
Switzerland
www.barox.ch

Publication Date: August 2019
Version: 1.3

TABLE OF CONTENTS

1 INTRODUCTION

These Operating Instructions describe the commissioning of the switches and the configuration of the most important basic functions.

All persons using this manual should have the following skills:

- Knowledge of how to install and operate electronic devices
- Experience with using computer systems
- Knowledge of Local Area Networks (LANs) and a general knowledge of IP communications
- Knowledge on working with web browsers

1.1 Contents

This Operating Manual is divided into the following chapters:

1. Introduction
2. Commissioning of the switches
3. Diagnostic tools and firmware upgrades

1.2 About Us

In all situations where a network is required to transmit high-quality video content fast and securely, barox Kommunikation's range of POWERHAUS switches guarantee pioneering connections.

barox Kommunikation designs, coordinates and supplies everything from a simple, point-to-point connection to a large area network running multicast applications.

1.3 Website

Information on our full range of switches as well as download links to our data sheets, documentation and the latest firmware are available on our website: www.barox.ch.

1.4 Support

Our POWERHAUS Partners are available to help you should you have any problems or questions regarding the configuration of your switches.

2 Short Description

All our RY switches are manageable, full Gigabit IP switches with layer 2/2+ functionality. We offer a range of different models with a varying number of optical and electrical ports which − depending on the model − can support anything up to PoE++.

2.1 Special Features for Video Networks

- **Active Camera Monitoring**

Cameras powered via a PoE connection from the switch are continually monitored. In the case of a camera failure, the switch automatically restarts the camera all by itself. Should this operation fail, the switch automatically sends out an alarm via SNMP.

- **Active Monitoring of the PoE Power Supply**

Should the amount of power requested from the switch be too high, e.g. through a defective camera, the switch will automatically send out an alarm via SNMP.

- **Active Management of the Level of PoE Power Supplied**

When the switch is started up, the individual PoE ports can be started up one after another to avoid overloading the PoE power supply.

- **Other Useful Features**

Jumbo Frames up to 9,600Bytes are supported at 1 Gbits and also 100 Mbits.
Port security by means of MAC address restriction and IP identification

Readability and provision of certificates, resp.
Extra high backplane performance for smooth video transmission at full port utilisation

Ports using PoE can be detected at the push of a button (front panel).

2.2 DMS (Device Management System)

The switch is equipped with an integrated network monitoring and control system that uses a very simple method to provide the user with an excellent overview of the whole network. The network Topology View provides a quick overview of all the switches and terminal equipment in the network, e.g. IP cameras and servers, together with information on their respective IP addresses, device types and device descriptions. Plans showing the floor layout and the local environment can be stored as background images. These allow the user to quickly access specific network equipment − even without special knowledge of the IP structure. Finalised plans can then be exported and included in the documentation.

3 Commissioning

The switches can be configured using a web browser. To do this, a PC/laptop can be connected to any desired RJ45 port. Care should be taken to ensure that the IP address of the PC/laptop belongs to the same network segment as the switch. For example: 192.168.1.111.

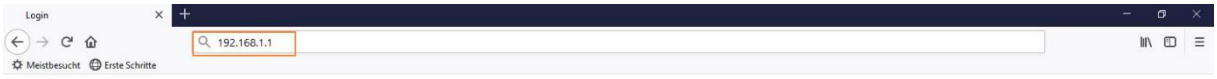
Alternatively, the switches can also be configured via a CLI (console port). In this document, the switch is configured using a web browser.

3.1 Factory Default and Login

The switches are supplied with the following factory default settings:

IP address: 192.168.1.1
Subnet mask: 255.255.255.0
User: admin
Password: admin

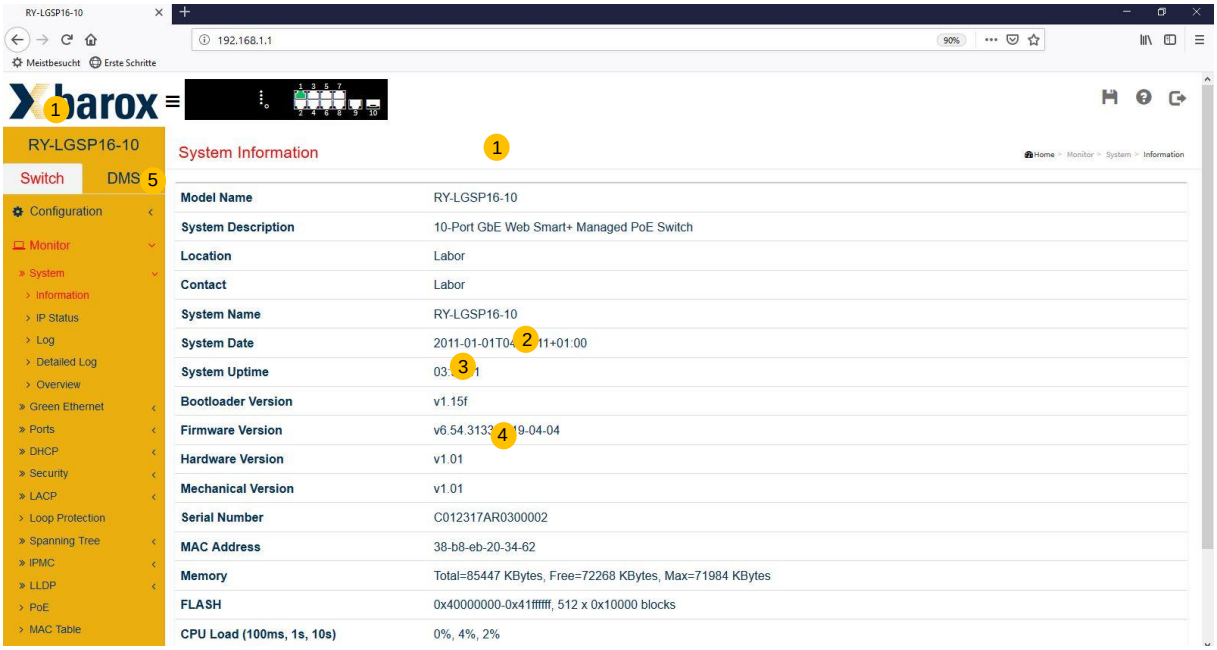
A connection can be made to the switch by entering the IP address of the switch (192.168.1.1) straight into a web browser. To log in, the user simply enters the user name and password listed above.



Once the login process has been successfully completed, the “System Information” page is automatically displayed showing the most important information on the switch.

3.2 System Information

This page displays the most important information on the switch.

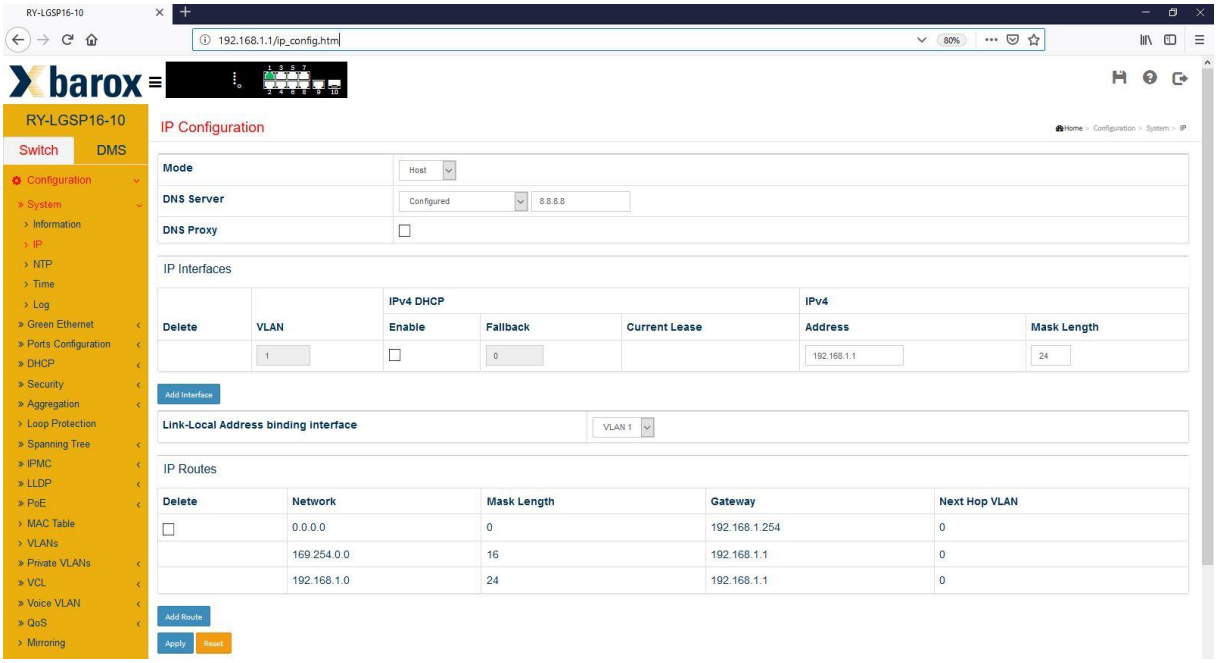


Key:

1. Name of the switch model
2. Firmware version
3. Hardware version
4. MAC address

3.3 Set a Static IP Address or use DHCP

The first step is to allocate an IP address to the switch. To do this, go to the "Configuration/System/IP" menu in the navigation tree.



Static IP Address

In the above image, one can see that the IP address of the switch is 192.168.1.1, that the subnet mask is 24 (255.255.255.0) and that it belongs to VLAN 1. This means that VLAN 1 is the management VLAN.

If the switch is to be allocated a new IP address, the existing IP address is simply overwritten and then confirmed by clicking on the "Apply" icon. The same applies, if the subnet mask needs to be changed.

DHCP

If the switch is to be integrated into a network where a DHCP server allocates the IP addresses, the check box underneath "IPv4 DHCP" needs to be checked.

The DHCP server will then allocate an IP address to the switch within the pre-defined range.

There are now two ways of finding out which IP address has been allocated.

a) Software tool, e.g.: SoftPerfect Network Scanner

https://www.heise.de/download/product/network-scanner-13270

b) Console port

This method requires using the console cable supplied with the switch. The console port of the switch is an RS232 interface, i.e. a PC/laptop with a serial interface or a USB-RS232 adapter is required.

To configure the switch via the CLI port, we recommend using the "PuTTY" software.

http://www.chip.de/downloads/PuTTY_12997392.html

The factory default settings of the CLI interface are as follows:

Bit rate:	115,200
Data bits	8
Parity:	None
Stop bits:	1
Flow control:	None

If the serial interface is used to connect up to the switch, the user needs to log on using the user name and password.

The following command can be used to show the IP address:
RY-LGSP23-26# *show ip interface brief*

➔ Important: This change now needs to be permanently saved.

To do this, access the switch by entering the new IP address in the web browser and then click on the diskette symbol at the top right-hand corner.

3.4 Gateway Configuration

If a new IP address is allocated to the switch, it is also mandatory to modify the gateway address accordingly.

To change the gateway address, the respective line first needs to be deleted and then re-created using the right address. The network address must be set to “0.0.0.0” and the mask length to “0”.

Then all that needs to be done is to rewrite the gateway address using one that corresponds to the network.

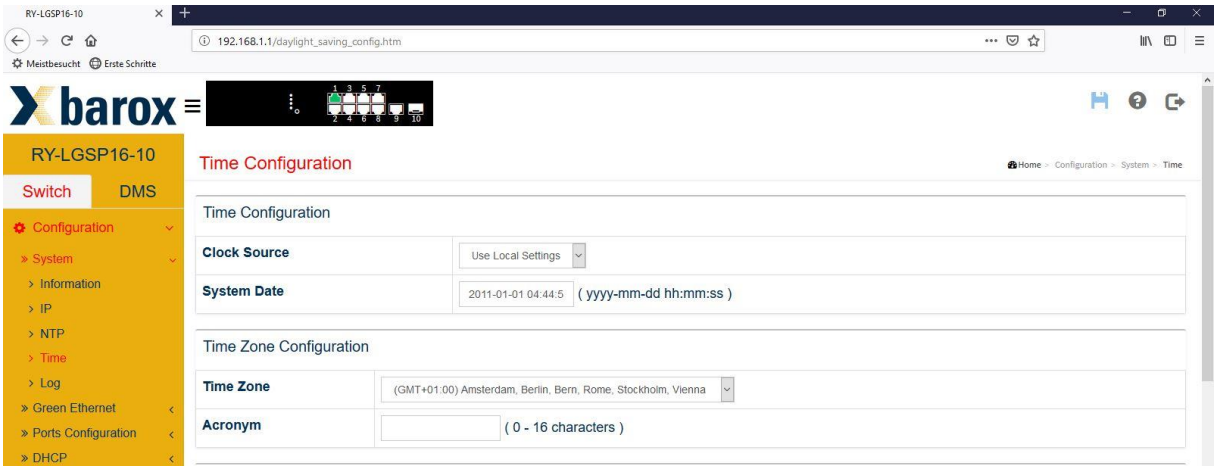
3.5 Time Configuration

The system time used by barox Kommunikation switches can either be configured manually or via an NTP server. The whole purpose of defining the time is to use it in the log file. If an error message is generated, a date stamp is added to the respective entry in the log file so that the downtime and/or the time when the error occurred is accurately recorded which helps to localise the possible cause.

3.5.1. Local Settings

In the “Configuration/System/Time” menu, select “Use Local Settings” as “Clock Source”. The date and time are then manually entered in the specified format in the field next to “System Date” and then confirmed using the “Apply” button.

➔ If the switch is restarted, the time is deleted and needs to be re-configured as the switch does not have its own backup battery.



3.5.2. NTP (Network Time Protocol)

The Network Time Protocol is a standard for synchronising clocks in computer systems using packet-based communication networks.

Configuration is done in two steps.

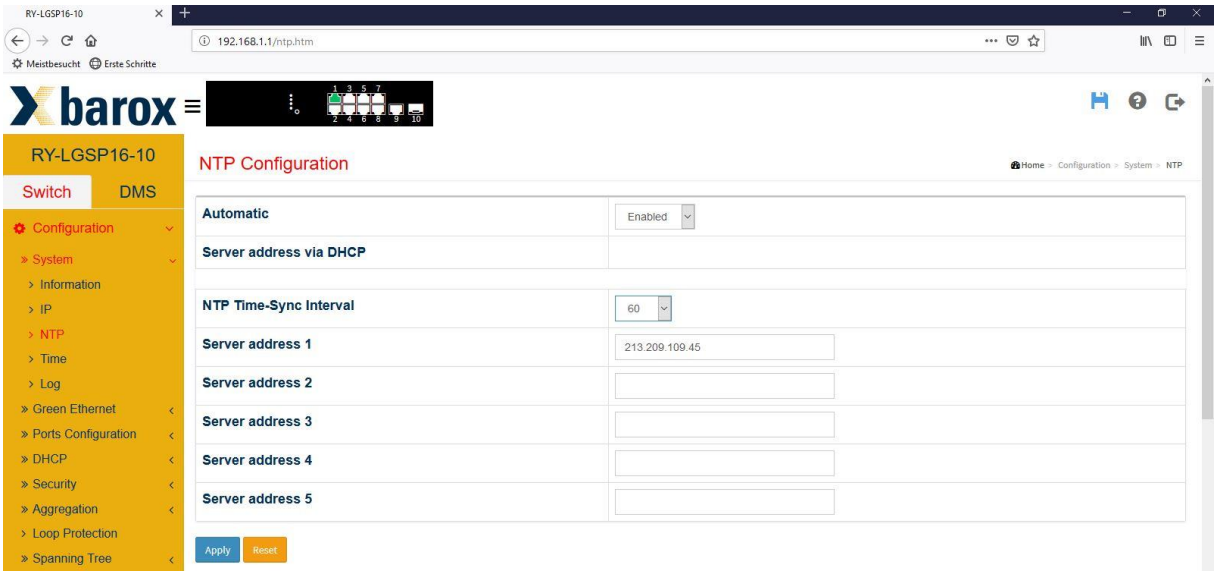
3.5.2.1. NTP Server

The first step is to tell the switch where it needs to go to get the time.

If the time is to be retrieved directly from the DHCP server, the entry in the “Automatic” field has to be set to “Enabled”. The IP address of the DHCP server is then displayed in the line below.

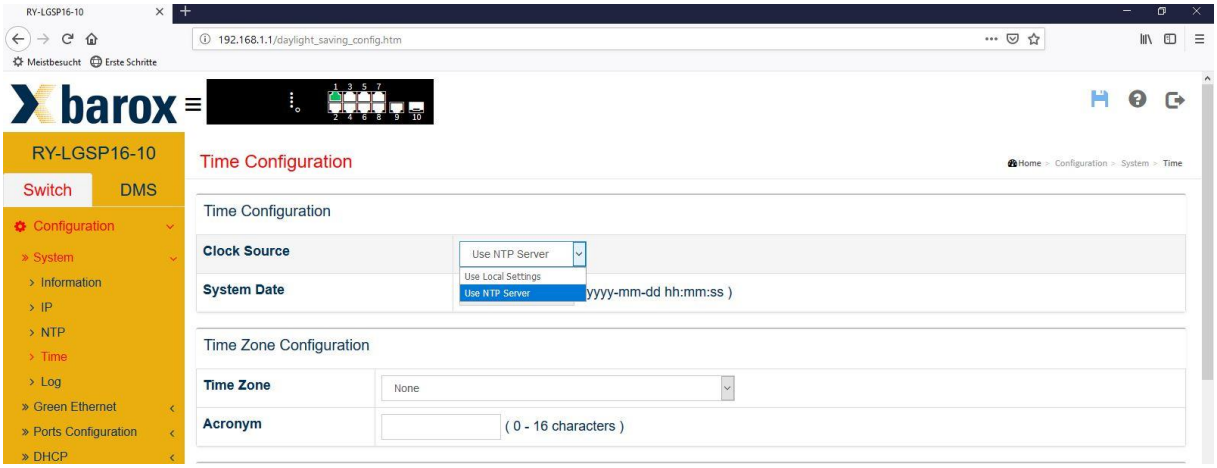
However, if the time is to be retrieved from another specific source, for example from a time server, NTP server, firewall etc., the respective IP address must be entered in the “Server address 1” field. This is the only way of ensuring that the switch can actually contact the respective IP address. Up to 5 sources can be defined.

If there is no time source available in one’s own network and the time is to be retrieved from an external source via the Internet, it is possible to enter the external NTP server details directly, e.g. 213.209.109.45 at http://www.pool.ntp.org/de/

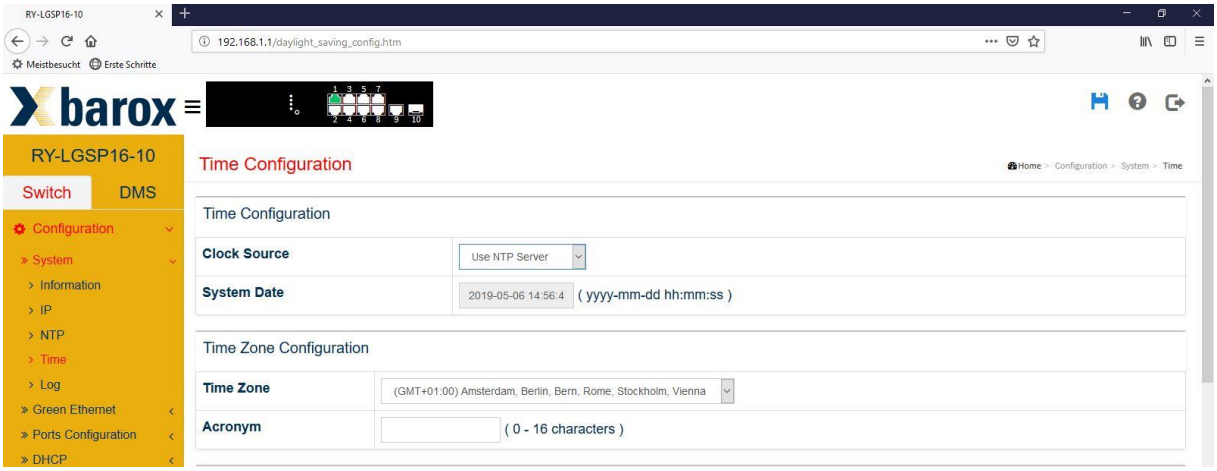


3.5.2.2. Time Settings

Now the “Clock Source” must be set to “Use NTP Server” in the “Configuration/System/Time” menu.



As time servers generally broadcast Greenwich Mean Time, the “Time Zone” must be selected accordingly to ensure that 1) the time is correct and 2) the system switches correctly between summer and winter time.



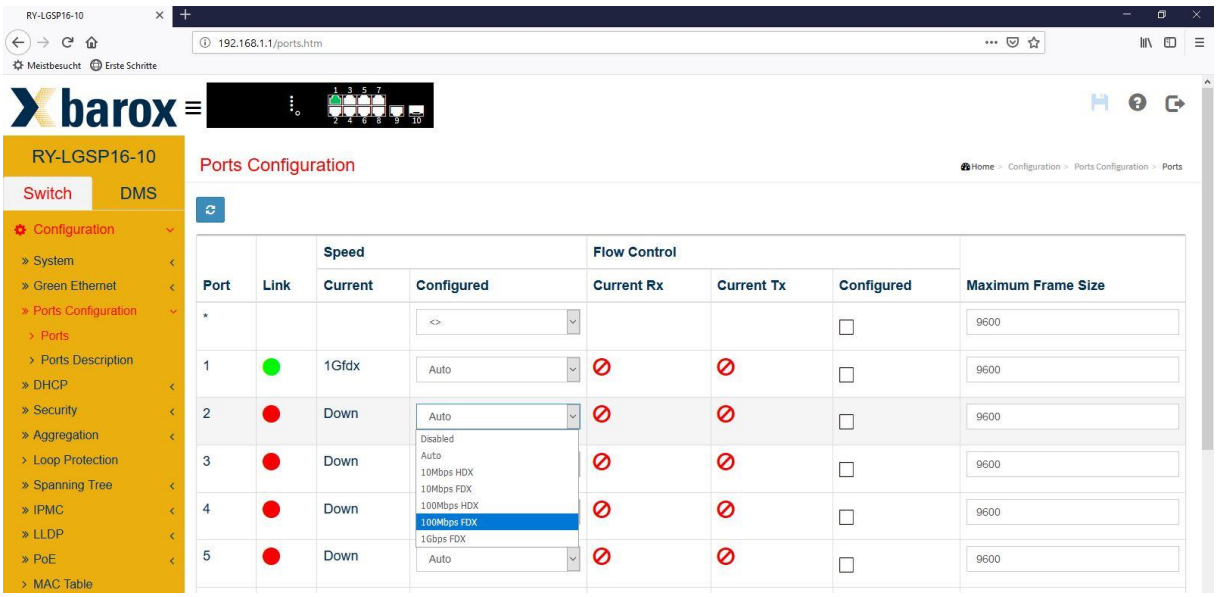
As soon as the switch can access the time and date, the correct date is shown in the “System Date” field.

3.6 Port Configuration

The ports are set to Auto mode when they leave the factory. Auto-negotiation is the procedure which allows two connected Ethernet network ports to independently negotiate and configure the highest-possible transmission speed as well as the duplex mode. This procedure only applies to twisted pair cables − not to fibre optic connections.

Nevertheless, in some cases the terminal device may not be correctly recognised. This sometimes occurs when using a camera with a 100 Mbps interface. In this case, the port must be manually set to 100 Mbps.

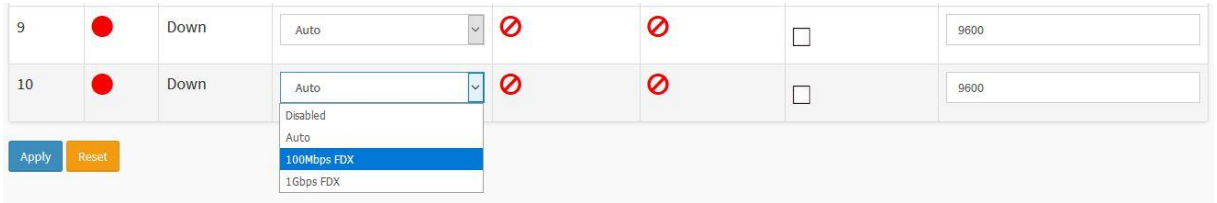
If a port is not to be used for security reasons, this can be disabled completely. In this case, the configuration mode should be set to “Disabled”.



3.6.1. SFP Port

The SFP ports are also equipped with an Auto mode. This is different to the auto-negotiation procedure used by copper ports. SFP ports are only capable of recognising the transmission speed through auto-negotiation and only support full duplex mode.

In some cases, a switch may not correctly detect whether an SFP is a 100 Mb or 1000 Mb model which will prevent the latter from functioning. In such cases, the port data rate needs to be set manually.



The SFP ports of the switches are not coded. This means that SFPs supplied by other manufacturers can be used − whereby no guarantee is supplied that these will function properly.

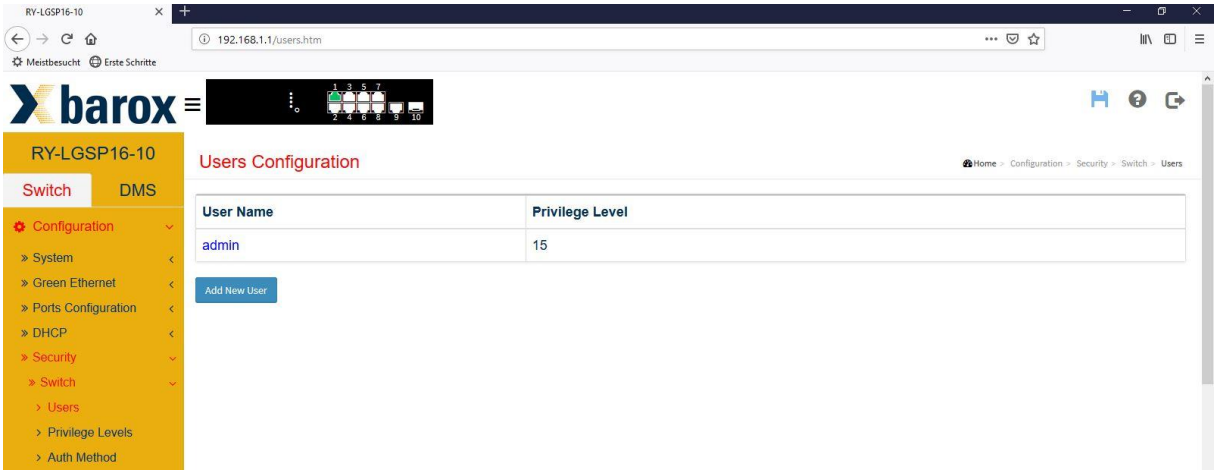
The barox Kommunikation product range includes SFPs for multi and single mode fibres with transmission speeds of 100 Mbps, 1 Gbps and 10 Gbps. Distances of between 550 m and 120 km can be achieved depending on the type of fibre and transmission speed.

➔ Please also refer to http://www.barox.ch/cm/produkte/product/ip-produkte/zubehoer/ac-sfp

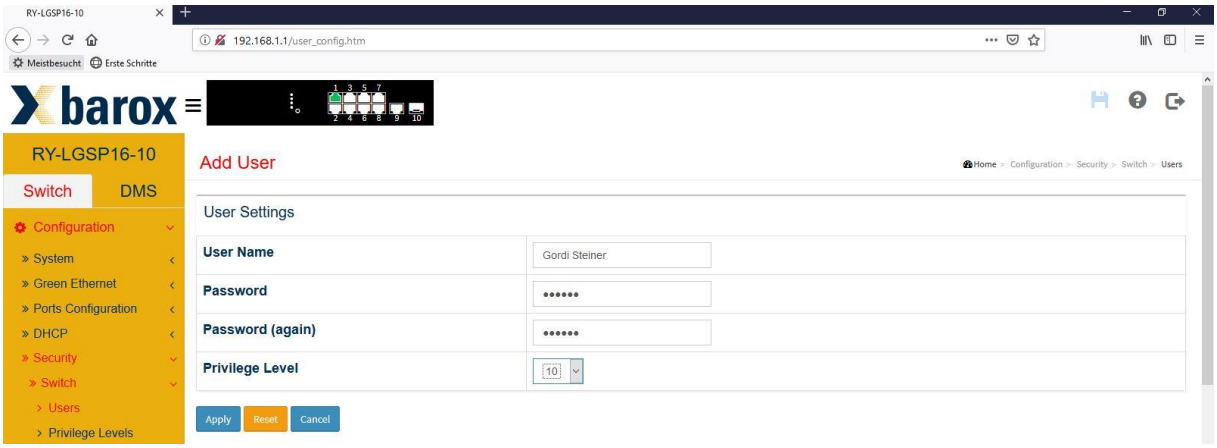
3.7 Change of User Name and Password

barox Kommunikation switches offer the option of generating a number of users with different rights. Up to 15 different levels can be defined.

Level 15 is the highest level and is intended to be used by the administrators.

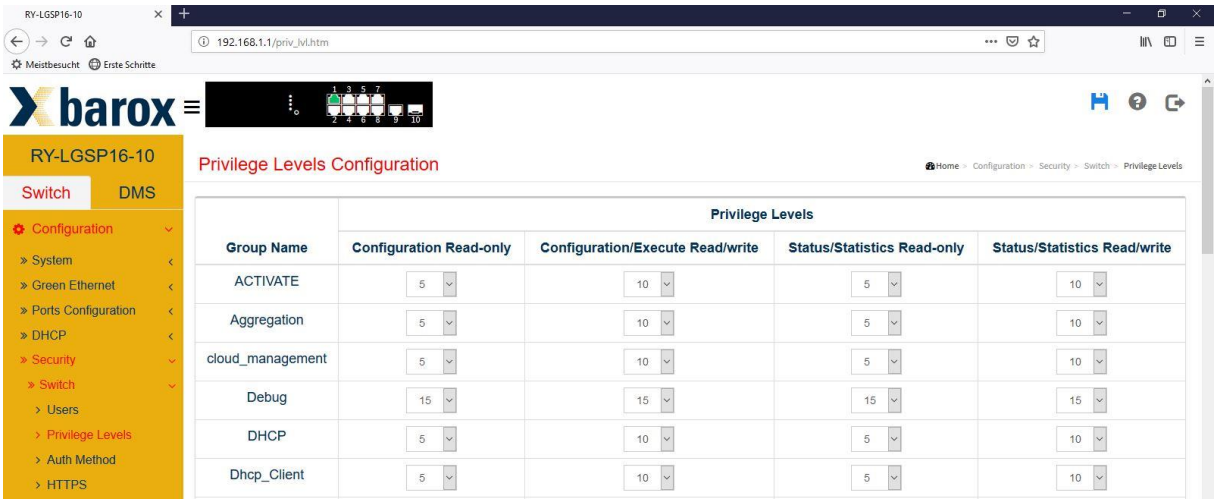


Another user can be generated by clicking on “Add New User”. Then the “User Name”, “Password” and “Privilege Level” need to be defined.



The exact range of rights applying to the new user can now be defined in the “Privilege Level” menu.

In the following example, the technician concerned has a privilege level of 10, i.e. he/she is allowed to configure everything based on his/her Read/Write rights. However, this technician’s “Debug” rights are so limited that he/she cannot even read “Debug” data.



This table is highly complex which allows extremely precise rights to be granted. For example, it is possible to define a user who can only read the MAC table.

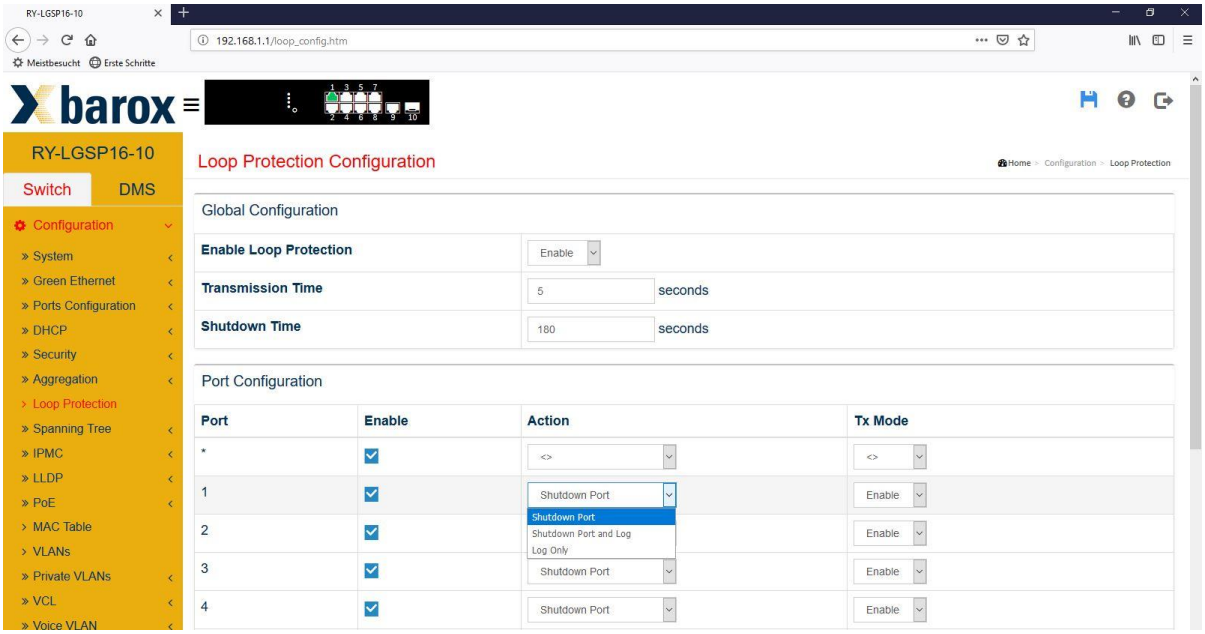
3.8 Loop Protection

In larger networks, it is very easy to accidentally, resp. unintentionally, make physical connections that result in a loop. If no loop protocol (e.g. RSTP) has been activated, the whole network hangs and becomes inoperative.

The “Loop Protection” feature was specially designed to handle such situations. Once this feature has been activated, it is possible to define whether the respective port should be shut down, merely an entry made in the log file or both (“Shutdown Port and Log”), if a loop is accidentally created.

➔ Ports already actively running RSTP must not additionally be monitored using the Loop Protection feature. This would lead to massive malfunctions within the network.

“Shutdown Time” shows how long a port is to remain disabled, should a loop be detected. Possible time entries: 0 – 604,800 s (7 days). If “0” is entered here, the port will remain deactivated until the switch is rebooted.



3.9 Ring Configuration

To guarantee redundancy within the network, it is crucial to set up a ring topology. To ensure that the network is not overloaded by a broadcast storm, a protection mechanism is required.

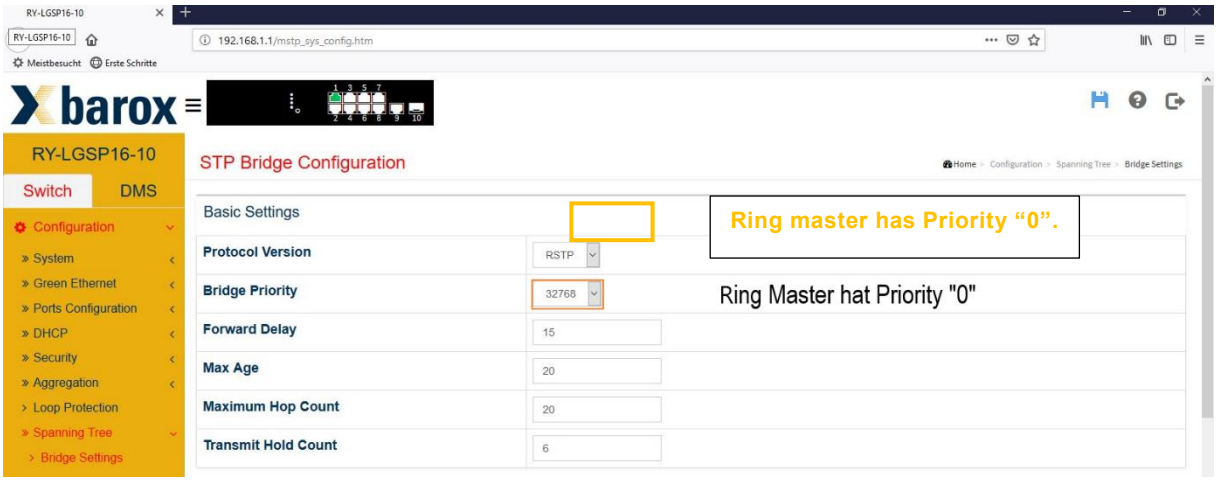
RSTP (Rapid Spanning Tree Protocol) is one of the fundamental protocols used in an Ethernet network. It ensures that no network loops are created within individual network segments. Unlike an IP packet, an Ethernet frame does not have a maximum Time to Live (TTL) and, therefore, may potentially go around in circles for an indefinite period of time. This, in turn, could overload the network and, in the worst case, bring the network to a standstill.

How the Rapid Spanning Tree Protocol works is explained in detail in Wikipedia.
https://de.wikipedia.org/wiki/Spanning_Tree_Protocol

3.9.1. Ring Master

In a ring topology, one switch must be defined as the master which then assumes the task of monitoring the ring. In the event that a connection is interrupted, this master then notifies all the other switches in the ring so that the alternative connection can be activated. The switch with Priority 0 is the ring master.

The RSTP protocol is designed to automatically make the switch with the lowest MAC address the ring master, if no ring master has been defined.

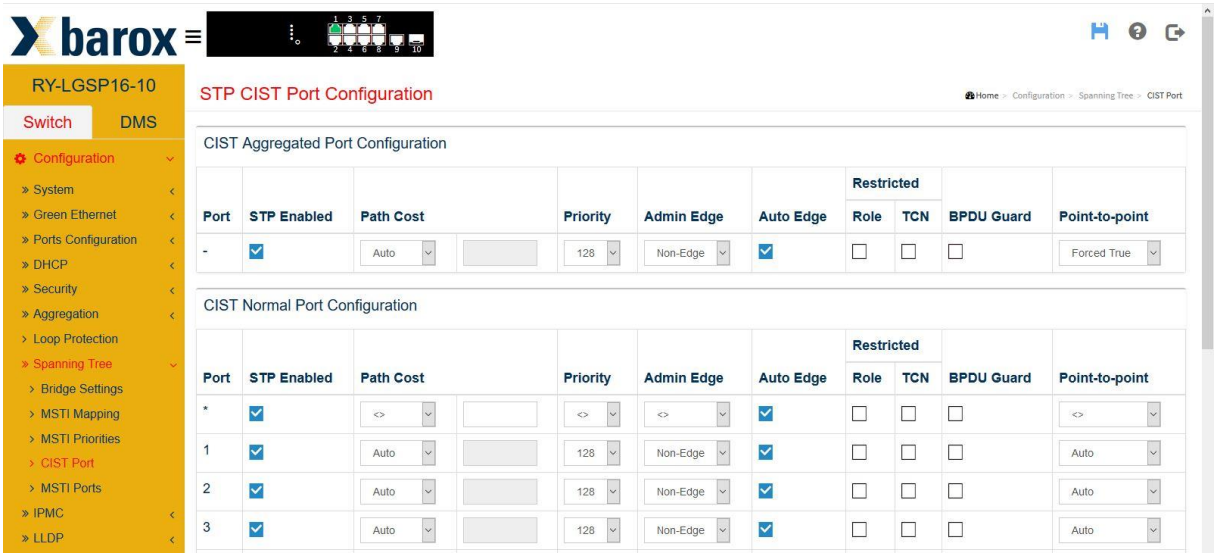


The desired protocol version must be selected in the “Spanning Tree/Bridge Settings” menu. RSTP is supported by all switch manufacturers - making it compatible with third-party manufacturers.

The switch factory default is set to “Bridge Priority” 32768. If the switch is to act as master, the Bridge Priority must be set to “0”. All the other values can be left as they are.

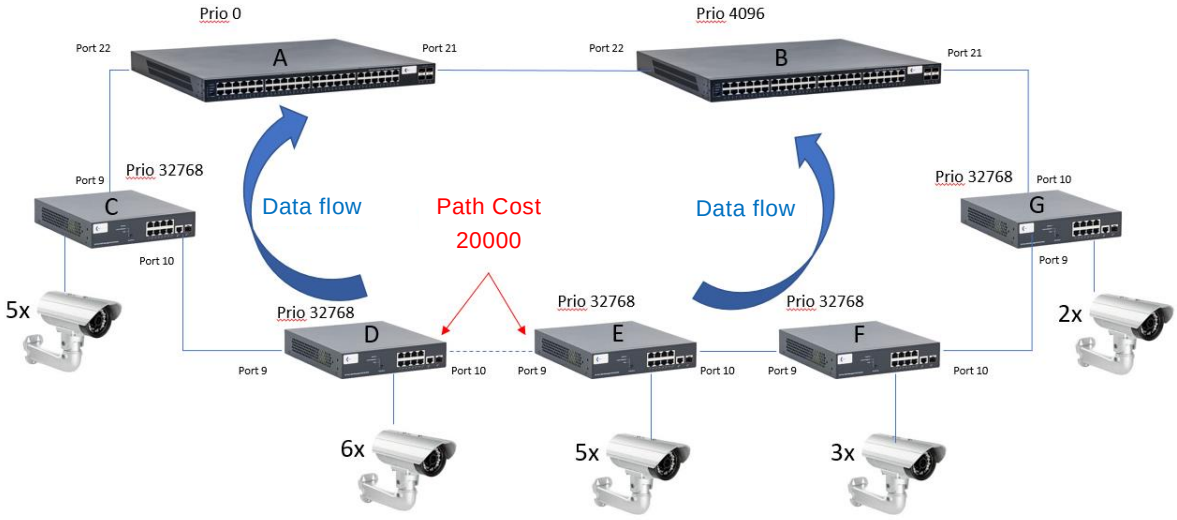
3.9.2. Port Configuration

The factory default for all ports is “STP Enabled”. This means that, in theory, the ring can be created using any desired port. To optimally distribute the load across the network, it is possible to define that the data packet flow be channelled using Path Cost. The term “Path Cost” originates from the time when lines were leased for A to B connections which meant that they were expensive.



Example:

In a larger ring with numerous terminal devices and larger data volumes it makes sense to channel the data flow within the ring to distribute the load evenly across the switches (load-sharing). To achieve this, the path cost needs to be defined.



In the above example, the network consists of two central switches (A+B) and 5 other switches that form the ring. All in all, 21 cameras have been installed − each supplying 5 Mbps of video data, i.e. a total of over 100 Mbps of data.

Scenario 1: Only RSTP is active on all the switches

The switch with the lowest MAC address functions as the master. This may be the smallest switch in the ring with the lowest CPU performance. The direction of data flow is not known.

In the case of an interruption, the switch-over may take a little longer as this small switch cannot process the data so quickly.

Scenario 2: RSTP is active on all the switches, switch A has Prio 0 and switch B Prio 4096

In this case, switch A has been defined to assume the role of master. If this switch fails, switch B will take over the role of master. Switch A monitors the ring. Should network traffic be interrupted, switch A's CPU has enough power to be able to react quickly. Port 21 of switch A may be marked as being "Blocked". The data from all the video cameras will then be provided via port 22. Small switch C then has to process the data from all the video cameras, causing a bottleneck.

Scenario 3: RTSP active, the master and Path Cost have been defined

This configuration precisely defines how the data should flow. The load is distributed on two sides. None of the switches is pushed to the limit. As the Path Cost of switch D, port 10 and switch E, port 9, is higher than that of all the other ports in the ring, this route will only be activated, if network traffic is interrupted.

Path Cost − default setting:

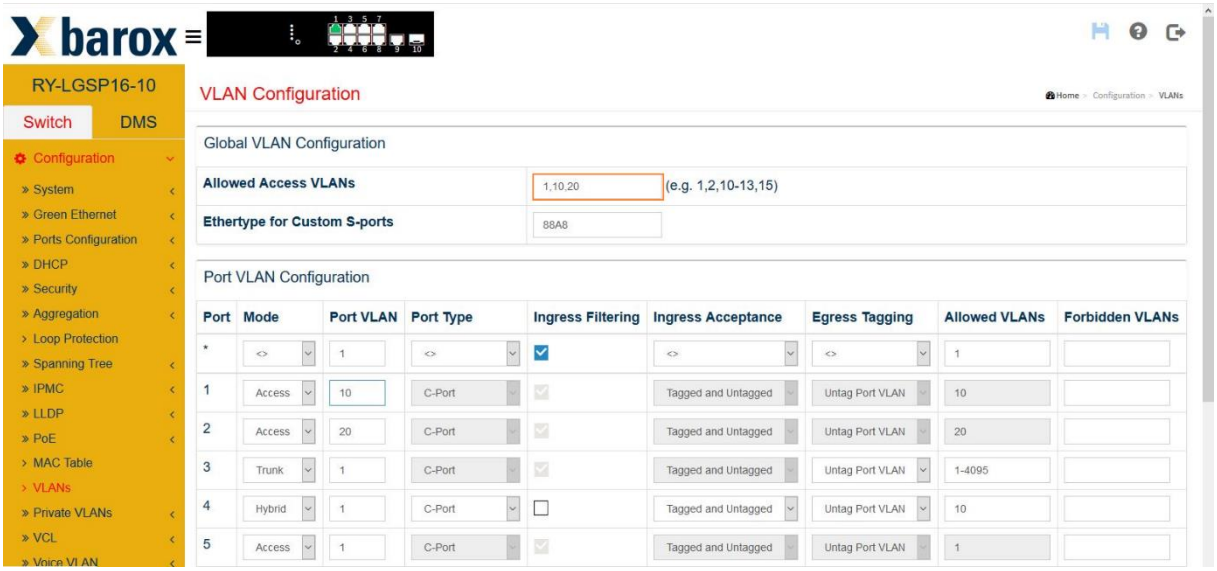
The cost depends on the distance from the root bridge (master) and the available uplink to the target. Normally, the Path Cost of reaching the target via a 100 Mbps uplink is higher than that of a 1 Gbps uplink. In this case, the 100 Mbps link would be blocked from being used as a redundant path. Although Path Costs have been standardised according to the IEEE provisions, different values can be manually specified, for example, to select a preferred uplink where the speeds are identical so as to reflect the real cost of a dedicated line.

➔ **Wherever possible, one should aim to realise a configuration that corresponds to the one illustrated in the above image.**

3.10 VLAN Configuration

VLAN configuration is effected on one single page.

All the VLAN numbers requiring configuration must be listed in the field “Allowed Access VLANs”.



Once the VLAN numbers have been entered, the individual ports can be allocated to a specific function and VLAN.

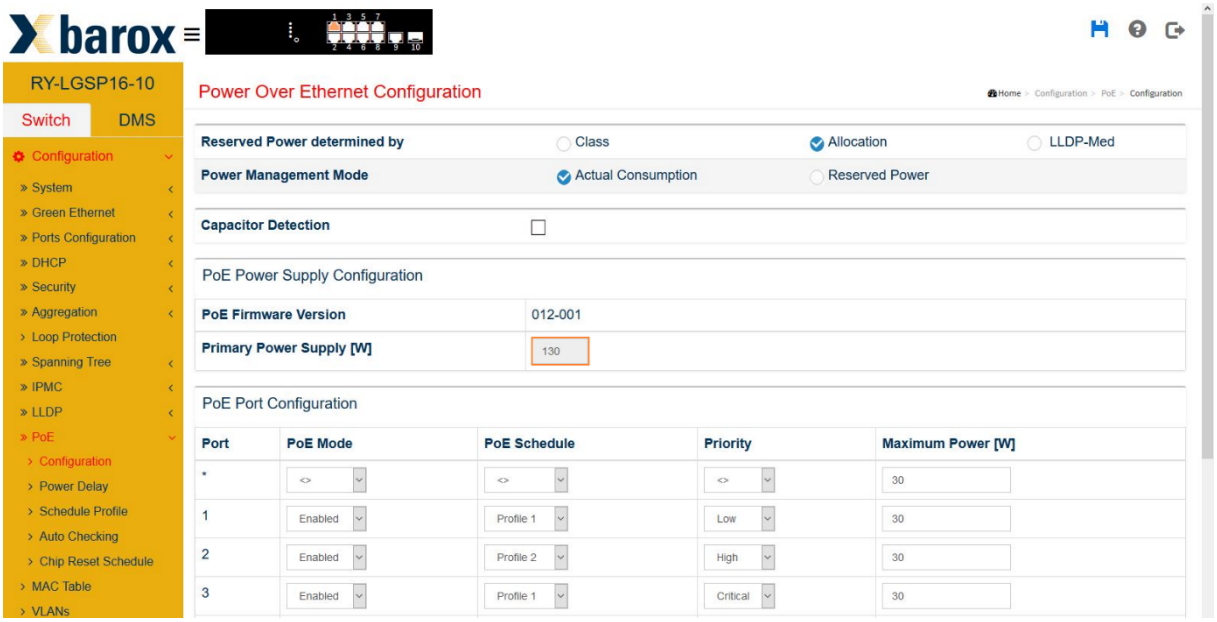
Mode	VLAN	Function
Access	No.	A terminal device is to be connected to this port
Trunk	---	Connection between two switches
Hybrid	---	Connection between two switches or to a terminal device

The allowed VLANs can be defined in the “Allowed VLANs” column both in “Trunk” and “Hybrid” mode.

3.11 Power over Ethernet (PoE)

With respect to PoE, the switch has numerous options for optimising PoE implementation. Power can be controlled, resp. turned on or off, on a time or event-triggered basis. In addition, powered devices (e.g. PoE cameras) can be monitored and rebooted, if required. The PoE chip in the camera can also be reset. This makes sense, for example, in cases where a camera shows no picture although it can be pinged.

3.11.1. PoE Configuration



Every switch has a pre-defined performance capacity. This describes how much power can be supplied via the PoE ports. The crucial component here is the power supply installed in the switch. In the above example using an RY-LGSP16-10 switch with 8 PoE+ ports, a maximum of 130 W can be supplied. This means that it is impossible to connect a 30 W terminal device to each of the 8 ports as this would require a total of 240 W. The integrated power unit cannot supply this much power.

This means that it is important to keep track of how much power is being supplied per port.

POE appliances are divided into various categories depending on their respective consumption.

Class	Power available to the powered device	Classification signature
0	0.44 – 12.96 W	0 to 4 mA
1	0.44 – 3.84 W	9 to 12 mA
2	3.84 – 6.49 W	17 to 20 mA
3	6.49 – 12.95 W	26 to 30 mA
4	12.95 – 25.50 W (only 802.3at/Type 2)[4]	36 to 44 mA

https://de.wikipedia.org/wiki/Power_over_Ethernet

Reserved Power determined by

One can define how the maximum amount of power to be supplied is determined in the section “Reserved Power determined by”.

- Class = corresponds to the class to which the terminal device says it belongs
- Allocation = according to the value stated in the “Maximum Power (W)” column
- LLDP-Med = ditto Class mode, pulls the information via LLDP (where possible)

If the terminal device exceeds the predefined power limit, the port turns PoE off.

Power Management Mode

This is where one defines how the switch should behave should the maximum possible power level be exceeded.

- **Actual Consumption**

Should the amount of power demanded by the devices exceed the maximum possible amount of power that the switch can provide, PoE is turned off completely. If the power limit is only exceeded by one single port, PoE is only turned off to this port.

The importance of the individual ports is defined in the “Priority” column. Ports set to “Low” are turned off immediately, whereas ports set to “Critical” are turned off last should the maximum power level be exceeded.

- **Reserved**

Ports set to “Reserved” are only turned off, if the power reserved for them in the “Maximum Power (W)” column is exceeded.

PoE Schedule

Each individual port can be allocated to a time schedule. A total of 16 time schedules can be created.

3.11.2. PoE Power Delay

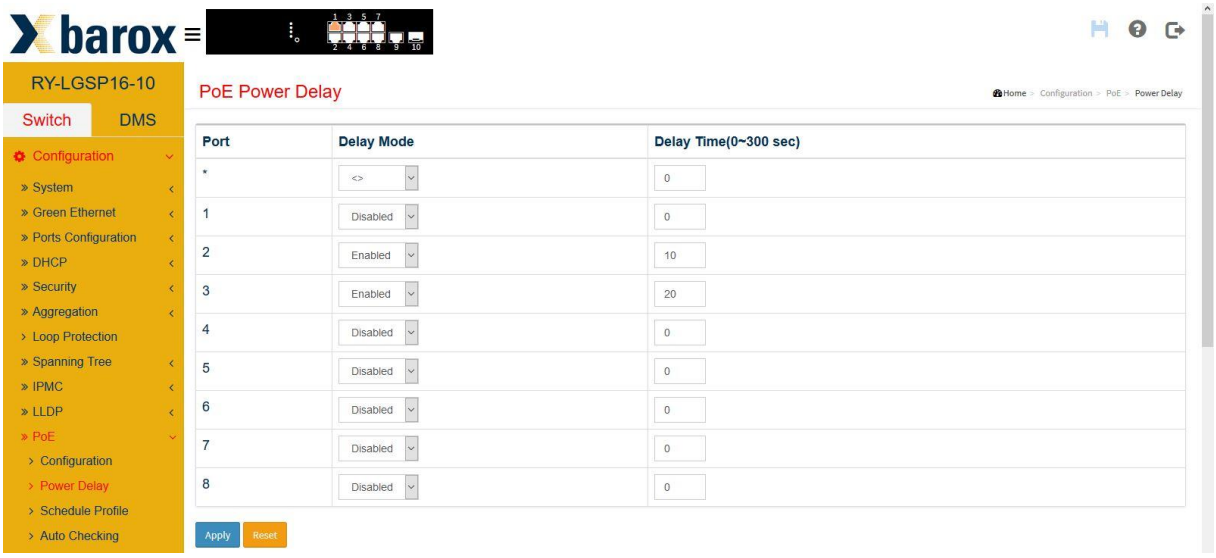
As already mentioned, the switch can provide a limited amount of power.

However, today’s IP cameras require an ever-increasing amount of power. If a pan/tilt camera with an integrated heater and IR emitter is used, the amount of power required will climb even higher.

When rebooting, switching between day and night mode, turning on the heater or IR emitter etc., a camera needs considerably more power (peak power supply) than during steady, uninterrupted operation.

Should several cameras connected to one switch all log in at the same time, the maximum amount of power that can be supplied by this switch might be exceeded. Exceeding this maximum power level will cause the switch to immediately log itself back off and may also cause damage to the power supply, if numerous unsuccessful attempts are made.

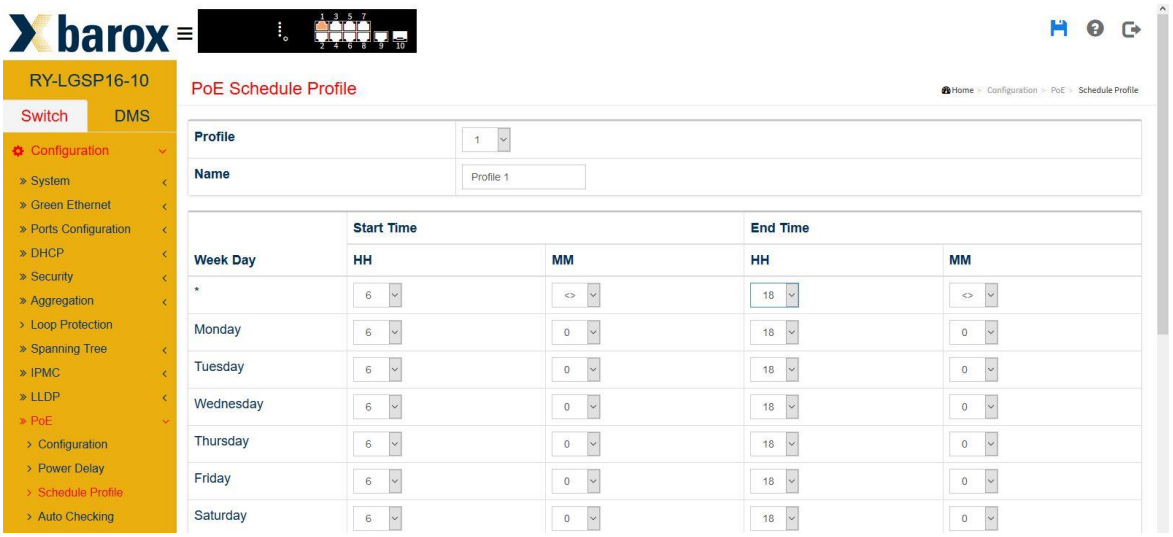
To avoid this problem, one can configure the individual ports to start up one after the other in the following menu. In the example below, ports 1 and 2 are immediately activated − with 2 more ports then being activated every 10 seconds after that.



3.11.3. PoE Schedule

Turning the power on and off can also be controlled using a weekly schedule. Up to 16 different profiles can be created. Each individual port can be allocated to a specific profile.

In the following example, PoE is turned on every day from 06:00 to 18:00 Hrs. in Profile 1.

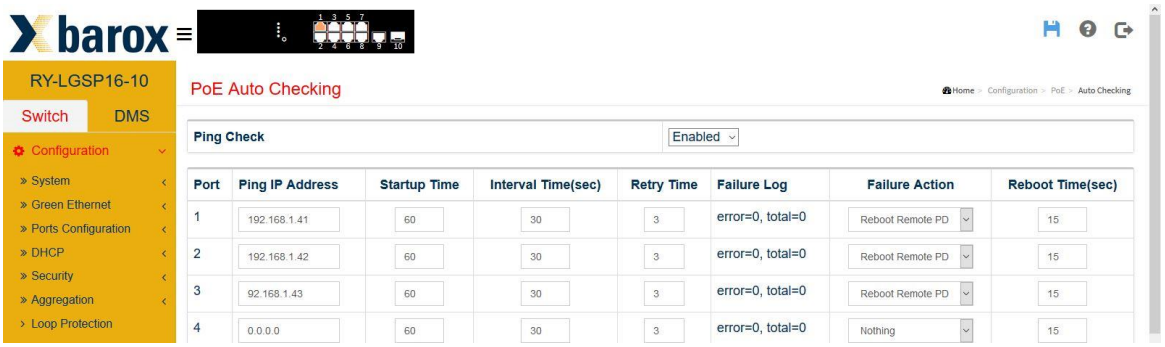


3.11.4. PoE Auto Checking

PoE Auto Checking is used to monitor functionality. For example, the camera connected to port 1 with IP address 192.168.1.25 can be pinged every 30 seconds to check its availability.

After 3 failed attempts, PoE to port 1 is turned off and turned back on after 15 seconds. This forces the camera to reboot.

60 seconds after the camera has rebooted, the ping monitoring mechanism will kick in again.



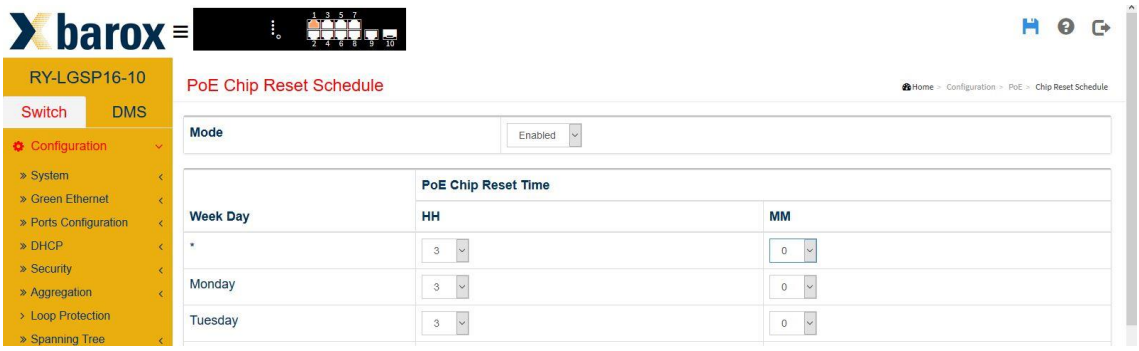
3.11.5. PoE Chip Reset Schedule

Sometimes a camera can still be pinged although it is showing no picture.

In most devices, PoE is managed by a separate chip. This means that the CPU might still reply to a ping although the video stream is no longer being transmitted.

As a preventative measure, the PoE Chip Reset command can be sent daily or once a week, for example at 03:00 Hrs.

This command causes the PoE chip in the camera to reboot.

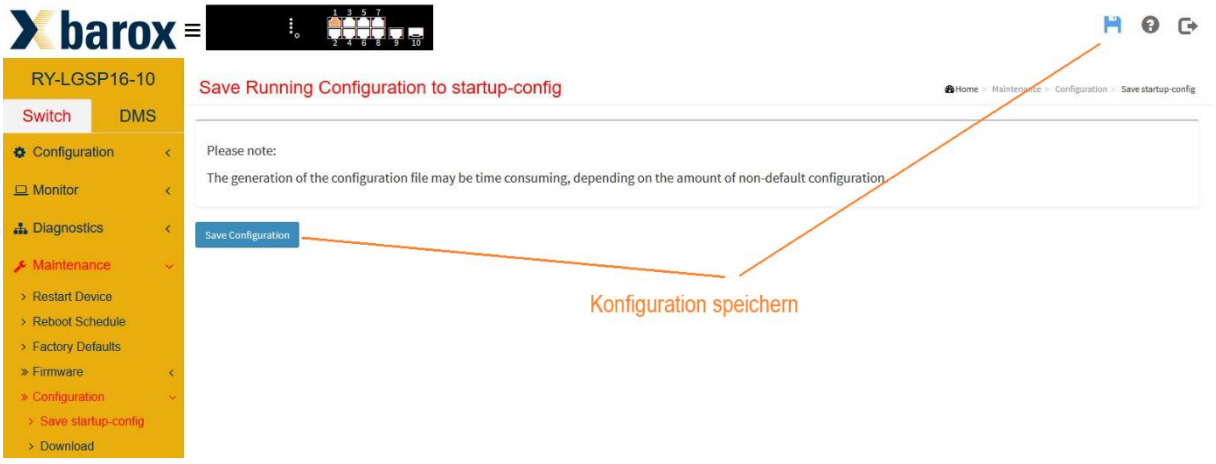


3.12 Saving and Retrieving the Configuration

All changes must be saved. Clicking on “Apply” saves the change to the memory. However, if the device is rebooted, the memory is deleted and all these changes are lost. This means that all changes need to be permanently saved.

There are two ways to do this:

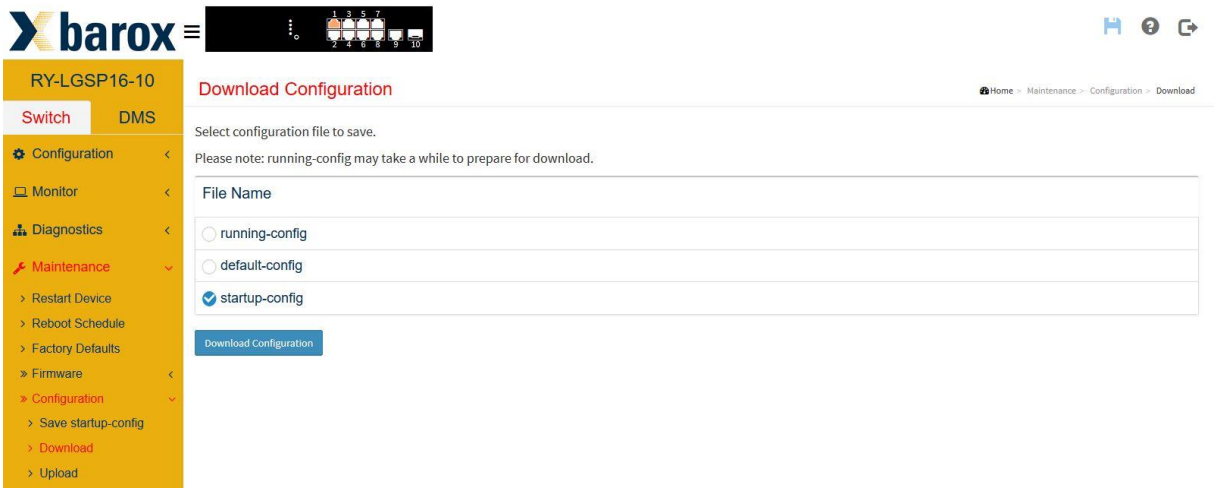
- Diskette symbol on each screen
- Maintenance/Configuration/Save startup-config menu item



3.12.1. Download Configuration

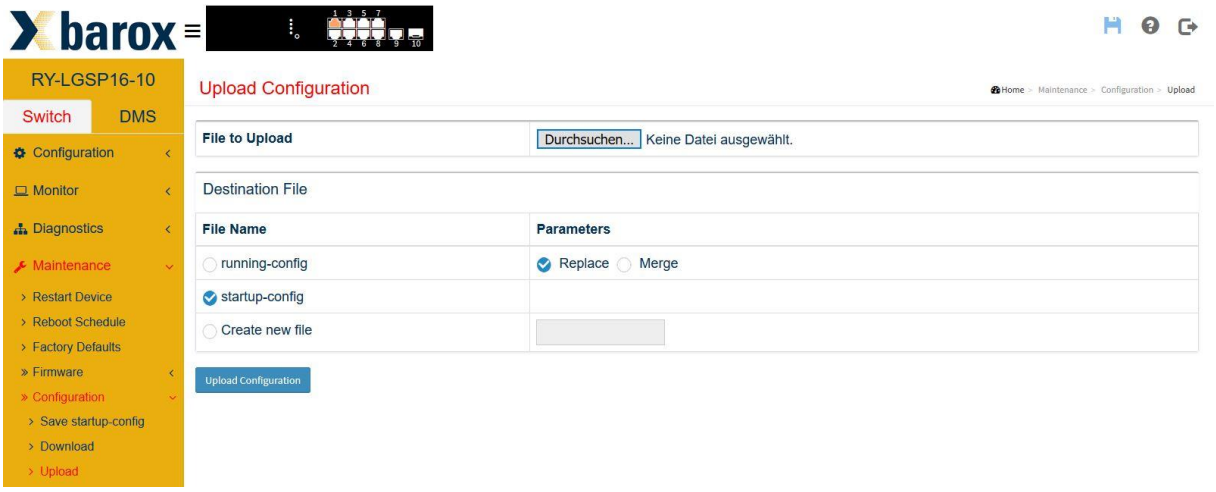
The current switch configuration can be downloaded and saved separately. The configuration file thus generated can be uploaded, if the switch is replaced, or used in cases where several switches are to be identically configured and only the respective IP address changed. That saves a huge amount of time.

We strongly recommend saving the “startup-config file”.



3.12.2. Upload Configuration

The opposite scenario is uploading a configuration file to the switch. In this case, the path where the file is stored and the respective file type need to be specified. As a rule, this is the “startup-config file”.



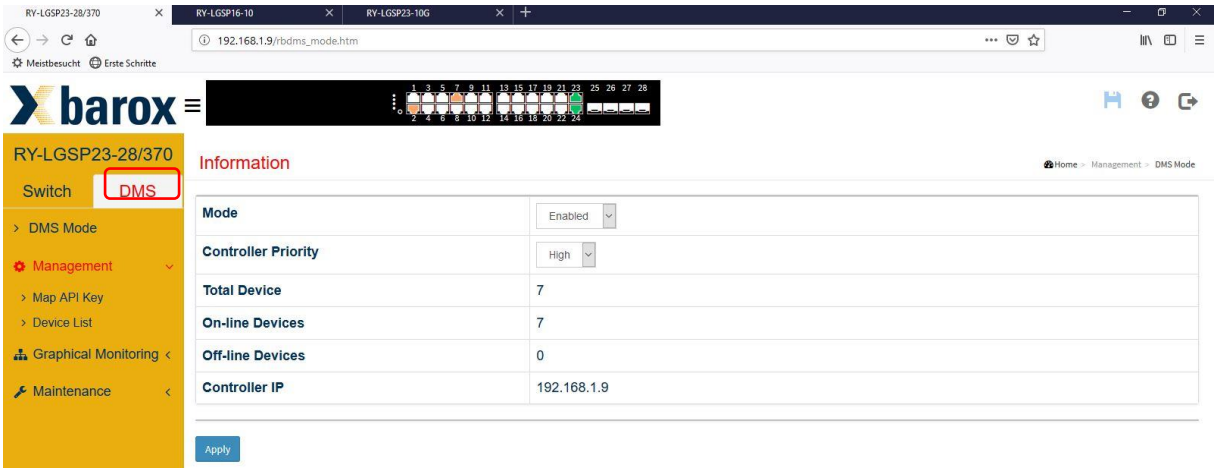
4 DMS Device Management System

The switch is equipped with an integrated network monitoring and control system that uses a very simple method to provide the user with an excellent overview of the whole network. The network topology view provides a quick overview of all the switches and terminal equipment in the network, e.g. IP cameras and servers, together with information on their respective IP addresses, device types and device descriptions. Plans showing the floor layout and the local environment can be stored as background images. These allow the user to quickly access specific network equipment − even without special knowledge of the IP structure. Finalised plans can then be exported and included in the documentation.

4.1 Management

To use DMS functionality, one needs to switch over to the “DMS” tab. DMS is activated as a factory default. The Information page (Management/DMS Mode) shows how many devices have been recognised in the network, how many of these are on-line (active), resp. off-line (inactive). Off-line devices are those that are either turned off or have failed (defective terminal device) or are no longer available in the network (e.g. service laptop that is taken home by the installation technician after having completed the configuration).

To be able to use DMS, one switch in the network must have been defined as the master. This switch collects all the information and then passes this on to all the DMS-capable switches in the network. The Controller IP field shows which switch (IP address) functions as the master.



Determining the DMS Master:

The mode „High” must be selected in the field „Controller Priority” of the switch, which is supposed to be the master. The definition of the most powerful switch for this task is recommended, as the DMS requires additional computing power. Further switches in the network can be rated as „Mid” or „Low” depending on their power capability.

The controller priority of a switch shall be set to „none” where a switch shall never be used as a switch master.

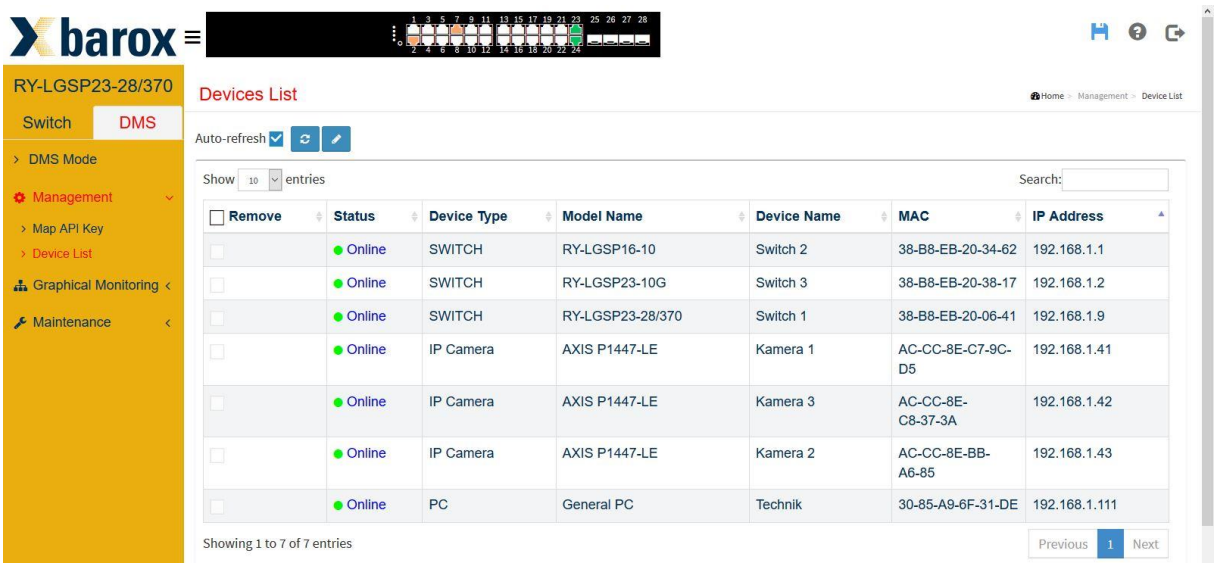
In case of a very high network load the DMS can be switched on at the switch with the lowest usage rate (and deactivated at the other switches), resp. Attention shall be paid as some functions can only be used in a limited way and this method is recommended in case of a homogenous structure using barox switches.

The master switch can be determined using the IP address in the line „Controller IP“.

Devices List

This page shows all the devices that are either online or offline in the network. The device type, status, device name as well as the MAC and IP addresses are provided in tabular form.

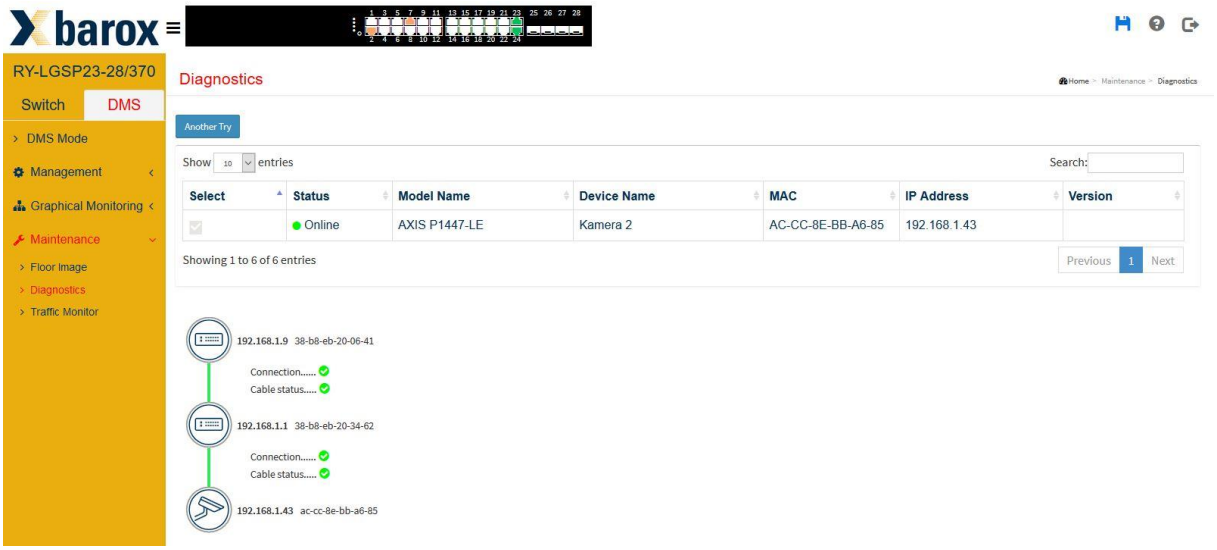
All the devices − including those with IP addresses in other network segments − are listed. This useful function helps when a non-configured device is integrated into the network, the IP address of which is unknown.



The connection to a device can be checked − even across a row of switches − simply by clicking on the “Online”, resp. “Offline” symbol in the “Status” column.

Should there be in interruption anywhere in the connection chain, this can be seen here.

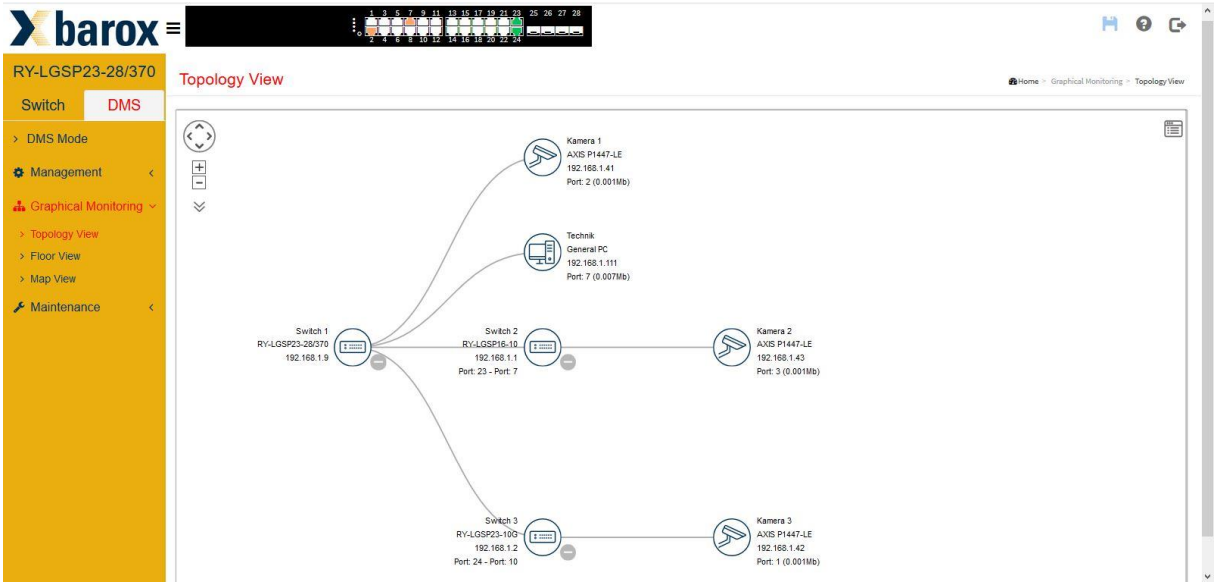
The same information can be checked using the “Maintenance/Diagnostics” menu.



4.2 Graphical Monitoring

Topology View

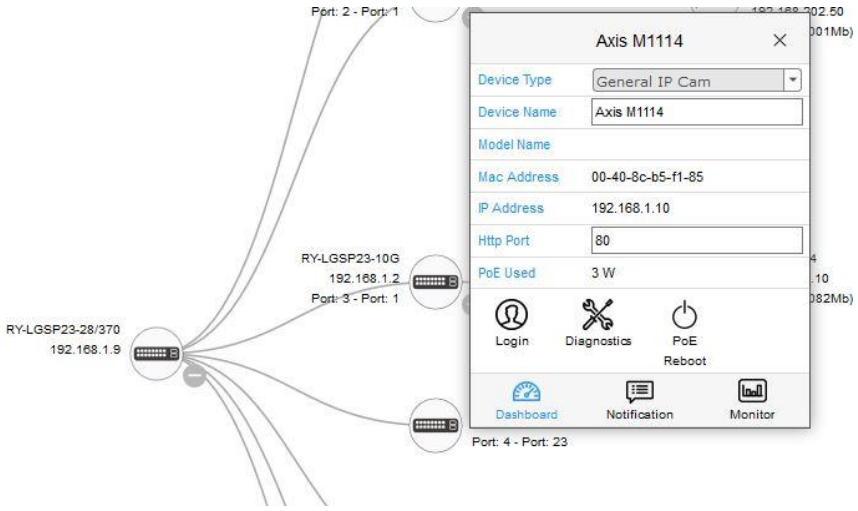
In the topology view, the whole network, incl. all the connected IP terminal devices, is automatically displayed in a diagram. If a terminal device is correctly recognised, it is represented by a corresponding symbol (camera, switch, access point etc.). All the respective information, such as device name, IP address, data rate etc., are displayed next to the symbol. All the settings can also be manually configured.



By clicking on a symbol, the “Dashboard” of the respective device is displayed.

In this “Dashboard”, the device type and name can be defined. The MAC and IP addresses as well as the real-time PoE requirement, in as far as the device is a PoE appliance, can also be read.

Additionally, by clicking on “Login”, the device can be directly accessed or diagnostics on the connection carried out. The PoE appliance can also be easily rebooted by simply clicking on the “PoE Reboot” icon.

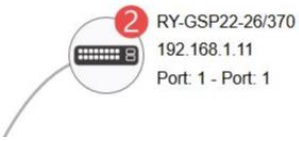


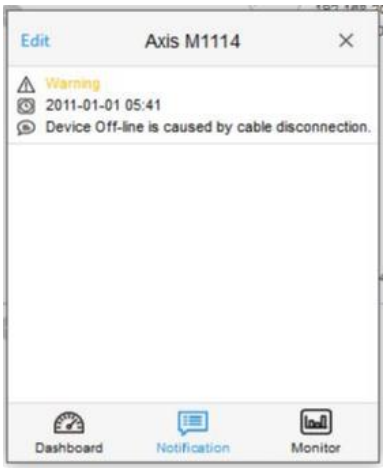
If a device

- was briefly unavailable (defective cable, appliance disconnected etc.)
- was not immediately viewable via ONVIF
- was connected using an existing IP address
- etc.

a red number appears next to the symbol. The red figure shows how many messages have been generated for this device.

By clicking on “Notification” in the menu, these messages can be read and edited.





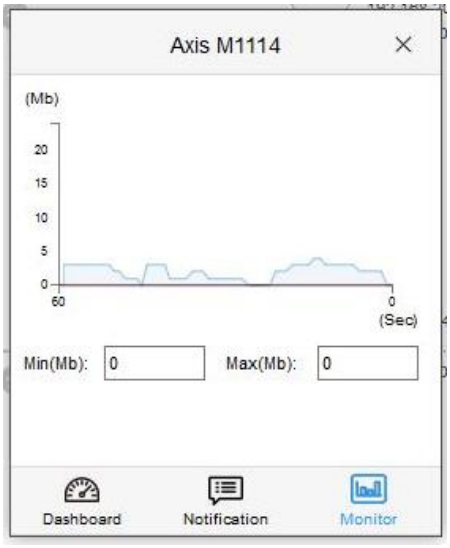
If a device is no longer available in the network, it is shown in red in the topology view and the “Remove” symbol is made available in the “Dashboard”. By clicking on “Remove”, this device is permanently removed from the topology view.

It is vital to select “Remove” when, for example, a defective camera is to be replaced by a new camera using the same IP address. The switch not only stores the IP address but also the MAC address. If the old IP address is not removed using the “Remove” tool, the switch expects the old camera with its original combination of IP and MAC address to return and will set the new camera back to the default IP address over and over again despite this having the same IP address. This occurs because the new camera has a different MAC address.

Another useful tool is the “Monitor” feature.

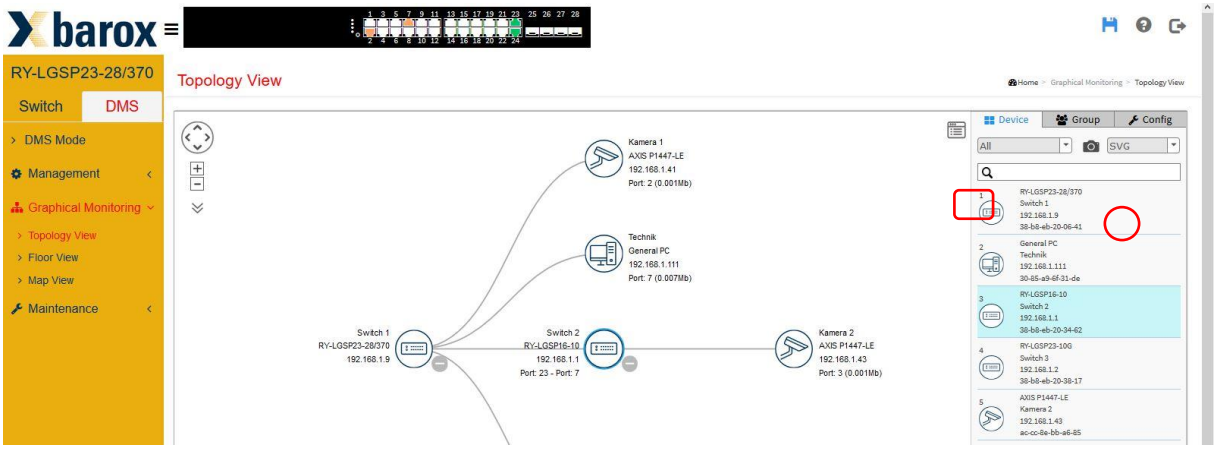
This shows the data flow (e.g. from a camera) in real time.

The thresholds within which the data flow should move can be set using Min(Mb) and Max(Mb). This means that one can see at a glance whether everything is alright.



At the top right of the topology view screen, there is a “Device” icon which can be used to display all the devices at once.

When an entry in the list is clicked on, the corresponding device is displayed in blue in the network diagram.



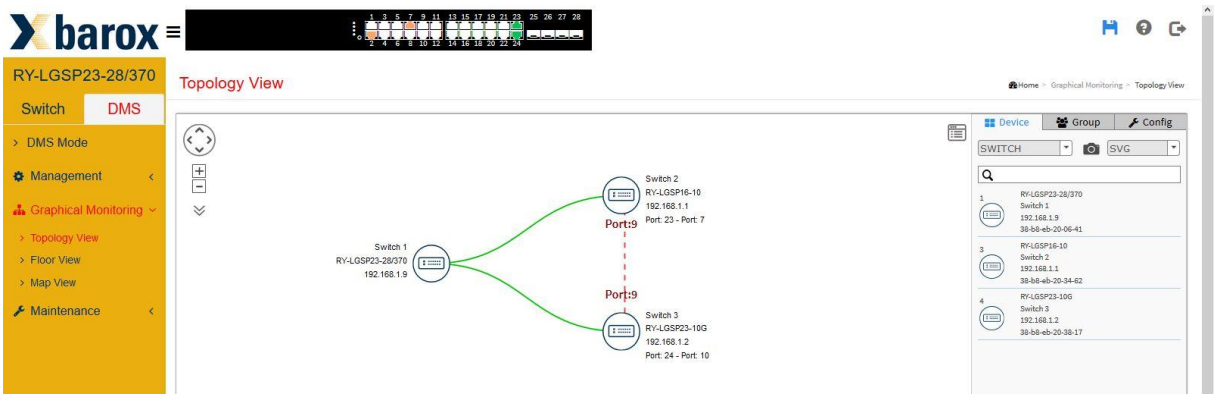
This tool also offers the option of printing out the network plan in SVG or PNG format − or directly to a PDF document. This requires first selecting the format and then clicking on the camera symbol.

The topology view provides the option of presenting the ring structure. To do so the list „Switches” must be selected in the tab „Device“. Following this the ring is displayed using a dashed red line showing the defined link and the ports, which are defined as alternative ports.

Two conditions must be fulfilled for this representation:

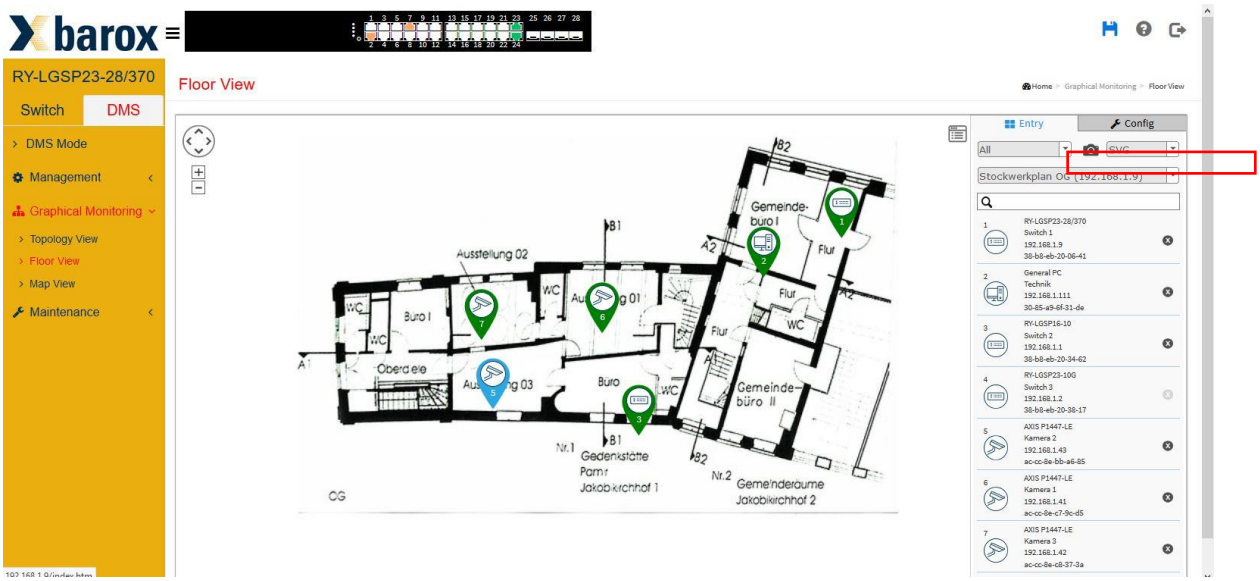
a) RSTP as ring protocol

b) The ring only consists of RY switches supporting the DMS



Floor View

Uploaded, resp. imported building and floor plans and/or plans of the local environment can be viewed in the floor view. This serves as a foundation, resp. background image, for portraying the network setup. This function provides a good guide for carrying out on-site tasks and can also be printed out to document the system, as described above.



To position a camera or switch in a plan, all that needs to be done is to click on the respective device in the list to select it and then to position this device in the plan − done.

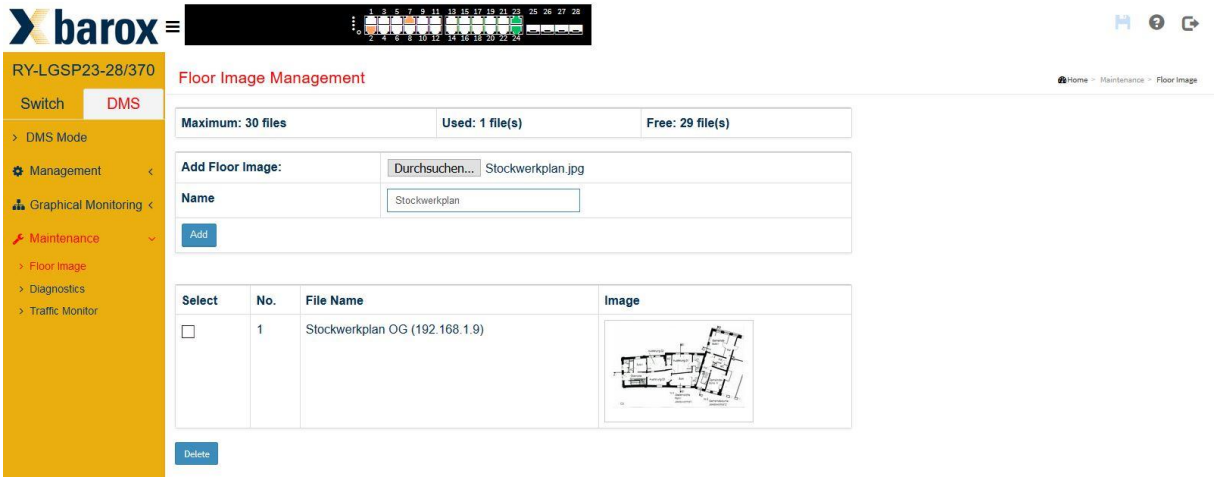
Map View

The same function is also possible using Map View. The background image is directly generated using Google Maps. This requires an internet connection and Google licences for using the service.

4.3 Maintenance

To use a plan as a background image, one needs to switch to the “Maintenance” menu.
The path and file name must be entered in the “Floor Image” menu and then uploaded using “Add”.

The uploaded plans are then listed in the lower section of the web page. Up to 50 files can be saved.



Diagnostics

This function was described and explained on page 25 under the heading “Devices List”.

Traffic Monitor

ATTENTION: Traffic monitoring is not supported by industrial switches.

Another useful diagnostics tool is the traffic monitor. The traffic of each individual port over a 24-hour period is displayed in the “Maintenance” menu.

The upper bar chart shows all the ports and all the data sent and received by each port during the course of the day. One can choose between displaying the information for a specific date or in a day or week view.

If one now clicks on the bar of any individual port, the amount of data transmitted − and when − is displayed in a diagram below on a scale of 0 - 23 Hrs.

This may be extremely useful when looking for the cause of errors, for example, if one sees that at 12 a.m. a large volume of data was generated at port 2 when there were problems with the recording process.

5 Switch Management in the Security Focus

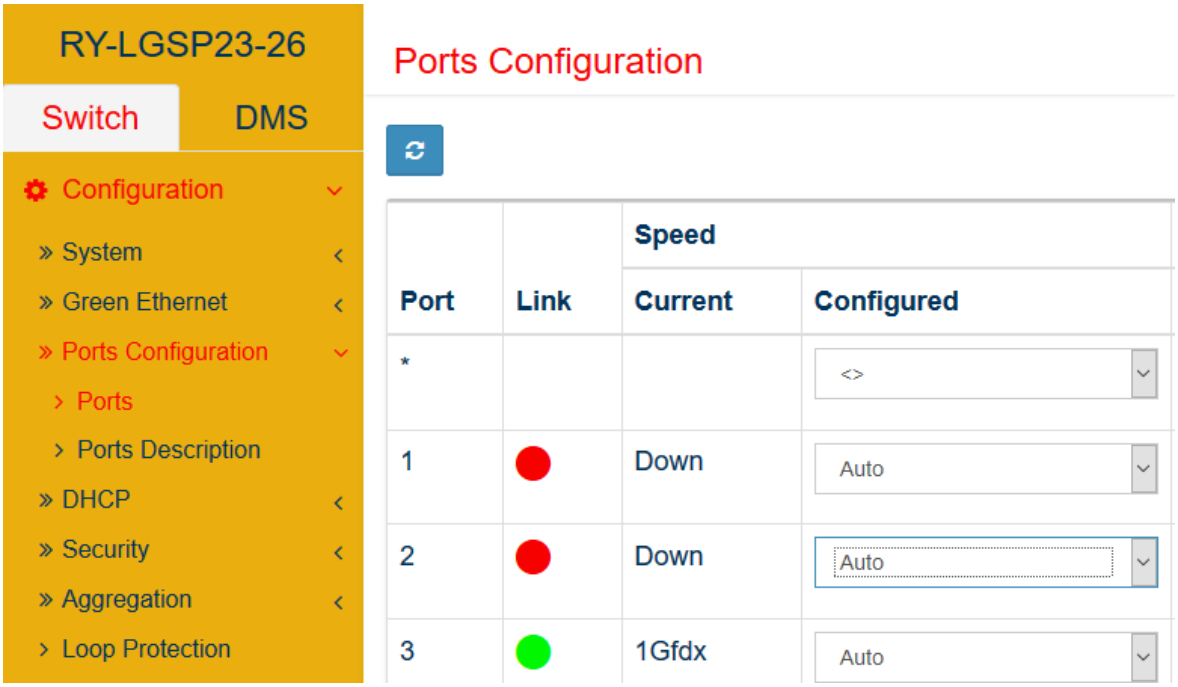
The following topics shall provide information on content and configuration of the extended network settings and the security. Knowledge and skills on commissioning such like IP configuration, login and VLAN configuration are basic preconditions for the configuration.

5.1 Management and Security on Switch Level (Layer 1 and 2)

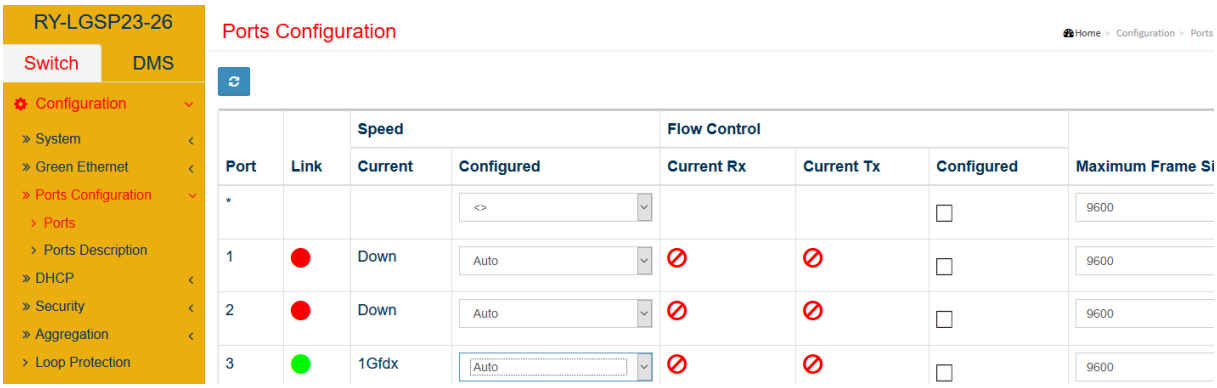
5.1.1. Bandwidth Settings and Restrictions

Port-based Ethernet settings

The manual selection of the required ETH standard is required in some scenarios. For example in case of a connection of network components, which do not provide an automatic negotiation of the standard or because of certain deployment scenarios, which demand a reduction of the ETH standard. The settings 10/100/1000/10000 FDX/HDX (ETH standard depending on the model) can be selectively set per port using the web GUI as illustrated thereafter.



Some applications require the adjustments of the Ethernet frame sizes. This can also be done in the menu section „Ports Configuration" in the field „Maximum Frame Size" as described in the following screenshot.



! Important, when setting the frame size: Please pay attention to set the exact values in order to avoid malfunctions!

5.1.2. Information regarding the general consideration of the bandwidth demand

The consideration of the following items is recommended when planning the bandwidth demand and the related deployment of suitable barox switches:

- Deployment of the required Ethernet standards (10/100/1000/10000) under consideration of possible terminal device upgrades
- Planning of reserves, scaled at the backplane power of the switch -> 30 % are frequently recommended
- The maximum Ethernet specification per terminal device shall be considered when calculating the demand

5.1.3. Securing the ports using MAC configuration settings

The MAC table

Besides the automatic management the MAC table can basically also be adjusted manually. This is often required where certain network terminal devices require a static allocation with regard to VLAN and port. Furthermore the manual allocation provides a basic protection and scalable access restriction, resp.

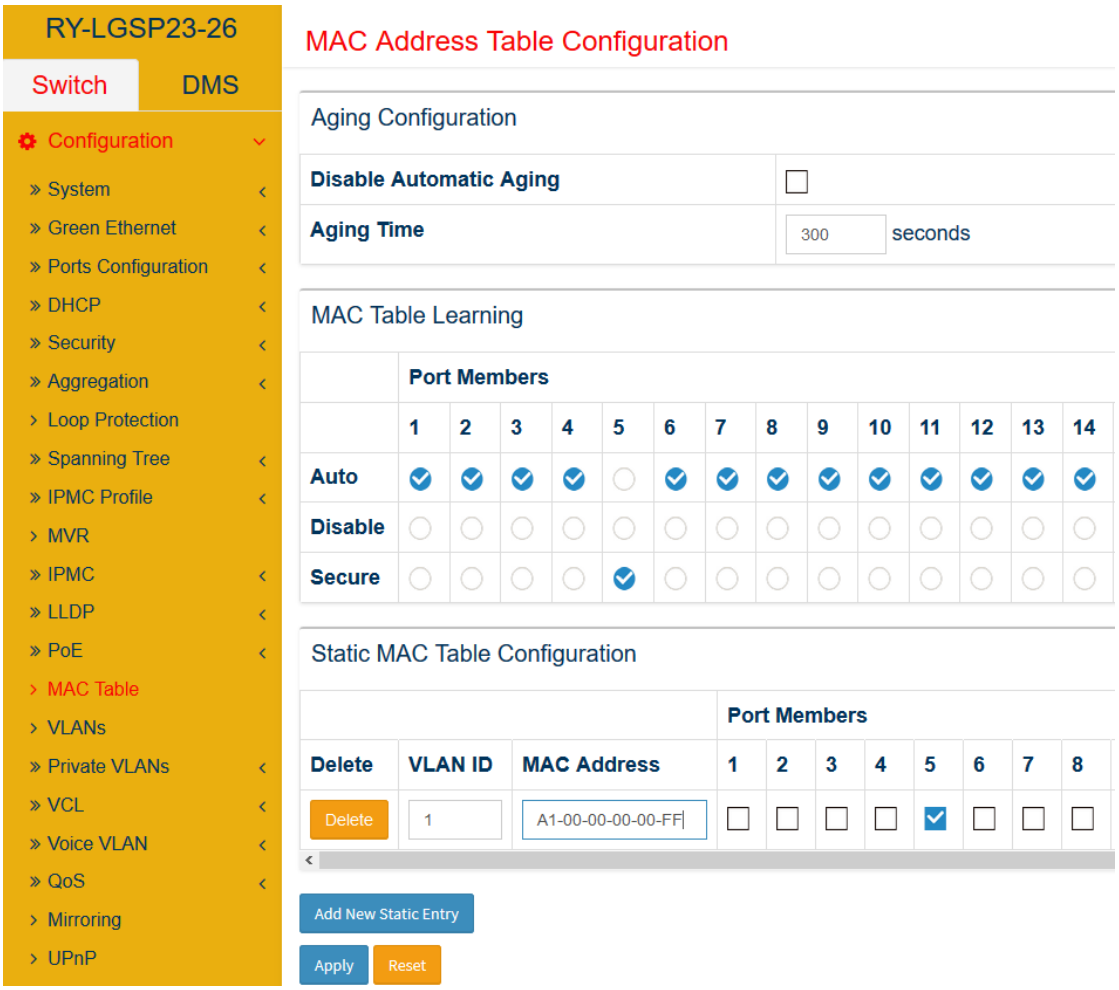
MAC Filtering and Port Configuration

Example configuration of a static MAC table:

The device with the MAC address A1:00:00:00:00:FF shall only be capable to use port 5 in VLAN1 for a connection.

1. Selection of „Add New Static Entry“ in the menu Switch -> Configuration -> MAC Table
2. Input of the VLAN ID, MAC address and setting the port members 5 in „MAC Table Learning“ to „Secure“
3. Confirmation of the entries by clicking „Apply“

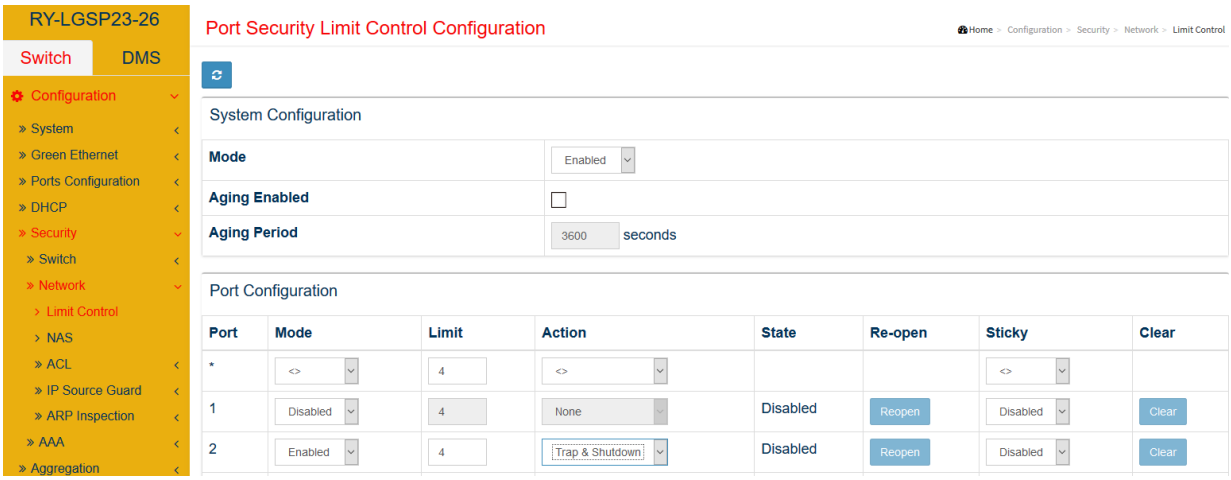
The following screenshot explains this.



The protection using MAC filtering provides a simple protection against an unwanted network access. Nevertheless it does not e.g. protect against the widely spread attack type „MAC-Spoofing“.

5.1.4. Port Security with Limit Control Settings

The use of Limit Control is recommended where unmanaged switches with terminal devices are connected to the barox switch. Basically this function prevents the blocking of the network communication of further unwanted IP/Ethernet terminals which are connected to free ports of the unmanaged switches. For planning purposes the complete number of network devices including the unmanaged switch, which are connected to the respective port of the barox switch, needs to be determined. E.g.: The total limit is 4 where one unmanaged switch with three further network terminals is connected to port 2 of the barox switch. The configuration must be activated first. Furthermore the respective port is activated, the limit is determined and the action selected, which applies in case of an exceedance. The learning of the terminal devices is activated and enabled using the *„Sticky”* function. During the configuration the devices must be physically connected to the barox switch using the port to be configured. The following screenshot shows a visual representation of the settings.



5.2 Use and Protection of IP Functions (Layer 3)

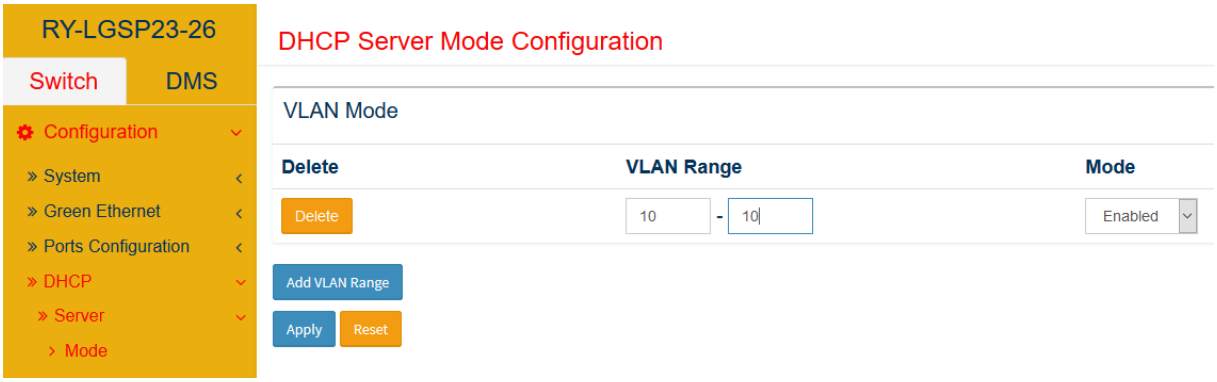
5.2.1. DHCP Server

Information regarding the use of DHCP servers in video networks

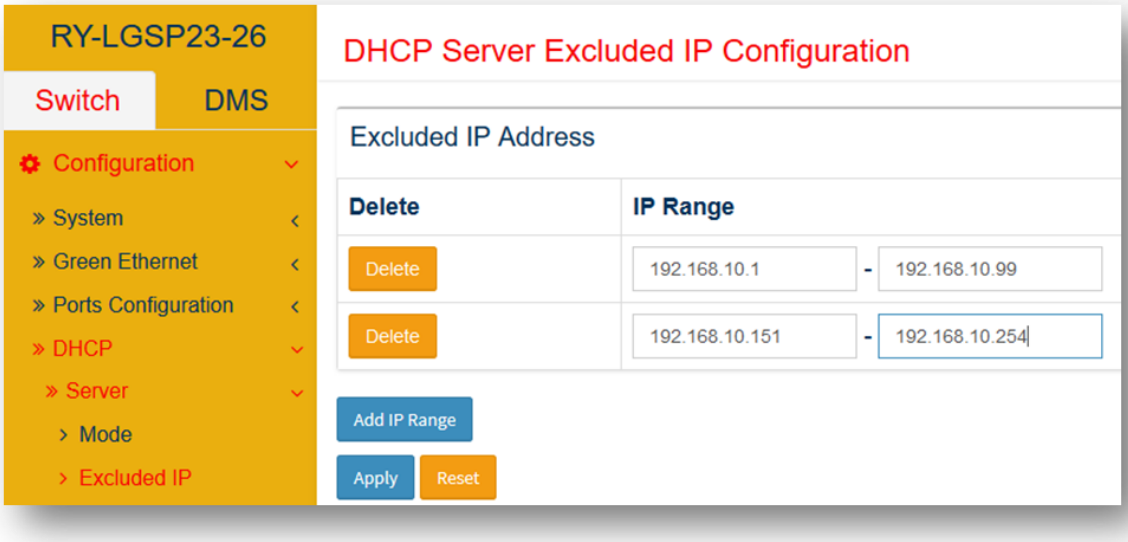
It has to be checked, whether the use of a DHCP server is generally required by the network design. This service provides the advantages of an automated network information distribution but also a variety of vulnerabilities.

Example of a basic configuration and commissioning of the DHCP service

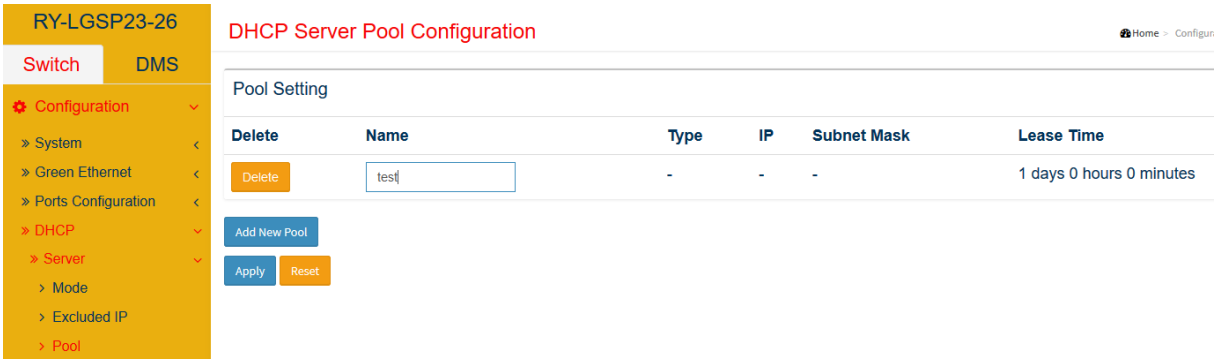
At first the VLAN range of the service is determined. Then the service is generally activated in the *Mode* with the setting *Enabled*. The service is activated by confirming the action as shown below.



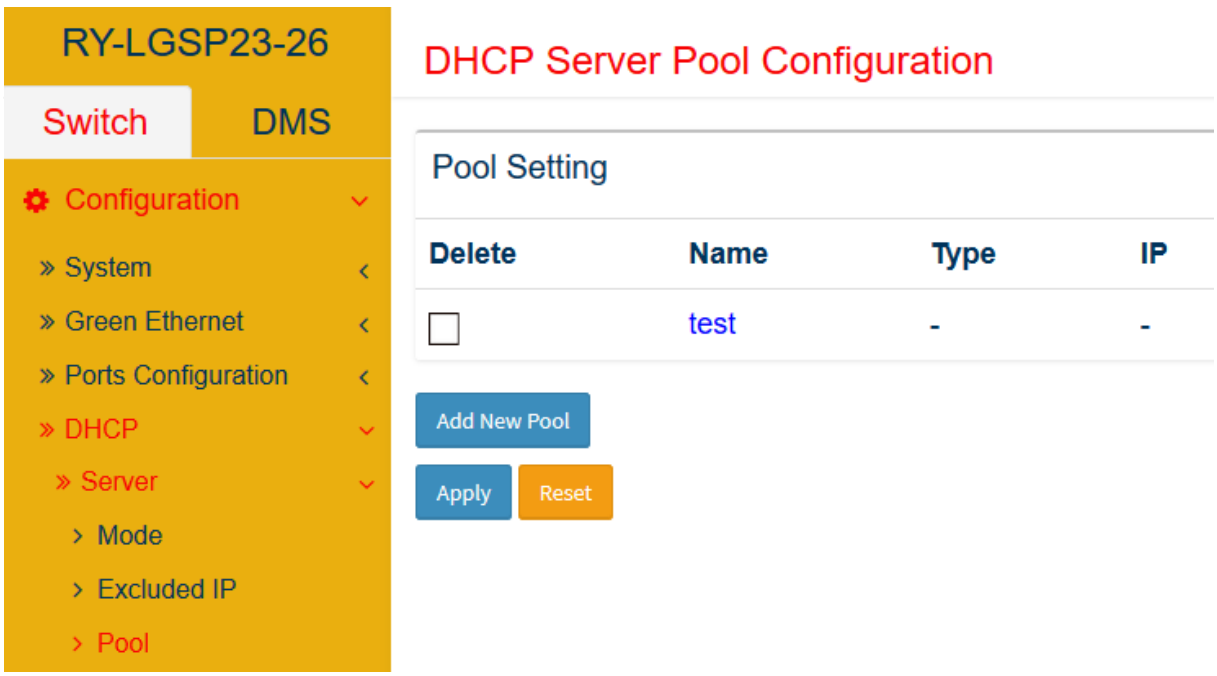
The setting of the IP address pool, which shall enable the distribution of 50 addresses, i.e. in the range of 192.168.10.100 – 192.168.10.150 by stating the surrounding addresses and IP ranges (exclusion procedure) to the IP clients in the respective VLAN is shown in the following screenshot.

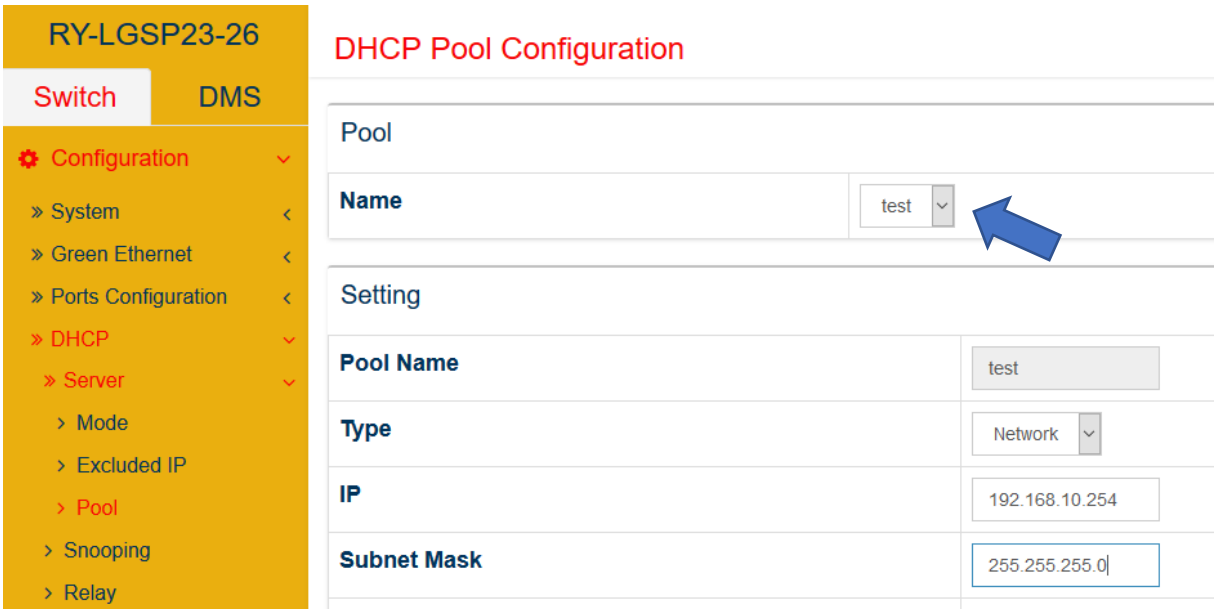


Following this a DHCP service name is determined and confirmed.



Following the determination of the name the settings are called up by selecting the name as shown below.

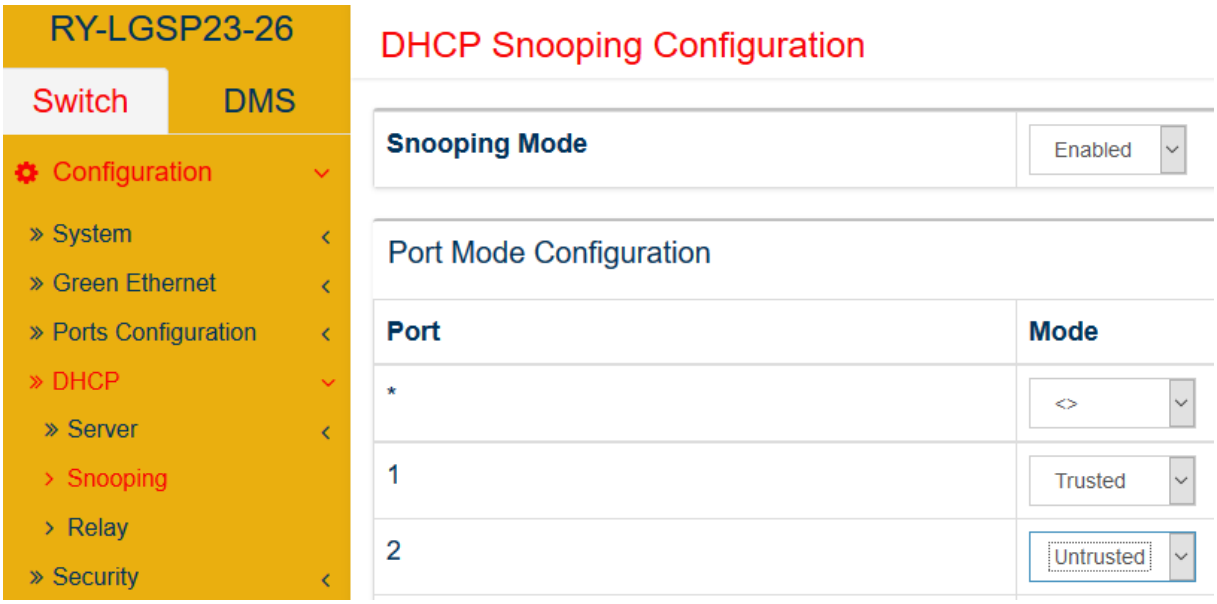




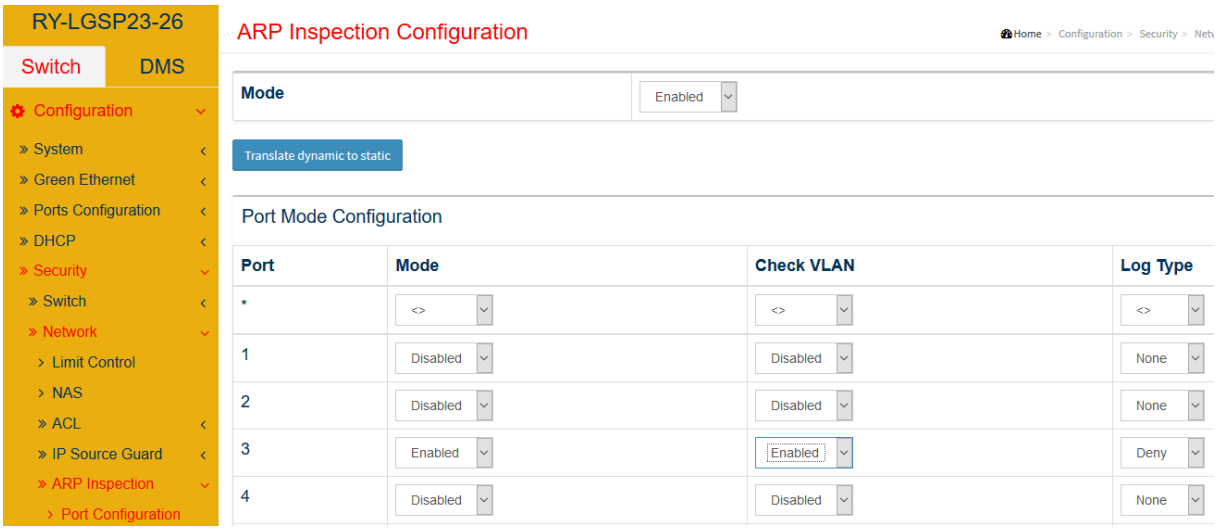
For the purpose of a simpler representation and reproduction, resp., only settings as shown above are required. Following this they are confirmed by confirming the configuration at the end of the page.

5.2.2. Protection of DHCP by ARP Inspection

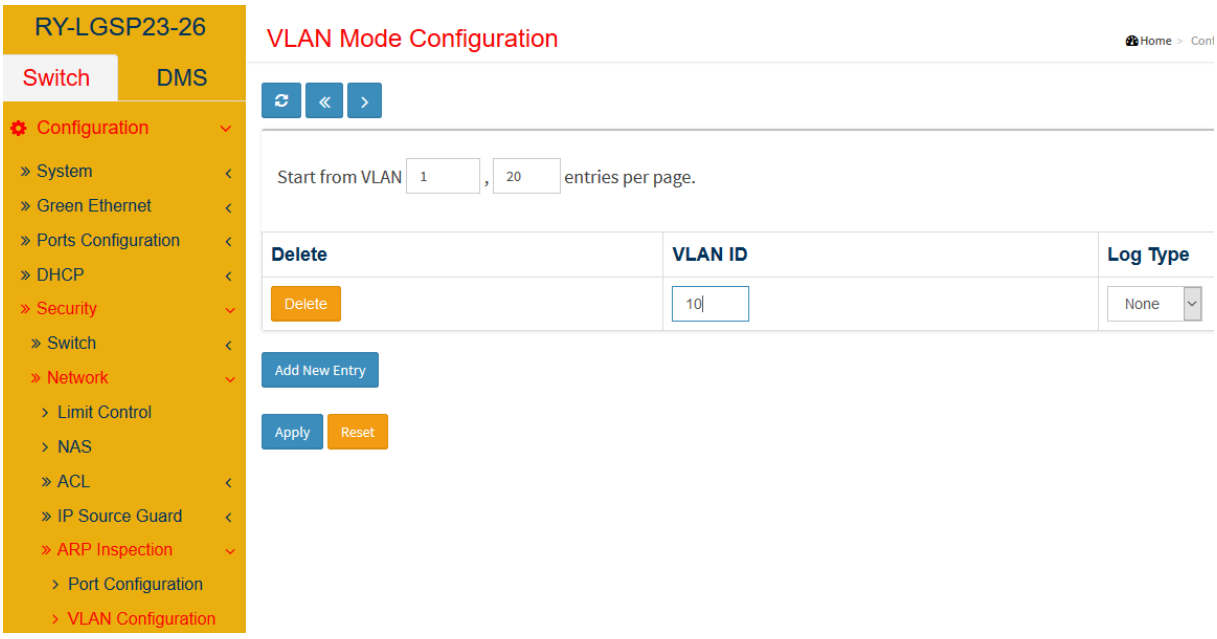
The protection against unwanted DHCP clients can be realised using ARP Inspection. Following activation of the functions the DHCP clients can be managed statically as recipients in a table. The setting of the size of the DHCP address pool using the number of clients is the basic precondition for a maximum security.
At first the Snooping function is generally activated in the menu *Snooping Mode* as shown below. Furthermore settings can be chosen for the trustworthy switch ports. The mode must be set to „Trusted“ for the inspection function to work.



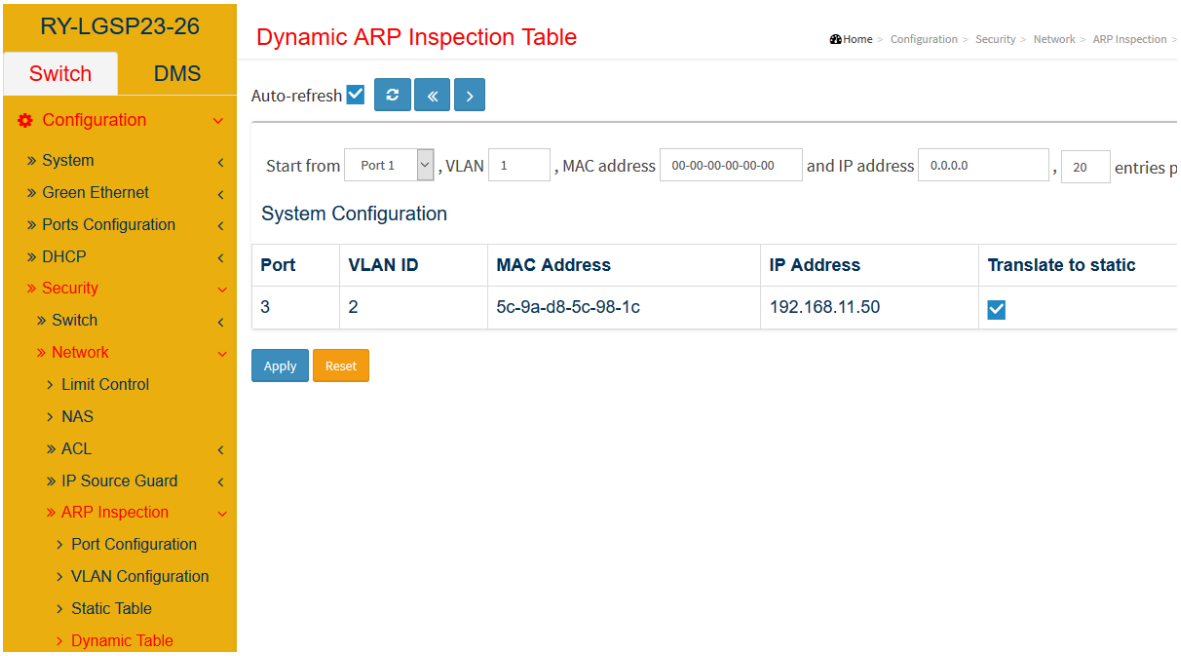
Furthermore the port parameters are activated and configured. The ARP Inspection is activated for port 3 as shown in the following example, the verification of the VLAN is activated and the log type is set to „none“.



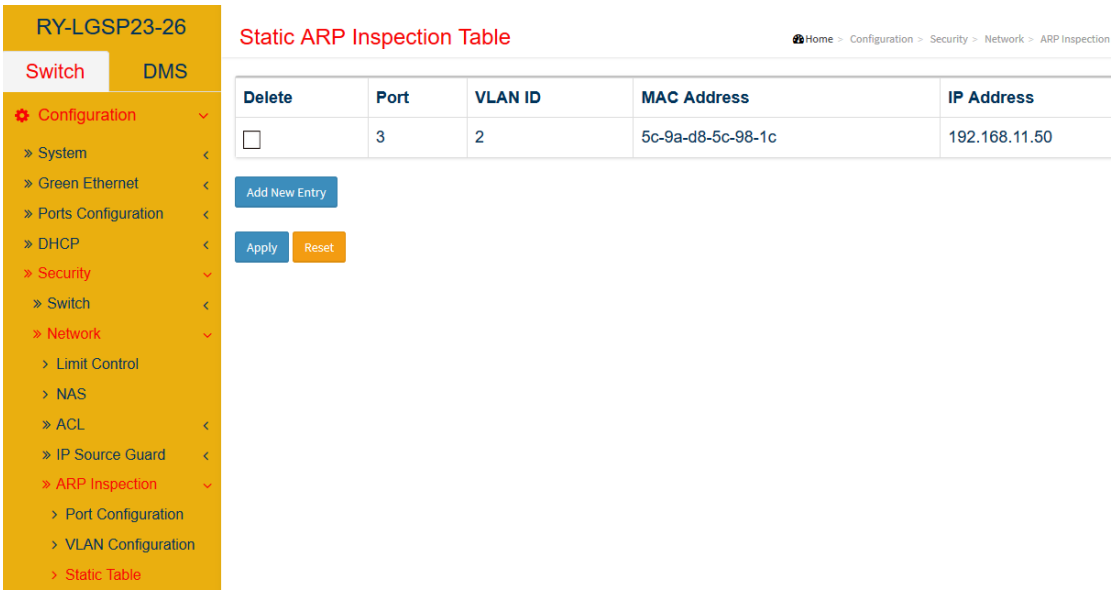
Following this the VLANs, which shall be included in the check, are determined and the log type (trust position) is determined as shown below.



The DHCP clients can be connected upon the completion of the settings. Following the distribution of the IP addresses by the DHCP service the clients and their layer 2 and 3 characteristics become visible in the dynamic ARP inspection table and can subsequently be translated into the static ARP inspection table.



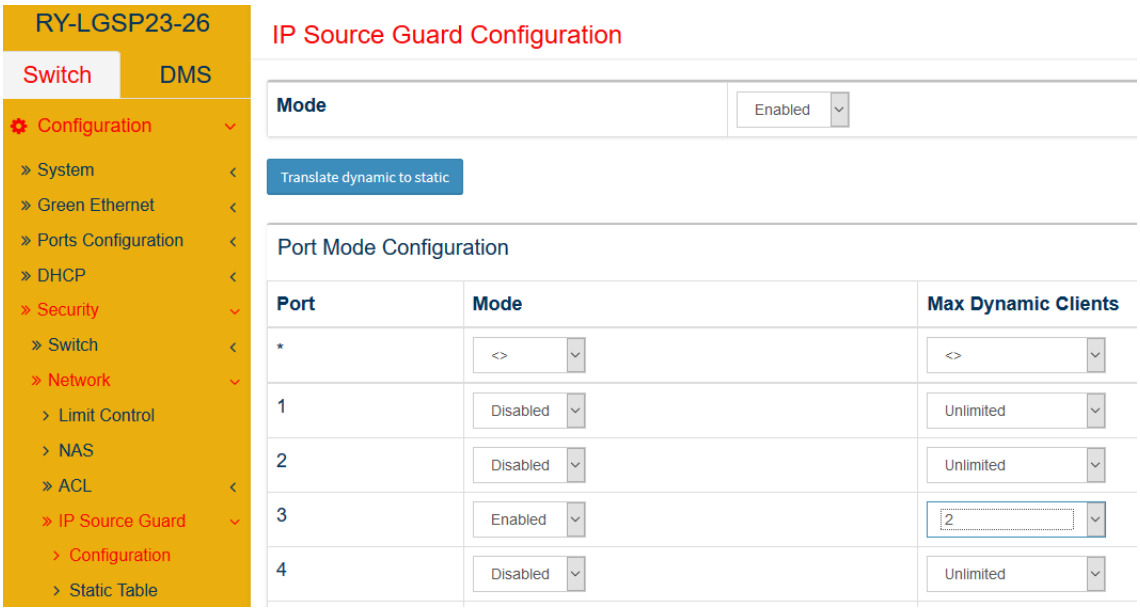
The following screenshot shows a static entry. An IP address is reserved for the client according to the table.



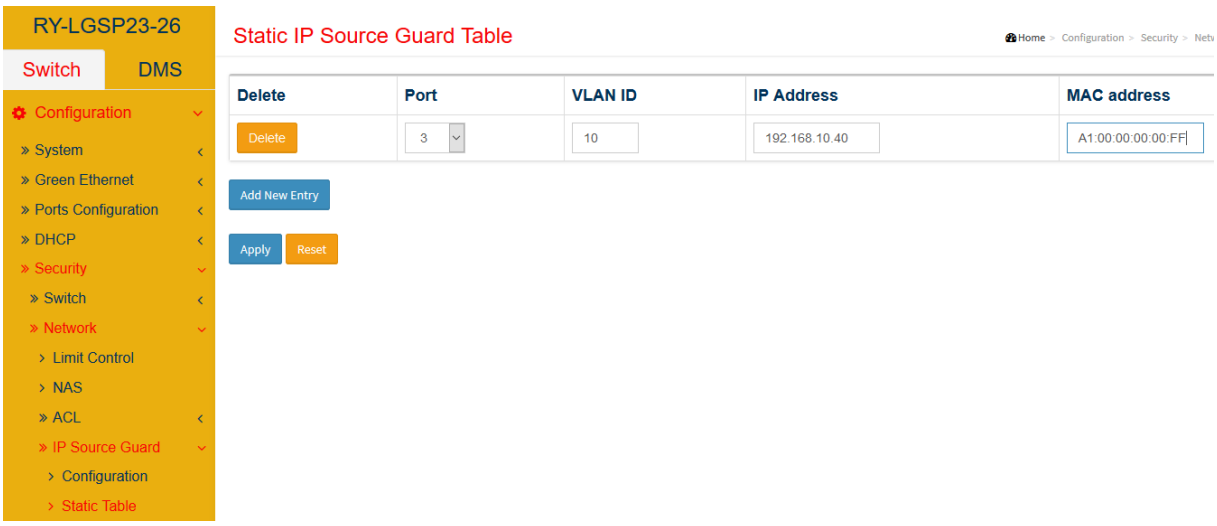
5.2.3. IP Source Guard

Deployment and Configuration

An extended function for the protection of the terminal side is provided by using the IP Source Guard function. This function links the predefined static IP address of the connected devices with the examination of the MAC addresses of the source terminal devices. As shown in the following screenshot this function is generally activated and can be adjusted on a per-port basis.



Once this function is switched on the configuration can be effected using static entries as shown below.



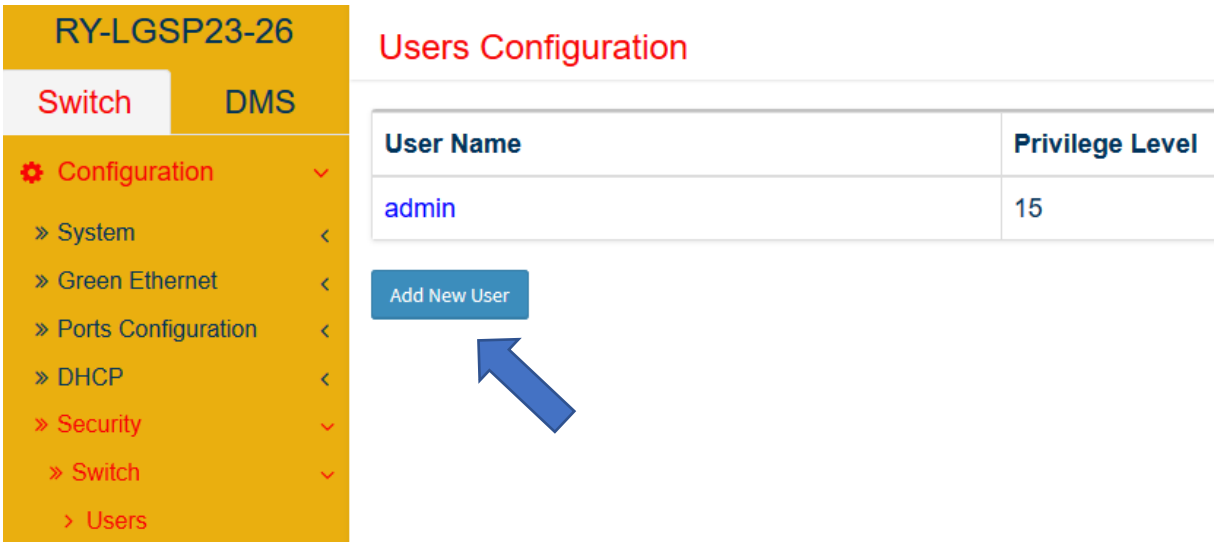
The use of IP Source Guard enables the extended protection function by securing the ports by means of the MAC and IP address. Compared to port security, where static MAC address entries per port prevent a potential attack, IP Source Guard provides the verification of the IP address of the connected device using static entries. The switch will block the port‘s network communication where the connected device does not comply with the allocated MAC and IP address. This means, that the attacker must know the MAC address and IP address of the device for gaining access to the network.

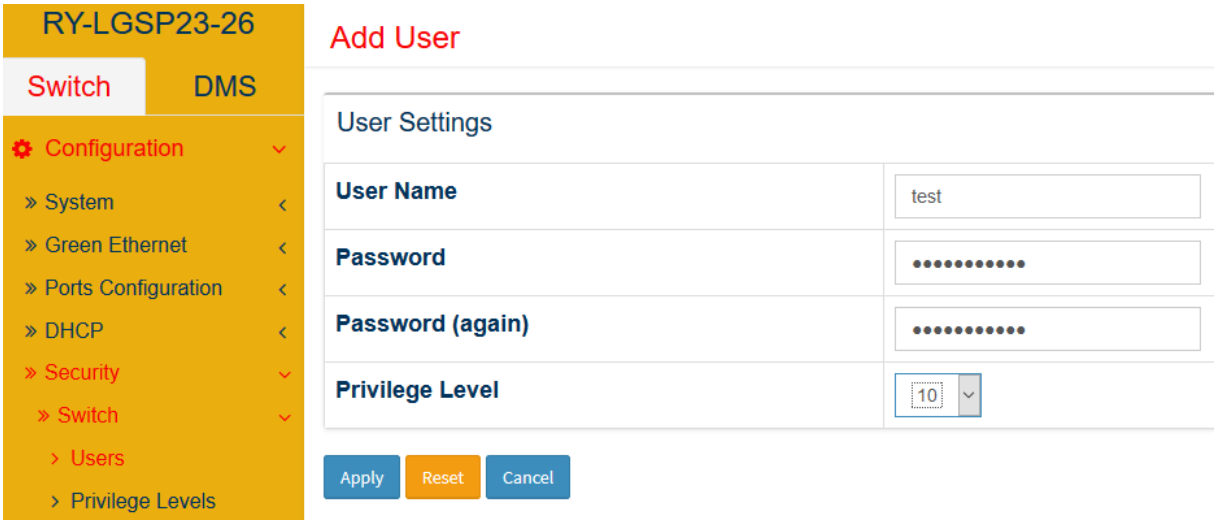
5.3 Protection of the Switch Management and Network Administration (Layer 3–7)

5.3.1. User Management and Configuration

User Generation

The following example shows the generation of a further user.

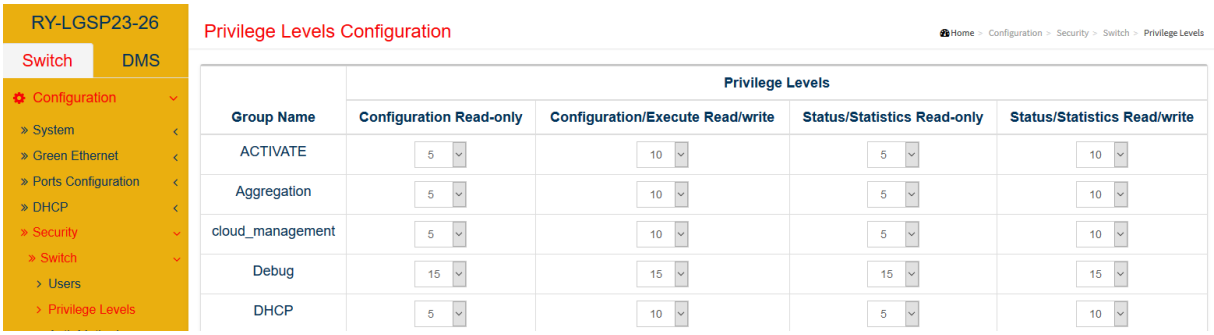




Basic settings of user rights and privileges

- The privilege level serves the purpose of grading the rights to apply configuration settings and read/write rights of such values, resp. It is generally recommended not to change the default values. Such rights should be allocated when generating new users.

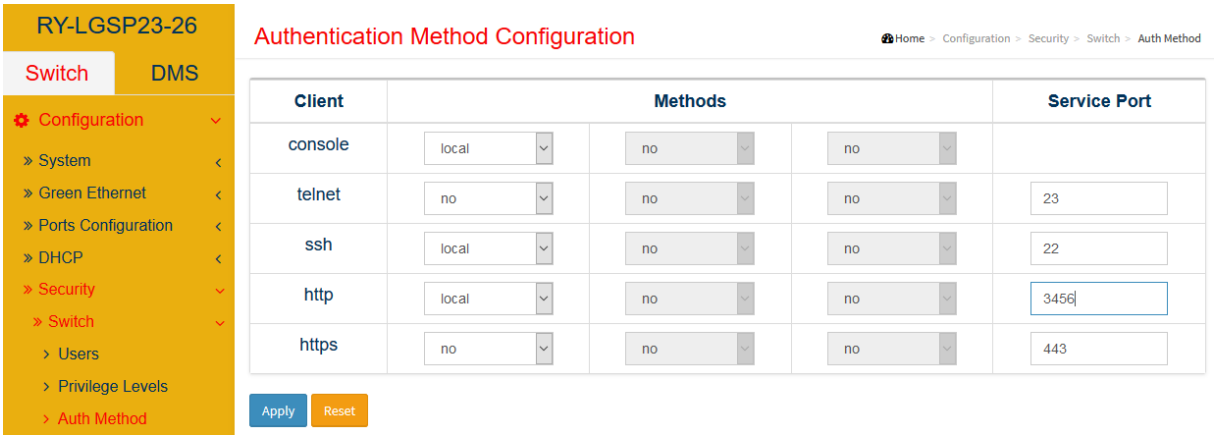
- Information: Scaling the rights of a further user on the basis of authorisation and competencies is helpful.



5.3.2. Deployment and Authentication Settings using the Switch Management

Securing access to the CLI **ssh** vs. **telnet**

The access method can be set and non-required functions can be disabled, resp., as shown below. The general deactivation of the Telnet access function is recommended where this is allowed by the network design. Configuration methods can be set as shown below.

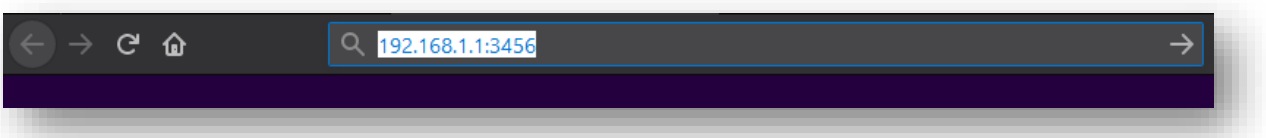


- The use of the SSH protocol for the command line-based management (CLI) is recommended, as this method provides the encrypted connection.

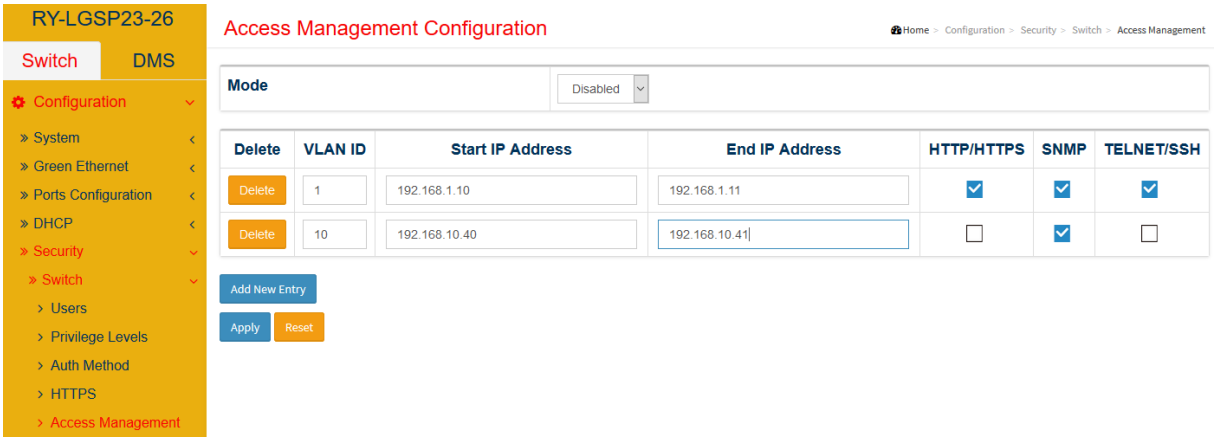
Management of the access to the web GUI using http

- The generation of a separate user for http is recommended.
- Change of port 80, information: Please pay attention to the port information when accessing via a browser!
- Access via HTTPs provides the highest level of protection due to the encryption of the connection.

The following example shows the entry of the management address using a changed port

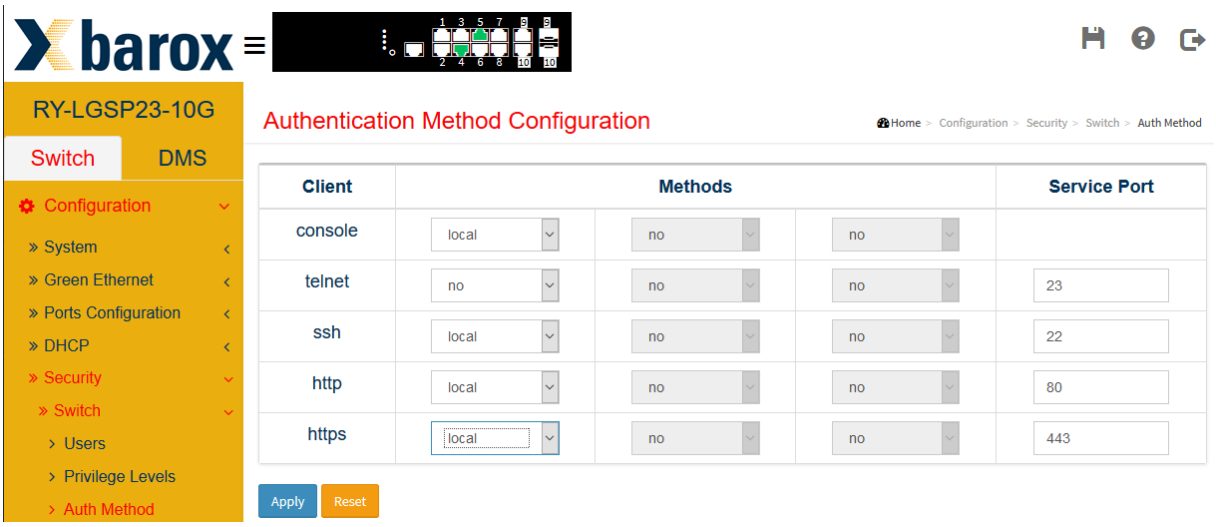


The restriction of the management access and its methods to certain IP address ranges and VLANs is possible. This can be effected in the access management as shown in the following example.



5.3.3. Access Management and Use of HTTPS

The setting option for using the HTTPS protocol is shown below.



The standard port can be changed also for this method.

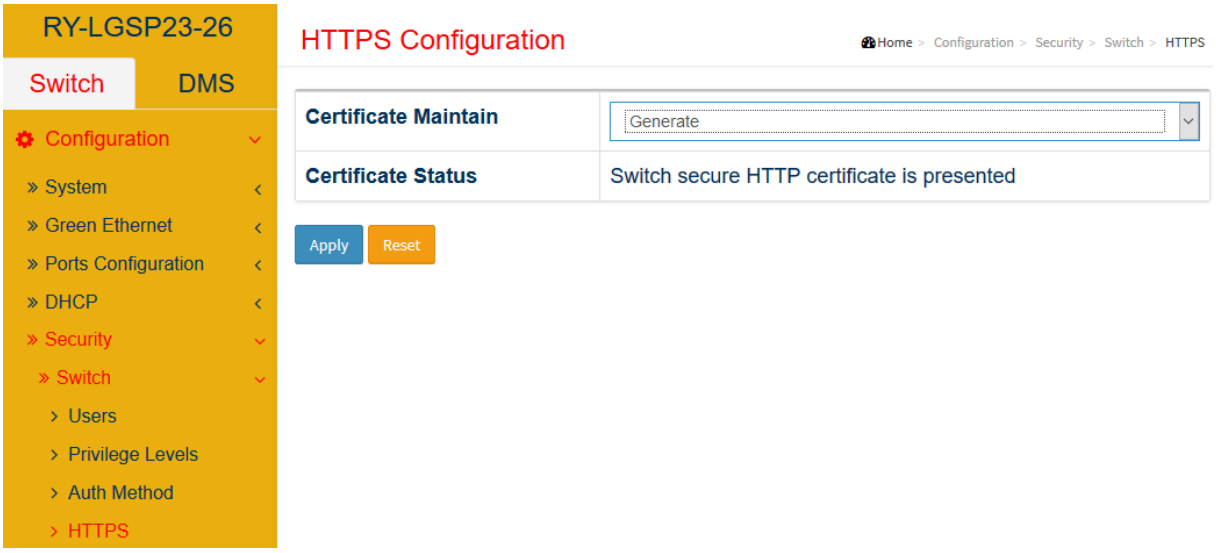
The http option should be disabled where this mode is activated. The switch GUI is called up in the browser using the HTTPS protocol phrase https://192.168.XX(IhreManagement IP):1234(IhrPort) in the URL field. Following this the browser communication to the management interface is effected using encryption.

5.3.4. Configuration and Use of Certificate-based Access to the Management

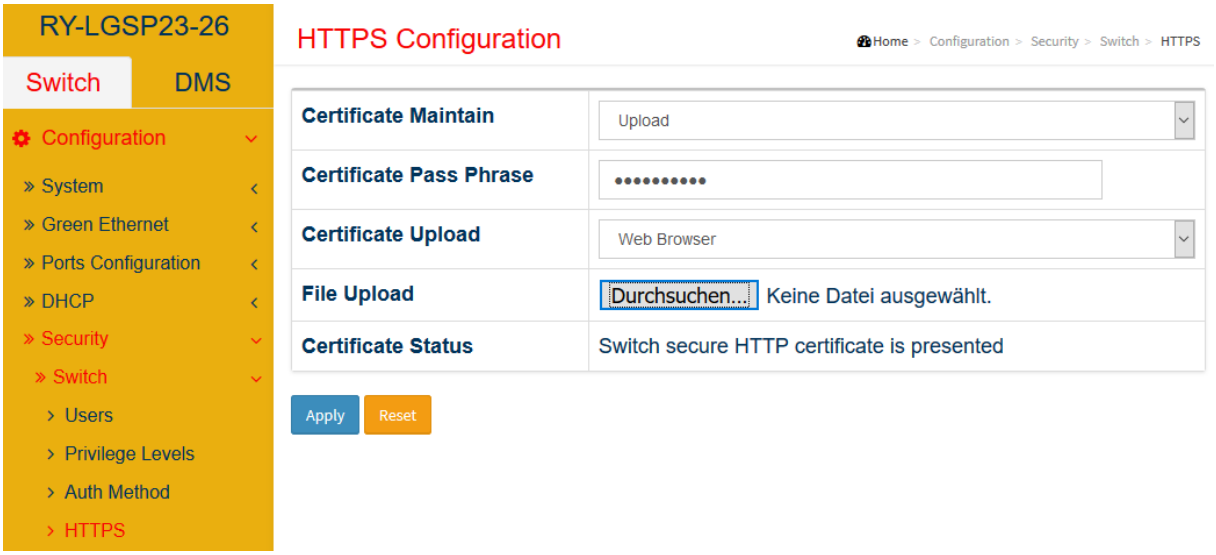
Brief information regarding the use of certificates:

A certificate-based connection enables one of the highest protection levels for network-based configuration services. Nevertheless the use should be verified, as the connection to the management can only be effected using the media with enabled certificate.

Setting options and methods, resp., are shown in the following.

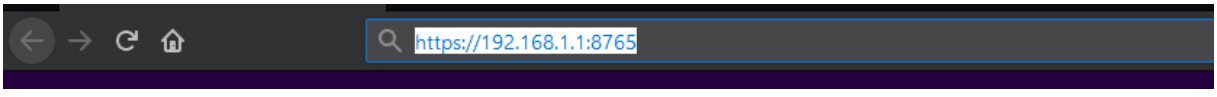


- Generation of the certificate for later use, which can be downloaded and installed using the browser.



- Upload of an externally generated certificate

- The browser access is effected following the installation of the certificate and determination of the HTTPs authentication method via the HTTPs protocol



5.4 SNMP – Monitoring- and Administration Function

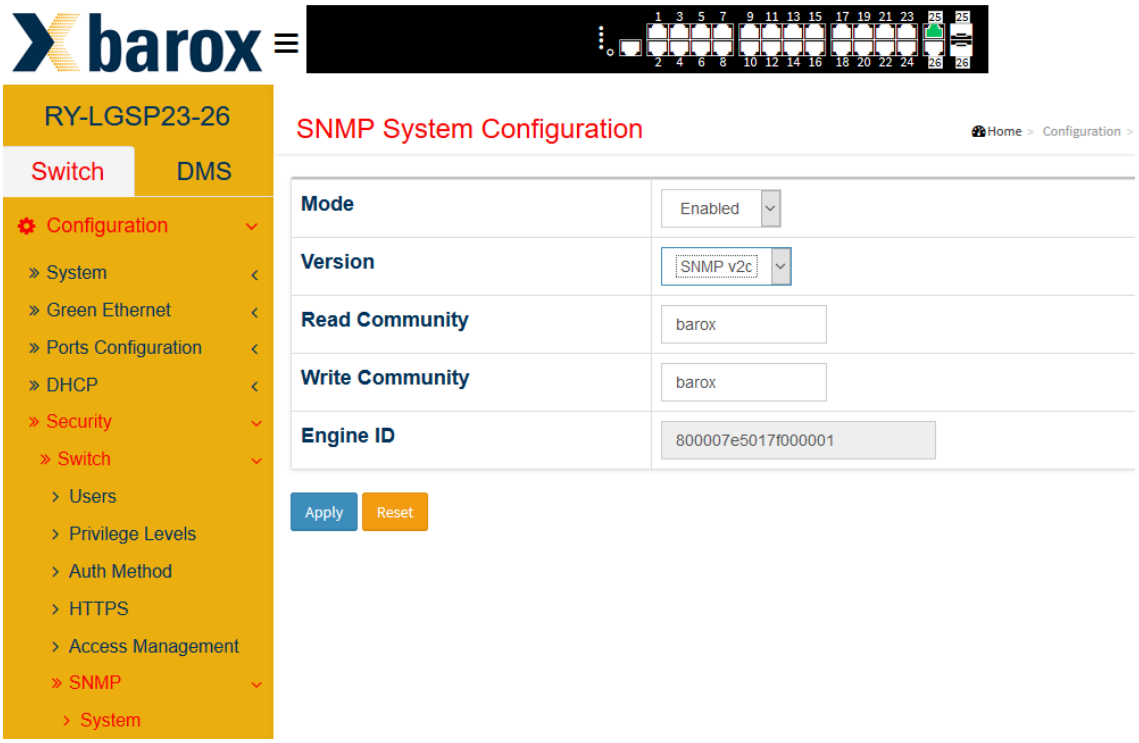
SNMP was developed by the IETF (Internet Engineering Task Force) and as a protocol serves the purpose of monitoring, control and configuration of network elements.

5.4.1. Configuration of SNMP v2c

The following example describes a basic SNMP v2 configuration for a system status enquiry or the transmission of system events via SNMP traps. The following steps shall show the use of an SNMP Community.

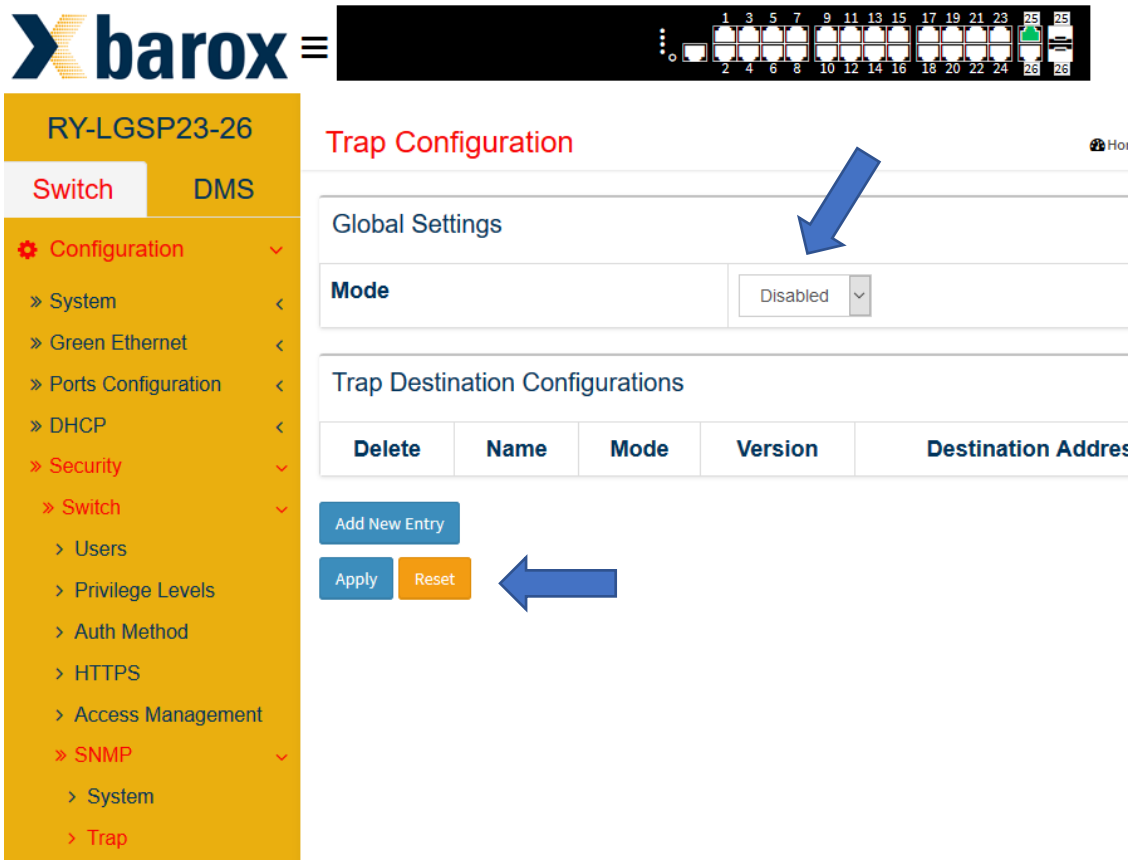
Activation of the SNMP v2 Function

The mode should be generally enabled and SNMP v2 should be selected in the SNMP configuration. Furthermore the names for the read and write communities are determined.



5.4.2. SNMP Trap Configuration

Prior to the configuration of new trap settings attention should be paid, that the global setting of the trap mode is disabled.



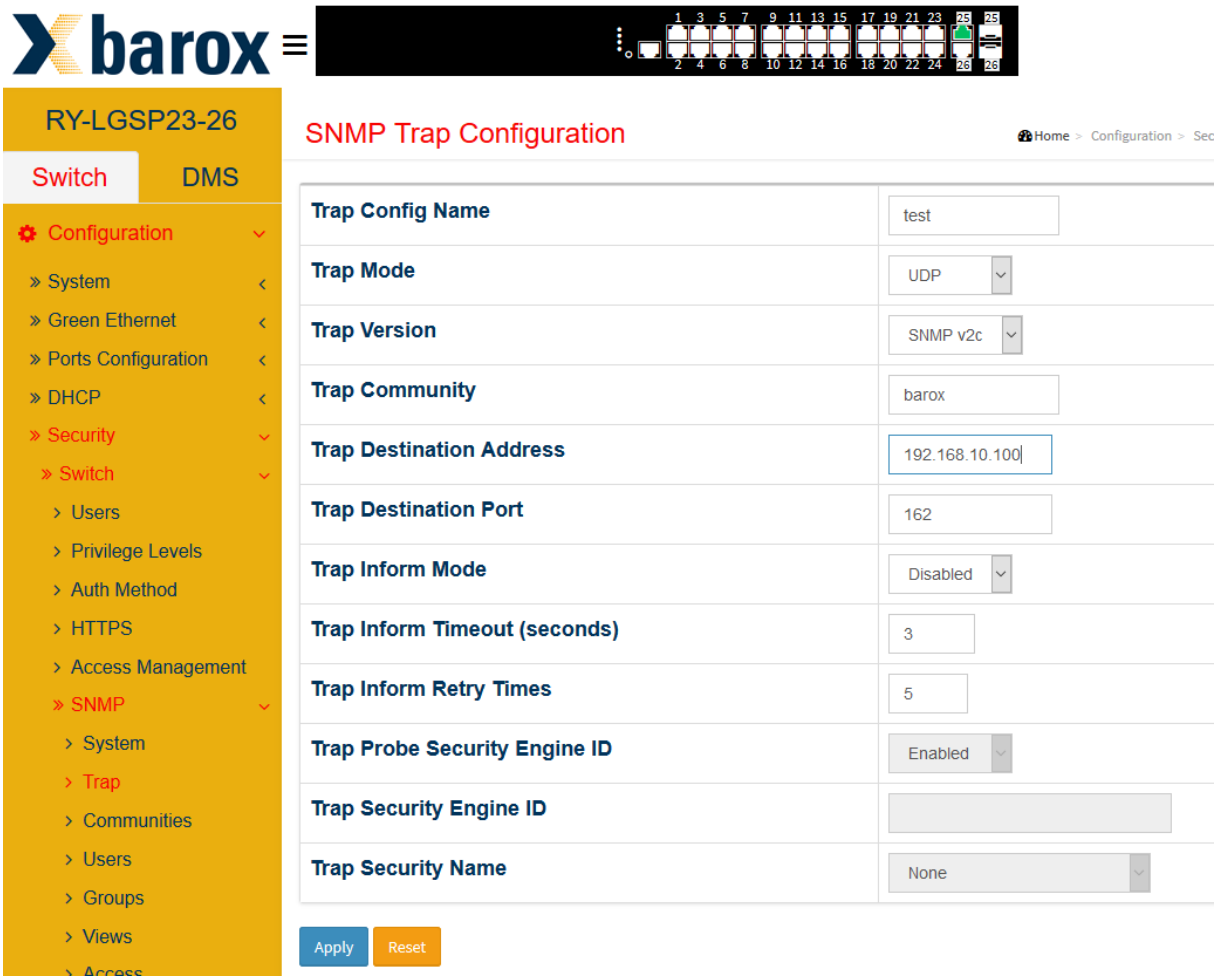
The new configuration is effected in two steps:

Step 1:

The next example shows the setting of the following values for a new configuration:

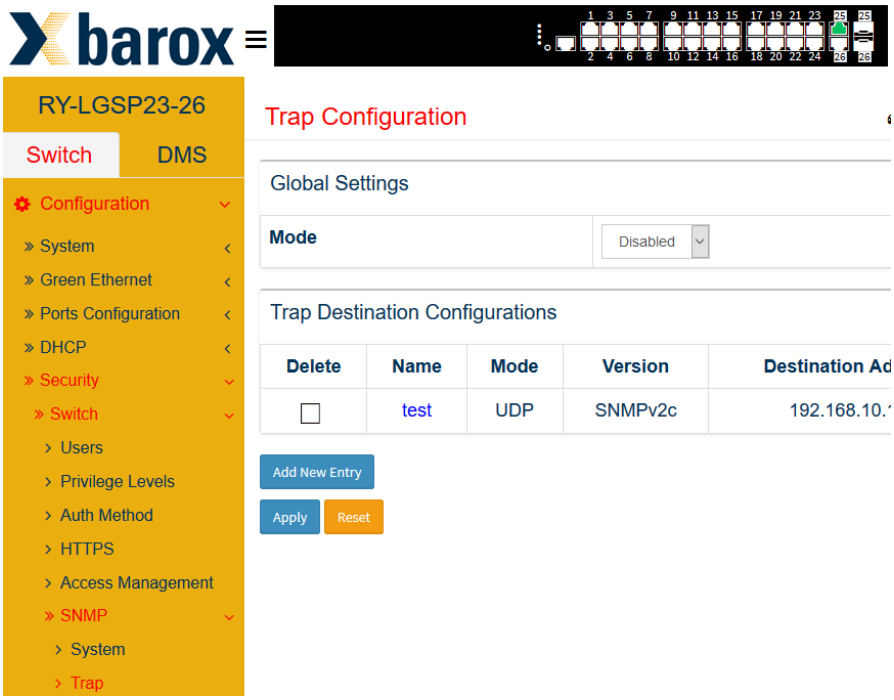
- Trap Config Name -> A name should be allocated
- Trap Mode -> UDP or TCP – As usual UDP should be used for a start
- Trap Version -> Selection of SNMP v2c
- Trap Community -> The previously generated community name must be entered here
- Trap Destination Address -> Entry of the IP address of the trap recipient
- Trap Destination Port -> Entry of the port at the recipient
- Trap Inform Mode -> Disabled in this example
- Trap Inform Timeout (seconds) -> 3 is entered (Standard)
- Trap Inform Retry Times -> 5 (Standard)

Following this the settings are confirmed by clicking „Apply“.



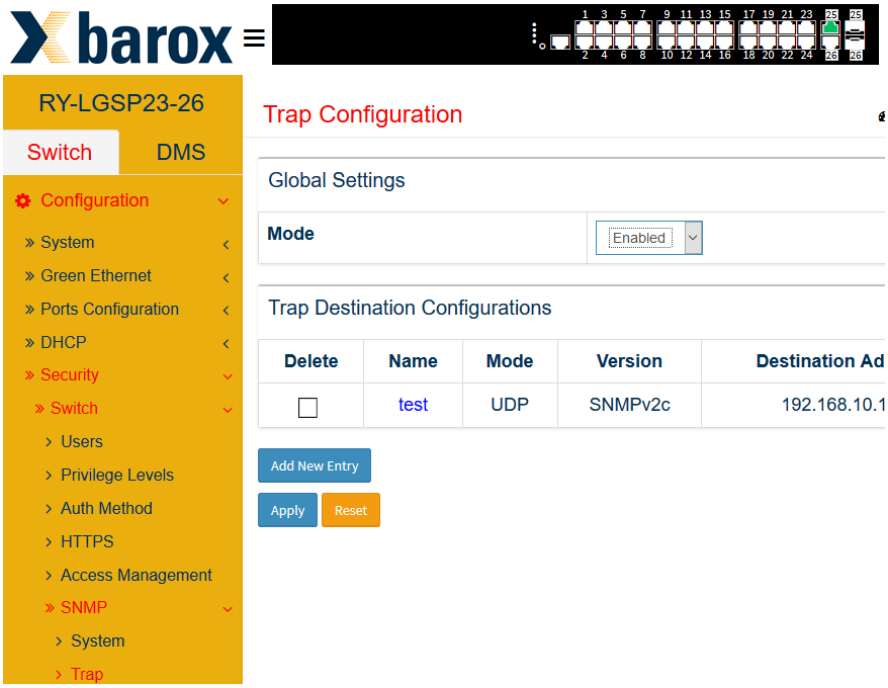
Step 2:

Following the generation of a new configuration such configuration is opened by selecting the name.



Activation of the SNMP Trap Function

The general mode must be enabled following completion of the trap configuration.



5.4.3. Supplementary Information regarding the Sending of SNMP Traps

Please assure yourself, that the events triggering a trap are configured accordingly. These settings can be configured per terminal device elsewhere in the configuration menu as shown in the following screenshot. Some events − such like e.g. port events − must also be set accordingly in the port configuration.

ATTENTION: For industrial switches, this setting can be found under Configuration/System/Alarm Notification.

Further information regarding the reading and testing of the configuration can be found in „5.6 Reading-out SNMP Traps“.

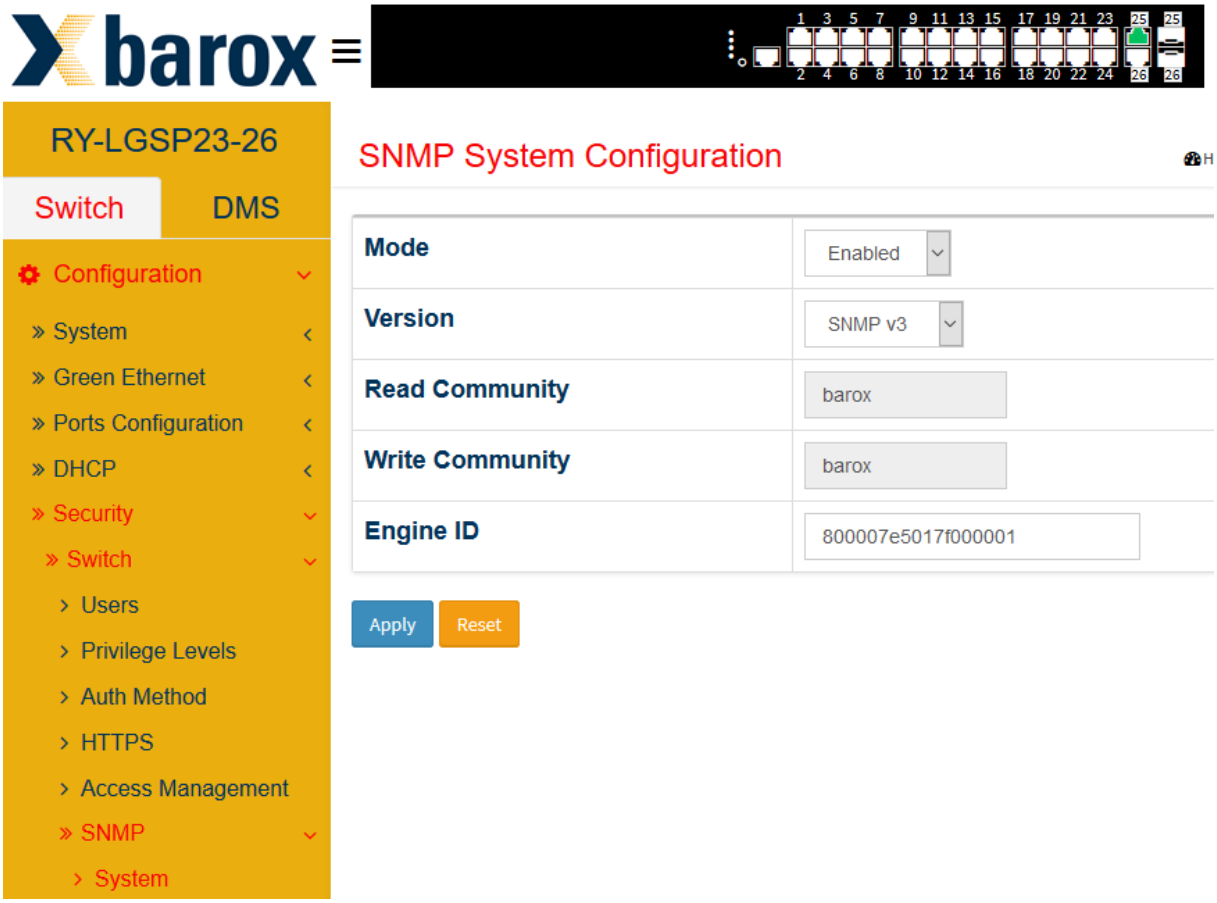
5.5 SNMP v3 Configuration

Starting position:

The increased need for network security generates raised requirements for administrating and monitoring network components. This can e.g. be effected using SNMP in version 3 with authentication. The following example describes a basic SNMP v3 configuration for a system status enquiry or the transmission of system events via SNMP traps. The following steps shall demonstrate the use of authentication and password protection.

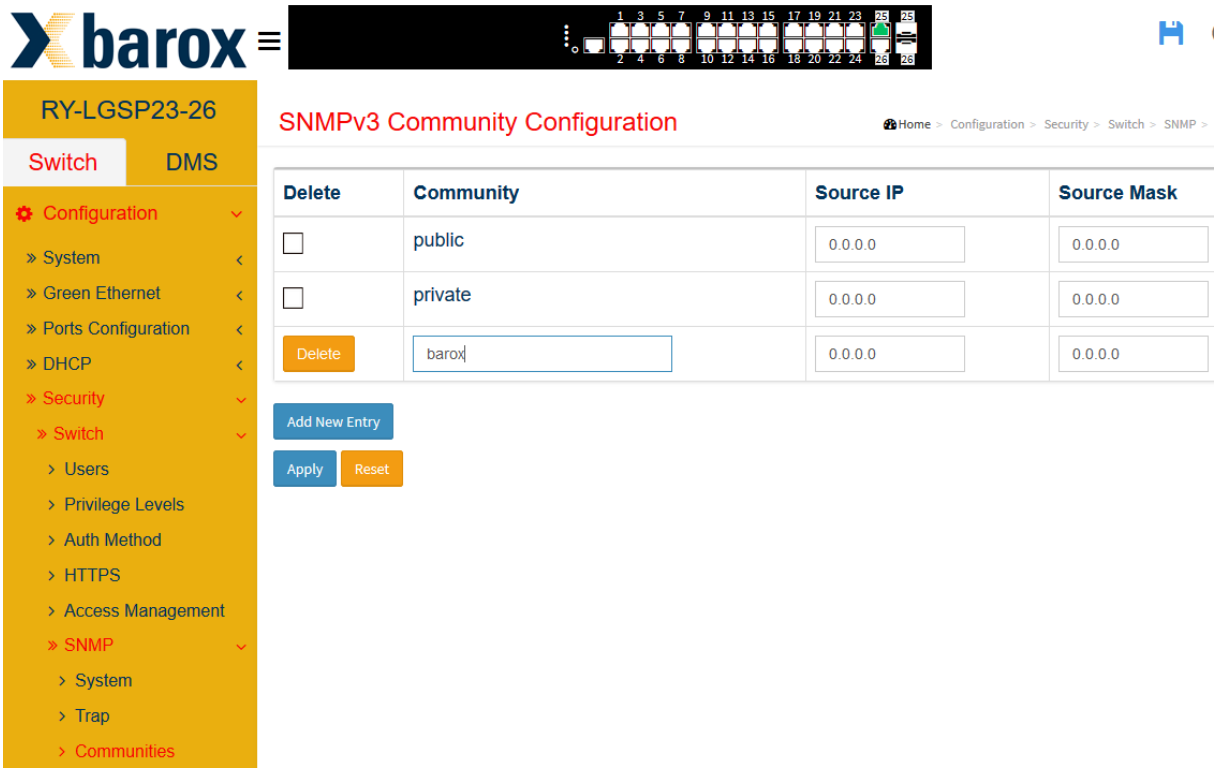
5.5.1. Activation of the SNMP v3 Function

The mode should be generally enabled and SNMP v3 should be selected in the SNMP configuration.



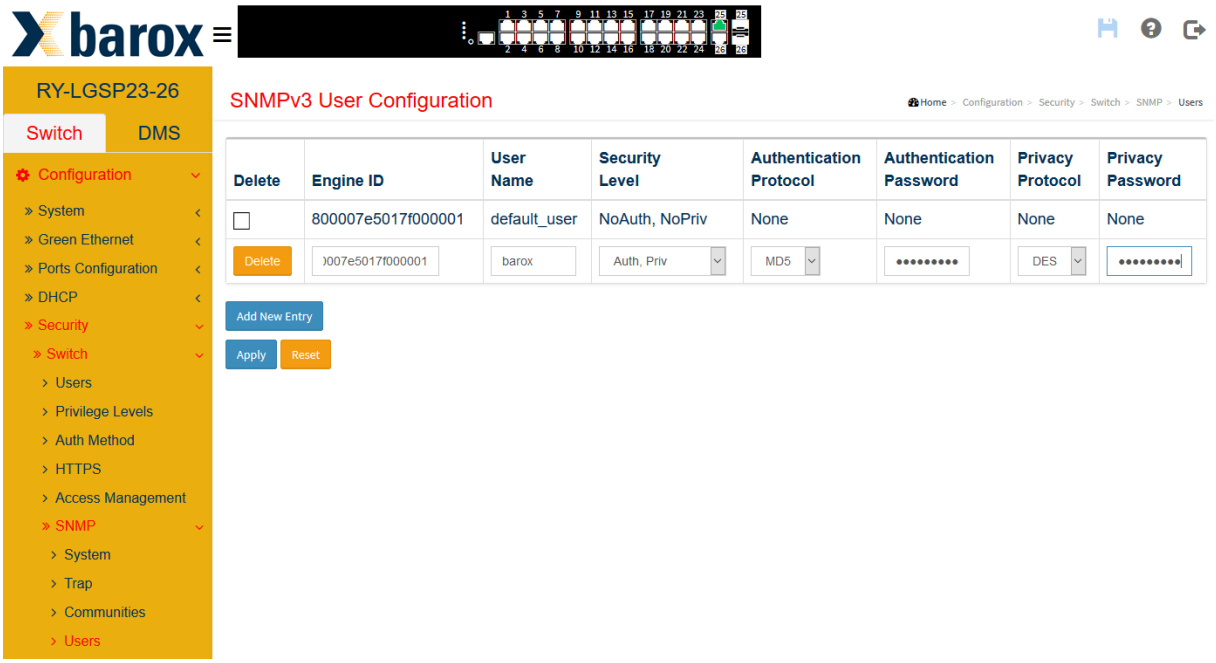
Generation of a dedicated Community

When generating the community the setting of source IP and mask can remain as 0.0.0.0 in each case. This enables the transmission and the receipt of SNMP messages across several subnetworks.



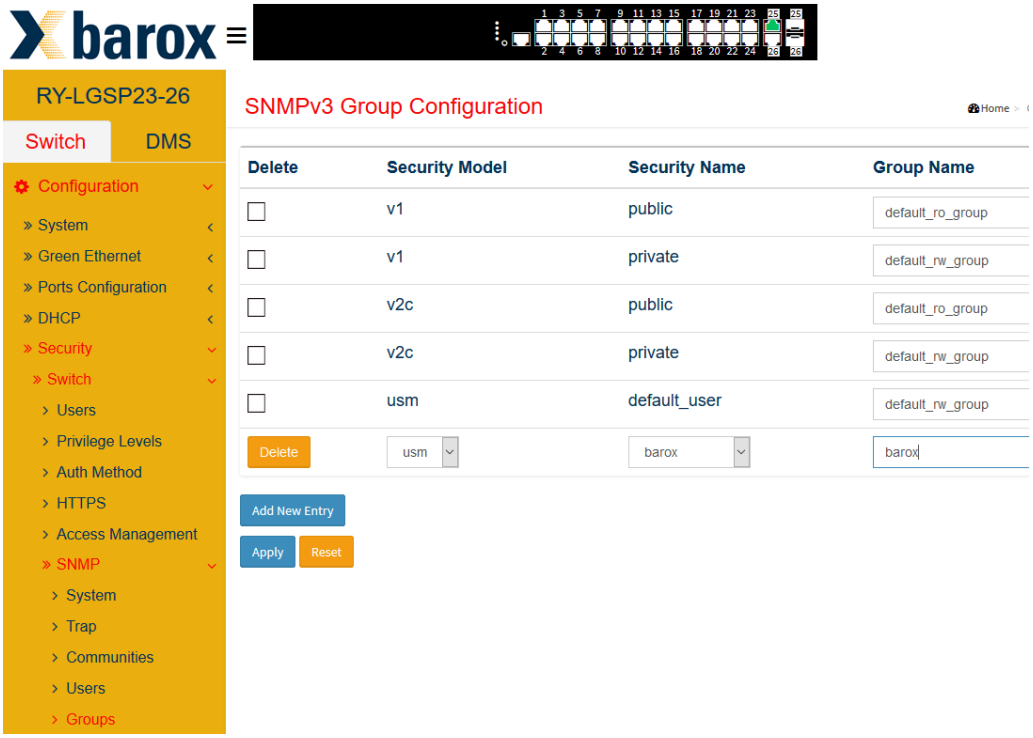
Generation of a new User

When configuring a new user attention should be paid for imperatively adding the Engine ID to the new user object. It can simply be copied and inserted from the „*default_user*“-entry. In this example the security level „*Auth, Priv*“ shall also be set along with the determination of the user name. When selecting the authentication „MD5“ and the privacy protocol DES attention shall be paid as the length of both passwords must be at least eight characters (numbers and character combinations).



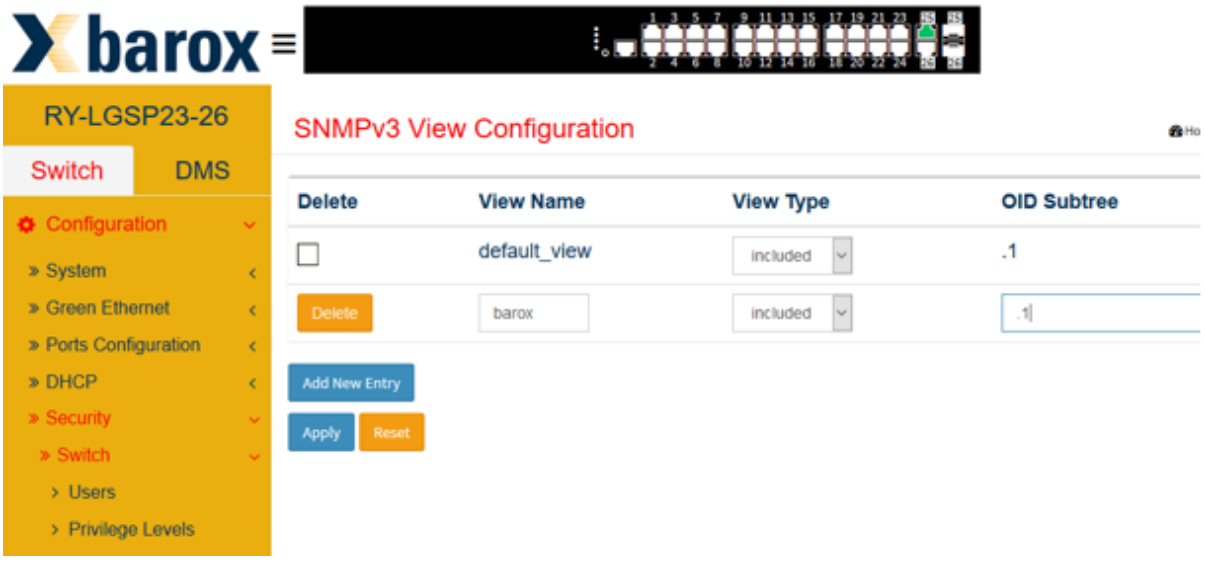
Generation of a Group

The security modell „*usm*“ shall be selected when configuring a new group in SNMP v3. The previously generated user name shall be selected as „*Security Name*“, following this a group name must be determined.



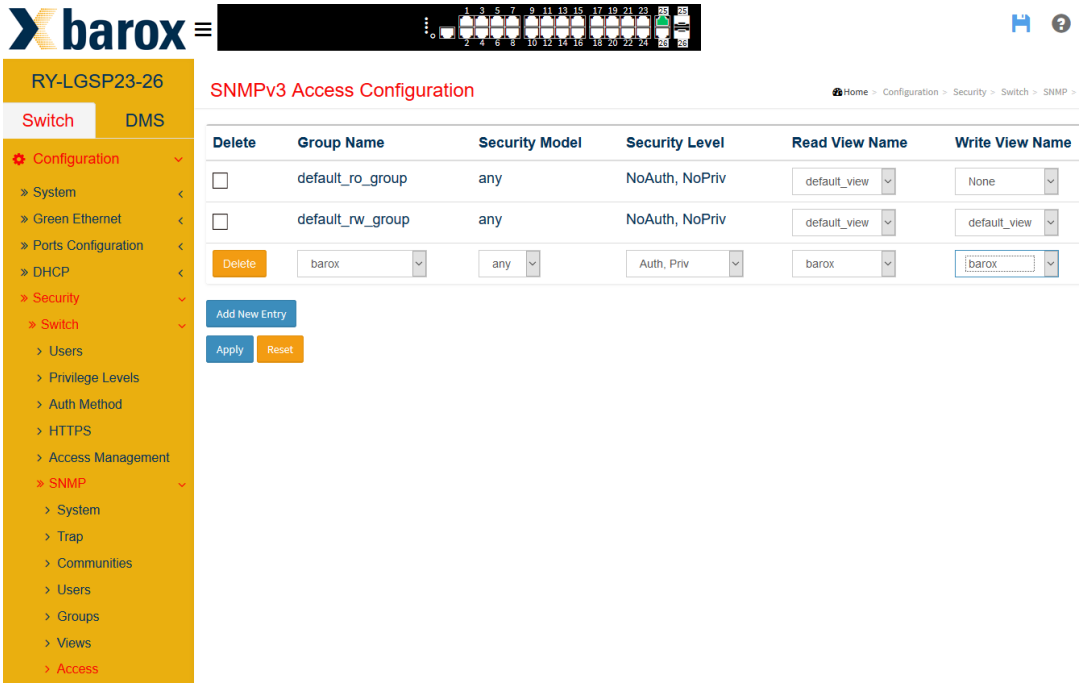
Setting the View Configuration

At the beginning the View Name is determined. Setting the OID to a value „.1“ is recommended providing all SNMP-relevant messages can be viewed. This enables the complete view to all distributed OIDs.



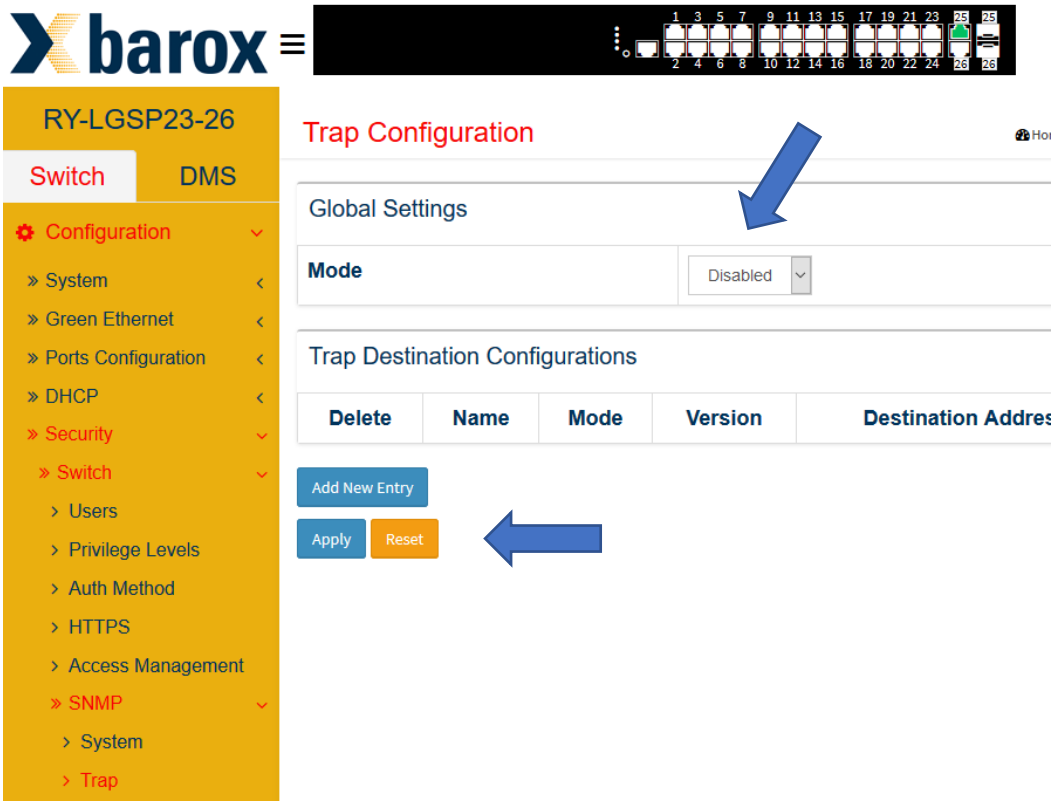
Configuration of the Access Method

A new entry with authentication and privatisation method shall be generated for doing so. At the beginning the previously generated group must be selected in „Group Name“. Furthermore the „*Security Model*“ „**usm**“ and the „*Security Level*“ „**Auth, Priv**“ are allocated to the group. The latter ones are required for reading and writing the views, which were previously generated in „Read View Name“ and „Write View Name“.



5.5.2. SNMP Trap Configuration

Prior to the configuration of new trap settings attention should be paid, that the global setting of the trap mode is disabled.



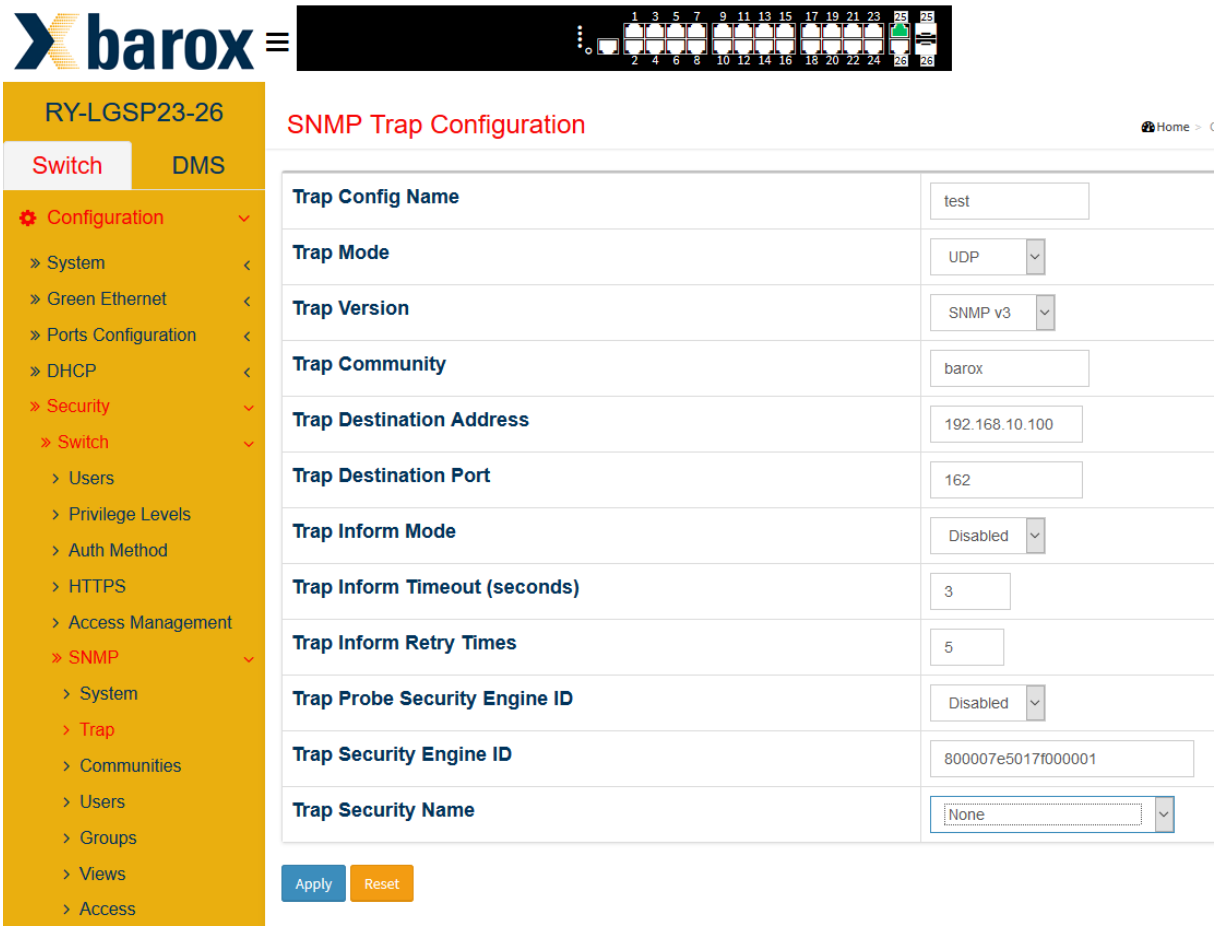
The new configuration is effected in two steps:

Step 1:

The next example shows the setting of the following values for a new configuration:

- Trap Config Name -> A name should be allocated
- UDP or TCP – UDP should be used for a start as usual
- Trap Version -> Selection of SNMP v3
- Trap Community -> The previously generated community name must be entered here
- Trap Destination Address -> Entry of the IP address of the trap recipient
- Trap Destination Port -> Entry of the port at the recipient
- Trap Inform Mode -> Disabled in this example
- Trap Inform Timeout (seconds) -> 3 is entered (Standard)
- Trap Inform Retry Times -> 5 (Standard)
- Trap Probe Security Engine ID -> Should be disabled
- Trap Security Engine ID -> The user‘s Engine ID must be entered here
- Trap Security Name -> Currently only „None“ can be selected

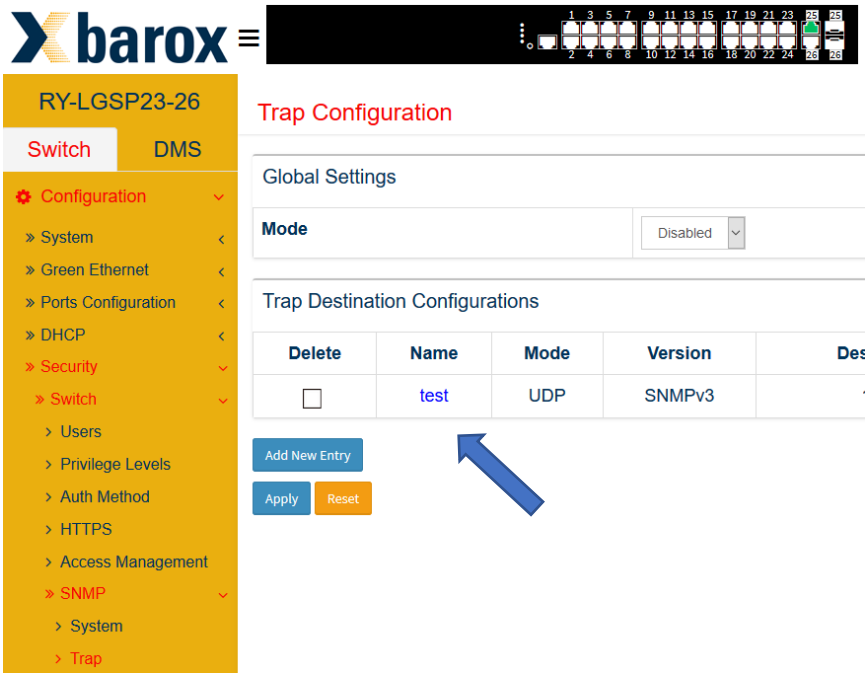
Following this the settings are confirmed by clicking „Apply“.



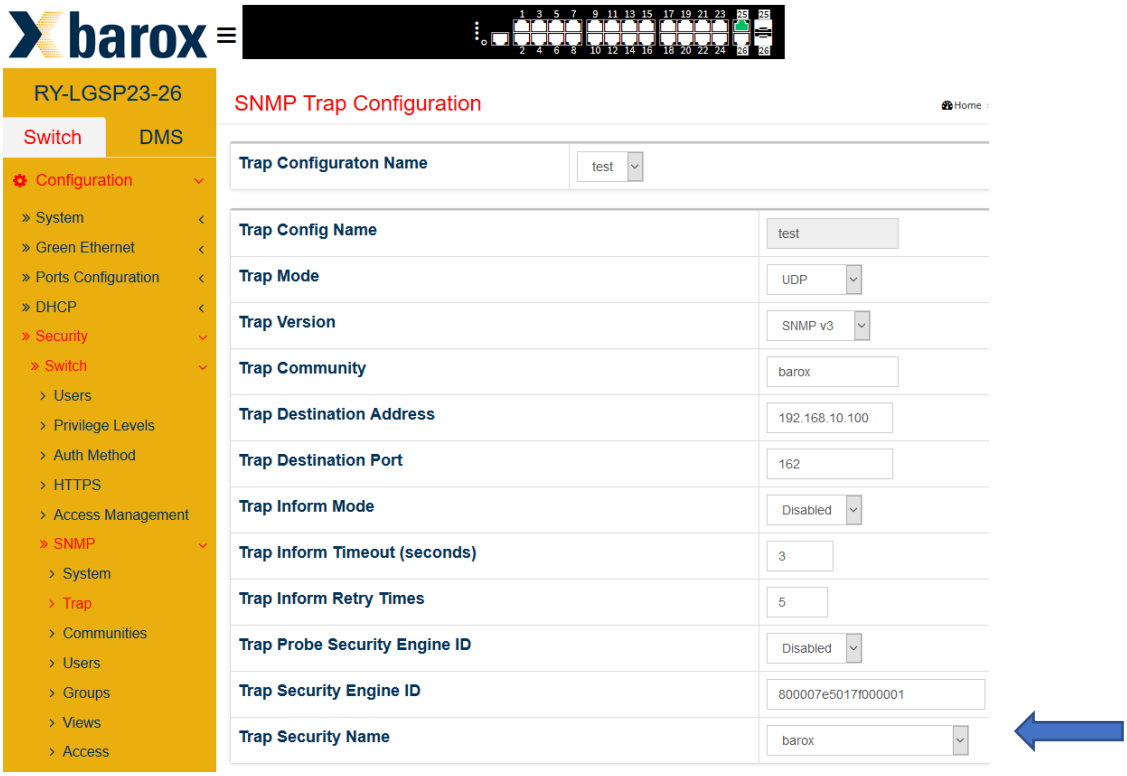
Following the confirmation of the configuration a note is displayed, that a respective Security Name should be set. This is configured in step 2.

Step 2:

Following the generation of a new configuration such configuration is opened by selecting the name.

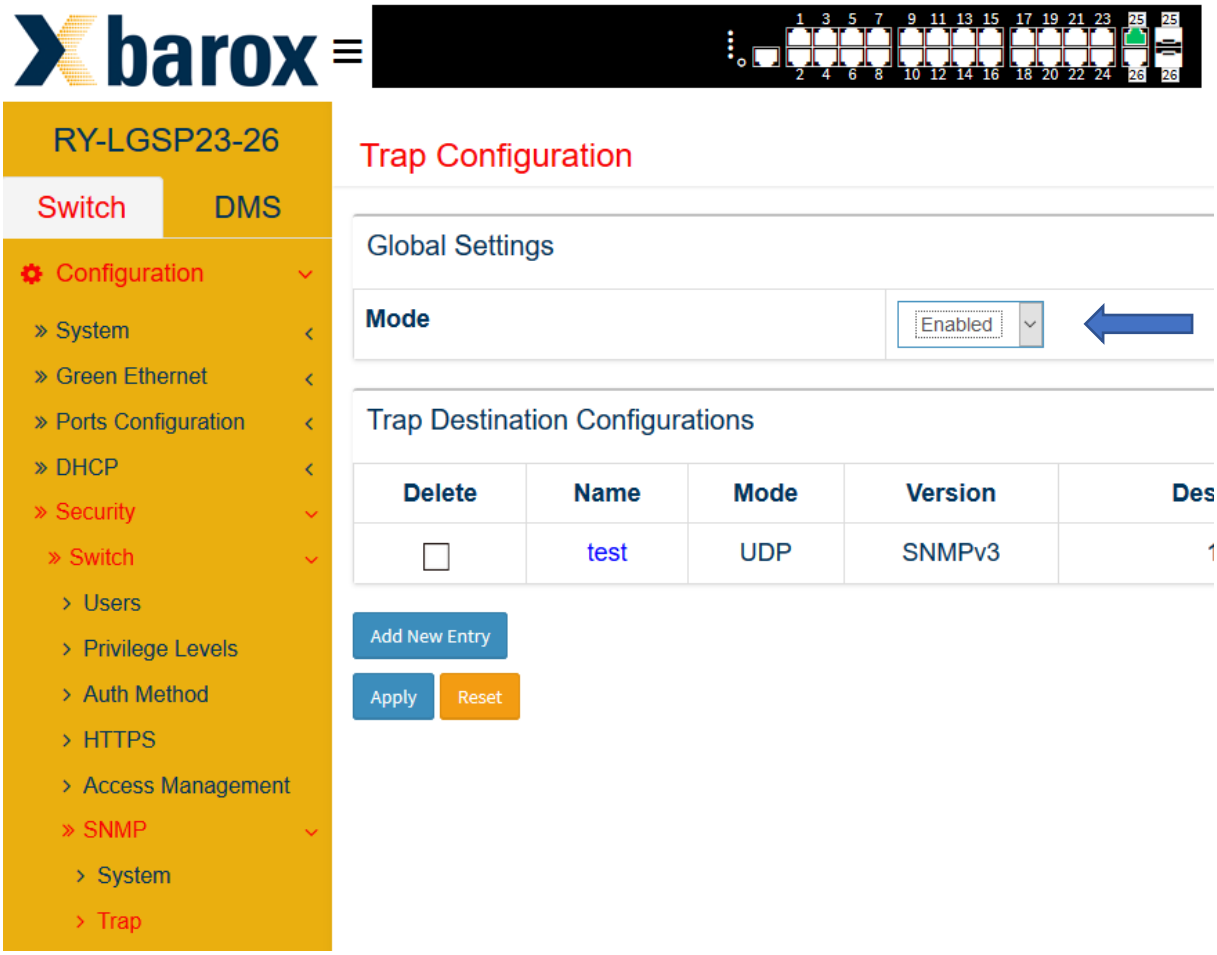


Now the entry „Trap Security Name“ can be set to the SNMP user name.



Activation of the SNMP Trap Function

The general mode must be enabled following completion of the trap configuration.



5.5.3. Supplementary Information regarding the Sending of SNMP Traps

Please assure yourself, that the events triggering a trap are configured accordingly. These settings can be configured per terminal device elsewhere in the configuration menu as shown in the following screenshot. Some events − such like e.g. port events − must also be set accordingly in the port configuration.

Further information on reading-out and testing the configuration can be found in „5.6 reading SNMP Traps“.

5.6 Reading SNMP Traps

Various parameters of the barox switch configurations can be read out and set, resp., using the SNMP protocol. So-called „SNMP/MIB Browser" are basically required for doing so. But also network-/recording-/ sniffer software can be utilised to read SNMP transmissions.

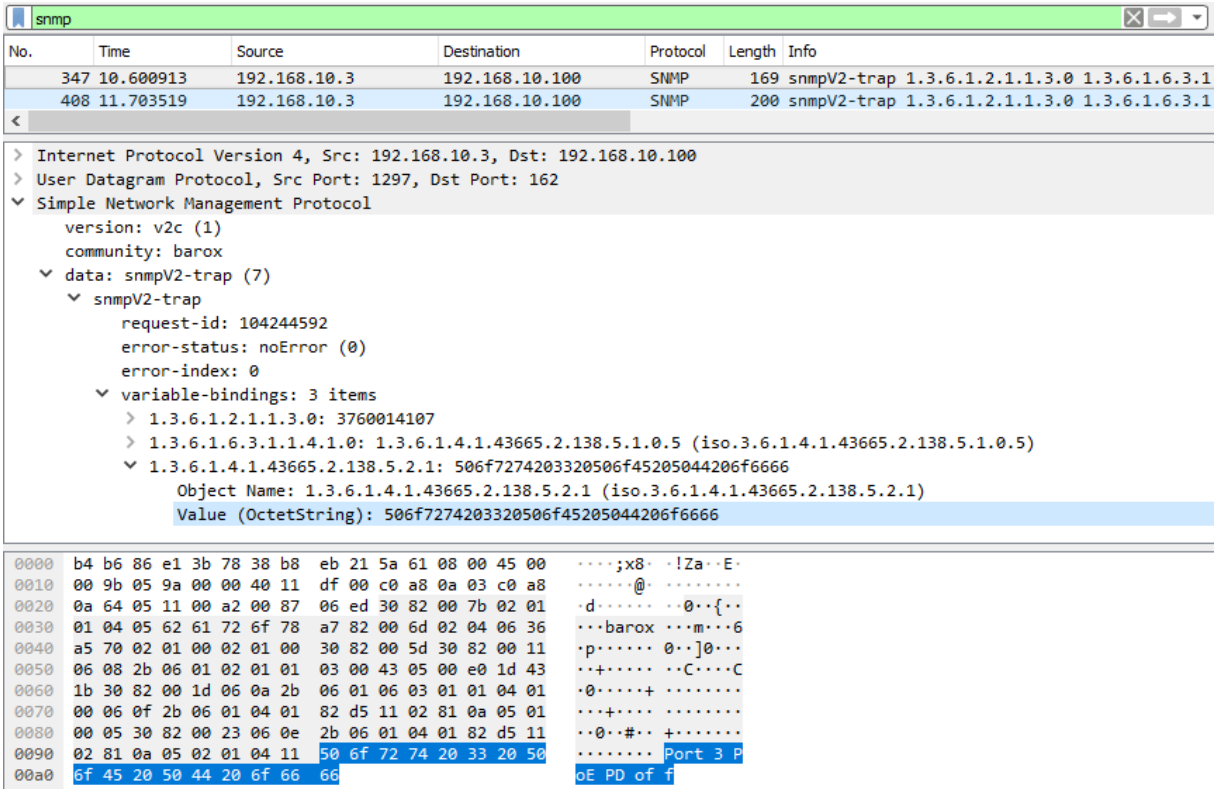
The reading-out of an SNMP v2 trap is briefly explained using the following example:

Starting position:

A PoE camera is unplugged and plugged in again at the Ethernet port 3 of the switch.
A PC in the network is configured for the receipt of SNMP traps. The software Wireshark (https://www.wireshark.org) for reading-out and for a user-friendly view *"iReasonning MIB Browser" (http://www.ireasoning.com/mibbrowser.shtml) are used.

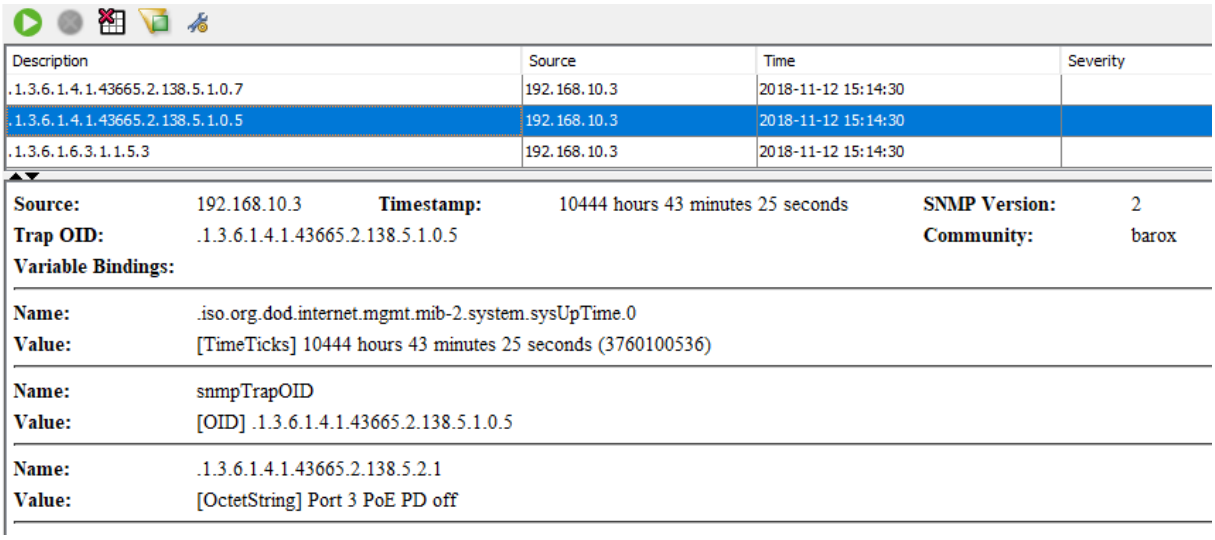
The PoE camera is ungplugged / PD device is offline:

Copy of the information, which is sent by the switch:



* Please pay attention to the respective software vendor's licencing conditions when using the software.

View of the information in the SNMP browser:



Description	Source	Time	Severity
.1.3.6.1.4.1.43665.2.138.5.1.0.7	192.168.10.3	2018-11-12 15:14:30	
.1.3.6.1.4.1.43665.2.138.5.1.0.5	192.168.10.3	2018-11-12 15:14:30	
.1.3.6.1.6.3.1.1.5.3	192.168.10.3	2018-11-12 15:14:30	

Source: 192.168.10.3 **Timestamp:** 10444 hours 43 minutes 25 seconds **SNMP Version:** 2
Trap OID: .1.3.6.1.4.1.43665.2.138.5.1.0.5 **Community:** barox
Variable Bindings:

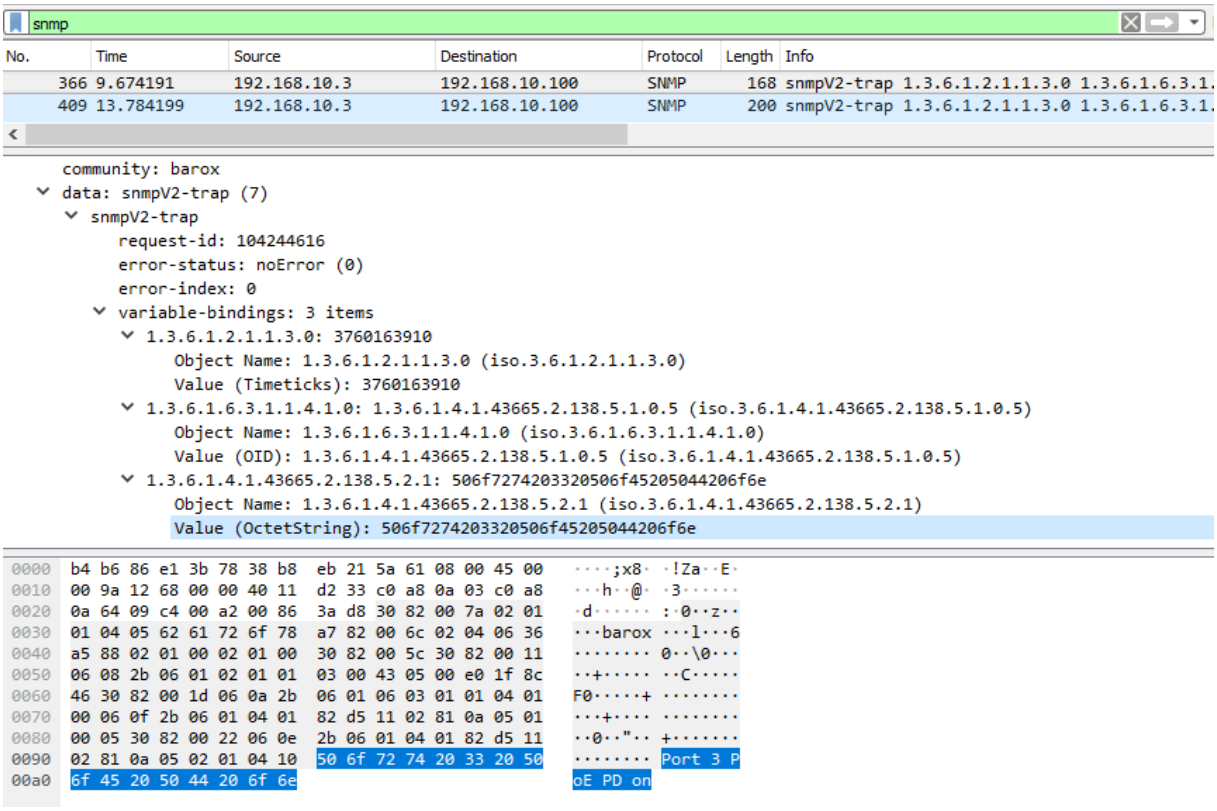
Name: .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0
Value: [TimeTicks] 10444 hours 43 minutes 25 seconds (3760100536)

Name: snmpTrapOID
Value: [OID] .1.3.6.1.4.1.43665.2.138.5.1.0.5

Name: .1.3.6.1.4.1.43665.2.138.5.2.1
Value: [OctetString] Port 3 PoE PD off

PoE camera is connected again / PD device is online:

Recording of the information, which is sent by the switch:



snmp

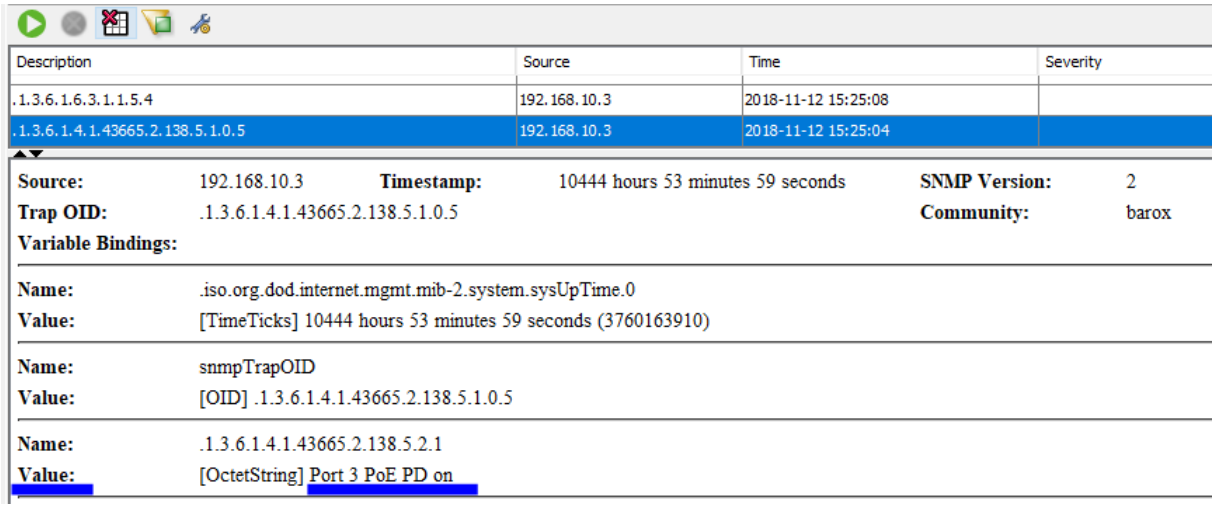
No.	Time	Source	Destination	Protocol	Length	Info
366	9.674191	192.168.10.3	192.168.10.100	SNMP	168	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.
409	13.784199	192.168.10.3	192.168.10.100	SNMP	200	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.

```
community: barox
data: snmpV2-trap (7)
  snmpV2-trap
    request-id: 104244616
    error-status: noError (0)
    error-index: 0
    variable-bindings: 3 items
      1.3.6.1.2.1.1.3.0: 3760163910
        Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
        Value (Timeticks): 3760163910
      1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.4.1.43665.2.138.5.1.0.5 (iso.3.6.1.4.1.43665.2.138.5.1.0.5)
        Object Name: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0)
        Value (OID): 1.3.6.1.4.1.43665.2.138.5.1.0.5 (iso.3.6.1.4.1.43665.2.138.5.1.0.5)
      1.3.6.1.4.1.43665.2.138.5.2.1: 506f7274203320506f45205044206f6e
        Object Name: 1.3.6.1.4.1.43665.2.138.5.2.1 (iso.3.6.1.4.1.43665.2.138.5.2.1)
        Value (OctetString): 506f7274203320506f45205044206f6e
```

```
0000  b4 b6 86 e1 3b 78 38 b8  eb 21 5a 61 08 00 45 00   ····;x8· ·!Za··E·
0010  00 9a 12 68 00 00 40 11  d2 33 c0 a8 0a 03 c0 a8   ···h··@· ·3······
0020  0a 64 09 c4 00 a2 00 86  3a d8 30 82 00 7a 02 01   ·d····· :·0··z··
0030  01 04 05 62 61 72 6f 78  a7 82 00 6c 02 04 06 36   ···barox ···l···6
0040  a5 88 02 01 00 02 01 00  30 82 00 5c 30 82 00 11   ········ 0··\0···
0050  06 08 2b 06 01 02 01 01  03 00 43 05 00 e0 1f 8c   ··+····· ··C·····
0060  46 30 82 00 1d 06 0a 2b  06 01 06 03 01 01 04 01   F0·····+ ········
0070  00 06 0f 2b 06 01 04 01  82 d5 11 02 81 0a 05 01   ···+···· ········
0080  00 05 30 82 00 22 06 0e  2b 06 01 04 01 82 d5 11   ··0··"·· +·······
0090  02 81 0a 05 02 01 04 10  50 6f 72 74 20 33 20 50   ········ Port 3 P
00a0  6f 45 20 50 44 20 6f 6e                           oE PD on
```

View of the information in the SNMP browser:

Frequently a value used for reading and interpreting, resp., the status/message of the SNMP message is added to the related OIDs (Object Identifier for Information Units) of the traps. In this example the last line is marked for illustration purposes.



5.7 Use of MIB Files for Reading-out and Control of the Switches

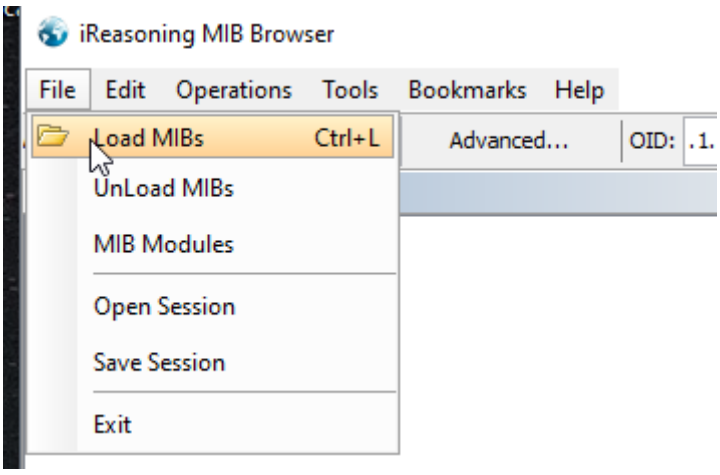
Fundamentally status enquiries for manageable devices in the network such as switches, routers or servers must mostly be effected using the SNMP functionality. For security reasons or because of manufacturer-specific aspects so-called MIB files are frequently required for enquiring the devices. These files comprise information about the identification parameters of the functions.

Enquiry of Switch Status Functions using SNMP and MIB Files

As an introduction the use of an MIB browser is fundamentally recommended. The *“iReasonning MIB Browser“ (http://www.ireasoning.com/mibbrowser.shtml) is used in the example for a user-friendly view. Furthermore the browser must be configured with the respective SNMP parameters for connecting to the respective switch.

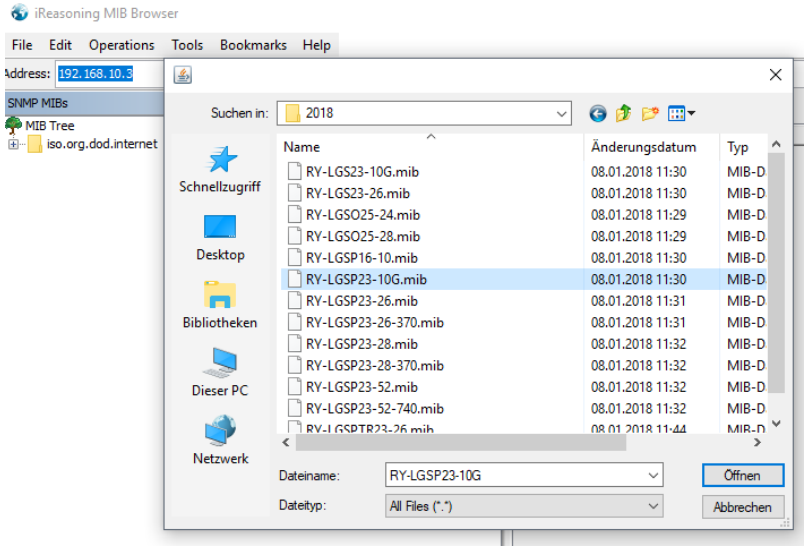
Step 1: Import of the MIB File

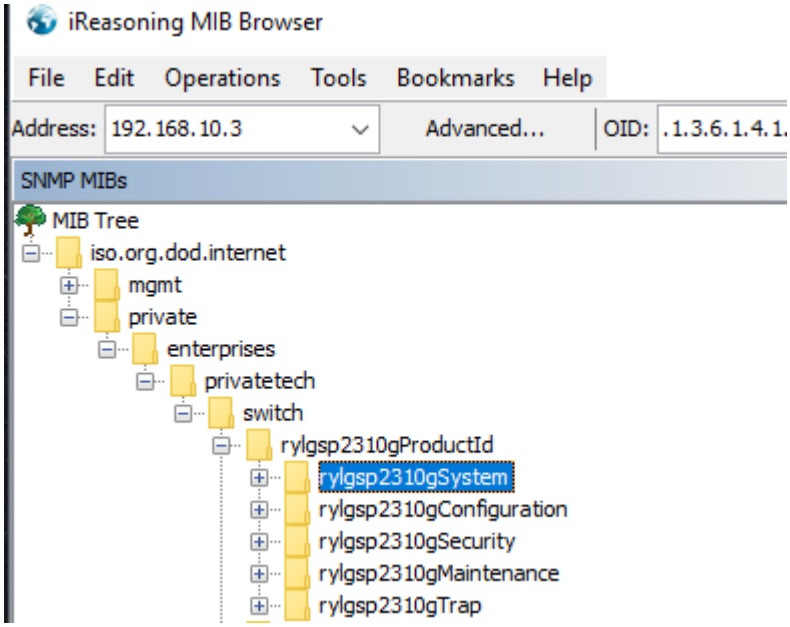
During the import attention must be paid for selecting the suitable MIB file for the respective switch. The required MIB files can be identified by their prefix „mib“.



* Please pay attention to the respective software vendor‘s licencing conditions when using the software!

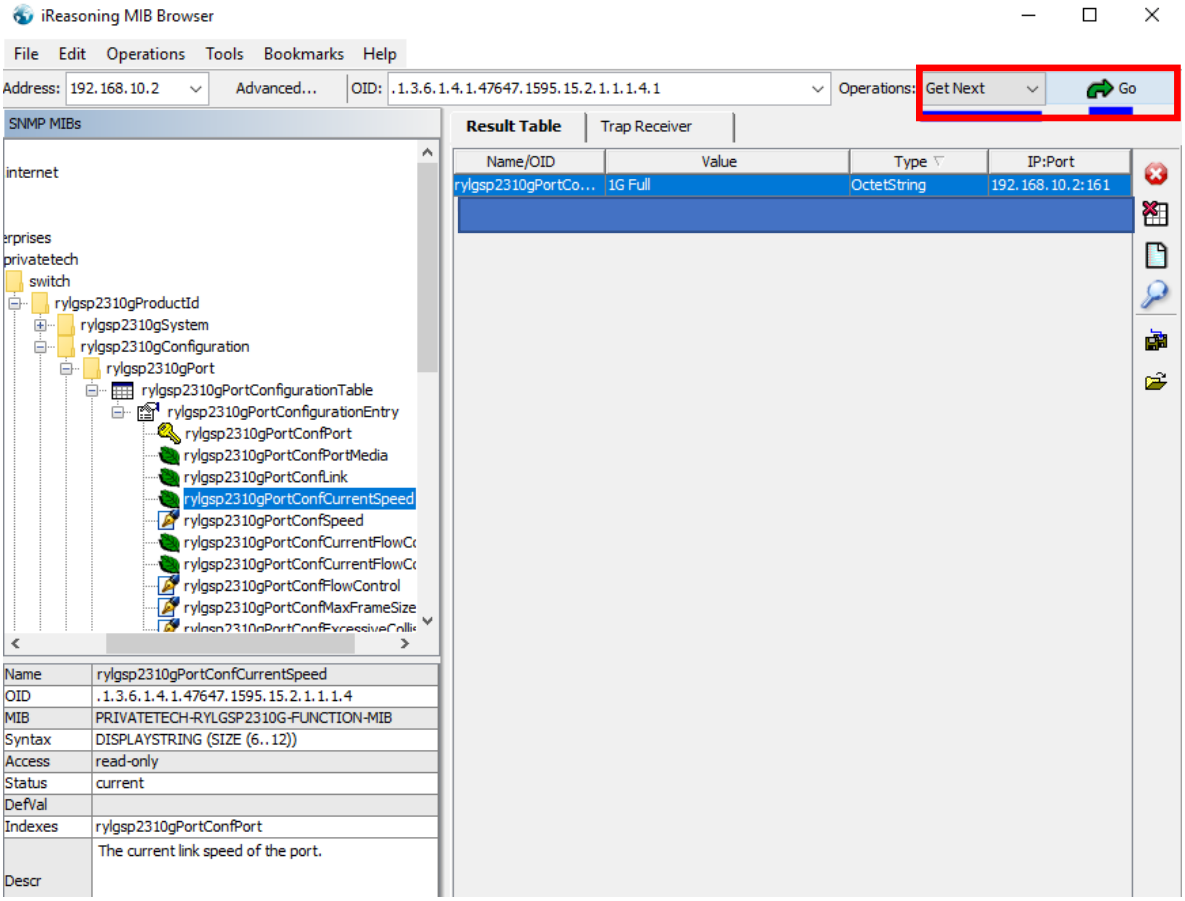
Following the successful import the MIB structures are available as shown below.





Step 2: Generating Enquiries

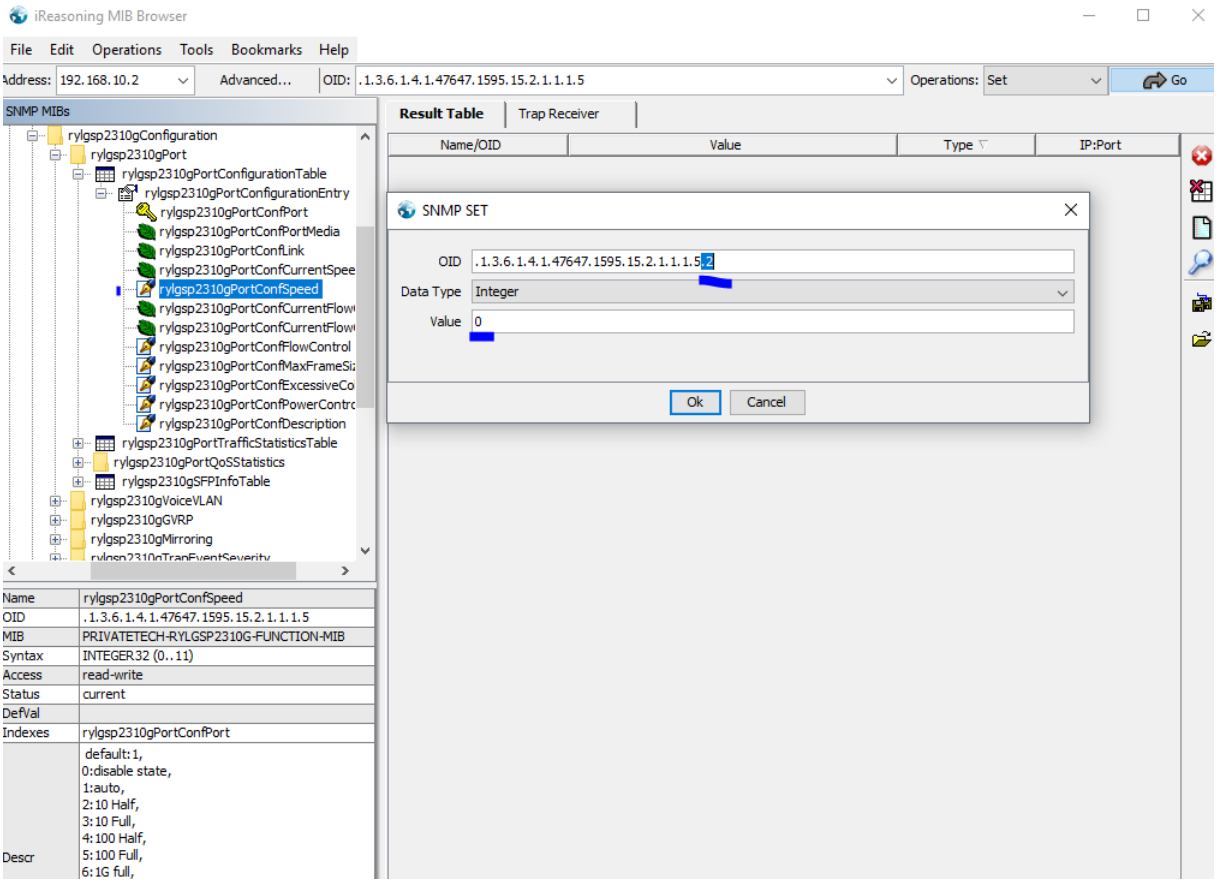
For generating an enquiry the desired status is selected first. The enquiry is then generated using the operation „*Get Next*“ and clicking „Go“. Upon completion of a successful enquiry the status information is displayed in the results table as shown in the following example.

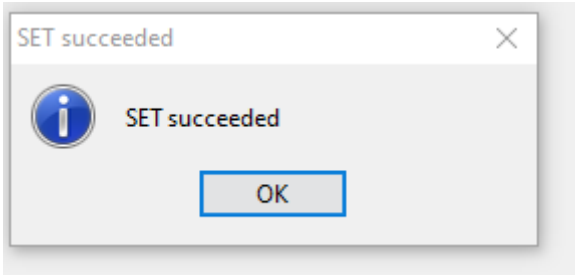


5.8 Control of Switch Functions via SNMP and MIB using the „SET“ Operation

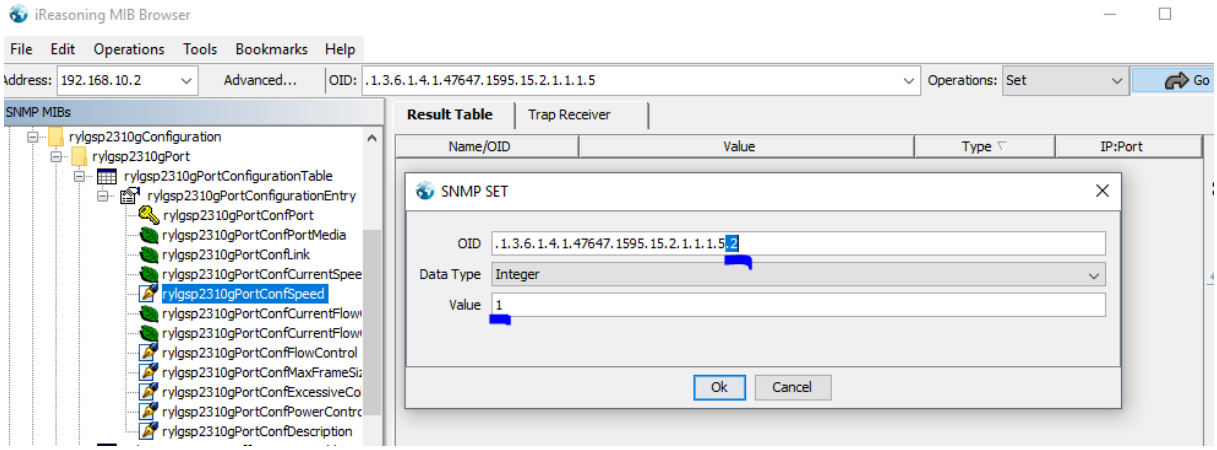
The „SET” operation via the SNMP protocol can be a further method for controlling barox switches. The basic SNMP configurations at the switch and of the MIB browser are preconditions. In the following an example for using the SET operation for triggering a port deactivation and re-activation at the switch is shown.

For the deactivation of port 2 of the switch the port configuration is searched in the MIB directory. When doing so attention must be paid for selecting the right information block with write function. The SET operation is opened by a click on „*Go”* and the OID entry is complemented by „ *.2”* (label of port 2). In addition to this the value „*0”* (for deactivation) is entered and confirmed by „OK“. A respective success message is generated upon a successful operation.



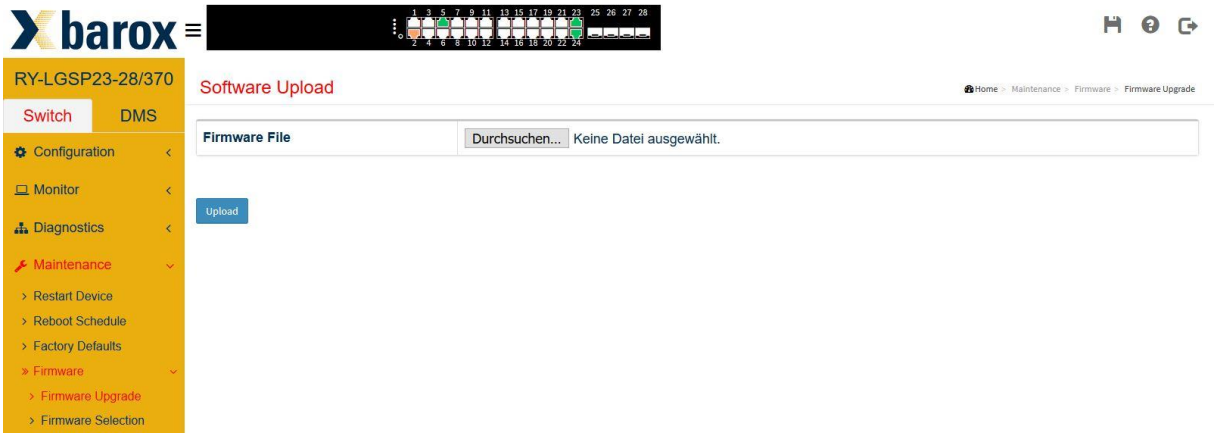


For the activation of port 2 of the switch the port configuration is searched in the MIB directory. When doing so attention must be paid for selecting the respective information block with write function. The SET operation is opened by a click on „*Go*“ and the OID entry is complemented by „ *.2*“ (label of port 2). In addition to this the value „*1*“ (for activation) is entered and confirmed by „OK“. A respective success message is generated upon a successful operation.

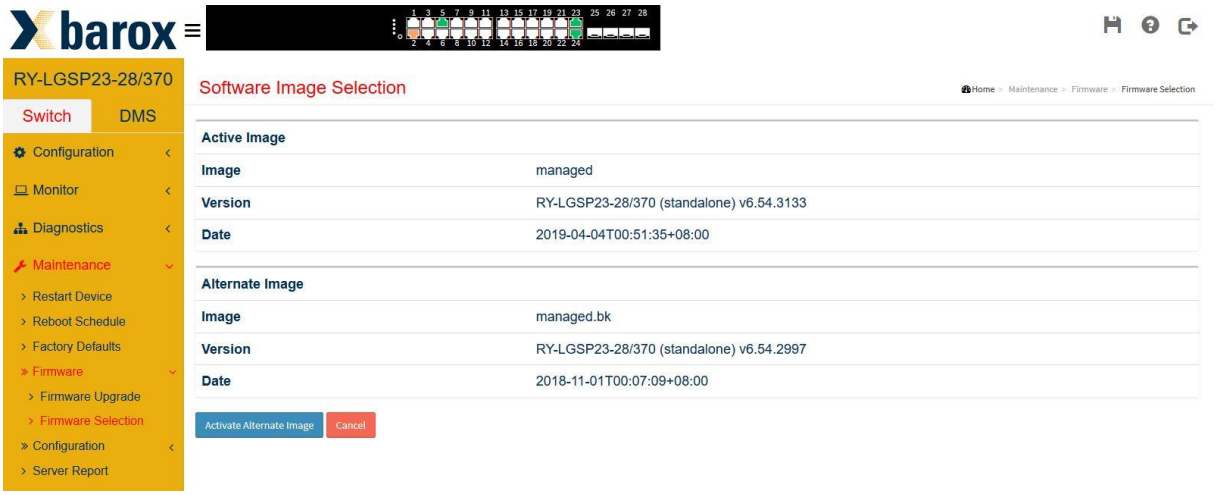


6 Firmware Upgrade

It is recommended to sporadically update the firmware as the software is regularly updated to remove bugs. New features are also introduced.



Following the upgrade the new firmware is immediately available. Any old firmware can very simply be re-activated in the menu „Firmware Selection" where the old firmware shall be applied again for some reason.

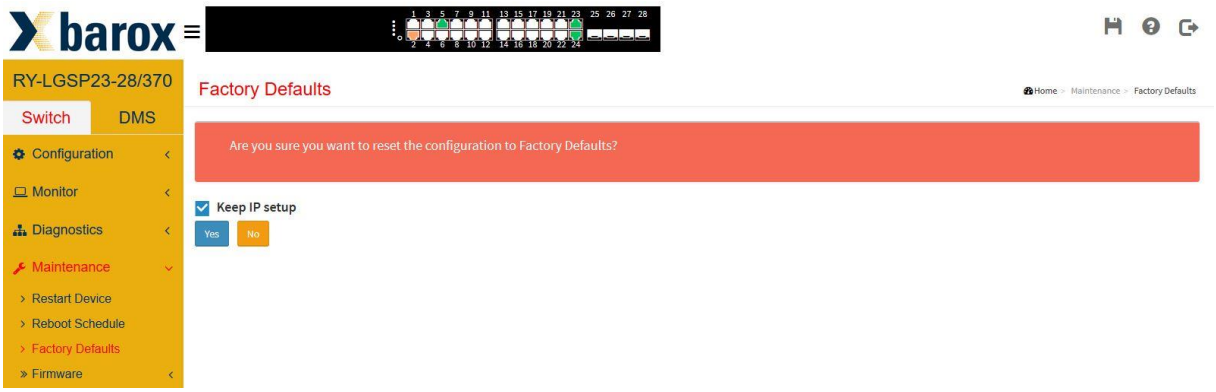


7 Factory Defaults

The switches can be reset to the factory defaults at any time.

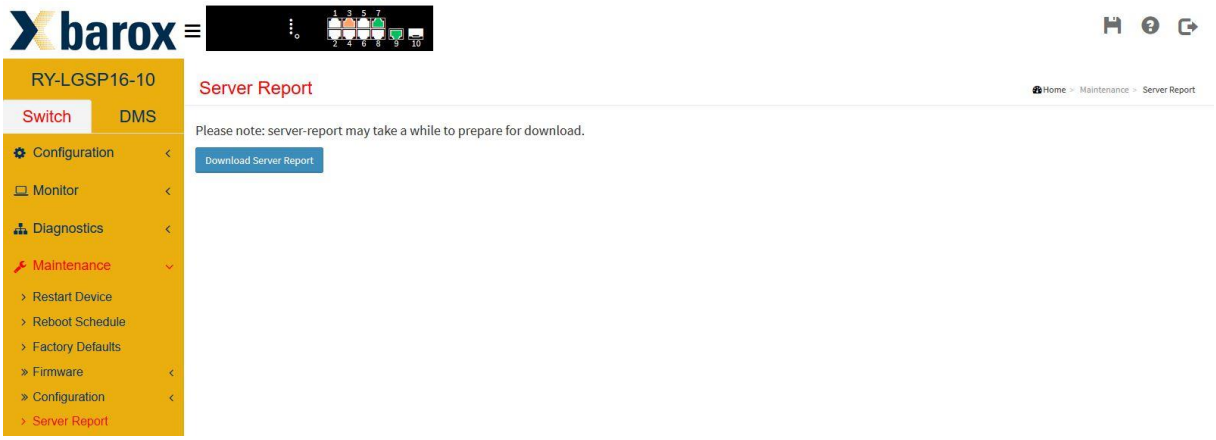
This is done either via the “Maintenance/Factory Defaults” menu or by pressing the reset button at the front (for longer than 10 seconds).

Checking the “Keep IP setup” box ensures that the switch retains the configured IP address. Otherwise, everything is reset to the factory defaults.



8 Server Report

When submitting a request for support, the server report should also be provided. This contains a description of the whole configuration as well as useful information for the support technician.



Excerpt from a Server Report

server-report - Editor

Datei Bearbeiten Format Ansicht ?

```
----- System Overview -----

Model Name: RY-LGSP16-10

Connected Devices: 1
PoE Power Consumption: 0 [W]
Total PoE Available: 130 [W]

Firmware Version: v6.54.2729 2017-12-22
MAC Address: 38-b8-eb-20-34-62
System Uptime: 02:57:16

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254
Primary DNS: 8.8.8.8

----- running-config -----

hostname RY-LGSP16-10username admin privilege 15 password encrypted YWRtaW4=!vlan 1!!!ip route 0.0.0.0 0.0.0.
t-to-point!!line console 0!line vty 0!line vty 1!line vty 2!line vty 3!line vty 4!line vty 5!line vty 6!line
----- System log -----

2011-01-01T01:00:03+01:00 RY-LGSP16-10 [ Warning ] Switch just made a cold boot
2011-01-01T01:00:03+01:00 RY-LGSP16-10 [ Info    ] Password of user 'admin' was changed
2011-01-01T01:00:05+01:00 RY-LGSP16-10 [ Warning ] Link up on port 6
2011-01-01T01:00:09+01:00 RY-LGSP16-10 [ Info    ] topologyChange
2011-01-01T01:00:11+01:00 RY-LGSP16-10 [ Info    ] topologyChange
2011-01-01T01:00:52+01:00 RY-LGSP16-10 [ Info    ] Topology: New Device(192.168.1.111) add
2011-01-01T01:01:03+01:00 RY-LGSP16-10 [ Info    ] Topology: Device(TECHNIK-ASUS 192.168.1.111) Off-line is
2011-01-01T01:01:04+01:00 RY-LGSP16-10 [ Warning ] Link down on port 6
2011-01-01T01:01:04+01:00 RY-LGSP16-10 [ Info    ] topologyChange
2011-01-01T01:01:06+01:00 RY-LGSP16-10 [ Warning ] Link up on port 6
2011-01-01T01:01:06+01:00 RY-LGSP16-10 [ Info    ] topologyChange
```

9 WARRANTY

barox Kommunikation guarantees that their products shall remain free from material and machining faults for the duration of the warranty period specific to the country in question. The warranty provided by barox Kommunikation is totally independent from any other guarantee commitment on the part of the vendor resulting from the respective purchase contract with the end customer and shall not affect this commitment in any way.

barox Kommunikation shall remedy any product defects caused by poor material quality and/or a machining error of which barox Kommunikation is notified during the warranty period. barox Kommunikation shall then decide at their own discretion what measures to take to alleviate the defect. The warranty for any repaired or replaced components shall then continue to apply for the remaining warranty period.

The warranty programme shall not apply to any products from which the serial numbers have been removed, rendered illegible or changed. In addition, the warranty shall not cover the following damage:

1. Damage caused by an accident or improper or incorrect operation of the device, in particular, non-compliance with the instructions for use applying to the respective product
2. Damage caused by using components not manufactured or sold by barox Kommunikation
3. Damage caused by changes made without the prior written approval of barox Kommunikation
4. Damage caused by maintenance work not carried out by barox Kommunikation or authorised representatives of barox Kommunikation
5. Damage caused during transport, through negligence, fluctuations in or loss of the power supply, force majeure or the operating environment
6. Damage due to normal wear and tear
7. Damage caused by computer viruses or other software
8. Damage caused by setting, resp. reconfiguring passwords

For any services supplied by barox Kommunikation in connection with remedying defects or damage as a result of any of the grounds for exclusion listed above, an additional fee for manpower, transport and parts shall be incurred. An additional fee shall be charged for reinstalling the original software.