# Bedienungsanleitung

**19"- RY-Switche der L-Serie**

- 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 Industrie-Switche der L-Serie**

- RY-LPIGE-602GBTME
- RY-LPIGE-804GBTME
- RY-LPITE-802GBTME
- RY-LPITE-804GBTME
- RY-804GBTME, ohne PoE

**19"-Switche:**
**RY-Switche der L-Serie**
**Firmware Release v6.54.3133**
**Hardware Version 1.01**

**Industrie-Switche:**
**Firmware Release v7.10.1972**
**Hardware Version v1.01**



Haftung
Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. barox Kommunikation behält sich das Recht vor, Änderungen an den Geräten und/oder am Handbuch ohne Vorankündigung zu tätigen.
Unser Produkt kann unbeabsichtigte technische und/oder typografische Fehler beinhalten. Änderungen werden regelmässig vorgenommen, um unser Produkt zu verbessern.
Die aktuelle Bedienungsanleitung ist jeweils auf unserer Webseite erhältlich.
www.barox.ch

Herausgeber:

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

Erscheinungsdatum: August 2019
Version: 1.3

# INHALTSVERZEICHNIS

# 1 EINLEITUNG

Diese Bedienungsanleitung beschreibt die Inbetriebnahme der Switche und die Konfiguration der wichtigsten Grundfunktionen.

Der Nutzer dieses Handbuch sollte folgende Kenntnisse aufweisen:

- Installations- und Handhabungskenntnisse über elektronische Geräte
- Vertraut mit Computersystemen
- Kenntnisse über Local Area Networks (LANs) und Basiswissen über IP-Kommunikation
- Umgang mit Webbrowser

## 1.1 Inhalt

Das Bedienungshandbuch ist in folgende Kapitel unterteilt:

1. Einleitung
2. Inbetriebnahme der Switche
3. Diagnostik Möglichkeiten und Firmware Upgrade

## 1.2 Über uns

Überall dort, wo Netzwerke für die Videoübermittlung in höchster Qualität prompt und sicher transportiert werden müssen, sorgt barox Kommunikation mit seinen POWERHAUS Switchen für wegweisende Verbindungen.

barox plant, koordiniert und liefert einfache Punkt-zu-Punkt-Verbindungen genauso wie ausgedehnte Netzwerke mit Multicast-Anwendungen.

## 1.3 Website

Informationen über die gesamte Switch-Produktlinie sowie die Links zum Herunterladen von Datenblättern, Dokumentationen und aktueller Firmware stehen auf unserer Web-Seite: www.barox.ch zur Verfügung.

## 1.4 Support

Bei möglichen Problemen oder Rückfragen zur Konfiguration der Switche stehen Ihnen unsere POWERHAUS Partner zur Verfügung.

# 2 Kurzbeschreibung

Alle RY-Switche sind Full-Gigabit IP-Switche mit Layer 2/2+ Funktionen, mit unterschiedlicher Anzahl optischer und elektrischer Ports bestückt, managebar und unterstützen je nach Modell bis zu PoE++.

## 2.1 Besonderheiten für Videonetzwerke

- **Aktive Überwachung der Kamera**

Vom Switch über PoE gespeiste Kameras werden dauernd überwacht. Bei einem Kameraausfall startet der Switch die Kamera selbständig wieder neu. Gelingt dies nicht, setzt der Switch eine Alarmmeldung über SNMP ab.

- **Aktive Überwachung der PoE-Speisung**

Wird z.B. durch eine defekte Kamera zu viel Leistung vom Switch verlangt, alarmiert der Switch über SNMP.

- **Aktive Verwaltung der PoE-Leistung**

Beim Aufstarrten des Switches können die einzelnen PoE-Ports zeitversetzt auf gestartet werden, um eine Überlastung der PoE-Netzteile zu verhindern.

- **Weitere nützliche Eigenschaften**

Jumbo Frames bis 9600Bytes werden bei 1Gbits und auch bei 100Mbits unterstützt.
Portsicherheit durch MAC-Adresseneinschränkung sowie IP-Erkennung.

Einlesbarkeit bzw. Bereitstellung von Zertifikaten.
Extra hohe Backplane Leistung für ruckelfreie Videoübertragung bei voller Portbelegung.

Per Knopfdruck (Frontpaneel) erkennbar, welche Ports PoE beziehen.

### 2.2 DMS (Device Management System)

Der Switch besitzt ein integriertes Netzwerküberwachungs- und Steuerungssystem, dass dem Nutzer auf sehr einfache Weise einen guten Überblick über das gesamte Netzwerk gibt.
Die Ansicht der Netzwerktopologie erlaubt einen schnellen Überblick aller im Netzwerk vorhandenen Switche und Endgeräte wie z.B. IP-Kameras oder Server mit Angabe der IP-Adresse, der Geräteart und -bezeichnung. Es können Grundriss- und Umgebungspläne als Hintergrundbilder hinterlegt werden, mit denen der Nutzer auch ohne Kenntnisse der IP-Struktur schnell auf bestimmte Netzwerkgeräte zugreifen kann.
Fertig erstellte Pläne können wieder exportiert und Dokumentationsunterlagen beigelegt werden.

## 3 Inbetriebnahme

Die Switche können mittels Webbrowser konfiguriert werden. Hierfür kann der PC/Laptop an einem beliebigen RJ45-Port angeschlossen werden. Zu beachten ist, dass der PC/Laptop mit der IP-Adresse im gleichen Netzwerk-Segment ist wie der Switch. Zum Bsp.: 192.168.1.111

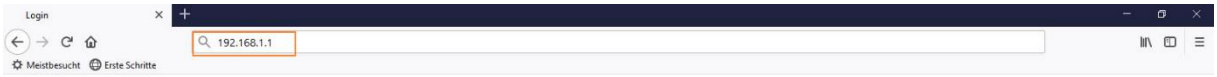
Alternativ können die Switche auch über CLI (Consolen-Port) konfiguriert werden. In dieser Dokumentation wird die Konfiguration des Switches mittels Webbrowser erklärt.

### 3.1 Werkeinstellung und Login

Ab Werk haben die Switche folgende Einstellungen:

IP-Adresse : 192.168.1.1
Subnet-Mask : 255.255.255.0
User : admin
Passwort: admin

Durch Eingabe der IP-Adresse des Switches (192.168.1.1) direkt im Webbrowser, wird die Verbindung zum Switch hergestellt. Die Anmeldung erfolgt mittels Eingabe des Usernames und Passwortes.

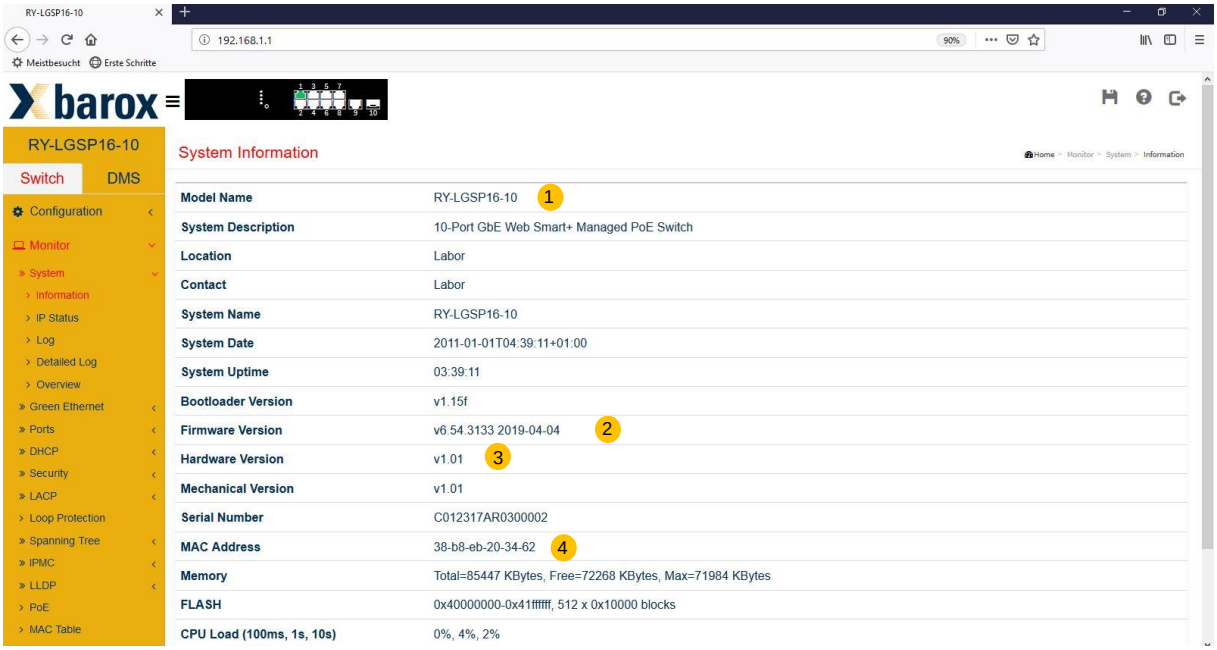




Nach erfolgreichem Login wird automatisch die Seite "System Information" angezeigt, in der die wichtigsten Angaben zum Switch ersichtlich sind.

### 3.2 System Information

Auf dieser Seite sind die wichtigsten Angaben zum Switch ersichtlich.

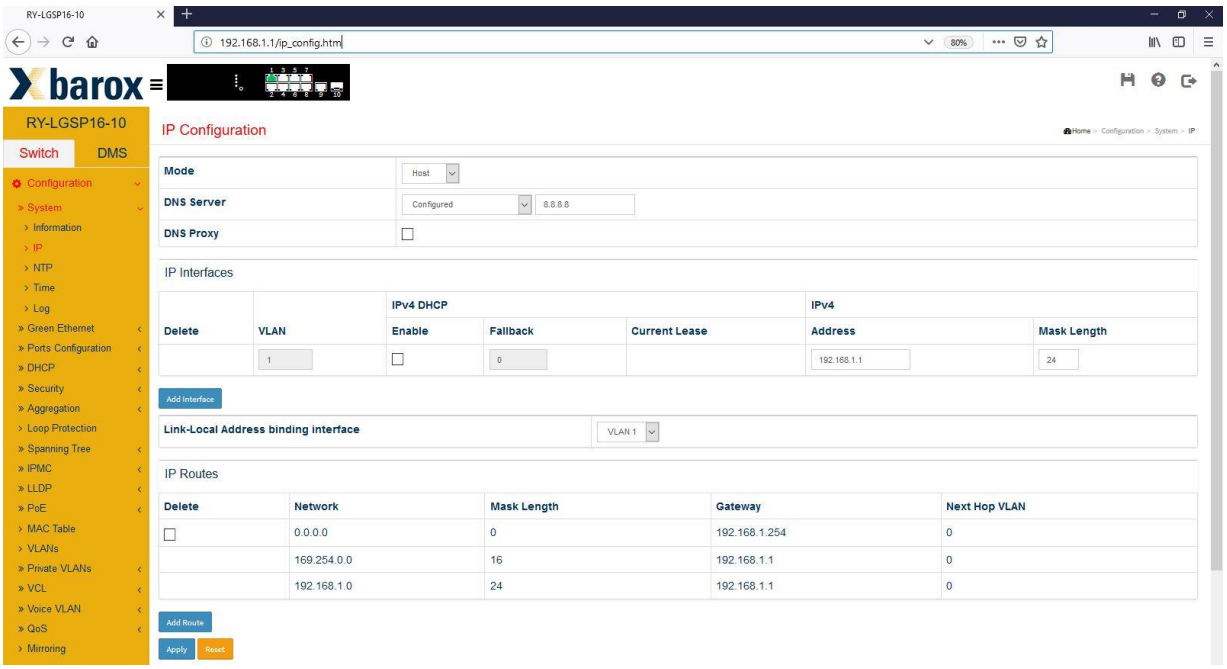



Legende:

1. Model Name des Switches
2. Firmware Version
3. Hardware Version
4. MAC-Adresse

### 3.3 Fixe IP-Adresse vergeben oder DHCP

Als erster Schritt ist dem Switch eine IP-Adresse zu vergeben. Hierfür wird in der Baumstruktur der Menüpunkt "Configuration/System/IP" gewählt.



Fixe IP-Adresse

Im oberen Bild sieht man, dass der Switch die IP-Adresse 192.168.1.1 hat, die Subnet-Mask 24 (255.255.255.0) und dem VLAN 1 angehört. Das VLAN 1 ist somit das Management-VLAN.

Soll dem Switch eine neue IP-Adresse vergeben werden, ist die bestehende IP-Adresse zu überschreiben und mit dem Icon "Apply" zu bestätigen. Das Gleiche gilt, falls die Subnet-Mask geändert werden muss.

DHCP

Wird der Switch in einem Netzwerk integriert, in dem ein DHCP-Server die IP-Adressen vergibt, muss das Feld unterhalb "IPv4 DHCP" markiert werden.

Der DHCP-Server vergibt dem Switch eine IP-Adresse im vordefinierten Bereich.

Um nun die erhaltene IP-Adresse ausfindig zu machen, gibt es zwei Möglichkeiten.

a) Software-Tool, zum Bsp.: SoftPerfect Network Scanner

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

b) Konsolen-Port

Hierfür kommt das mitgelieferte Konsolen-Kabel zum Einsatz. Der Konsolen-Port am Switch ist eine RS232-Schnittstelle. Es wird also ein PC/Laptop mit serieller Schnittstelle oder einen USB–RS232-Wandler benötigt.

Als Software empfehlen wir "PuTTy", um den Switch via CLI-Port zu konfigurieren.

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

Die CLI-Schnittstelle hat ab Werk folgende Einstellung:

| | |
|---|---|
| Bitrate: | 115'200 |
| Daten-Bits: | 8 |
| Parität: | keine |
| Stop-Bits: | 1 |
| Flusssteuerung: | keine |

Ist die Verbindung mit der seriellen Schnittstelle hergestellt, ist eine Anmeldung mittels Username und Passwort erforderlich.

Mit nachfolgendem Befehl kann die IP-Adresse erfragt werden:

RY-LGSP23-26# *show ip interface brief*

➔ Wichtig: die Änderung muss nun definitiv gespeichert werden.

Hierfür via Web-Browser mit der neuen IP-Adresse auf den Switch zugreifen und oben rechts auf das Diskettensymbol klicken.

### 3.4 Gateway konfigurieren

Wurde dem Switch eine neue IP-Adresse vergeben, muss die Gateway Adresse zwingend entsprechend angepasst werden.


Um die Gateway Adresse zu ändern muss die Zeile zuerst gelöscht und dann mit der richtigen Adresse neu erstellt werden. Die Network Adresse muss auf "0.0.0.0" und die Mask Length auf "0" gesetzt sein.

Nur die Gateway Adresse ist entsprechend dem Netzwerk neu zu schreiben.

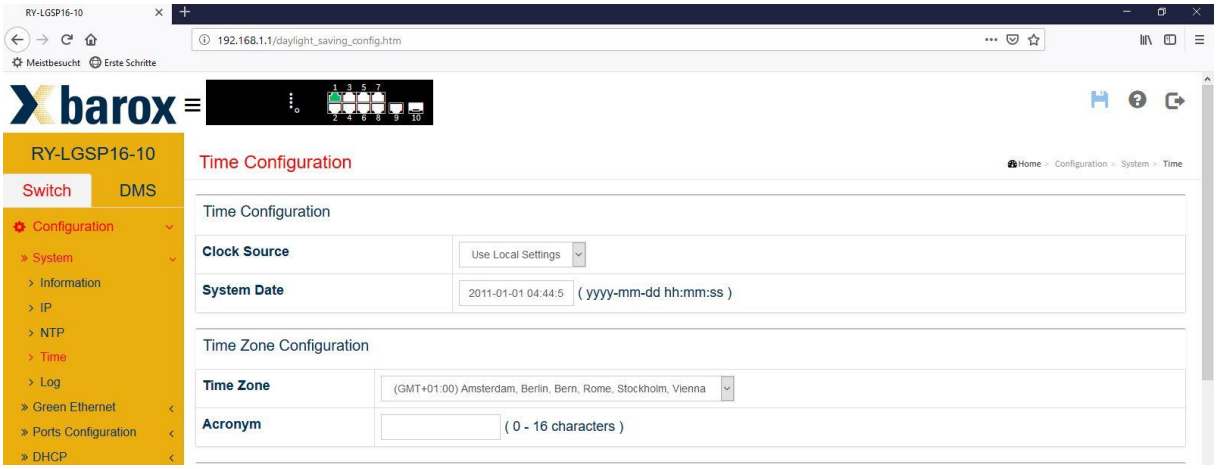
### 3.5 Uhrzeit einstellen

Die Systemuhrzeit der barox Switche kann manuell oder mittels NTP-Server konfiguriert werden. Sinn und Zweck der Uhrzeitdefinition ist das Log-File. Bei einer Fehlermeldung wird der Eintrag im Log-File mit einem Zeitstempel ergänzt, so dass Störungs- und Fehlerzeiten genau hinterlegt und mögliche Ursachen lokalisiert werden können.

#### 3.5.1. Local Settings

Im Menüpunkt "Configuration/System/Time" wird als "Clock Source" "Use Local Settings" gewählt. Im Feld unterhalb "System Date" wird dann, entsprechend der Formatvorgabe, das Datum und die Uhrzeit manuell eingetragen und mit der Taste "Apply" bestätigt.

➔ Bei einem Neustart des Switches geht die Uhrzeit verloren und muss wieder neu konfiguriert werden, da der Switch nicht über eine Stützbatterie verfügt.




#### 3.5.2. NTP (Network Time Protocol)

Das Network Time Protocol ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze.

Die Konfiguration erfolgt in zwei Schritten.

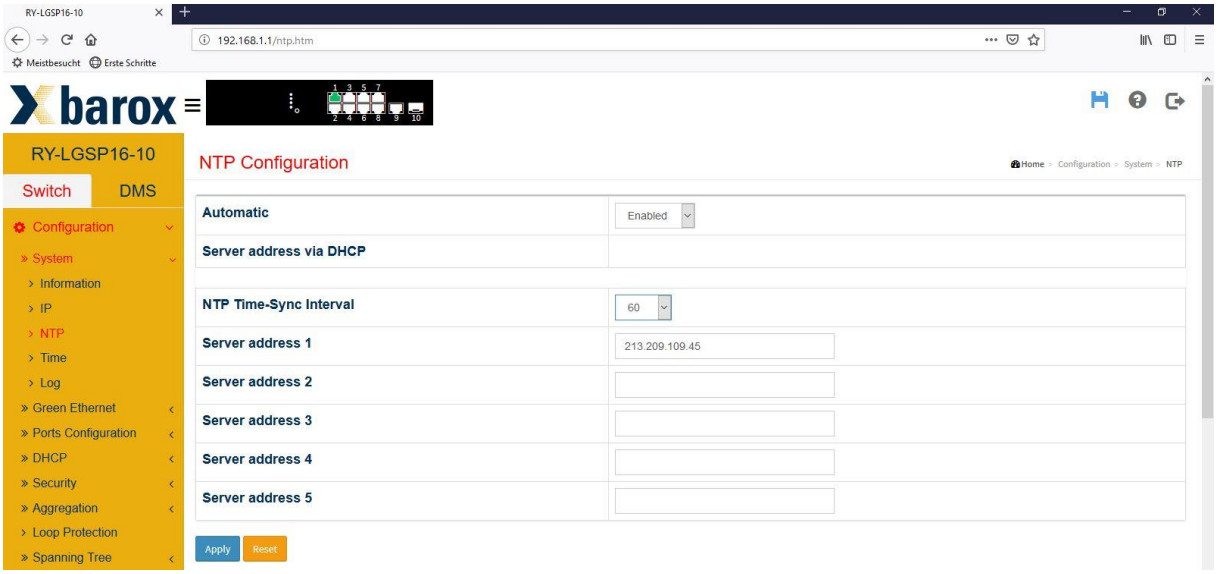
### 3.5.2.1. NTP-Server

Im ersten Schritt muss dem Switch mitgeteilt werden, woher es die Uhrzeit beziehen soll.

Soll die Uhrzeit direkt vom DHCP-Server bezogen werden, ist das Feld "Automatic" auf "Enabled" zu setzen. In der Zeile unterhalb wird dann die IP-Adresse des DHCP-Servers dargestellt.

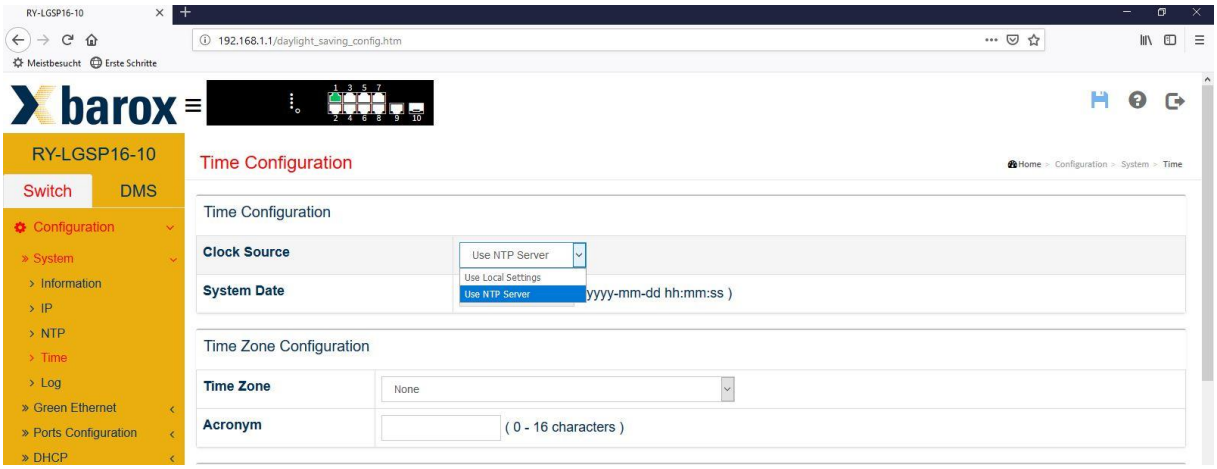
Soll die Uhrzeit von einer bestimmten Quelle, zum Beispiel von Zeitserver, NTP-Server oder Firewall etc. bezogen werden, ist die entsprechende IP-Adresse im Feld "Server address 1" einzutragen. Nur so wird sichergestellt, dass der Switch die IP-Adresse auch erreichen kann. Es besteht die Möglichkeit, bis zu 5 Quellen zu definieren.

Falls im eigenen Netzwerk keine Zeitquelle zur Verfügung steht und eine Quelle von ausserhalb via Internet bezogen werden soll, kann auch ein externer NTP-Server direkt eingetragen werden, wie zum Beispiel 213.209.109.45 von [http://www.pool.ntp.org/de/](http://www.pool.ntp.org/de/)

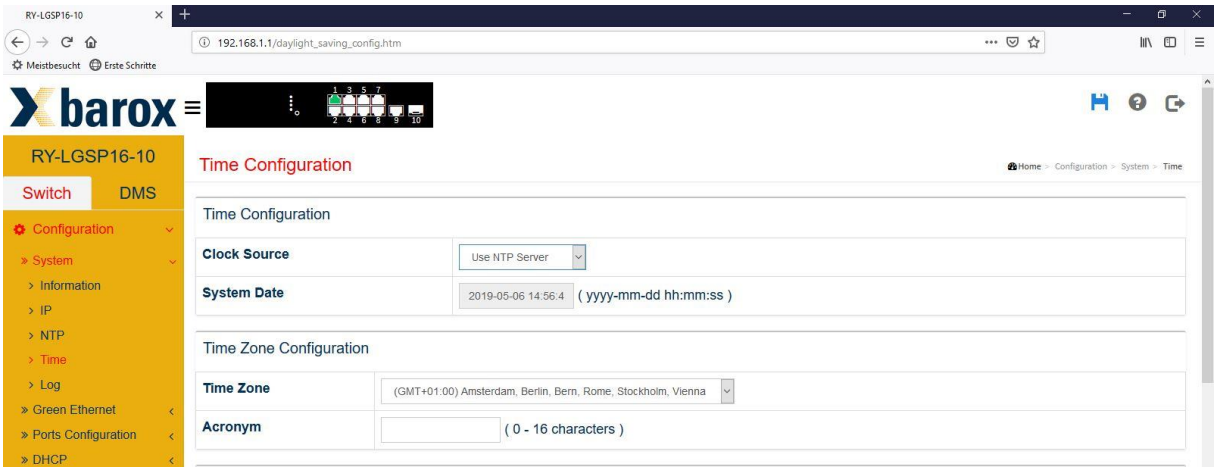



### 3.5.2.2. Time Settings

Im Menüpunkt "Configuration/System/Time" muss nun als "Clock Source" "Use NTP Server" gewählt werden.



Da die Zeitserver in der Regel die Greenwich Mean Time ausgeben, muss entsprechend die "Time Zone" gewählt werden, damit a) die Uhrzeit stimmt und b) die Sommer-/Winterzeit korrekt umgestellt wird.



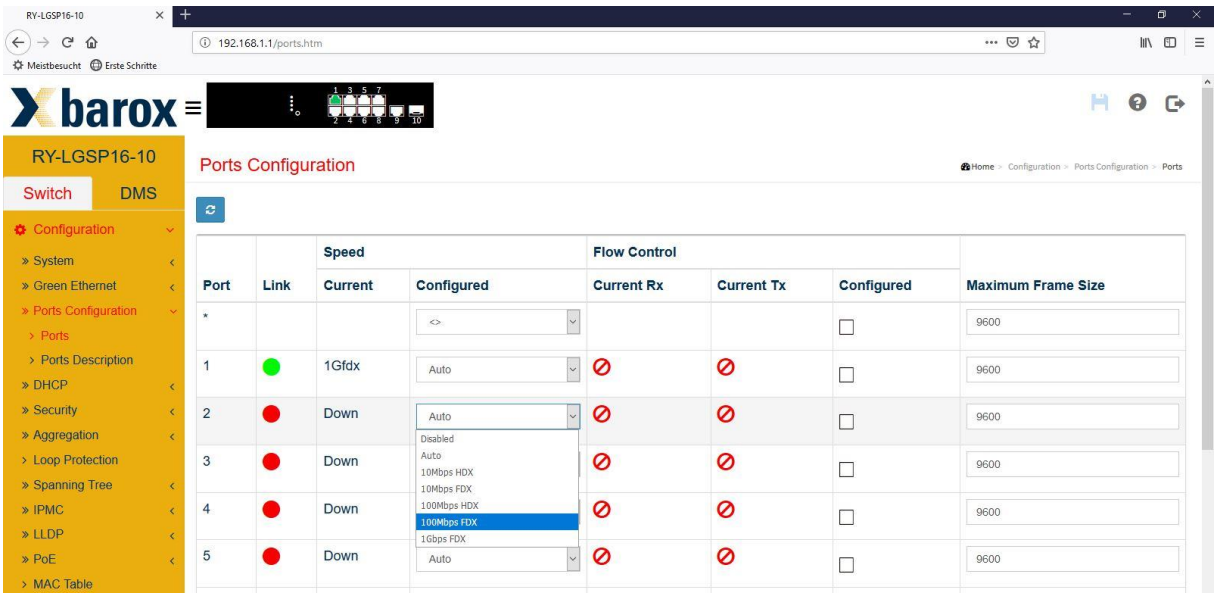

Sobald der Switch Uhrzeit und Datum beziehen kann, wird die korrekte Uhrzeit im Feld "System Date" dargestellt.

### 3.6 Port Konfiguration

Die Ports sind ab Werk im Auto-Modus eingestellt. Autonegotiation bezeichnet ein Verfahren, das zwei miteinander verbundenen Ethernet-Ports erlaubt, die maximal mögliche Übertragungsgeschwindigkeit und das Duplex-Verfahren selbstständig miteinander auszuhandeln und zu konfigurieren. Das Verfahren gilt nur für Twisted-Pair-Kabel – nicht für Glasfaserverbindungen.

Trotzdem kann es vorkommen, dass das Endgerät nicht richtig erkannt wird. Dies kommt ab und zu bei Kameras mit 100Mbit/s Interface vor. In diesen Fällen muss der Port manuell auf 100Mbit/s eingestellt werden.

Soll ein Port aus Sicherheitsgründen nicht nutzbar sein, kann es auch ganz ausgeschaltet werden. Hierfür ist der Konfigurationsmodus auf "Disabled" zu setzen.



### 3.6.1. SFP-Port

Die SFP-Ports verfügen auch über einen Auto-Modus. Dieser unterscheidet sich vom Autonegotiation der Kupfer-Ports. SFP-Ports können mit Autonegotiation nur die Übertragungsgeschwindigkeit erkennen und unterstützten nur Fullduplex.

Es kann vorkommen, dass der Switch einen SFP nicht richtig erkennt, ob es ein 100Mb oder 1000Mb-SFP ist und deshalb nicht funktioniert. In diesem Fall muss die Datenrate am Port manuell konfiguriert werden.


Die SFP-Ports der Switche sind nicht codiert. Das heißt, es können auch SFPs anderer Hersteller eingesetzt werden, jedoch ohne Funktionsgarantie.

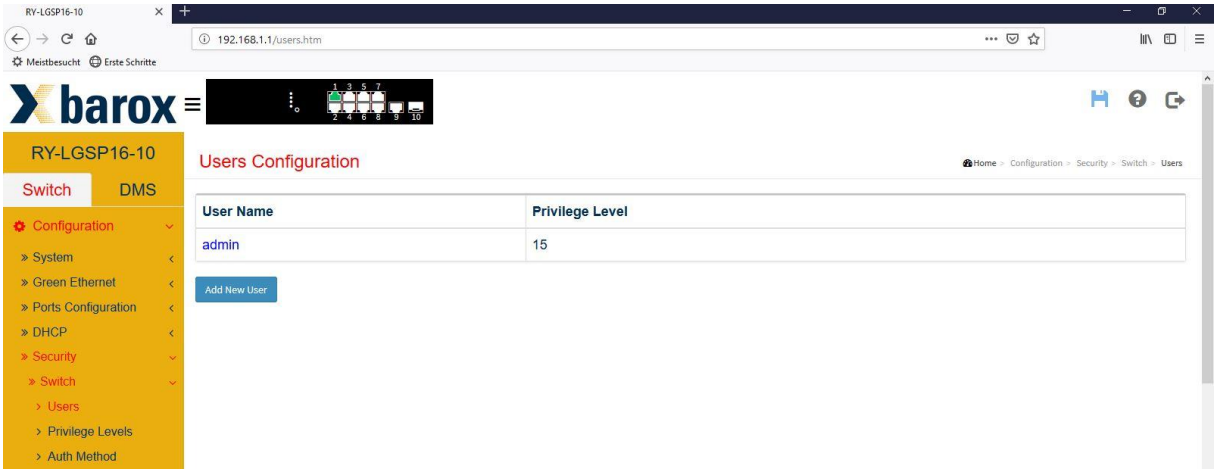
Das barox Sortiment umfasst SFPs für Multi- und Singlemode Fasern mit 100Mbit/s, 1Gbit/s oder 10Gbit/s Übertragungsgeschwindigkeiten. Die möglichen Distanzen variieren je nach Fasertyp und Übertragungsgeschwindigkeit zwischen 550m und 120km.

➔ Siehe http://www.barox.ch/cm/produkte/product/ip-produkte/zubehoer/ac-sfp

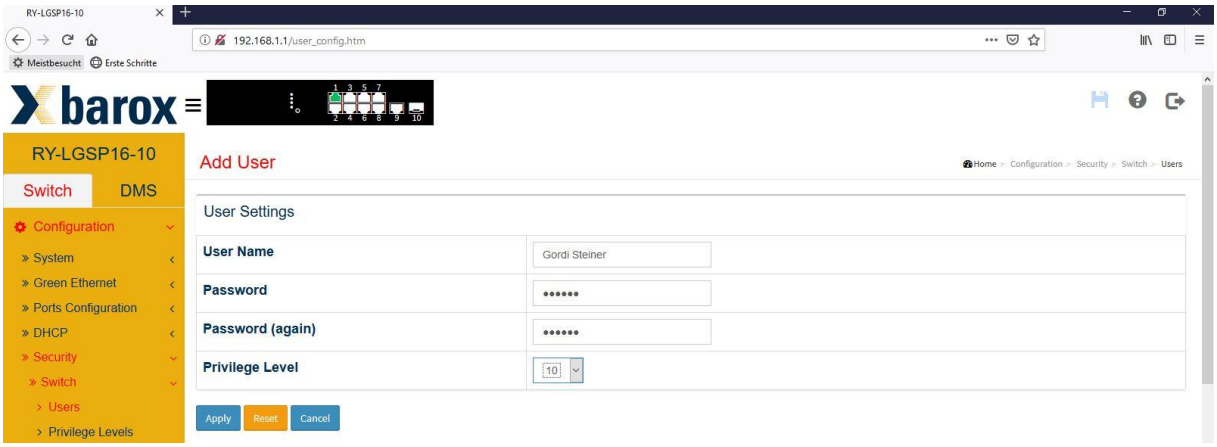
## 3.7 Username und Passwort ändern

barox Switche bieten die Möglichkeit, mehrere Nutzer mit unterschiedlichen Berechtigungen zu generieren. Es können bis zu 15 verschiedene Level definiert werden.

Level 15 ist der höchste Level und für Administratoren gedacht.

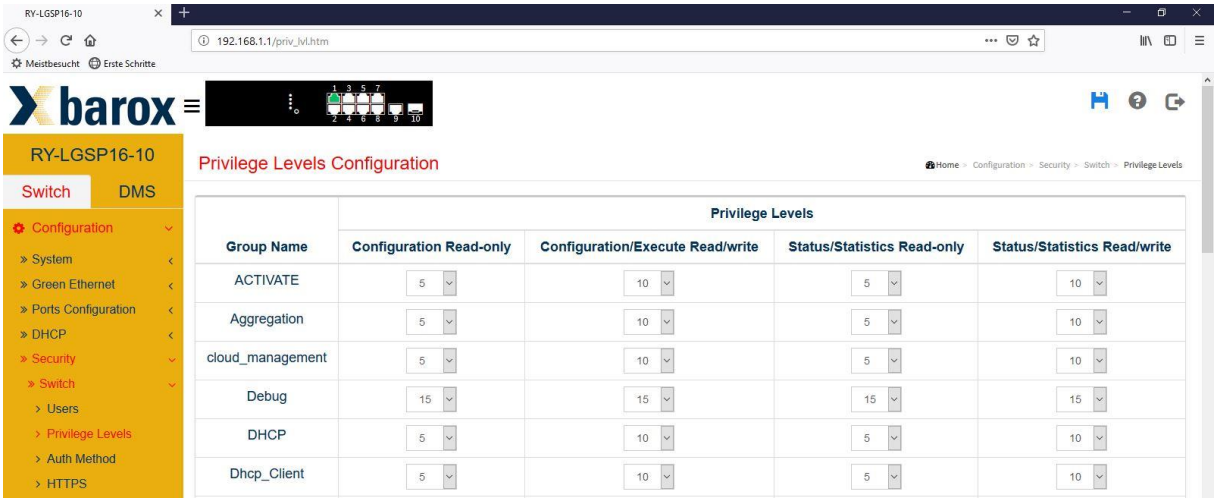



Mit "Add New User" kann ein weiterer Nutzer generiert werden. Zu definieren sind der Name des Users, das Passwort und der Berechtigungslevel.




Im Menüpunkt "Privilege Levels" kann nun die genaue Berechtigungsvielfalt des neuen Nutzers definiert werden.

Im nachfolgenden Beispiel hat der Techniker die Berechtigungsstufe 10. Das heißt, er darf aufgrund der Lese- und Schreibberechtigung alles konfigurieren. Für das "Debug" hat er jedoch eine zu niedrige Berechtigungsstufe, so dass er "Debug" nicht einmal lesen darf.




Die Tabelle ist sehr umfangreich und so können Berechtigungen sehr detailliert vergeben werden. Man könnte zum Beispiel einen Nutzer definieren, der nur die MAC-Tabelle lesen darf.

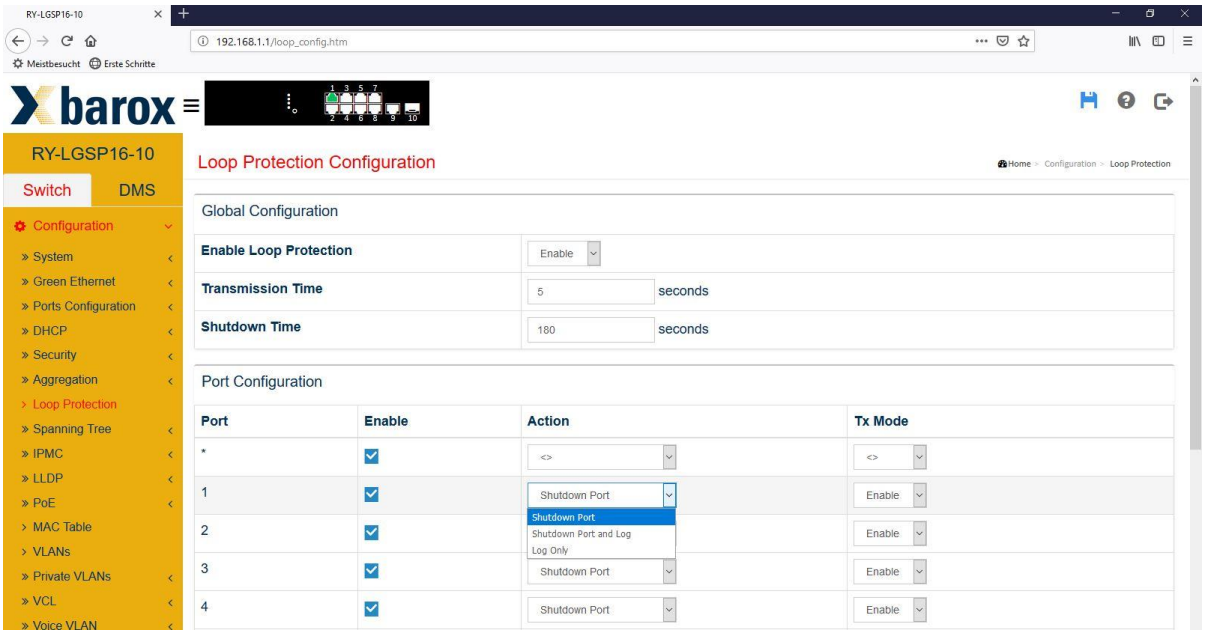
### 3.8 Loop Protection

Bei größeren Netzwerken kann es schnell vorkommen, dass man versehentlich bzw. ungewollt einen Ring physikalisch zusammensteckt. Ohne aktiv geschaltetem Ring-Protokoll (z. B. RSTP) hängt sich das gesamte Netzwerk auf und wird funktionsuntauglich.

Für solch eine Situation dient das Leistungsmerkmal "Loop Protection". Ist dieser aktiviert, kann bei dem versehentlich zusammengesteckten Ring definiert werden, ob der Port ausgeschaltet oder nur ein Eintrag im Log-File getätigt werden soll oder beides ("Shutdown and Log").

➔ Ports, die bereits mit RSTP aktiv geschaltet sind, dürfen nicht zusätzlich mit Loop Protection überwacht werden. Dies führt zu massiven Störungen im Netzwerk.

Die "Shutdown Time" sagt aus, wie lange ein Port deaktiviert bleiben soll, falls eine Loop detektiert wird. Mögliche Zeiteingabe: 0 – 604800s (7 Tage). Mit der Eingabe "0" bleibt der Port deaktiviert bis der Switch neu gestartet wird.




## 3.9 Ring-Konfiguration

Um eine Redundanz im Netzwerk sicherzustellen, ist der Aufbau einer Ringtopologie zwingend erforderlich. Damit das Netzwerk durch einen Broadcast-Sturm nicht überlastet wird, wird ein Schutzmechanismus benötigt.

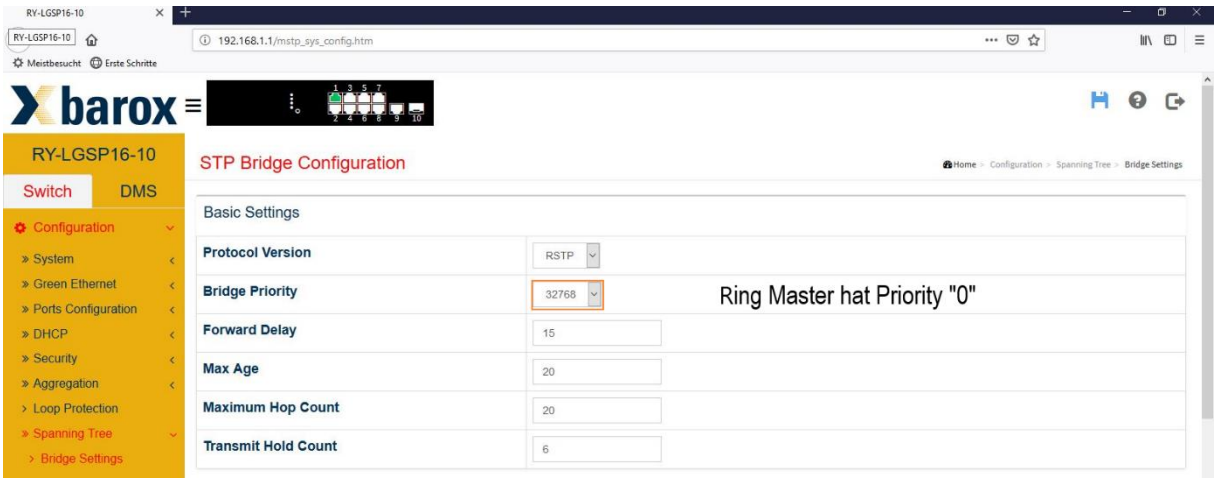
RSTP (Rapid Spanning Tree Protocol) ist eins der grundlegenden Protokolle in Ethernet-Netzwerken. Es sorgt dafür, dass in einem Netzwerksegment keine Netzwerkschleifen entstehen. Ethernet-Frames haben im Gegensatz zu IP-Paketen keine maximale Lebensdauer (Time to Live, TTL) und bewegen sich deshalb potenziell unendlich lange im Kreis, was wiederum das Netzwerk überlasten und im schlechtesten Fall zum Erliegen bringen kann.

Auf Wikipedia ist die Funktion des Rapid Spanning Tree Protocol (RSTP) ausführlich erklärt.
https://de.wikipedia.org/wiki/Spanning_Tree_Protocol

### 3.9.1. Ring Master

In einer Ring-Topologie muss ein Switch als Master, der die Ringüberwachung übernimmt, definiert werden. Bei einem möglichen Verbindungsunterbruch meldet er dies allen Switchen im Ring, so dass die alternative Verbindung aktiv geschaltet wird. Der Switch mit der Priority 0 ist der Ring Master.

Das RSTP-Protokoll ist so konzipiert, dass ohne definiertem Ring Master der Switch mit der kleinsten MAC-Adresse automatisch Ring Master wird.

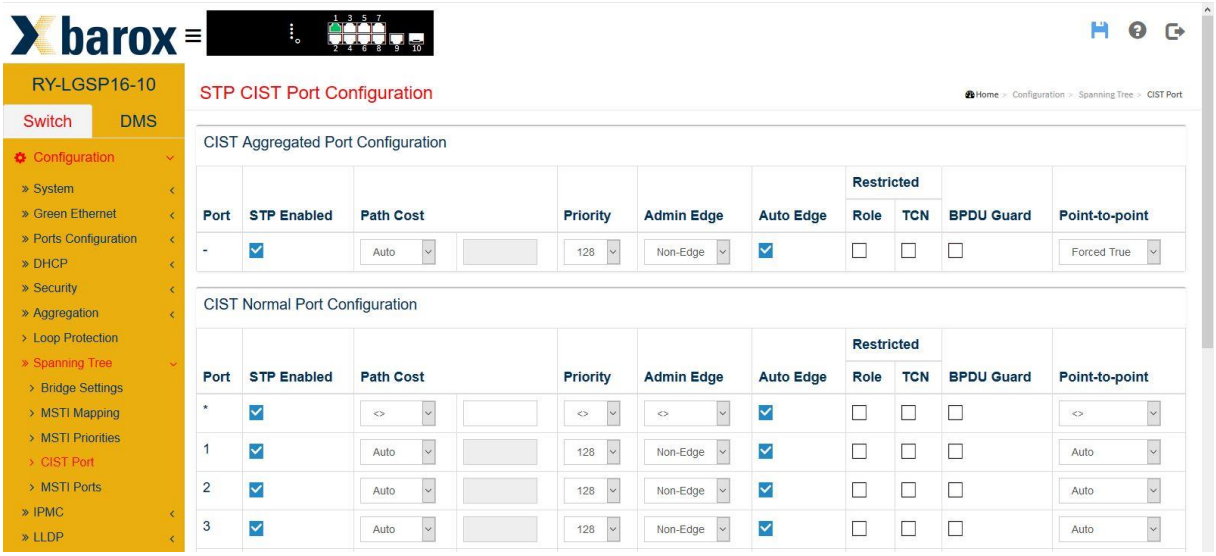


Im Menüpunkt "Spanning Tree / Bridge Settings" muss die gewünschte Protokollversion gewählt werden. RSTP wird von allen Switch-Herstellern unterstützt und ist somit kompatibel zu Dritt-Herstellern.

Per Default haben die Switche die "Bridge Priority" 32768. Soll der Switch als Master fungieren, muss die Bridge Priority auf "0" gesetzt werden. Alle anderen Werte können so belassen werden wie sie sind.

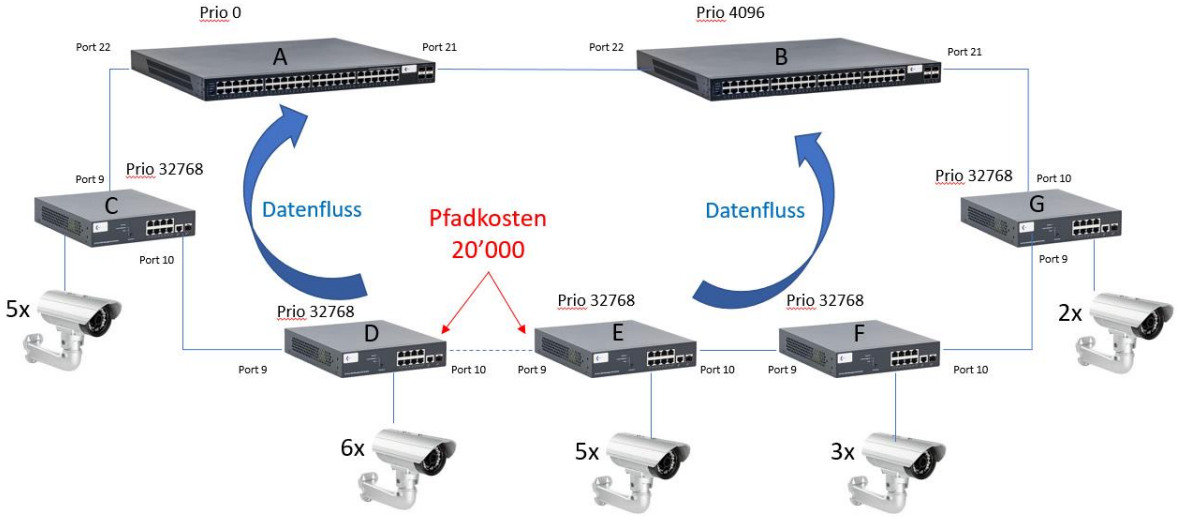
### 3.9.2. Port Konfiguration

Ab Werk ist bei allen Ports "STP Enabled" aktiv. Somit kann der Ring theoretisch an einem x-beliebigen Port gebildet werden. Zur optimalen Lastverteilung im Netzwerk, kann per Definition mittels Pfadkosten der Datenpaketfluss gelenkt werden. Der Name Pfadkosten stammt von der Zeit als Mietleitungen für die Verbindung von A nach B gemietet wurden und somit teuer waren.




Beispiel:

Bei einem größeren Ring mit mehreren Endgeräten und größeren Datenmengen, macht es durchaus Sinn, den Datenfluss im Ring zu lenken, damit die Switche gleichmäßig belastet werden (Lastverteilung). Hierfür sind die Pfadkosten zu definieren.



Im dargestellten Beispiel besteht das Netzwerk aus zwei zentralen Switchen (A+B) und 5 weiteren Switchen, die gemeinsam einen Ring bilden. Insgesamt sind 21 Kameras installiert, die je 5Mbits Videodaten liefern. Insgesamt also über 100Mbits Daten.

**Szenario 1: nur RSTP an allen Switchen aktiv**

Der Switch mit der niedrigsten MAC-Adresse übernimmt die Master Funktion. Eventuell handelt es sich um den kleinsten Switch mit geringster CPU-Leistung im Ring. Die Richtung des Datenflusses ist unbekannt.

Bei einem Unterbruch kann die Umschaltzeit etwas länger dauern, da der kleine Switch die Daten nicht so schnell verarbeiten kann.

**Szenario 2: RSTP an allen Switchen aktiv, Switche-A Prio 0 und Switch-B Prio 4096**

Per Definition übernimmt in diesem Fall Switch A die Master Funktion. Fällt er aus übernimmt Switch B die Master Funktion. Switch A überwacht den Ring und bei einem Unterbruch im Netzwerk hat die CPU genügend Leistung, um schnell zu agieren. Am Switch A ist unter Umständen der Port 21 als "Blocked" markiert. Das heisst, der Datenfluss aller Videokameras kommt über Port 22. Der kleine Switch C muss die Daten aller Videokameras verarbeiten, es entsteht ein Flaschenhals.

**Szenario 3: RTSP aktiv, Master definiert und Pfadkosten definiert**

Mit dieser Konfiguration wird der Datenfluss genau definiert. Die Last wird auf zwei Seiten verteilt. Kein Switch kommt an seine Grenzen. Dadurch, dass am Switch D, Port 10 und am Switch E, Port 9 die Pfadkosten teurer sind als bei allen anderen Ports im Ring, wird diese Strecke nur bei Unterbruch im Netzwerk aktiv geschaltet.

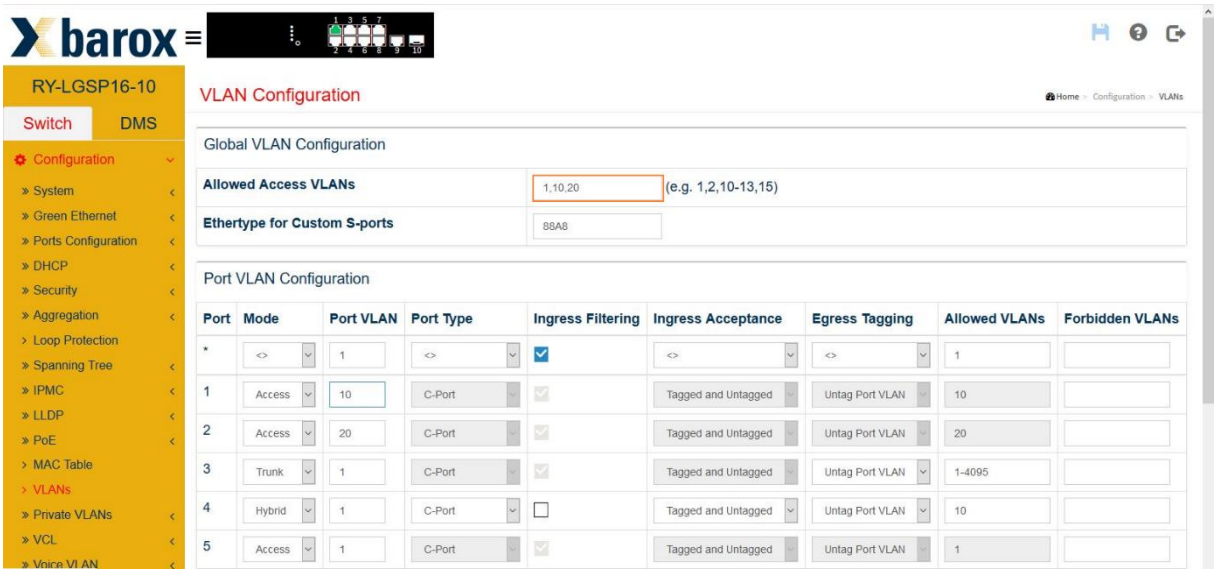
Pfadkosten Werkeinstellung:

Die Kosten sind abhängig vom Abstand zur Root Bridge (Master) und dem zur Verfügung stehenden Uplink zum Ziel. Ein 100 Mbit/s-Uplink hat üblicherweise höhere Pfadkosten als ein 1Gbit/s-Uplink zum gleichen Ziel, der 100 Mbit Link würde daher als redundanter Pfad geblockt werden. Die Pfadkosten sind nach IEEE-Vorgaben genormt, können aber manuell abweichend festgelegt werden, beispielsweise, um bei gleicher Geschwindigkeit einen bevorzugten Uplink auszuwählen, um so die reellen Kosten von Standleitungen widerzuspiegeln.

➔ **Wenn immer möglich sollte die Konfiguration wie im Bild dargestellt angestrebt werden.**

### 3.10 VLAN Konfiguration

Die VLAN Konfiguration findet auf einer einzigen Seite statt.
Im Feld "Allowed Access VLANs" müssen alle VLAN-Nummern aufgeführt werden, die eingerichtet werden sollen.




Sind die VLAN-Nummern aufgeführt können nun die einzelnen Ports einer Funktion und einem VLAN zugeteilt werden.

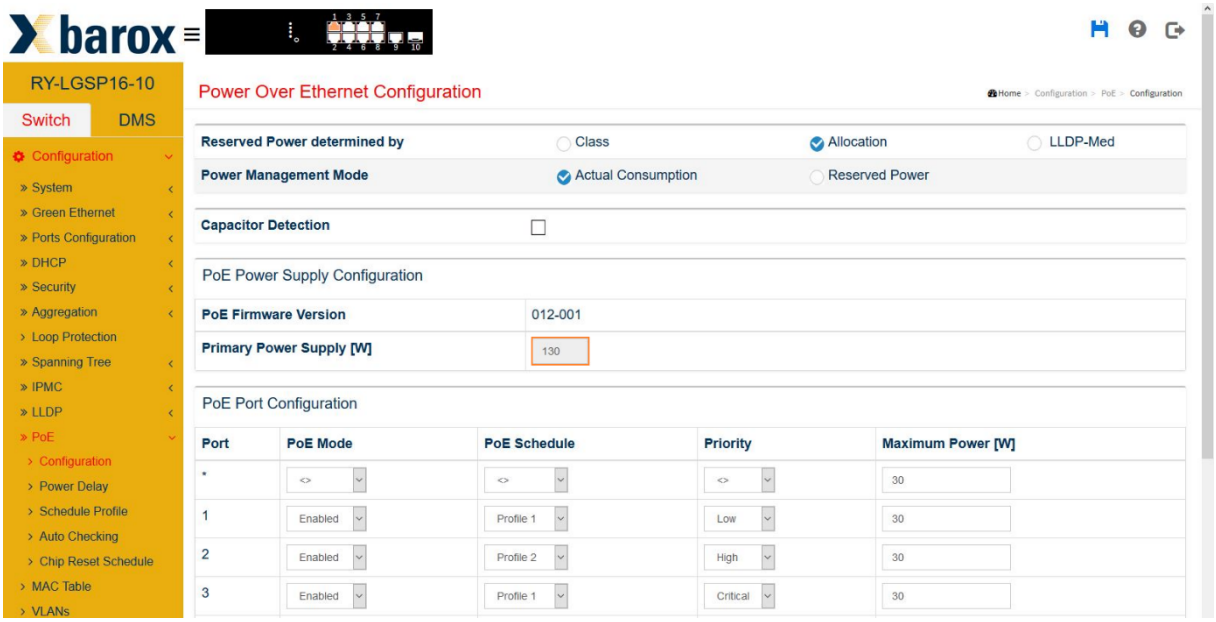
| Modus | VLAN | Funktion |
|---|---|---|
| Access | Nr | an diesem Port wird ein Endgerät angeschlossen. |
| Trunk | --- | Verbindung zwischen zwei Switchen |
| Hybrid | --- | Verbindung zwischen zwei Switchen oder zu einem Endgerät |

Sowohl im Trunk- als auch im Hybridmodus kann in der Spalte "Allowed VLANs" definiert werden, welche VLAN's erlaubt sind.

### 3.11 Power over Ethernet (PoE)

Im PoE-Bereich verfügt der Switch über viele Möglichkeiten, den Einsatz von PoE zu optimieren. Strom kann zeitlich oder Event gesteuert aus- bzw. eingeschaltet werden. Darüber hinaus lassen sich Powered Devices (z. B. PoE Kameras) überwachen und bei Bedarf neu starten und der PoE-Chip in der Kamera lässt sich resetten. Dies ist dann sinnvoll, wenn die Kamera zwar anpingbar ist, aber kein Bild zeigt.

### 3.11.1. PoE Konfiguration




Jeder Switch hat eine definierte Leistungsfähigkeit. Diese beschreibt, wie viel Leistung über die PoE-Ports abgegeben werden können. Massgebend ist das eingebaute Netzteil im Switch. In unserem Beispiel, ein RY-LGSP16-10 Switch mit 8 PoE+-Ports, stehen max. 130W zur Verfügung. Das heisst, es ist unmöglich an allen 8 Ports jeweils ein 30W Endgerät anzuschliessen, da dafür 240W erforderlich würden. Das integrierte Netzteil kann so viel Leistung nicht bereitstellen.

Deshalb ist die Leistungszuteilung pro Port zu beachten.

PoE-Verbraucher sind je nach Verbrauch in unterschiedlichen Klassen eingeteilt.

| Klasse | Verfügbare Leistung am versorgten Gerät | Klassifizierungssignatur |
|---|---|---|
| 0 | 0,44–12,96 W | 0 bis 4 mA |
| 1 | 0,44– 3,84 W | 9 bis 12 mA |
| 2 | 3,84– 6,49 W | 17 bis 20 mA |
| 3 | 6,49–12,95 W | 26 bis 30 mA |
| 4 | 12,95-25,50 W (nur 802.3at/Typ 2)[4] | 36 bis 44 mA |

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

**Reserved Power determined by**

Unter Reserved Power determined kann definiert werden, wonach sich die max. Leistungsbereitstellung richten soll.

- Class = entspricht der Klasse, mit der sich das Endgerät zu erkennen gibt
- Allocation = gemäss der Angabe in der Spalte "Maximum Power (W)"
- LLDP-Med = dito Class-Mode, bezieht die Information mittels LLDP (wenn möglich)

Überschreitet das Endgerät die vordefinierte Leistung, schaltet der Port das PoE ab.

**Power Management Mode**

Hier wird definiert wie sich der Switch verhalten soll, falls die max. mögliche Leistung überschritten wird.

- **Actual Consumption**

Überschreitet die bezogene Leistung aller Geräte die max. mögliche Leistung, die der Switch erbringen kann, wird das PoE komplett ausgeschaltet. Wird nur bei einem Port die Leistung überschritten, wird das PoE nur am jeweiligen Port ausgeschaltet.

In der Spalte "Priority" wird definiert, welcher Port wichtig ist. Mit „low“ markierte Ports werden sofort ausgeschaltet, während als "Critical" markierte Ports als letztes ausgeschaltet werden, falls die Gesamtleistung überschritten wird.

**Reserved**

Als „reserved“ markierte Ports werden nur dann abgeschaltet, wenn die reservierte Leistung in der Spalte "Maximum Power (W)“ überschritten wird.

**PoE Schedule**

Jeder Port kann einem Zeitplan zugeteilt werden. Insgesamt können 16 Zeitpläne erstellt werden.

### 3.11.2. PoE Power Delay

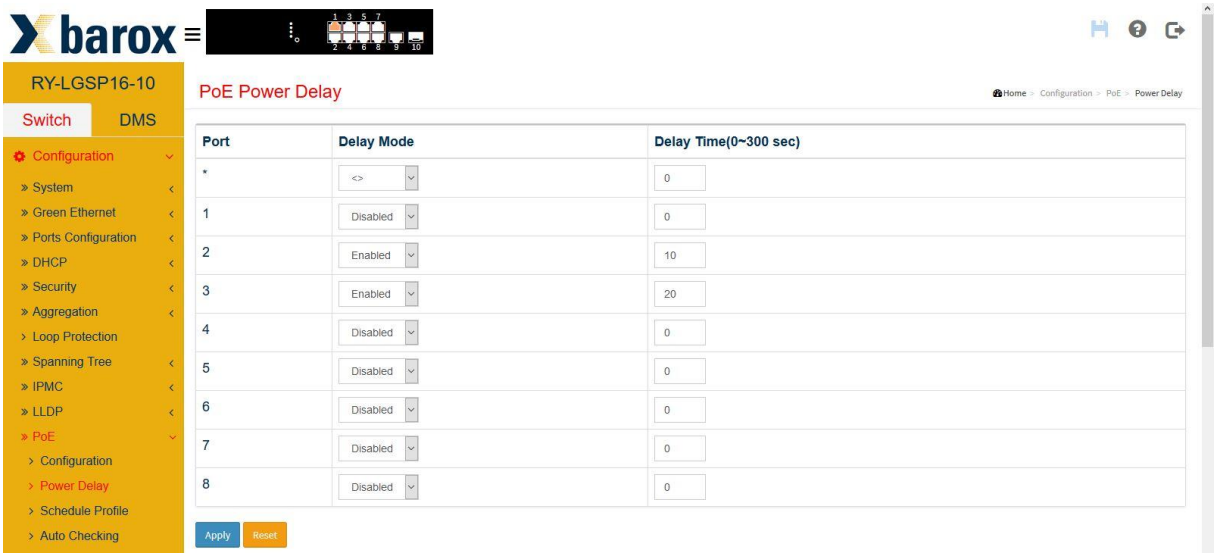
Wie bereits erwähnt kann der Switch eine begrenzte Leistung zur Verfügung stellen.

Heutige IP-Kameras benötigen immer mehr Leistung. Kommt eine Schwenk-Neigekamera mit eingebauter Heizung und IR-Strahler zum Einsatz steigt der Leistungsbedarf noch mehr.

Vor allem bei einem Neustart, bei Tag-Nacht-Umschaltung, Zuschaltung von Heizungen oder iR-Strahler usw. benötigen Kameras wesentlich mehr Strom (=Leistungspeaks) als im Dauerbetrieb.

Wenn nun mehrere Kameras an einem Switch angeschlossen sind und sich alle Kameras gleichzeitig anmelden, besteht die Möglichkeit, dass die maximal mögliche Switchleistung überschritten wird. Die Leistungsüberschreitung führt dazu, dass sich der Switch sofort wieder abmeldet und das Netzteil bei häufigen Fehlversuchen Schaden nimmt.

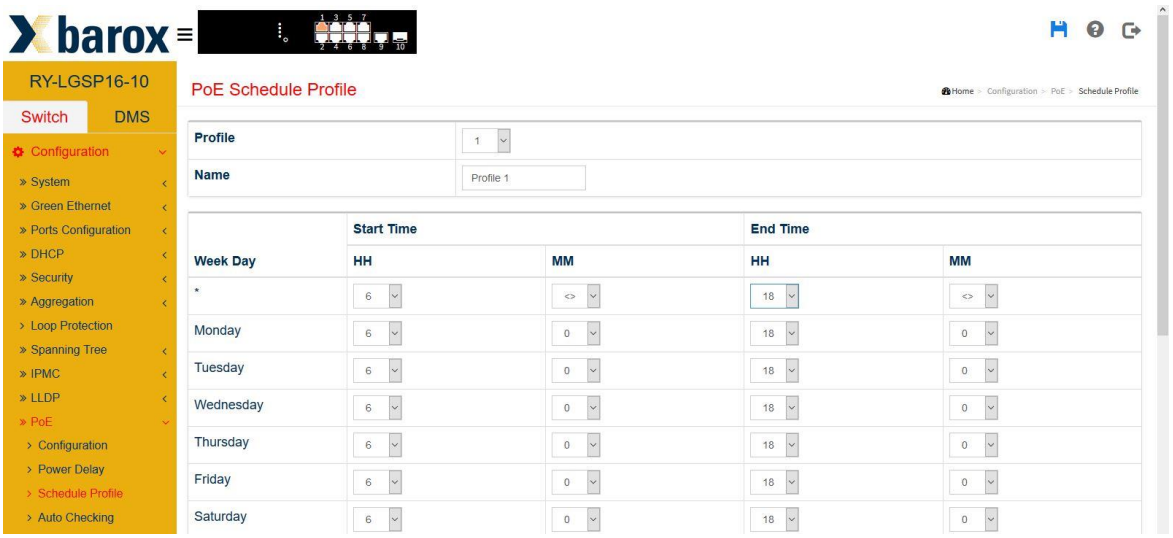
Um diese Problematik zu umgehen, kann im folgenden Menü ein zeitversetztes Aufstarrten jedes einzelnen Ports konfiguriert werden. Im nachfolgenden Beispiel werden Port 1 und 2 sofort aktiviert und dann immer 2 Ports jeweils 10 Sekunden später.




### 3.11.3. PoE Schedule

Das Ein- und Ausschalten des Stromes kann auch mit einem Wochenplan gesteuert werden. Es können bis zu 16 unterschiedliche Profile erstellt werden. Jeder Port kann einem Profil zugeteilt werden.

Im nachfolgendem Beispiel wird im Profil 1 PoE täglich von 06:00 bis 18:00 Uhr eingeschaltet.

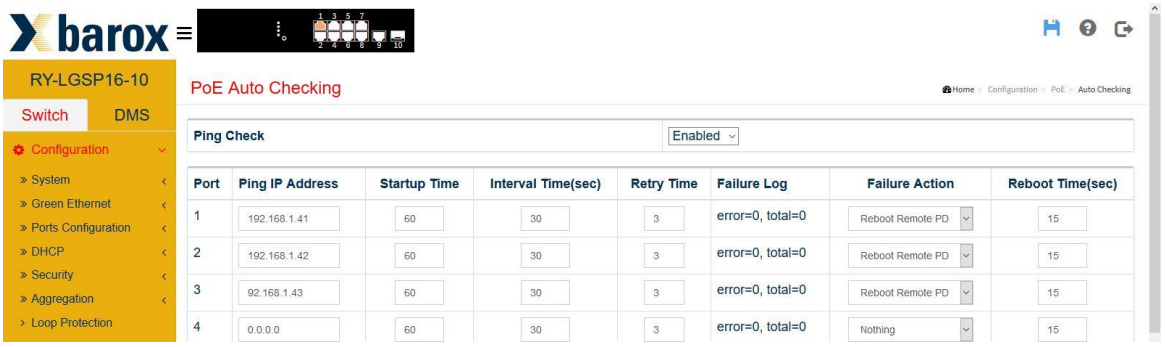



### 3.11.4. PoE Auto Checking

PoE Auto Checking dient der Funktionsüberwachung. Mittels Ping wird zum Beispiel alle 30 Sekunden die am Port 1 angeschlossene Kamera mit der IP-Adresse 192.168.1.25 auf deren Erreichbarkeit geprüft.

Nach 3 fehlerhaften Versuchen wird am Port 1 PoE ausgeschaltet und nach 15 Sekunden wieder eingeschaltet. So wird ein Neustart der Kamera erzwungen.

60 Sekunden nach dem Neustart läuft die Überwachung mittels Ping wieder an.



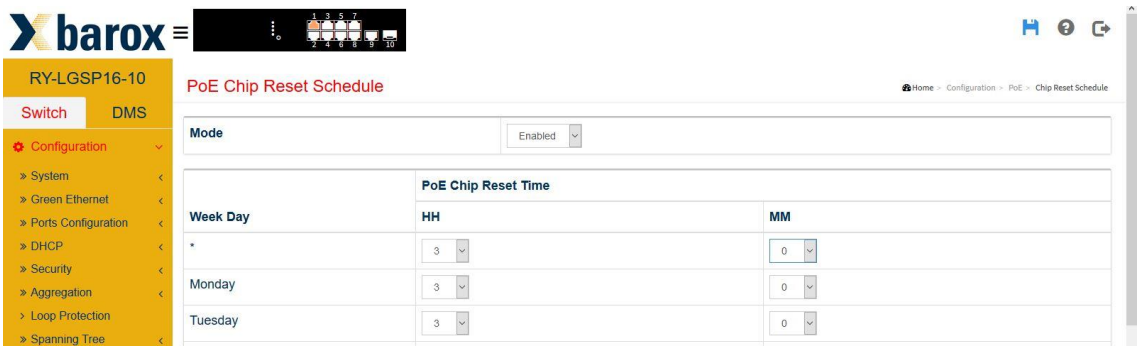

### 3.11.5. PoE Chip Reset Schedule

Es kommt vor, dass die Kameras mittels Ping noch erreichbar sind, jedoch kein Bild darstellen.

In den meisten Geräten ist die PoE-Steuerung auf einem separaten Chip. Es besteht die Möglichkeit, dass die CPU auf einen Ping Antwort gibt, der Videostream jedoch nicht übertragen wird.

Prophylaktisch kann der PoE Chip Reset Befehl täglich oder einmal wöchentlich, zum Beispiel um 03:00 Uhr gesendet werden.

Mit diesem Befehl wird der PoE-Chip der Kamera neu gestartet.

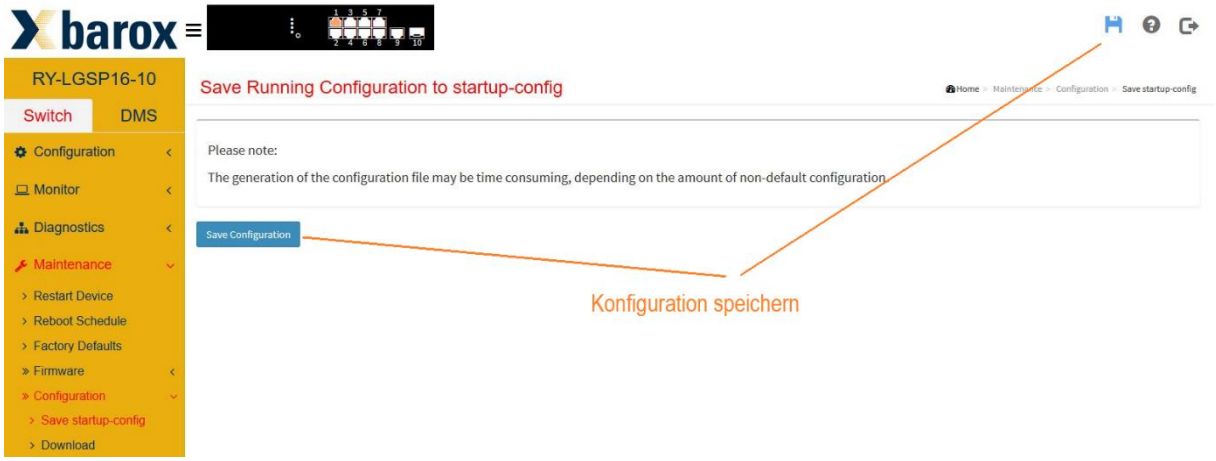


### 3.12 Speichern und Laden der Konfiguration

Jede Änderung muss gespeichert werden. Durch "Apply" wird die Änderung in den Arbeitsspeicher geschrieben. Bei einem Neustart leert sich der Arbeitsspeicher und die Änderungen gehen alle verloren. Die Änderungen müssen daher definitiv gespeichert werden.

Es gibt zwei Möglichkeiten:

- Disketten Symbol in jeder Maske
- Im Menü Maintenance/Configuration/Save startup-config

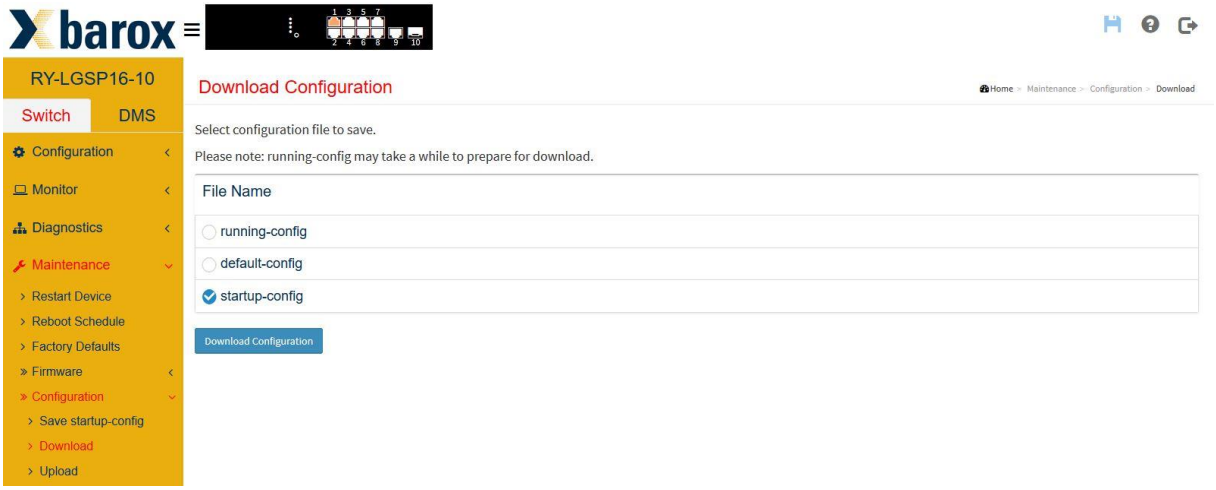



-

### 3.12.1. Konfiguration download

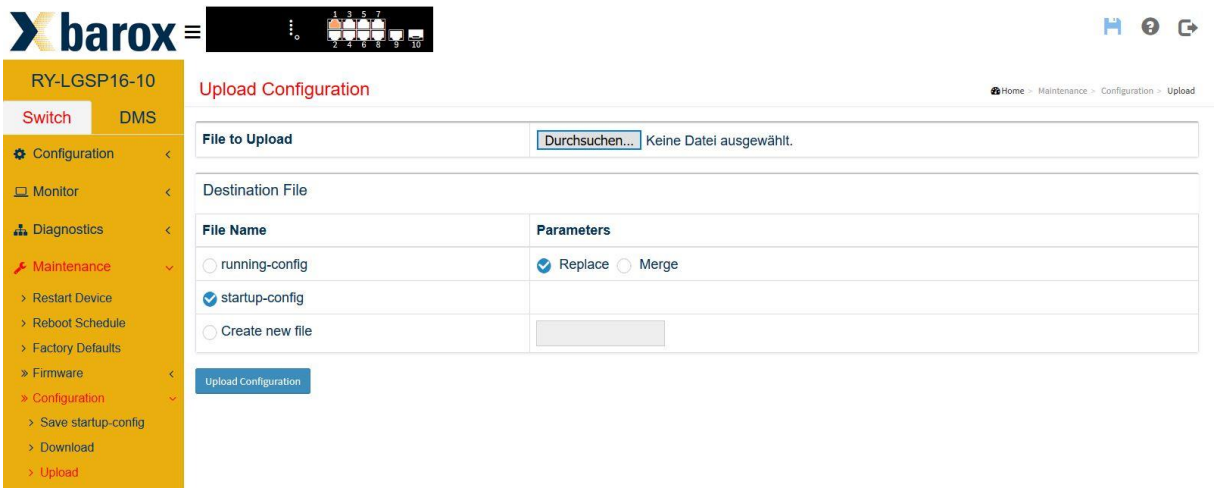
Die aktuelle Switch Konfiguration kann heruntergeladen und separat gespeichert werden. Das generierte Konfigurationsfile kann bei einem Switch Ersatz eingespielt oder verwendet werden, wenn mehrere Switche identisch konfiguriert werden müssen und nur die IP-Adresse zu ändern ist. Das erspart viel Zeit.

Wir empfehlen ausschliesslich das "startup-config File" zu speichern.




### 3.12.2. Konfiguration einspielen (upload)

Die umgekehrte Variante ist ein Konfigurationsfile in den Switch einzuspielen. Hierfür wird der Pfad des hinterlegten Files angegeben und um welchen Filetyp es sich handelt. In der Regel das "startup-config File".



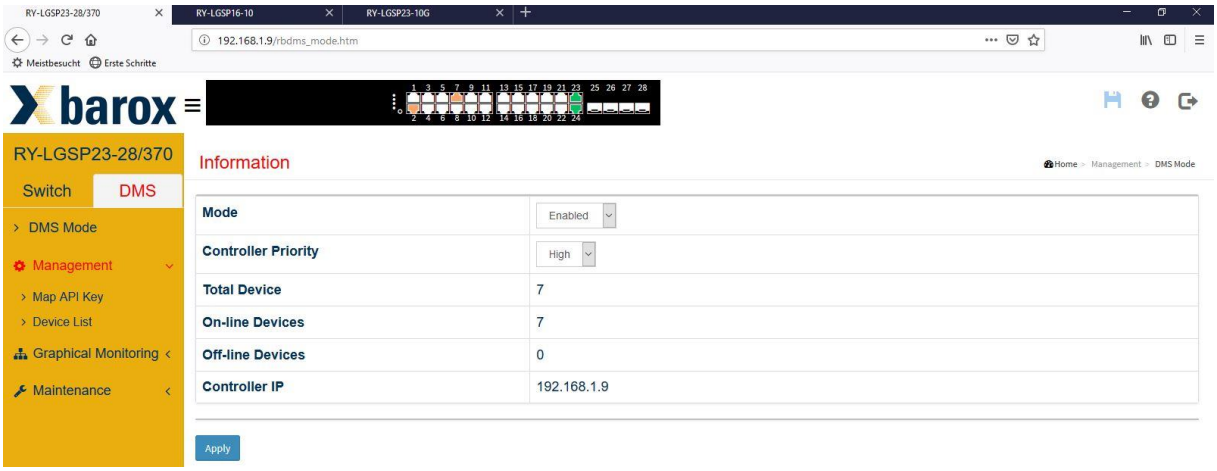

# 4 DMS Device Management System

Der Switch besitzt ein integriertes Netzwerküberwachungs- und Steuerungssystem, das dem Nutzer auf sehr einfache Weise einen guten Überblick über das gesamte Netzwerk gibt.
Die Ansicht der Netzwerktopologie erlaubt einen schnellen Überblick aller im Netzwerk vorhandenen Switche und Endgeräte wie z.B. IP-Kameras oder Server mit Angabe der IP-Adresse, der Geräteart und -bezeichnung. Es können Grundriss- und Umgebungspläne als Hintergrundbilder hinterlegt werden, mit denen der Nutzer auch ohne Kenntnisse der IP-Infrastruktur schnell auf bestimmte Netzwerkgeräte zugreifen kann.
Fertig erstellte Pläne können wieder exportiert und Dokumentationsunterlagen beigelegt werden.

## 4.1 Management

Um die DMS-Funktion zu nutzen, muss in das Register «DMS» gewechselt werden. Ab Werk ist DMS aktiviert. Auf der Informationsseite (Management/DMS Mode) ist ersichtlich, wie viele Geräte im Netzwerk erkannt wurden, wie viele davon on-line (aktiv) bzw. off-line (inaktiv) sind. Off-line sind Geräte, die entweder ausgeschaltet bzw. ausgefallen (defektes Endgerät) oder im Netz nicht mehr verfügbar sind (z. B. Servicelaptop, der vom Installateur nach Fertigstellung der Konfiguration mit nach Hause genommen wird).

Zur möglichen Nutzung des DMS, muss im Netzwerk ein Switch als Master definiert sein. Dieser Switch sammelt alle Informationen und gibt sie allen im Netzwerk befindlichen, DMS-fähigen Switches weiter. Das Feld Controller IP zeigt, welcher Switch (IP-Adresse) die Master-Funktion innehat.




**Bestimmung des DMS-Masters:**

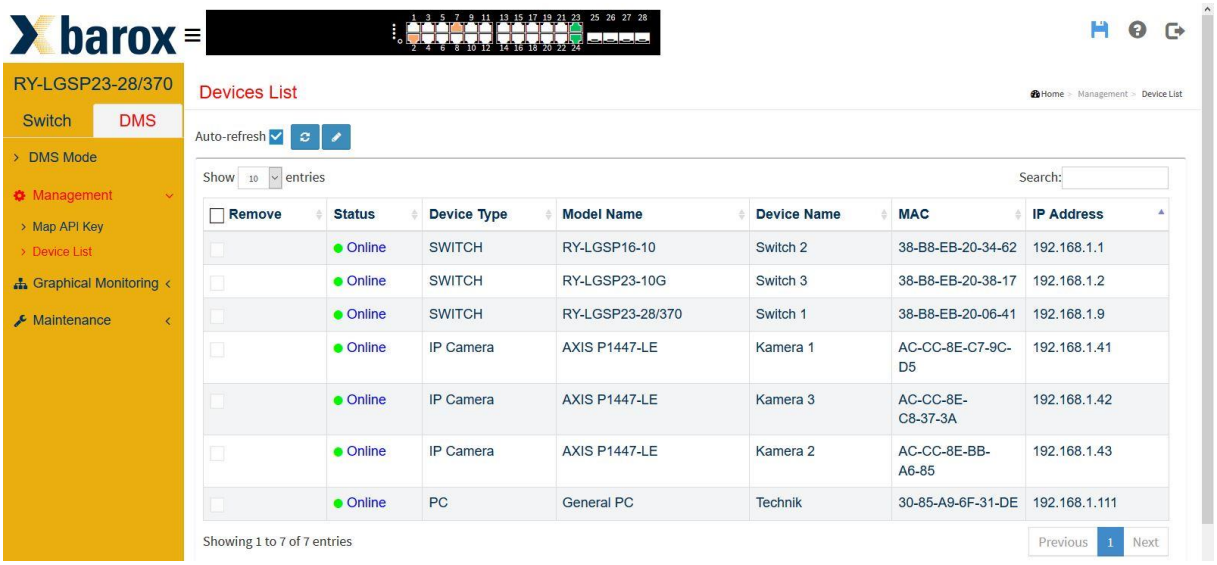
Bei dem Switch der Master sein soll, ist im Feld "Controller Priority", der Modus "High" zu wählen. Es empfiehlt sich, den leistungsstärksten Switch für diese Aufgabe zu definieren, da das DMS zusätzliche Rechenkapazität benötigt. Die weiteren Switche im Netzwerk können je nach Leistungsstärke abgestuft werden mit "Mid" oder "Low". Soll ein Switch nie ein DMS-Master werden, ist die Controller Priority auf "Non" zu setzen.

Bzw. kann bei sehr hoher Netzwerklast bei den am niedrigsten frequentierten Switch das DMS eingeschaltet und bei den anderen Switchen deaktiviert werden. Dabei ist zu beachten, dass einige Funktionen eingeschränkt sind und diese Methode bei einer homogenen Struktur mit barox Switchen empfohlen wird.

In der Zeile "Controller IP" wird mittels IP-Adresse angezeigt, welcher Switch der Master ist.

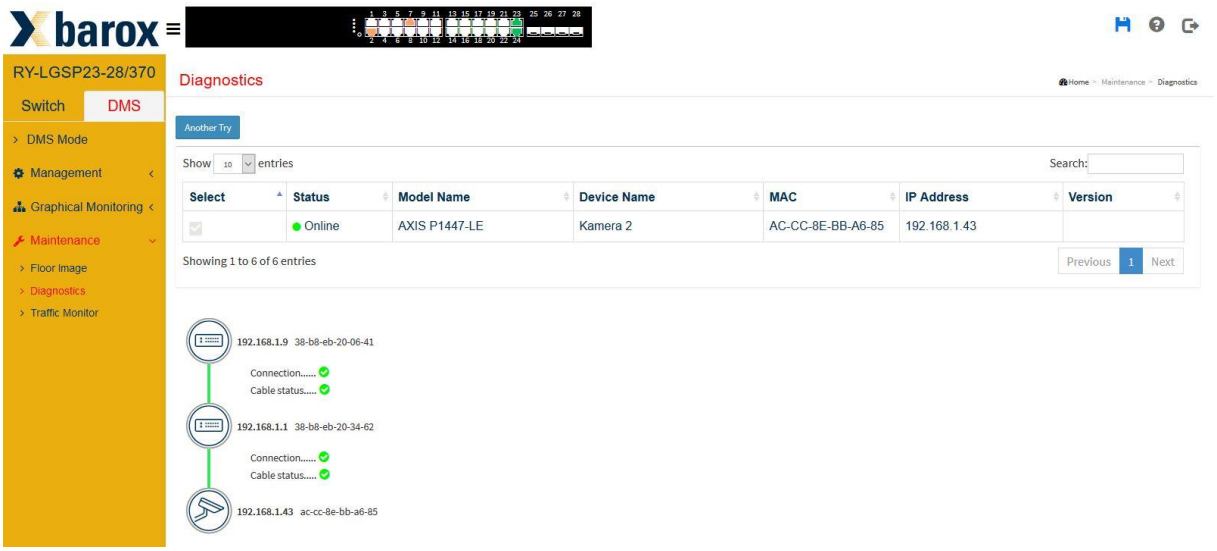
**Device List**

Auf dieser Seite werden alle Geräte aufgeführt, die im Netz on- oder off-line sind. In tabellarischer Form wird der Gerätetyp, der Status, Geräte Name sowie MAC- und IP-Adresse aufgelistet.
Sämtliche Geräte - auch die, deren IP-Adresse in einem anderen Netz-Segment angesiedelt sind, werden aufgeführt.
Diese nützliche Funktion hilft, wenn ein nicht konfiguriertes Gerät ins Netz integriert wird und die IP-Adresse unbekannt ist.




Mit einem Klick auf das Status-Symbol "Online" bzw. "Offline" kann die Verbindung zum Gerät – auch über mehrere Switche hinweg - überprüft werden.
Sollte irgendwo ein Unterbruch in der Verbindungskette sein, ist dies hier erkennbar.

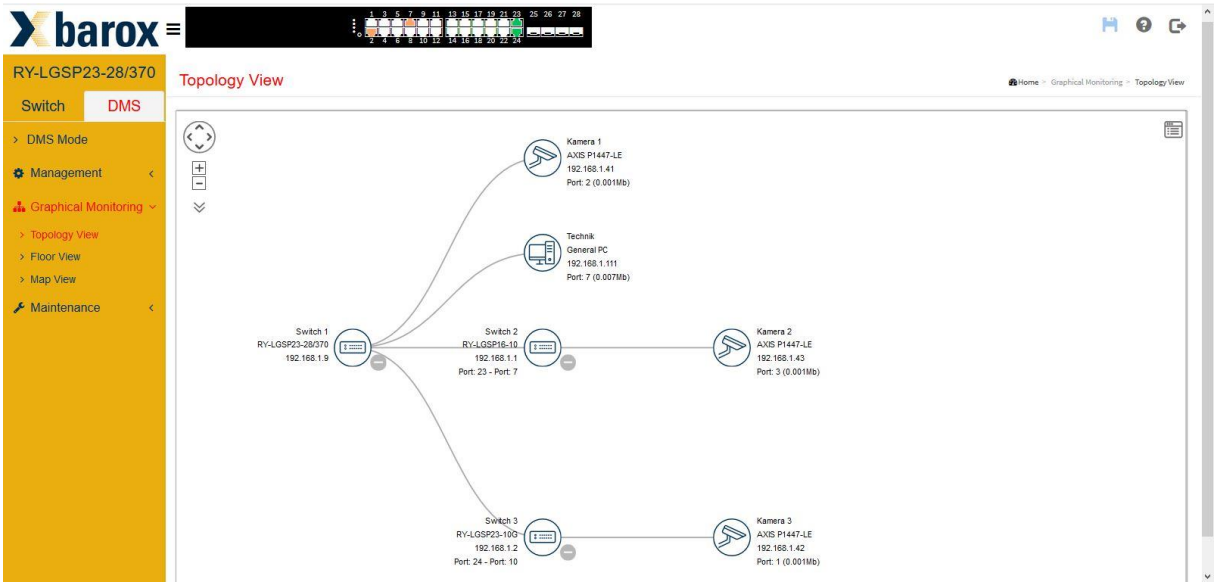
Die gleiche Überprüfung kann auch aus dem Menü "Maintenance/Diagnostics" durchgeführt werden.




## 4.2 Graphical Monitoring

### Topology View

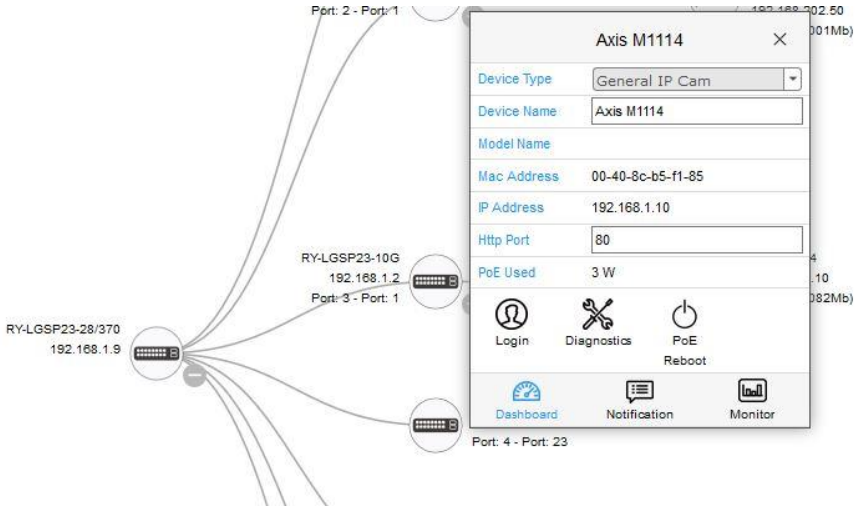
In der Topology View wird das Netzwerk inkl. aller angehängten IP Endgeräte automatisch grafisch dargestellt. Wird das Endgerät richtig erkannt, wird das entsprechende Symbol (Kamera, Switch, Accesspoint etc.) dargestellt. Sämtliche Informationen, wie Gerätename, IP-Adresse, Datenrate etc. erscheinen parallel zum Symbol. Alle Einstellungen lassen sich auch manuell konfigurieren.




Mit einem Klick auf das Symbol wird das "Dashboard" des entsprechenden Gerätes angezeigt.

Im "Dashboard" kann der Device-Typ und -Name definiert, MAC- und IP-Adressen sowie der in Echtzeit dargestellte PoE-Bedarf abgelesen werden, sofern es sich um einen PoE-Verbraucher handelt.

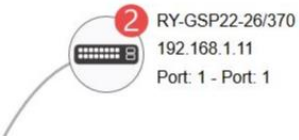
Zudem kann mittels "Login" direkt auf das Gerät zugegriffen oder eine Verbindungsdiagnose ausgeführt werden. Mit Klick des «PoE Reboot» Icons ist ein Neustart des PoE Verbrauchers problemlos möglich.

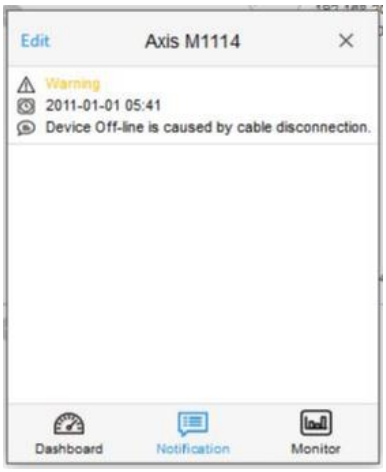



War ein Gerät

- kurzzeitig nicht erreichbar (Kabelfehler, Aussteckung des Verbrauchers etc.)
- nicht sofort per ONVIF lesbar
- mit bereits vorhandener IP Adresse angehängt worden
- usw.

erscheint neben dem Symbol eine rote Ziffer. Die rote Ziffer besagt, wie viele Meldungen zu diesem Gerät vorhanden sind. Im Menu "Notification" können die Meldungen gelesen und editiert werden.




Ist ein Gerät im Netzwerk nicht mehr vorhanden, wird es in der Topology-View rot dargestellt und im "Dashboard" das "Remove-Symbol" zur Verfügung gestellt. Mit einem Klick auf "Remove" wird das Gerät aus der Topology-View endgültig entfernt.

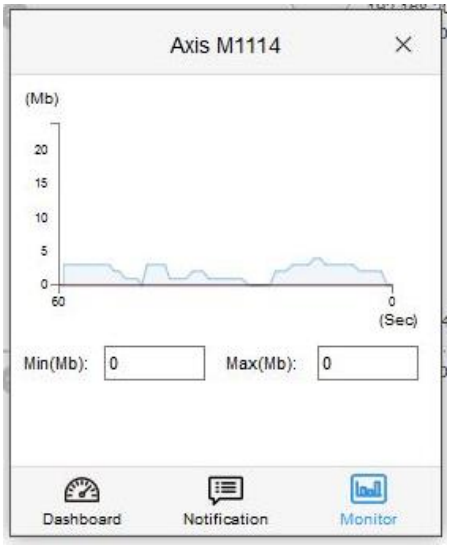
«Remove» muss unbedingt gewählt werden, wenn bspw. eine defekte Kamera durch eine neue Kamera mit gleicher IP-Adresse ersetzt werden soll. Der Switch speichert nicht nur die IP- sondern auch die MAC-Adresse. Wird die alte IP Adresse nicht per «Remove" entfernt, erwartet der Switch die alte Kamera mit der ursprünglichen IP- und MAC-Adressen Kombination zurück und setzt die neue Kamera trotz gleicher IP Adresse immer wieder auf die Default IP Adresse. Dies geschieht, da die neue Kamera eine andere MAC-Adresse hat.



Ein weiteres nützliches Tool ist die Funktion "Monitor".

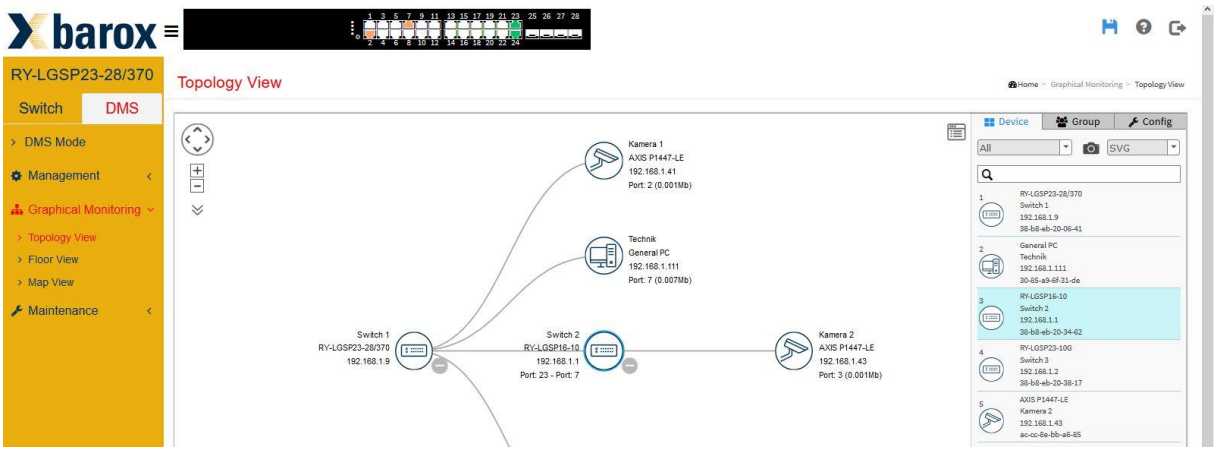
Hier wird der Datenfluss (z. B. von einer Kamera) in Echtzeit angezeigt.

Mit Min(Mb) und Max(Mb) können Schwellwerte gesetzt werden, in denen sich der Datenfluss bewegen sollte. So ist auf einem Blick optisch erkennbar, ob da alles in Ordnung ist.



Oben rechts in der Topology View ist ein Icon, mit dem alle Geräte "Device" aufgelistet werden.

Klickt man in der Liste auf einen Eintrag, wird das entsprechende Gerät im Netzdiagram blau markiert.



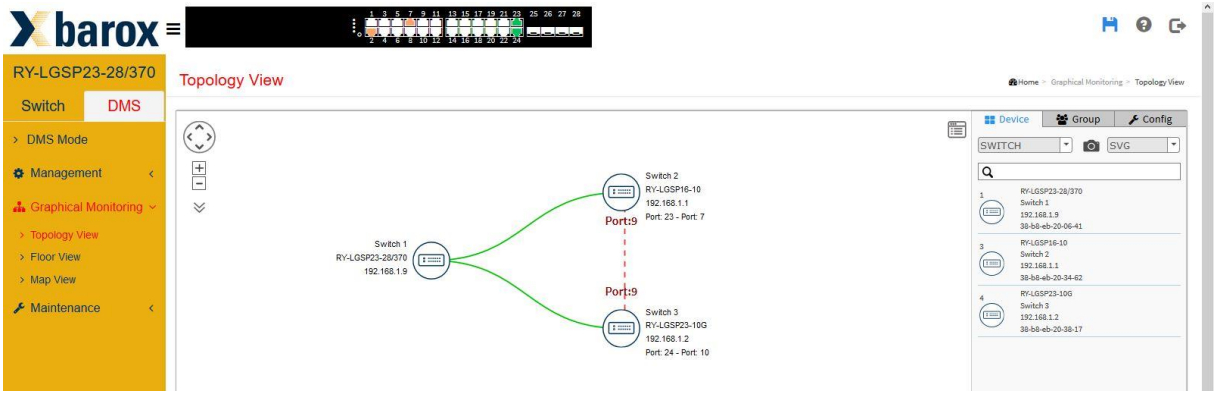

Das Tool bietet auch die Möglichkeit, den Netzwerkplan im Format SVG, PNG oder als PDF direkt aus der Topology View auszudrucken. Hierfür muss das Format gewählt und danach das Kamera Symbol angeklickt werden.

Die Topology View bietet auch die Möglichkeit, die Ringkonstellation darzustellen. Hierfür muss im Register "Device" die Auflistung "Switche" gewählt werden. Es wird sodann der Ring dargestellt und mittels rot gestrichelter Linie erkennbar, welche Strecke und welche Ports als alternative Ports definiert sind.

Für diese Darstellung müssen zwei Bedingungen erfüllt sein:

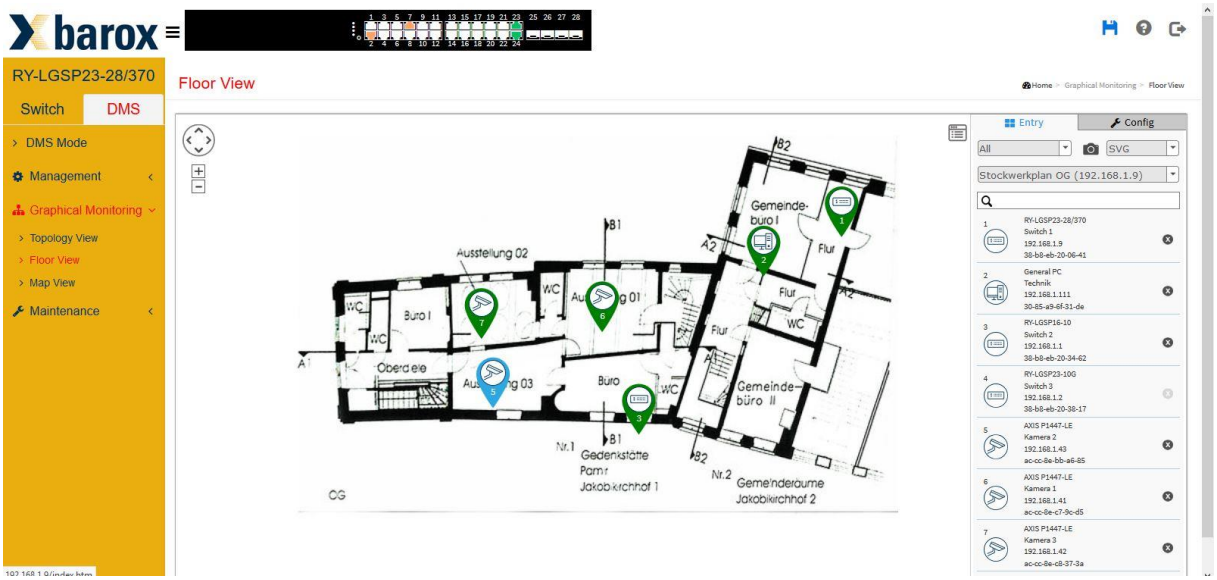
a) RSTP als Ringprotokoll

b) Ring besteht nur aus RY-Switche, die DMS unterstützen




### Floor View

In der Floor-View können hochgeladene bzw. importierte Gebäude-, Stockwerk- und/oder Umgebungspläne angesehen werden. Diese dienen als Grundlage bzw. Hintergrundbild, um das Netzwerk abzubilden. Diese Funktion bietet eine gute Orientierungshilfe bei Vor-Ort-Einsätzen und kann auch als Dokumentation ausgedruckt werden, so wie oben beschrieben.



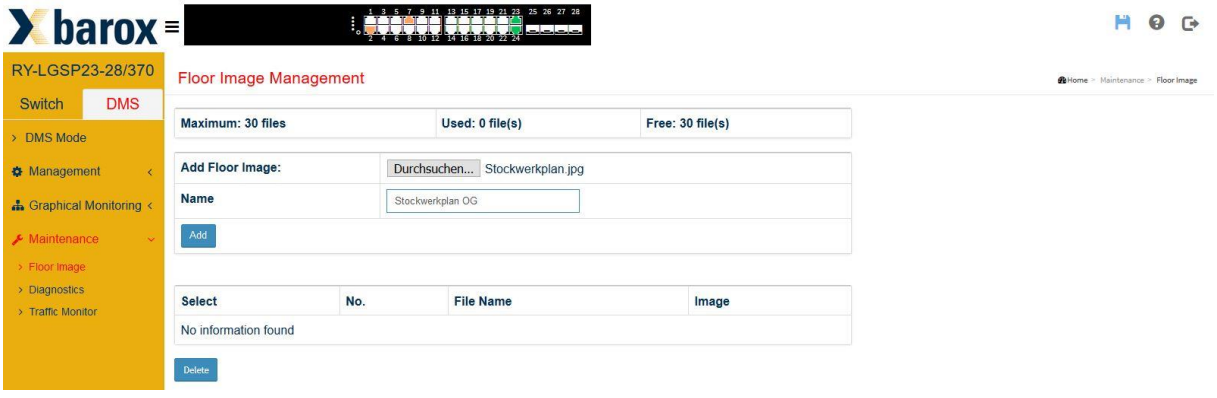

Um die Kamera oder den Switch im Plan zu platzieren ist nur das entsprechende Gerät in der Liste per Mausklick auszuwählen und im Plan zu platzieren, fertig.

**Map View**

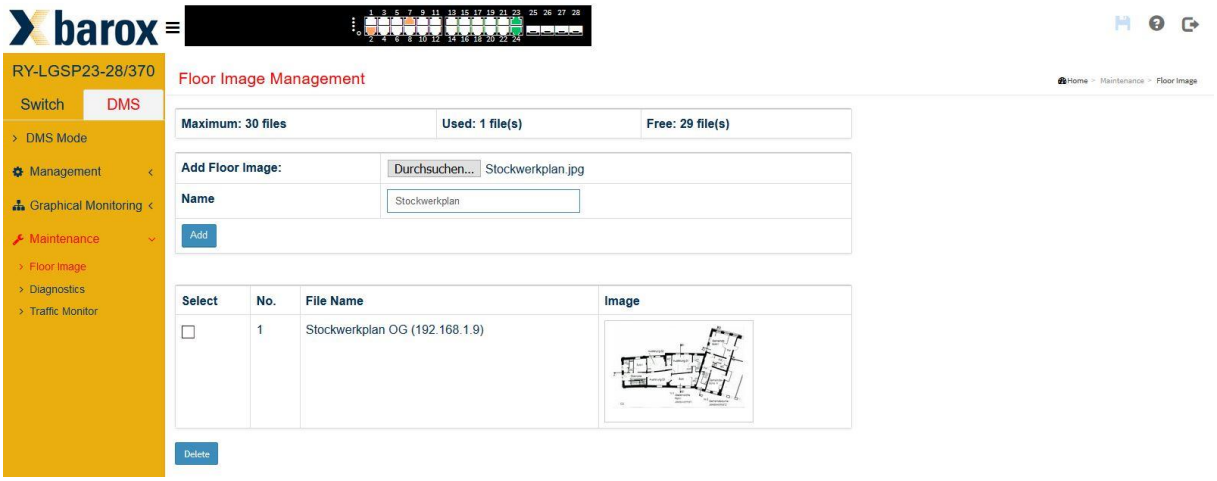
Die gleiche Funktion ist mit Map View möglich. Hier wird gleich mittels Google Map das Hintergrundbild generiert. Bedarf aber eine Internetverbindung und Google-Lizenzen, um den Dienst nutzen zu können.

### 4.3 Maintenance

Um einen Plan als Hintergrundbild zu nutzen muss im Menu "Maintenance" gewechselt werden. Im Menu "Floor Image" ist der Pfad sowie der Dateiname anzugeben und mit "Add" hochzuladen.




Im unteren Bereich der Webseite werden die eingelesenen Pläne aufgeführt. Es können bis zu 50 Files gespeichert werden.




## Diagnostic

Diese Funktion wurde auf der Seite 23 beim Thema "Device List" beschrieben und erklärt.

## Traffic Monitor

**ACHTUNG: Das Traffic Monitoring wird bei den Industrie-Switchen nicht unterstützt**

Ein weiteres nützliches Diagnose-Tool ist das Traffic Monitoring. Im Menu "Maintenance" wird der Traffic jedes einzelnen Ports über 24 Stunden dargestellt.

Das obere Balkendiagramm zeigt jeden Port an und alle Daten die im Laufe des Tages über den Port gesendet und empfangen wurden. Es kann nach Datum, pro Tag oder als Wochenansicht ausgewählt werden.

Klickt man nun auf den Balken eines Ports, wird im unteren Diagramm in einer Skala von 0 – 23 Uhr dargestellt, um welche Uhrzeit wie viele Daten übermittelt wurden.

Dies kann bei der Fehlersuche sehr nützlich sein, wenn man zum Beispiel erkennt, dass um 12 Uhr Mittag ein hoher Datenverkehr am Port 2 generiert wurde und Probleme bei der Aufzeichnung stattfanden.

# 5 Switch Management im Fokus der Security

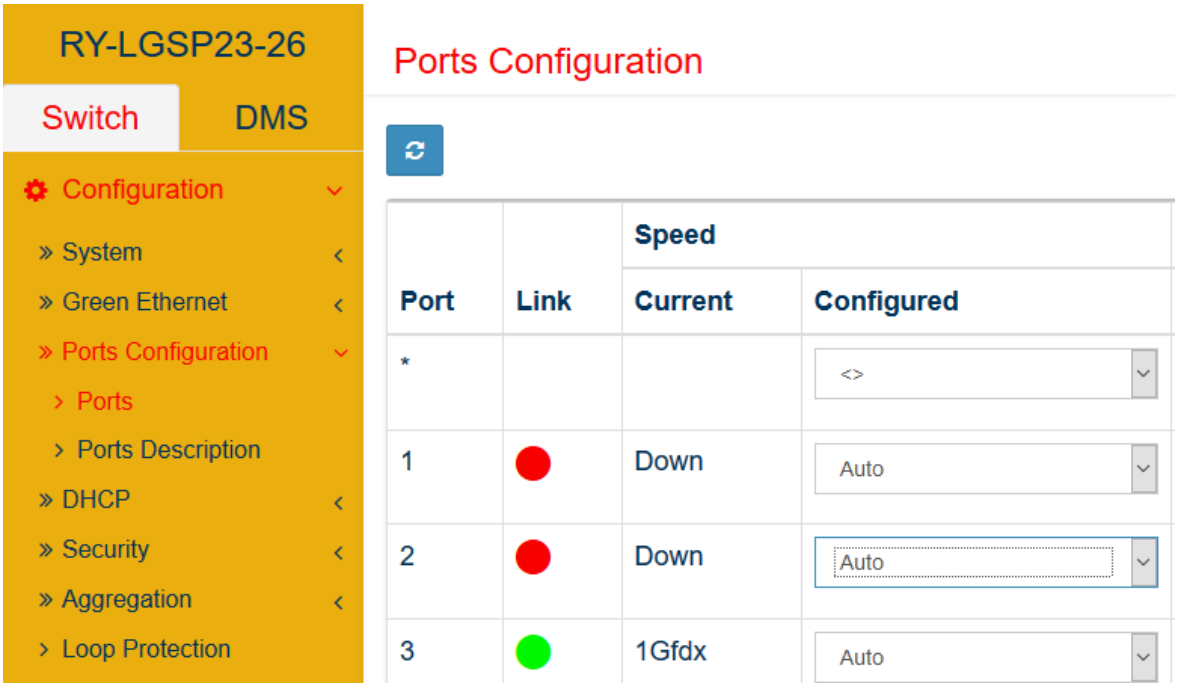
Folgende Themen sollen Aufschluss über Inhalte und Konfiguration der erweiterten Netzwerkeinstellungen und der Absicherung geben. Grundvoraussetzungen zur Konfiguration sind die Kenntnisse und Fertigkeiten der Themen aus Inbetriebnahme wie IP Konfiguration, Login und VLAN Konfiguration.

## 5.1 Verwaltung und Absicherung auf Switch Ebene (Layer 1 und 2)

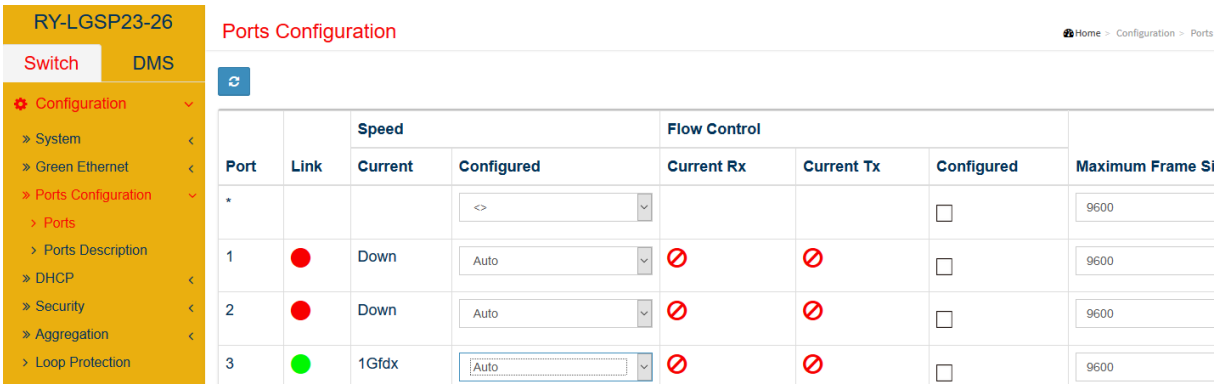
### 5.1.1. Bandbreiten Einstellungen und Beschränkungen

Port basierte Justierung Ethernet

In einigen Eisatzfällen ist es notwendig den benötigten ETH Standard manuell auszuwählen. Beispielsweise bei der Verbindung von Netzwerkkomponenten, die keine automatische Aushandlung des Standards liefern oder Aufgrund von bestimmten Einsatzbedingungen eine Herabstufung des ETH-Standards benötigen. Nachfolgend wie abgebildet, können die Einstellungen 10/100/1000/10000 FDX/HDX (ETH Standard Modelabhängig), selektiv je Port, über das Web GUI angepasst werden.




Einige Applikationen benötigen die Anpassungen der Ethernet Frame Größen. Diese können auch im Menüabschnitt der „Ports Configuration“ im Feld „Maximum Frame Size“, wie im folgendem Bildmittschnitt, erfolgen.




**! Wichtig, bei der Einstellung der Framesize ist die genaue Angabe der Werte zu beachten, um Fehlfunktionen zu vermeiden!**

### 5.1.2. Hinweise zur generellen Betrachtung des Bandbreitenbedarfs

Bei der Planung des Bedarfs an Bandbreiten und damit verbundenem Einsatz der passenden barox Switche empfiehlt es sich folgende Punkte zu berücksichtigen:

- Einsatz der benötigten Ethernet Standards (10/100/1000/ 10000) unter Berücksichtigung eventueller Endgeräte Upgrades
- Einplanung von Reserven, skaliert an der Backplane- Switch Leistung des Models -> empfohlen sind häufig 30 %
- Bei der Berechnung des Bedarfs die maximale Ethernet Spezifikation je Endgerät berücksichtigen

### 5.1.3. Absicherung der Ports durch MAC Konfigurationseinstellungen

Die MAC Tabelle

Grundlegend kann die MAC-Tabelle neben der automatischen Verwaltung auch manuell angepasst werden. Dies ist meist nötig, wenn bestimmte Netzwerkendgeräte eine statische Zuweisung in Beziehung VLAN und Port benötigen. Zudem kann mit der manuellen Zuweisung eine grundlegende Absicherung, bzw. Zugangsbeschränkung skaliert werden.

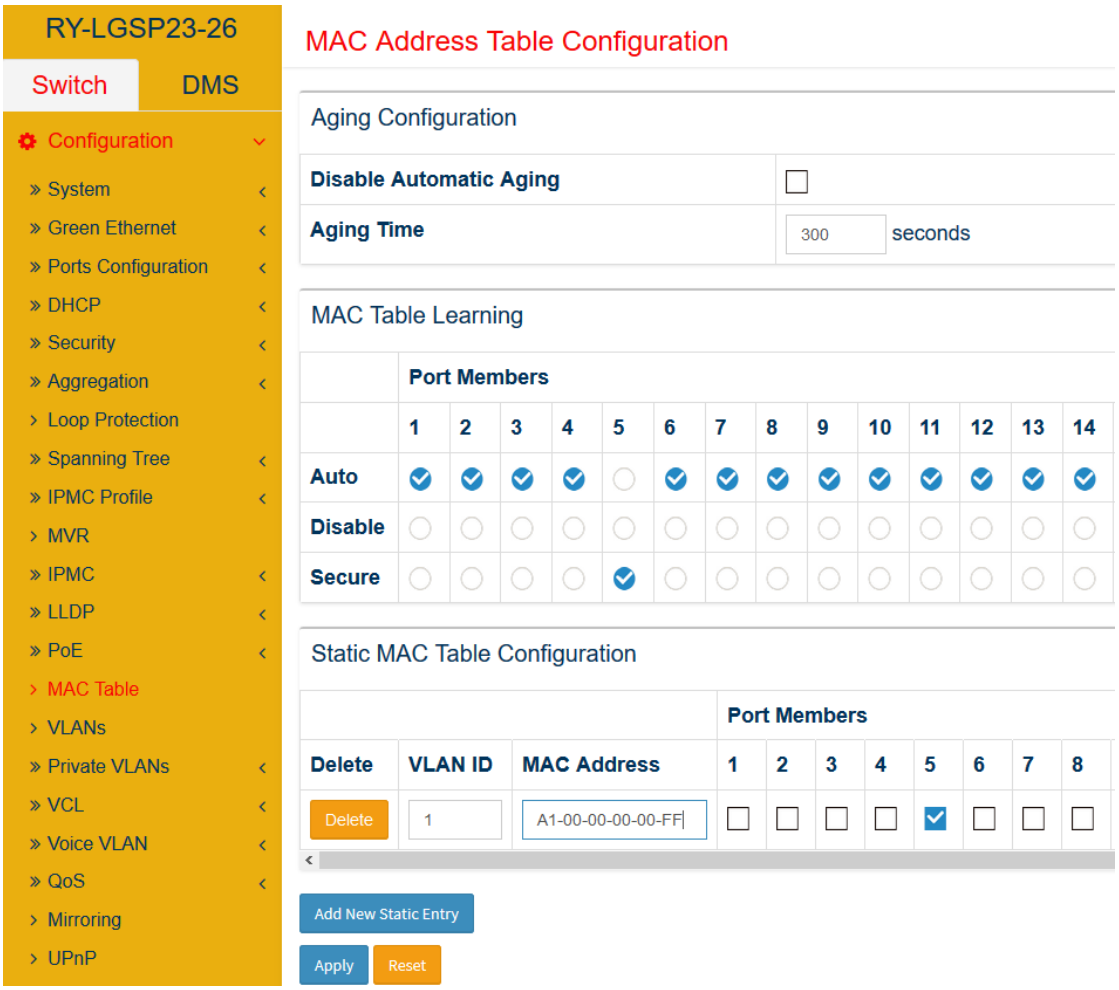
#### MAC Filterung und Port Konfiguration

Beispiel Konfiguration Static MAC Table:

Das Gerät mit der MAC Adresse A1:00:00:00:00:FF soll nur am Port 5 im VLAN 1 Verbindung herstellen können.

1. Auswahl von „Add New Static Entry“ im Menu Switch -> Configuration -> MAC Table
2. Eingabe der VLAN ID, MAC Address und setzen des Port Members 5 unter „MAC Table Learning“ auf „Secure“
3. Bestätigung der Eingaben mit „Apply“

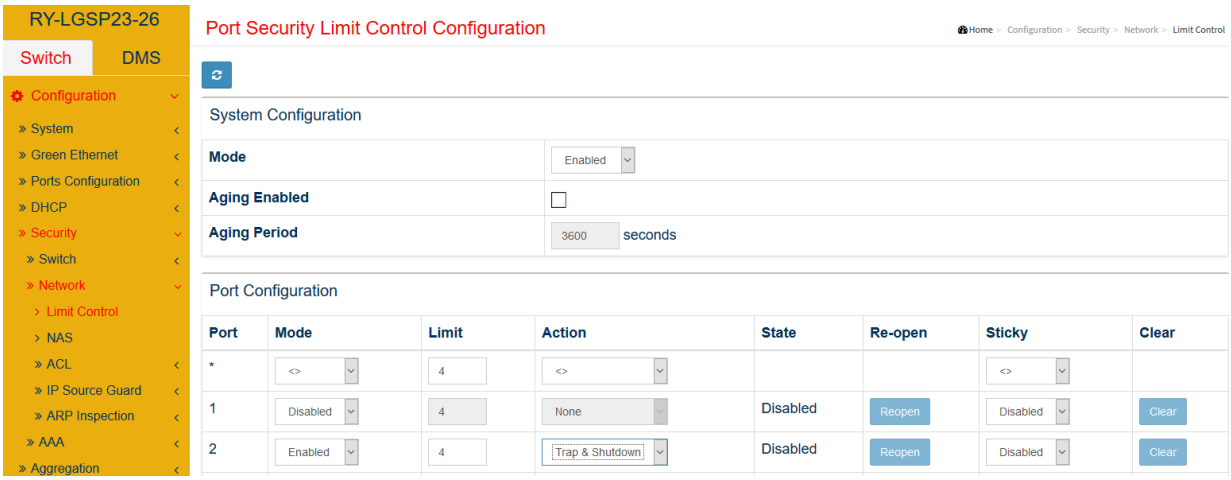
Zur Veranschaulichung dient nachfolgender Bildmitschnitt.




Die Absicherung über die MAC Filterung bietet einen einfachen Schutz vor nicht erwünschtem Netzwerkzugang. Dennoch schützt sie beispielsweise nicht vor dem weit verbreiten Angriff des „MAC-Spoofings“.

### 5.1.4. Port Security mit Limit Control Einstellungen

Werden am barox Switch nicht- gemanagte Switche mit Endgeräten angeschlossen, so empfiehlt es sich die Limit Control einzusetzen. Grundlegend ermöglicht diese Funktion, dass weitere nicht erwünschte IP/ Ethernet Endgeräte an freien Ports der nicht- gemanagten Switche der Zutritt zur Netzwerkkommunikation gesperrt wird. Zur Planung muss die gesamte Anzahl der Netzwerkgeräte, inklusive des nicht- gemanagten Switches, welche an dem jeweiligen Port des barox Switches angeschlossen werden, ermittelt werden. Bsp.: Wird an Port 2 des barox Switches ein nicht gemanagter Switch mit weiteren 3 Netzwerkendgeräten angeschlossen, so liegt die Gesamtzahl des Limits bei 4. Die Konfiguration muss zunächst aktiviert werden. Weiter wird der entsprechende Port aktiviert, das Limit festgelegt und für den Fall der Überschreitung die Aktion ausgewählt. Das Erlernen der Endgeräte wird mit der *„Sticky“* Funktion, aktiviert und ermöglicht. Während der Konfiguration ist es notwendig, dass die Geräte physikalisch mit dem barox Switch am zu konfigurierenden Port angeschlossen sind. Eine Veranschaulichung zu den Einstellungen ist folgend aufgezeigt.




## 5.2 Einsatz und Absicherung von IP Funktionen (Layer 3)

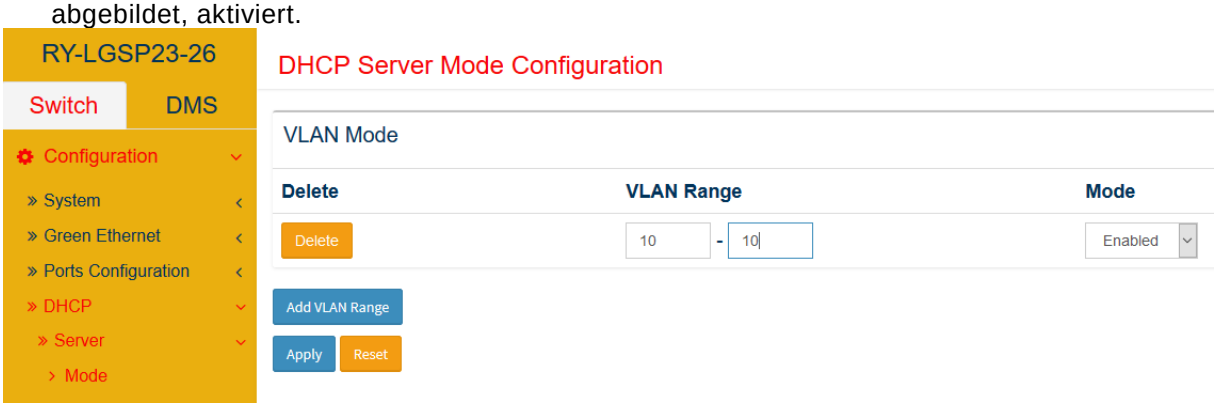
### 5.2.1. DHCP Server

#### Hinweise zum Einsatz von DHCP Servern in Video Netzwerken

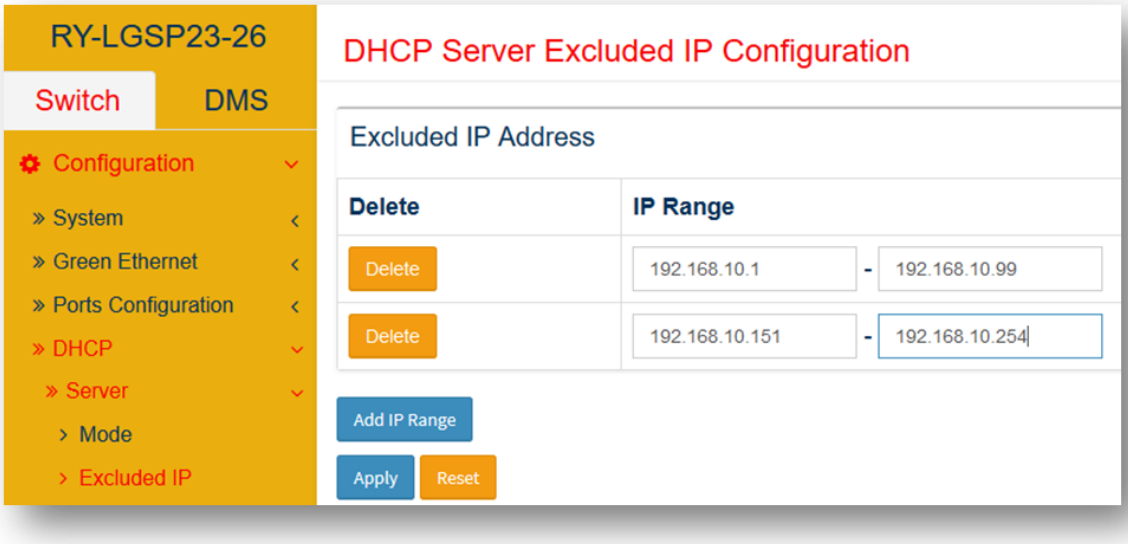
Es gilt zu prüfen, ob der Einsatz eines DHCP Servers generell vom Netzdesign nötig ist. Dieser Dienst bietet neben den Vorteilen der automatisierten Netzwerkinformationsverteilung aber auch verschiedenste Angriffspunkte

#### Grundlegende Konfiguration und Inbetriebnahme des DHCP Dienstes am Beispiel

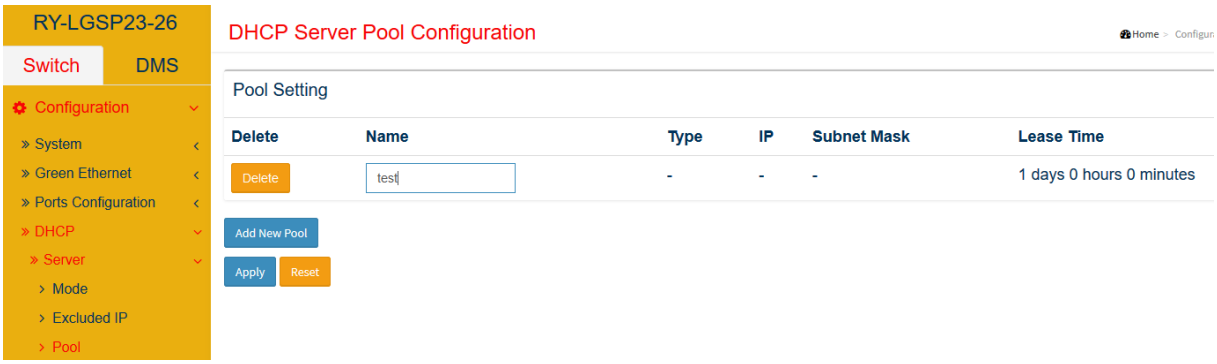
Beginnend wird die VLAN Range des Dienstes festgelegt und der Dienst generell im *Mode* mit der Einstellung *Enabled* aktiviert und abschließend mit Bestätigung, wie weiter stehend abgebildet, aktiviert.



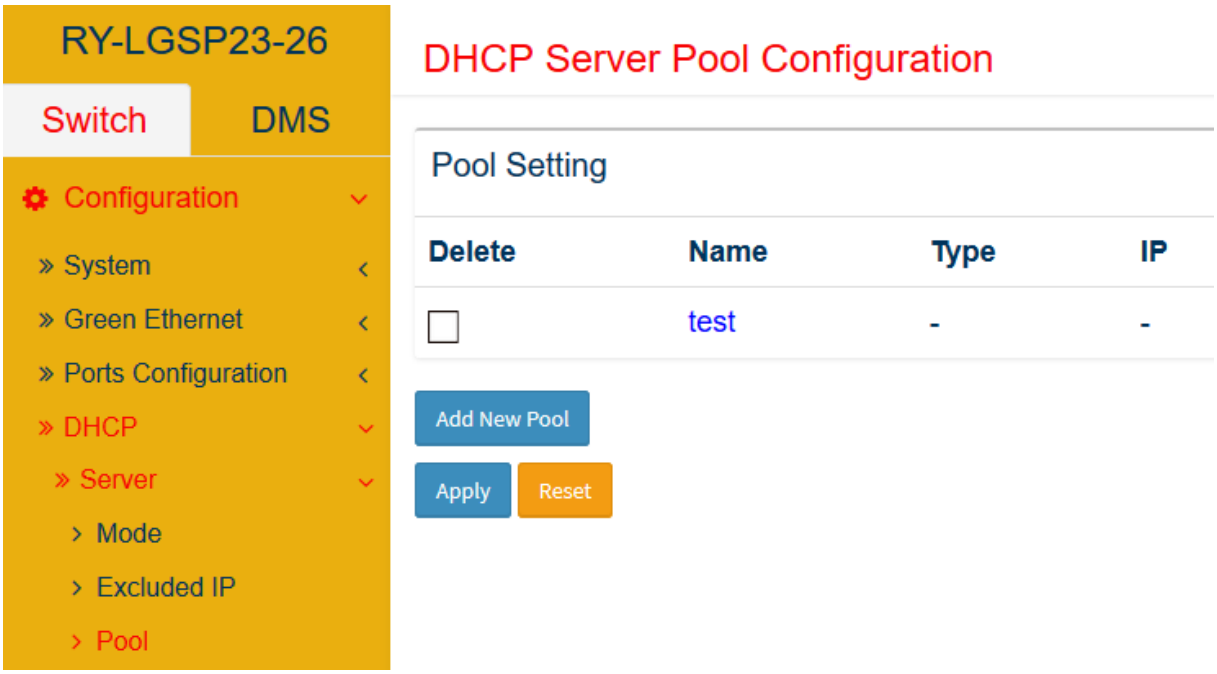

Folgend werden die Einstellungen des IP Adress- Pools, welche die Verteilung von 50 Adressen im Beispiel, d.h. Adressen im Bereich von 192.168.10.100 – 192.168.10.150 durch die Angabe der umliegenden Adressen, bzw. IP Reichweiten (Exklusionsverfahren) an die IP Clients im jeweiligen VLAN ermöglichen soll.



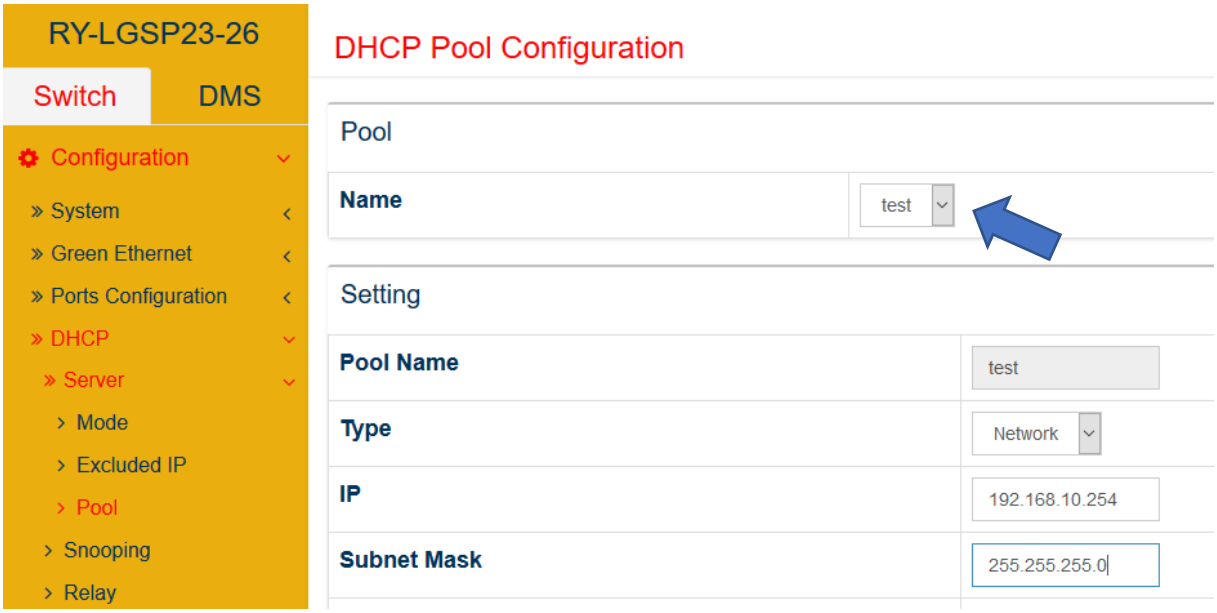

Anschließend wird ein Name des DHCP Dienstes festgelegt und bestätigt.




Nach der Festlegung des Namens werden die Einstellungen durch die Auswahl des Namens, wie weiter abgebildet aufgerufen.




Nach Aufruf des Pool Namens erscheint, wie folgend abgebildet die Konfiguration.

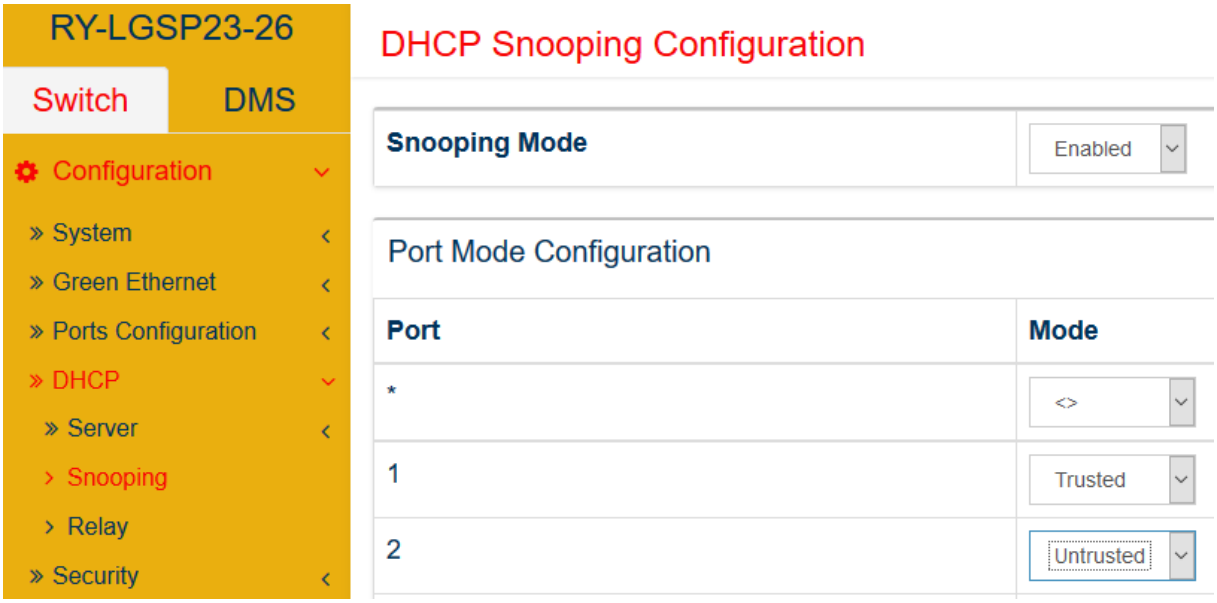



Zur einfachen Veranschaulichung, bzw. zum Nachvollzug, werden nur Einstellungen, wie überstehend abgebildet, benötigt und anschließend durch bestätigen der Konfiguration, am Ende der Seite, bestätigt.

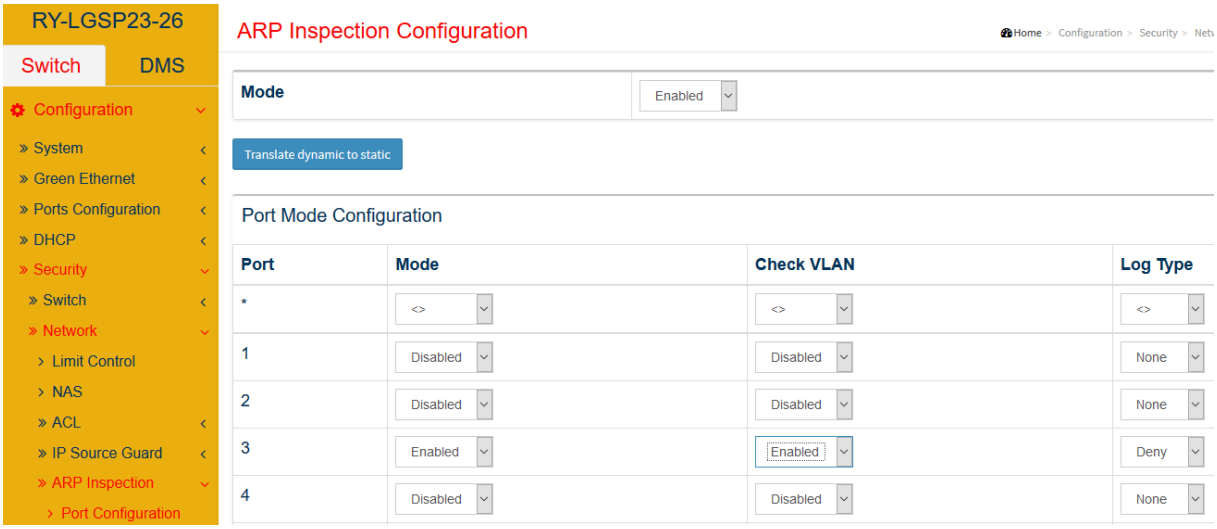
### 5.2.2. Absicherung des DHCP durch ARP Inspection

Die Absicherung vor unerwünschten DHCP Clients kann mit der ARP Inspection realisiert werden. Nachdem die Funktionen aktiviert sind können die DHCP Clients statisch als Rezipienten in einer Tabelle verwaltet werden. Grundvoraussetzung für die höchste Sicherheit ist, dass die Größe des DHCP Address Pools mit der Anzahl von Clients eingestellt wird.

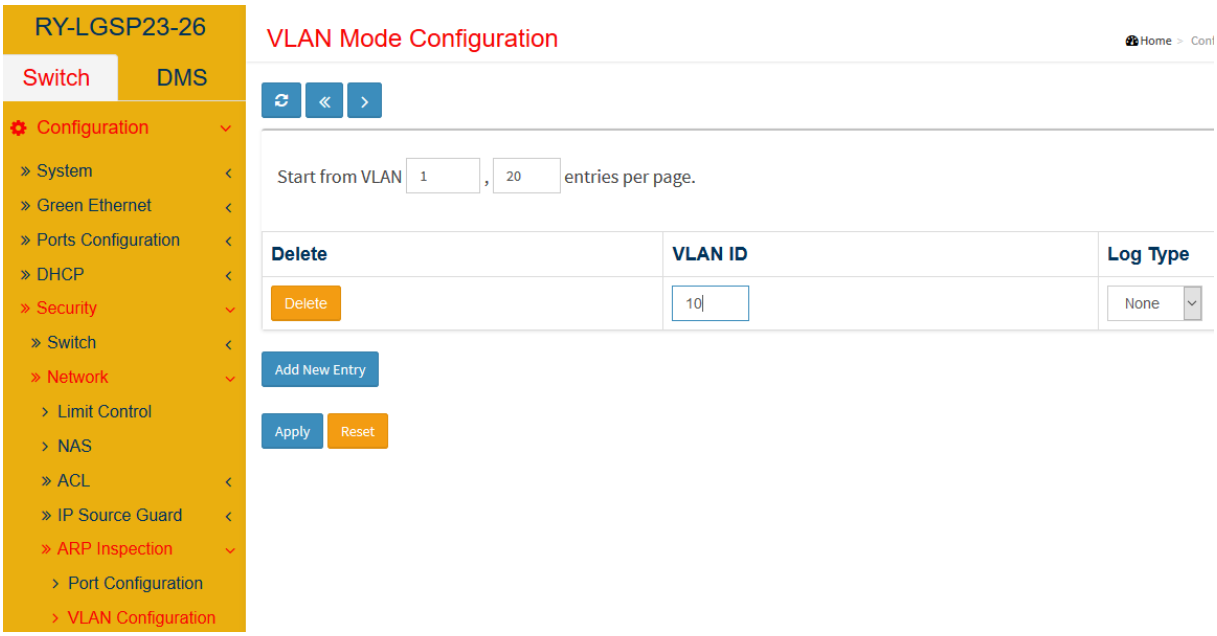
Zunächst wird die Snooping Funktion unter Snooping Mode generell aktiviert, wie folgend abgebildet. Weiter können für die Switch Ports die Vertrauens Stellungen ausgewählt werden. Für die Funktion der Inspection muss der Modus auf „Trusted“ gesetzt sein.



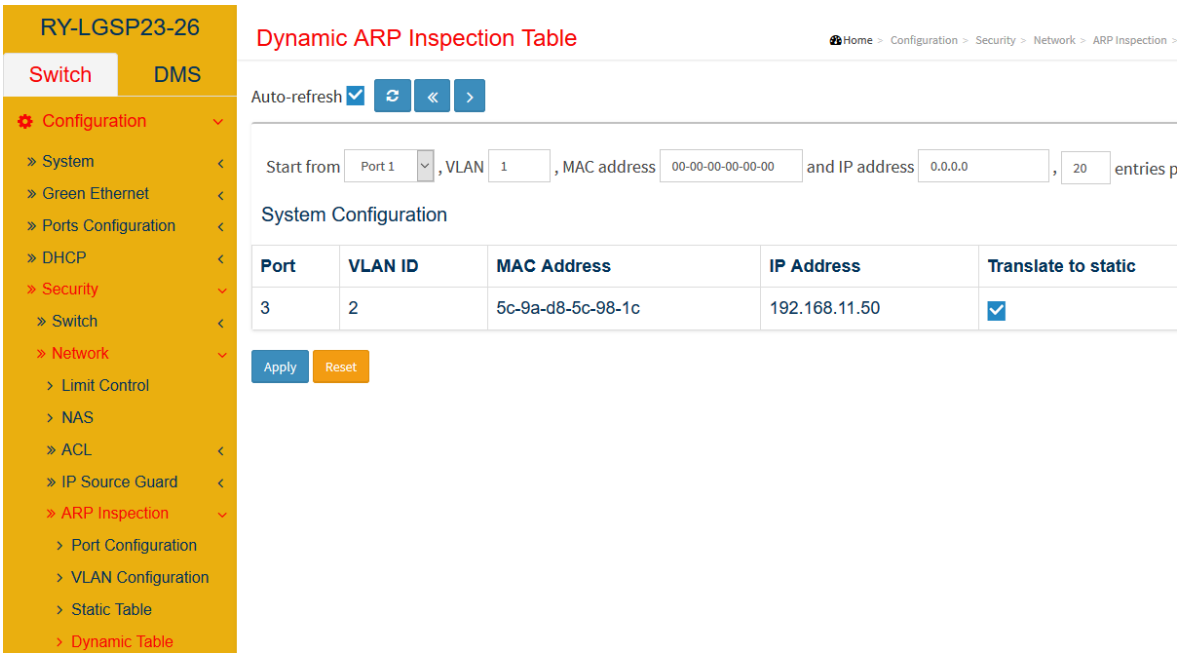

Weiter werden die Parameter für die Ports aktiviert und konfiguriert. Am Beispiel wie nachfolgend aufgezeigt wird die ARP Inspection für den Port 3 aktiviert, die Überprüfung des VLANs aktiviert und der Log Typ auf „verweigern“ eingestellt.



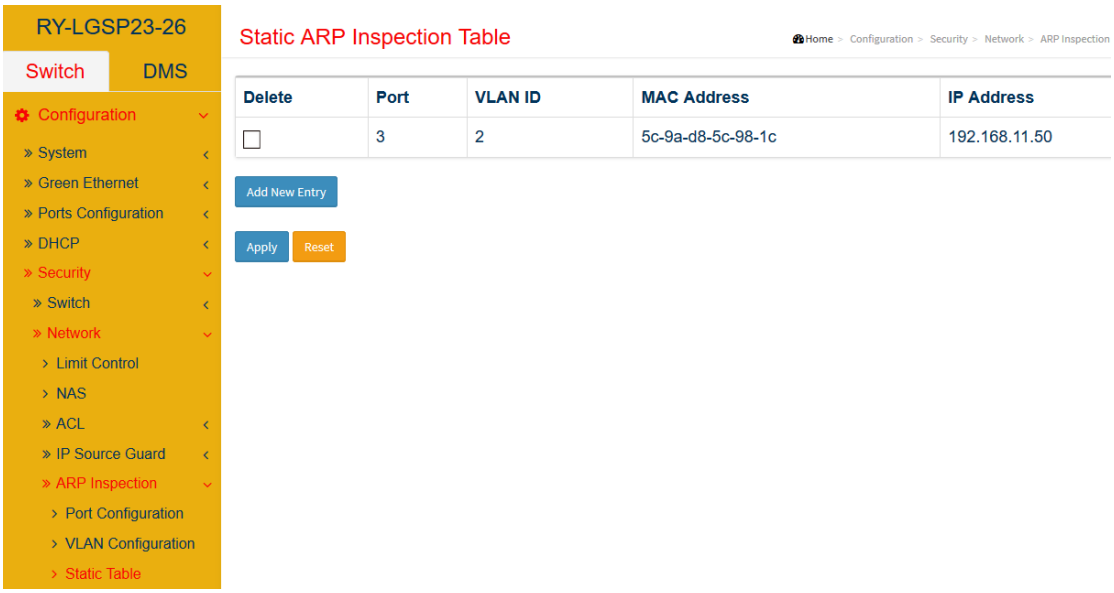

Im Anschluss werden die VLANs festgelegt welche in der Überprüfung eingeschlossen werden sollen und der Log Typ (Vertrauensstellung) wie weiter aufgezeigt, festgelegt.




Nach erfolgten Einstellungen können die DHCP Clients angeschlossen werden. Nachdem der DHCP Dienst IP Adressen verteilt werden die Clients mit den Layer2 und 3 Eigenschaften in der dynamischen ARP Inspection Tabelle sichtbar und können anschließend in die statische ARP Inspection Tabelle übersetzt werden



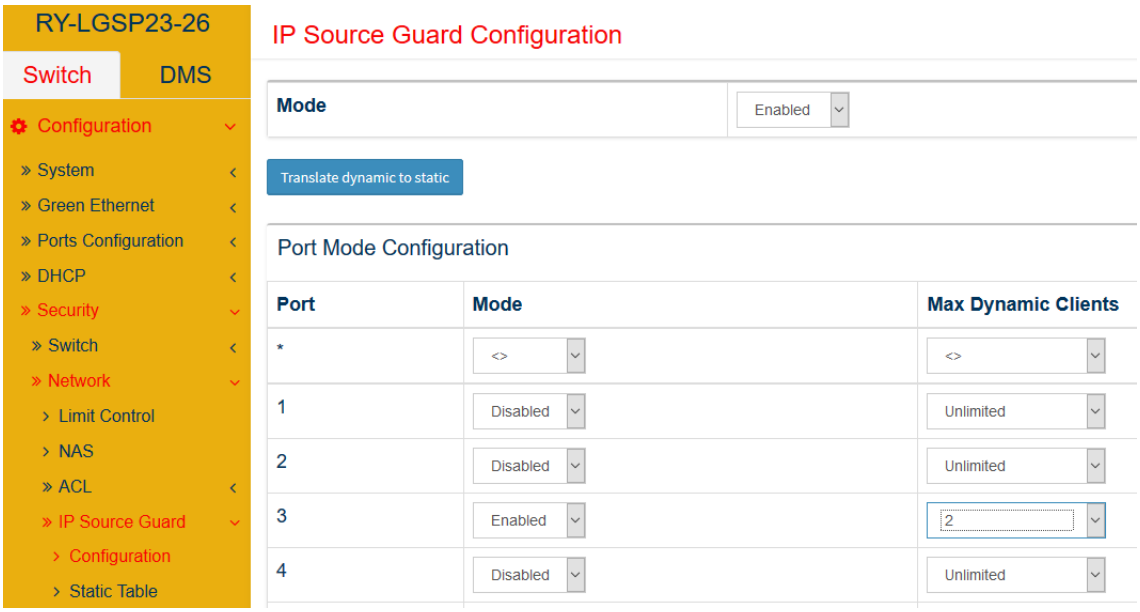

Nachfolgend abgebildet ist ein statischer Eintrag. Für den Client wird entsprechend der Tabelle die IP Adresse reserviert.



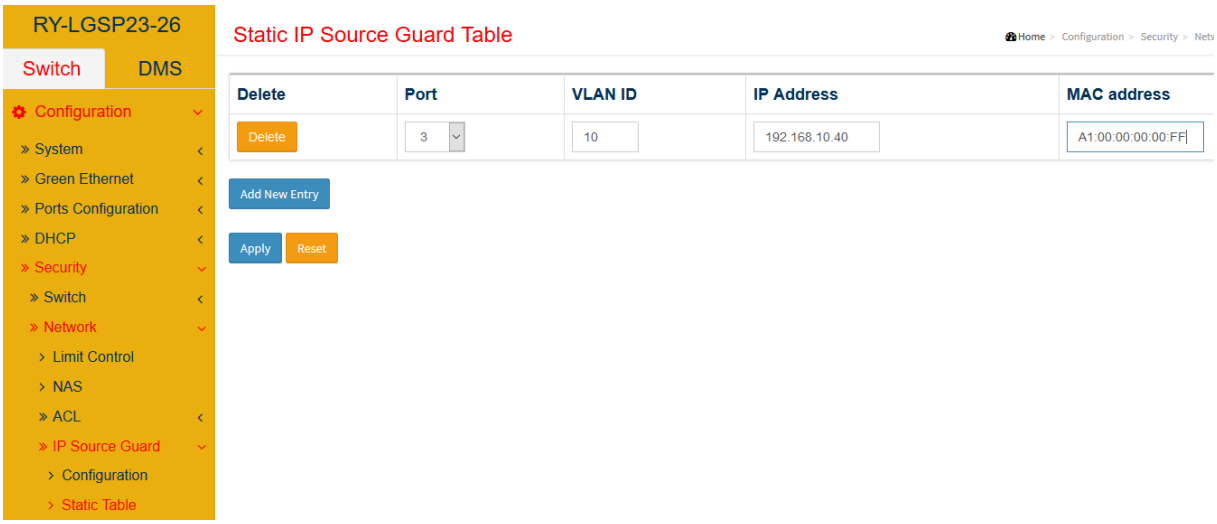

### 5.2.3. IP Source Guard

Einsatz und Konfiguration

Eine erweiterte Funktion zur Absicherung von Endgerät- Seite stellt der Einsatz der IP Source Guard Funktion dar. Diese verknüpft neben der Untersuchung der Quell- Endgeräte MAC Adresse zudem auch die vorgegebene statische IP Adresse der angeschlossenen Geräte. Wie nachfolgend aufgezeigt wird diese Funktion generell aktiviert und kann weiter, je Port granuliert, eingestellt werden.




Nach einschalten der Funktion kann die Konfiguration, mit statischen Einträgen, wie weiterführend abgebildet, erfolgen.



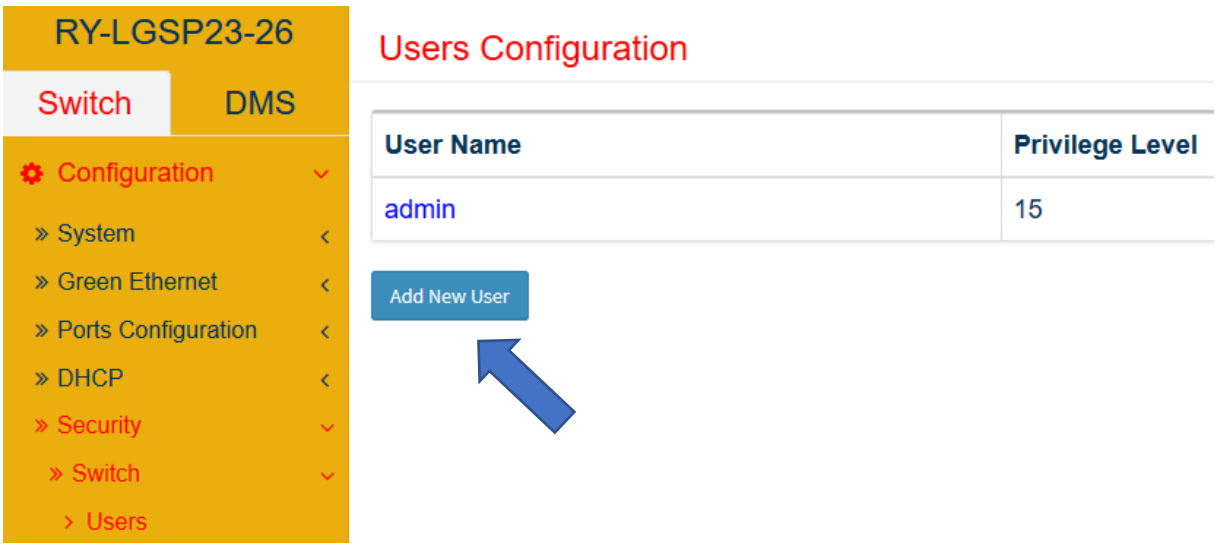

Der Einsatz des IP Source Guard ermöglicht die erweiterte Sicherheitsfunktion durch die Absicherung des Ports mit MAC und IP Adresse. Im Vergleich zur Port Security, wobei statische MAC Adresseinträge je Port einen möglichen Angriff verhindern sollen, bietet der IP Source Guard, mit statischen Einträgen, zusätzlich die Bedingung des angeschlossenen Gerätes die IP Adresse zu prüfen. Werden die Bedingungen, die zugewiesene MAC und IP am Port vom angeschlossenen Gerät, nicht erfüllt, so wird der Switch die Netzwerkkommunikation am Port blockieren. Dies Bedeutet, der Angreifer muss die MAC Adresse und die IP Adresse vom Gerät kennen, um sich Zugang zum Netzwerk zu verschaffen.

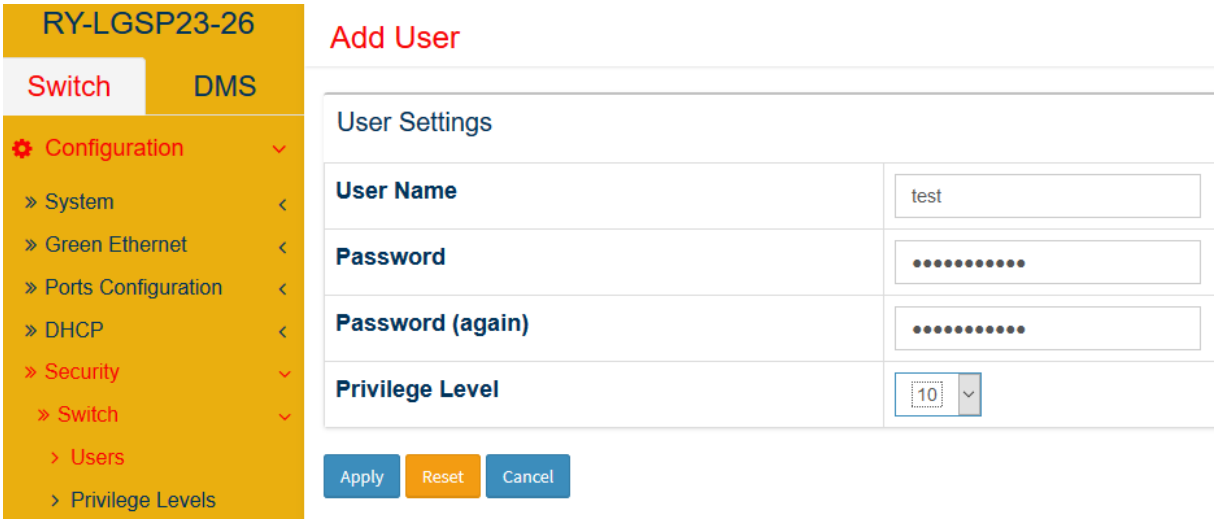
## 5.3 Absicherung des Switch- Managements und Netzwerkadministration (Layer 3–7)

### 5.3.1. Nutzerverwaltung und Konfiguration

Nutzer Anlegen

Nachfolgend ist ein Beispiel für einen weiteren Nutzer anzulegen aufgeführt.

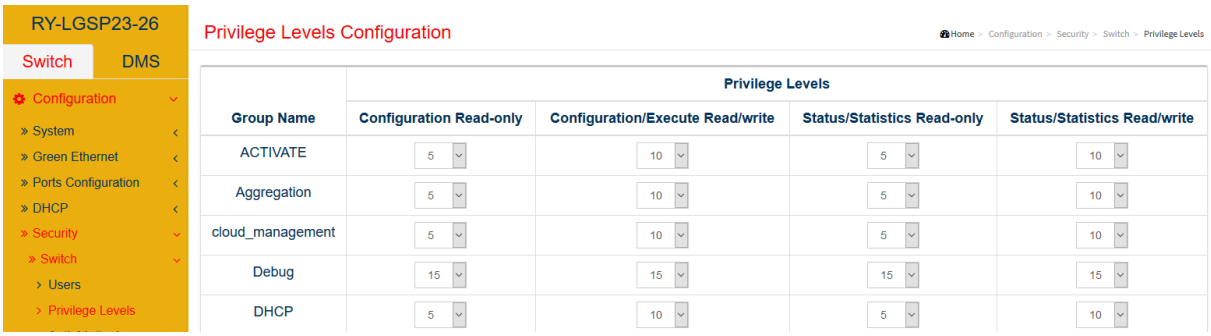





Grundlegende Einstellungen der Nutzerrichtlinien und Privilegien

- Die Privileg Level dienen der Abstufung der Rechte auf Konfigurationseinstellungen, bzw. der Lese und Schreibrechte der Werte. Es empfiehlt sich grundlegend die vorgegebenen Werte nicht zu ändern, sondern bei dem Anlegen neuer Nutzer diese zu vergeben.

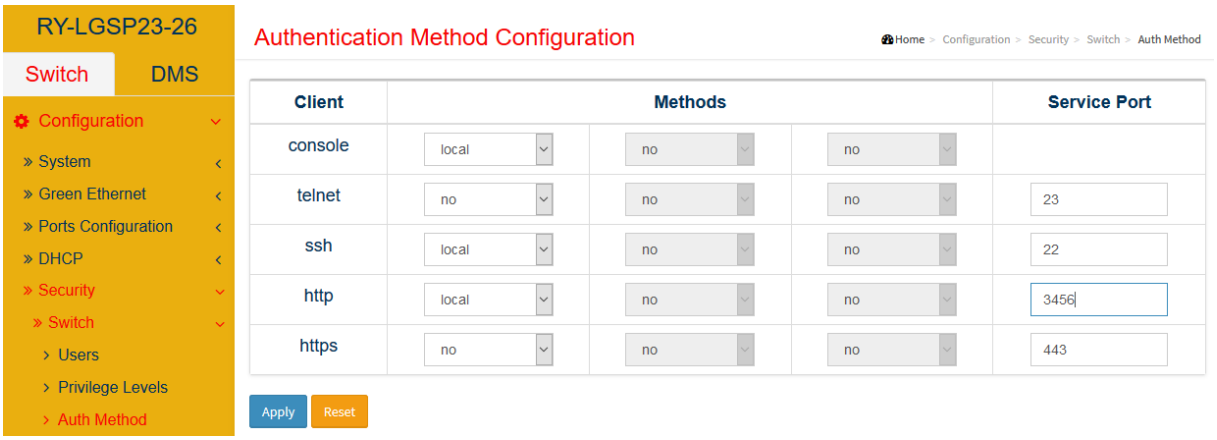
- Hinweis: Es ist hilfreich die Rechte für einen weiteren Nutzer nach Befugnissen und Kompetenzen zu skalieren.




### 5.3.2. Einsatz und Einstellungen der Authentisierung am Switch- Management

Absicherung des CLI Zugriffs **ssh** vs. **telnet**

Wie nachfolgend abgebildet, kann die Zugriffsmethodik eingestellt bzw. nicht benötigte Funktionen abgestellt werden. Es ist zu empfehlen, sofern das Netzwerkdesign es zulässt, die Telnet Zugangsfunktion generell abzuschalten. Wie nachfolgend abgebildet, können die Konfigurationsmethoden eingestellt werden.

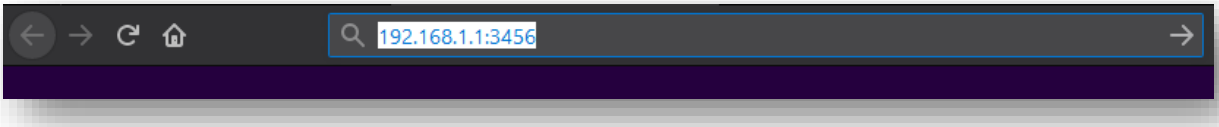



- Es empfiehlt sich, für die Kommandozeilen (CLI) basierte Verwaltung das SSH Protokoll zu nutzen, da diese Methode die Verschlüsselte Verbindung bietet.

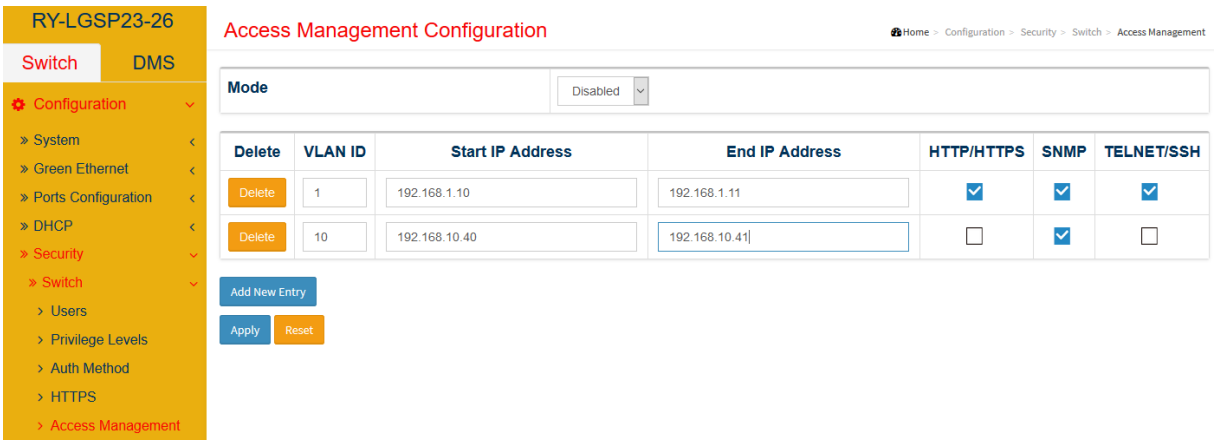
Verwaltung des Zugriffs auf die Weboberfläche (GUI) mit http

- Es empfiehlt sich einen separaten Nutzer für http anlegen
- Port 80 verändern, Hinweis: Port Angabe bei Zugriff im Browser beachten!
- Der HTTPs Zugriff bietet den höchsten Schutz, da die Verbindung verschlüsselt wird

Nachfolgend ist die Eingabe der Verwaltungsadresse mit verändertem Port, beispielhaft, abgebildet

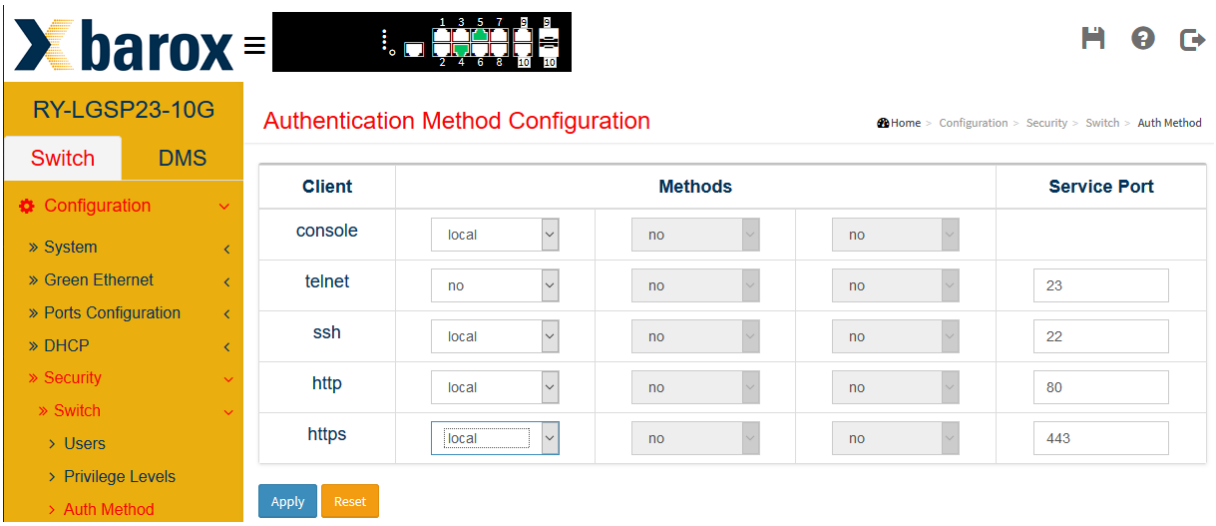



Die Einschränkung des Managementzugriffs und dessen Methoden kann auf bestimmte IP Adressbereiche und VLANs eingeschränkt werden. Dies kann im Access Management, wie weiter beispielhaft dargestellt erfolgen.



### 5.3.3. Zugriffsverwaltung und Einsatz von HTTPS

Weiter aufgezeigt ist die Einstellmöglichkeit der Verwendung des HTTPs Protokolls.




Auch bei dieser Methode kann der standardisierte Port verändert werden.

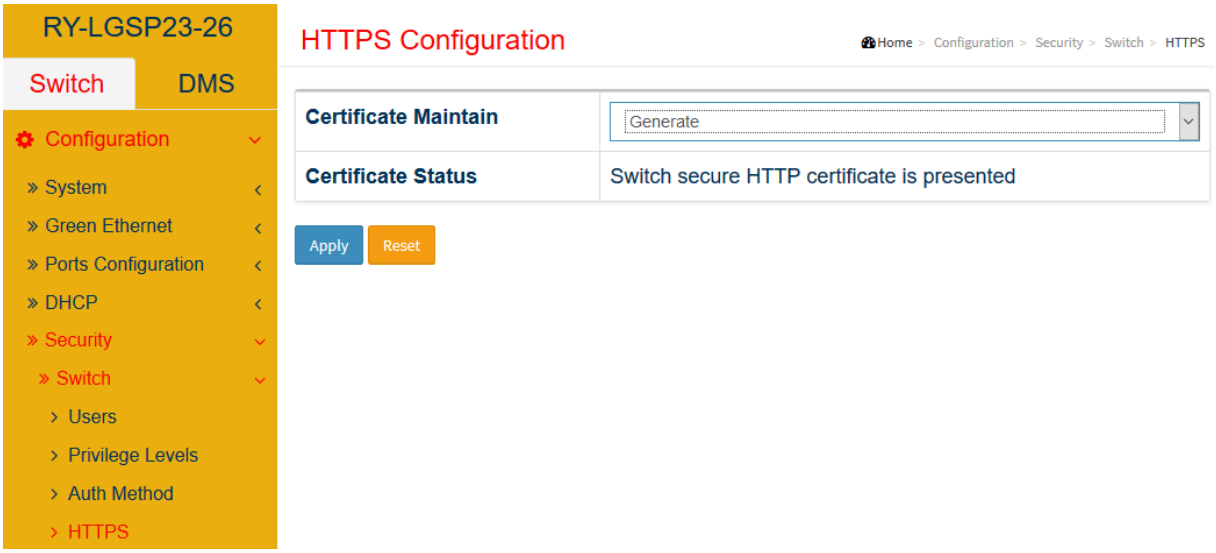
Wenn der Modus aktiviert ist, dann sollte die http Option ausgeschaltet werden. Der Aufruf der Switch- GUI erfolgt im Browser über die HTTPs Protokoll Phrase https://192.168.XX(IhreManagement IP):1234(IhrPort) im URL Feld. Nach Festlegung erfolgt die Kommunikation des Browsers mit der Managementschnittstelle verschlüsselt.

### 5.3.4. Konfiguration und Einsatz von zertifikatsbasiertem Zugriff auf das Management

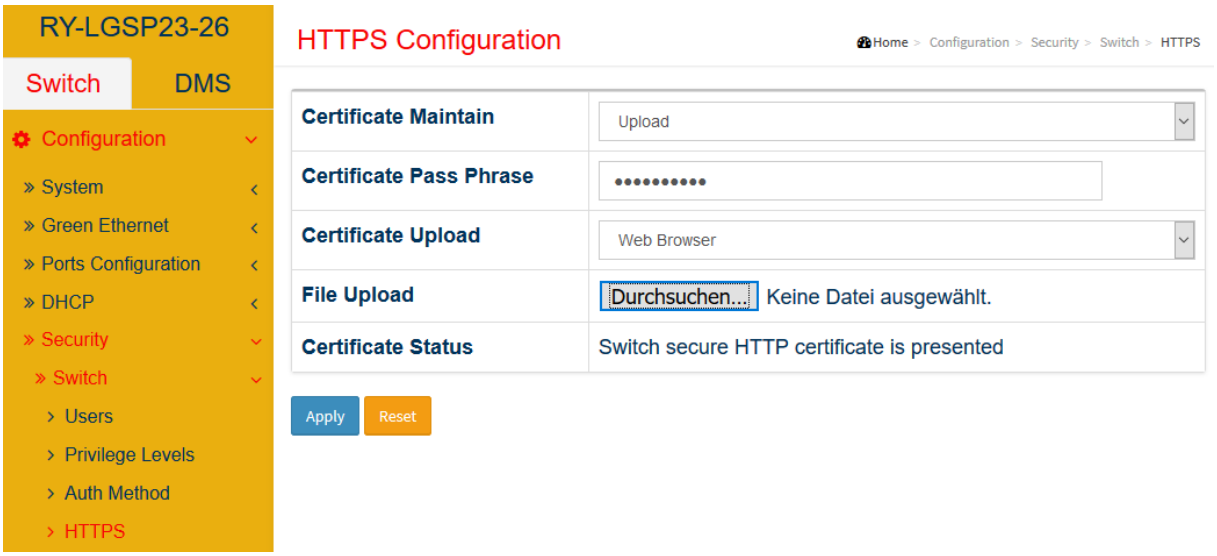
Kurzer Hinweis zur Verwendung von Zertifikaten:

Eine zertifikatsbasierte Anbindung ermöglicht einen der höchsten Zugangsabsicherungen für Netzbasierte Konfigurationsdienste. Dennoch sollte der Einsatz geprüft werden, da die Verbindung zum Management nur noch über die Medien, welche das Zertifikat eingepflegt haben, erfolgen kann.

Nachfolgend sind die Einstellmöglichkeiten, bzw. der Methoden aufgezeigt.

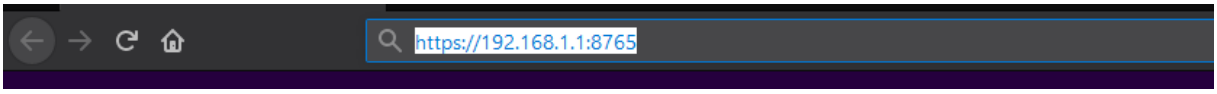


- Generierung des Zertifikates zur späteren Verwendung, welches über den Browser heruntergeladen und installiert werden kann




- Upload eines extern generierten Zertifikats

- Der Browser Zugriff erfolgt nach der Installation des Zertifikates und Festlegung der HTTPs Authentisierungsmethode über das HTTPs Protokoll




## 5.4 SNMP – Monitoring- und Administrations- Funktion

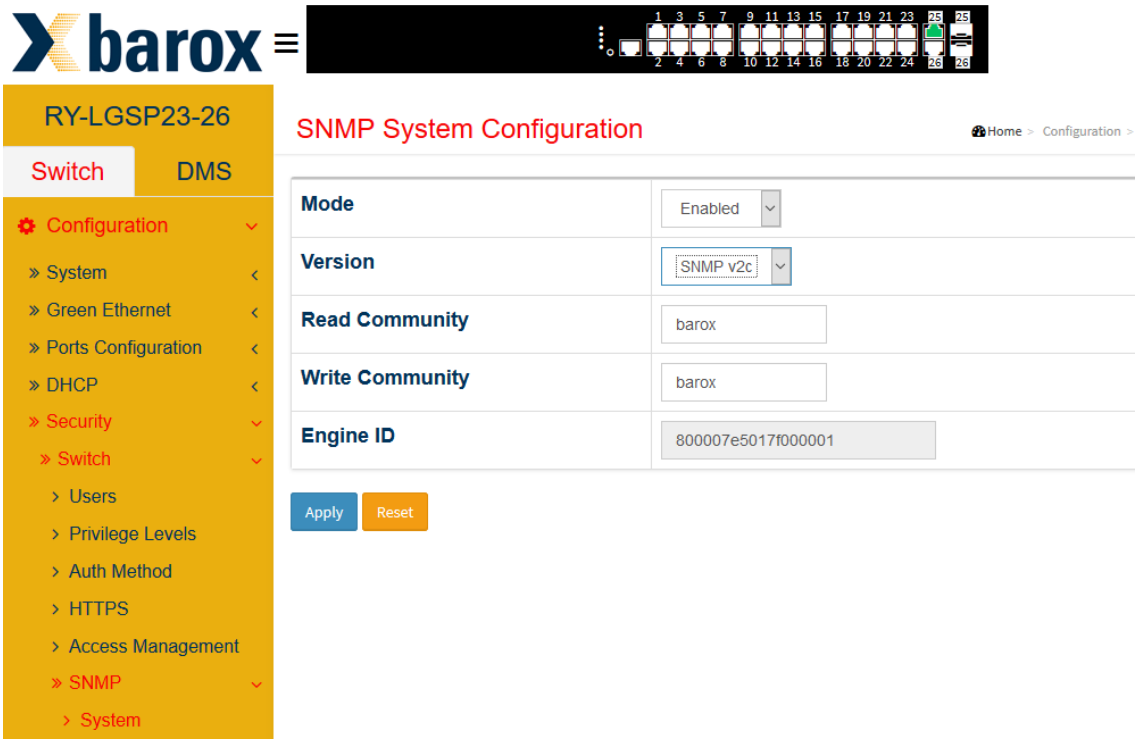
SNMP wurde von der IETF (Internet Engineering Task Force) entwickelt und dient als Protokoll zur Überwachung, Steuerung und Konfiguration von Netzwerkelementen.

### 5.4.1. Konfiguration SNMP v2c

Im Weiteren wird eine grundlegende SNMP v2 Konfiguration zur Systemstatusabfrage oder dem Versenden von Systemevents über SNMP Traps an einem Beispiel beschrieben. Die nachfolgenden Schritte sollen die Verwendung einer SNMP Community aufzeigen.

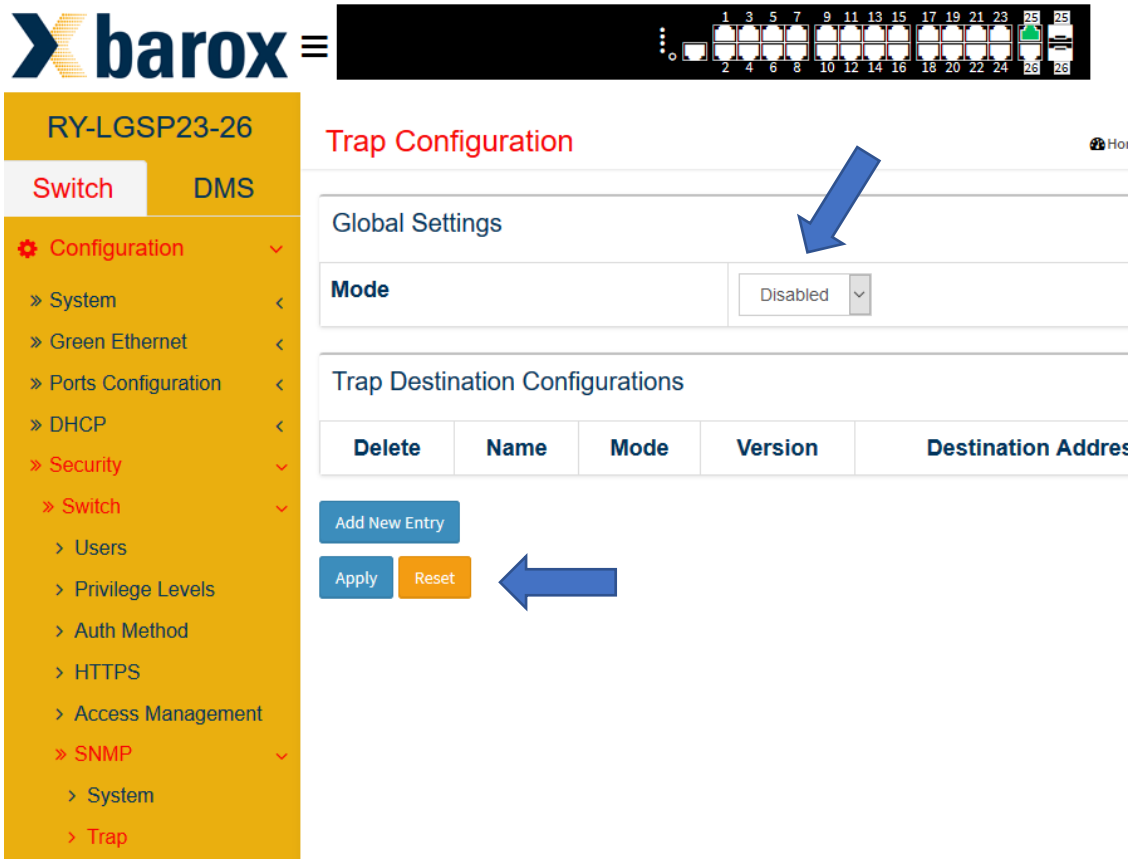
**Aktivierung der SNMP v2 Funktion**

Grundlegend ist der Modus zu aktivieren und die Version SNMP v2 in der SNMP Konfiguration auszuwählen. Weiter werden die Namen für die Read- und Write Communities festgelegt.




### 5.4.2. Konfiguration der SNMP Trap

Vor der Konfiguration der neuen Trap Einstellungen ist darauf zu achten, dass die globale Einstellung des Trap- Modus deaktiviert ist.



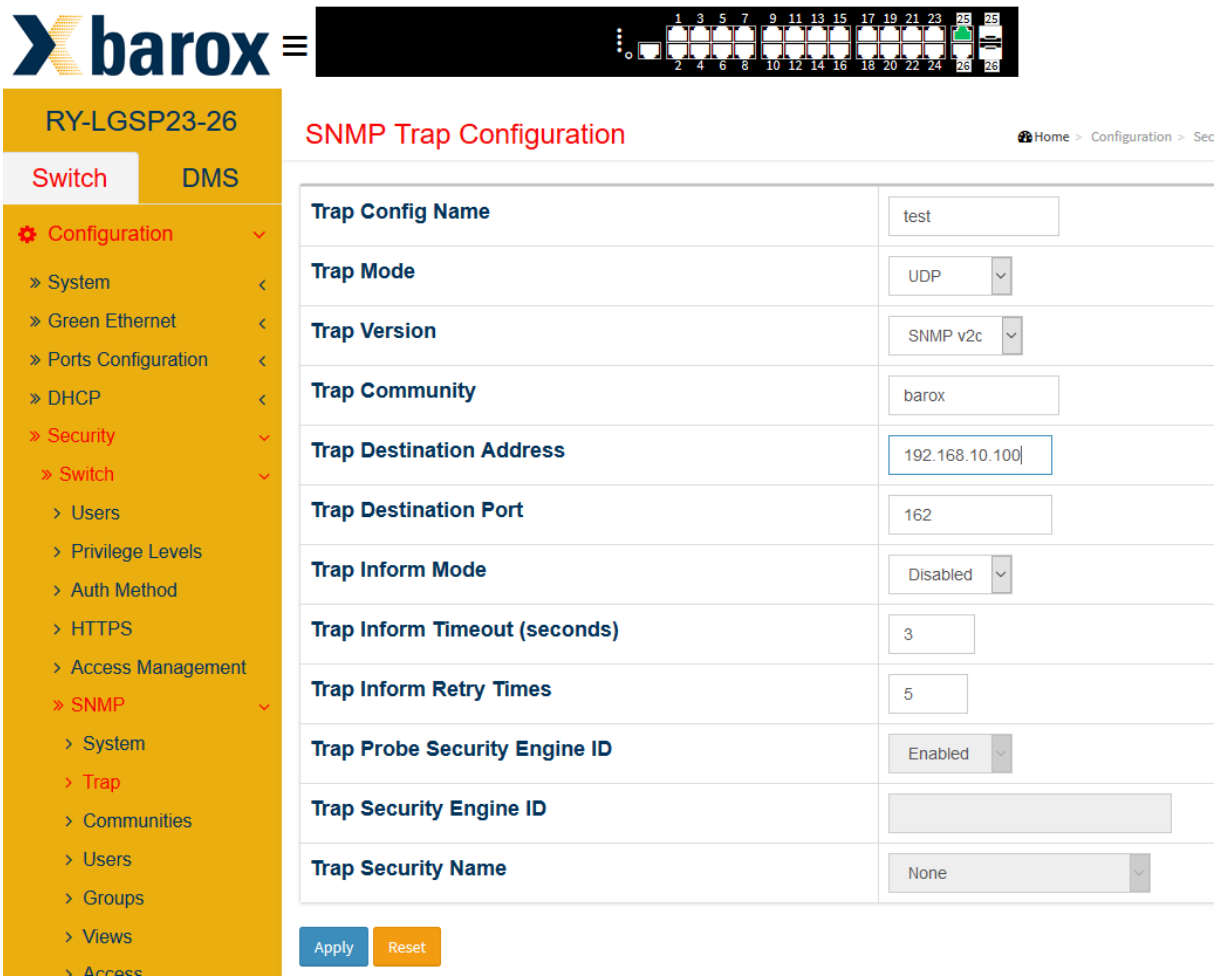
Die Neukonfiguration erfolgt in 2 Schritten:

**Schritt 1:**

Am Beispiel nachfolgend sind folgende Werte für eine neue Konfiguration einzustellen:

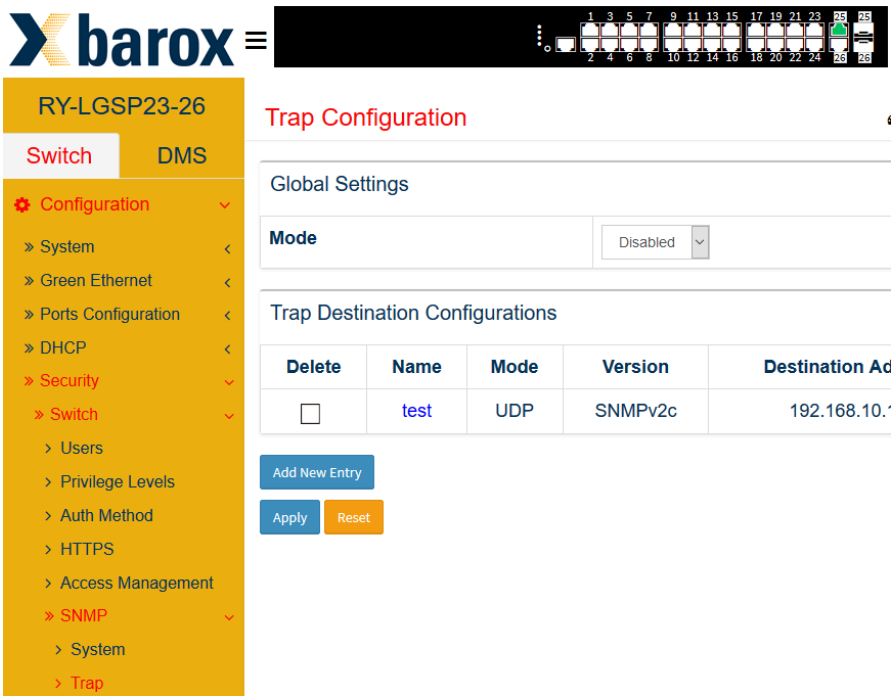
- Trap Config Name -> Ein Name soll vergeben werden
- Trap Mode -> UDP oder TCP – für den Anfang wie gebräuchlich UDP
- Trap Version -> auswählen von SNMP v2c
- Trap Community -> der vorher angelegte Community Name muss eingetragen werden
- Trap Destination Address -> Angabe der Trap Empfänger IP Adresse
- Trap Destination Port -> Angabe des Ports für den Empfänger
- Trap Inform Mode -> Hier im Beispiel auf deaktiviert
- Trap Inform Timeout (seconds) -> 3 eingetragen (Standard)
- Trap Inform Retry Times -> 5 (Standard)

Anschließend werden die Einstellungen mit „Apply“ bestätigt



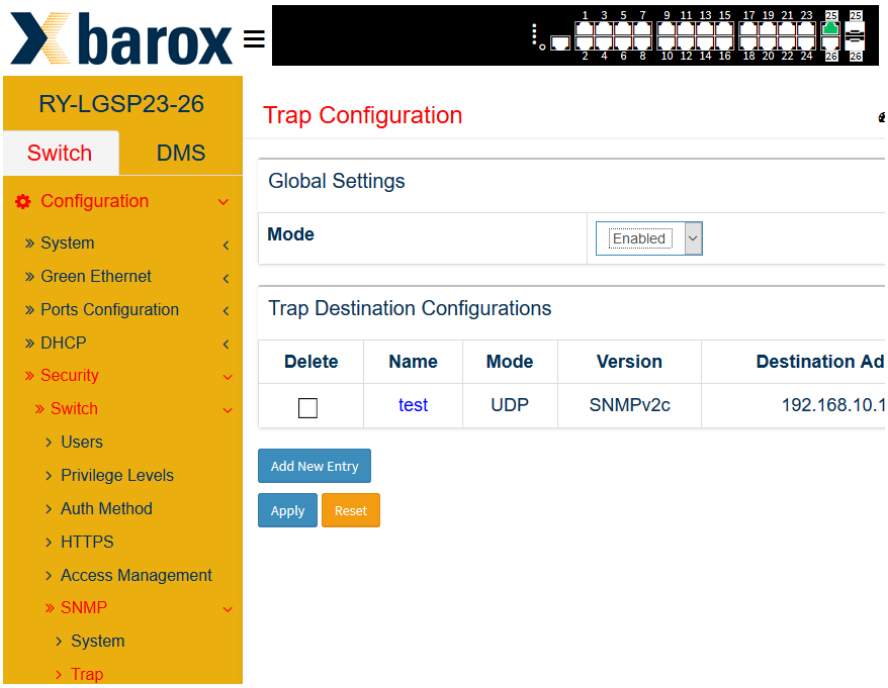

**Schritt 2:**

Nach dem Anlegen der neuen Konfiguration wird die Konfiguration durch auswählen des Name geöffnet.



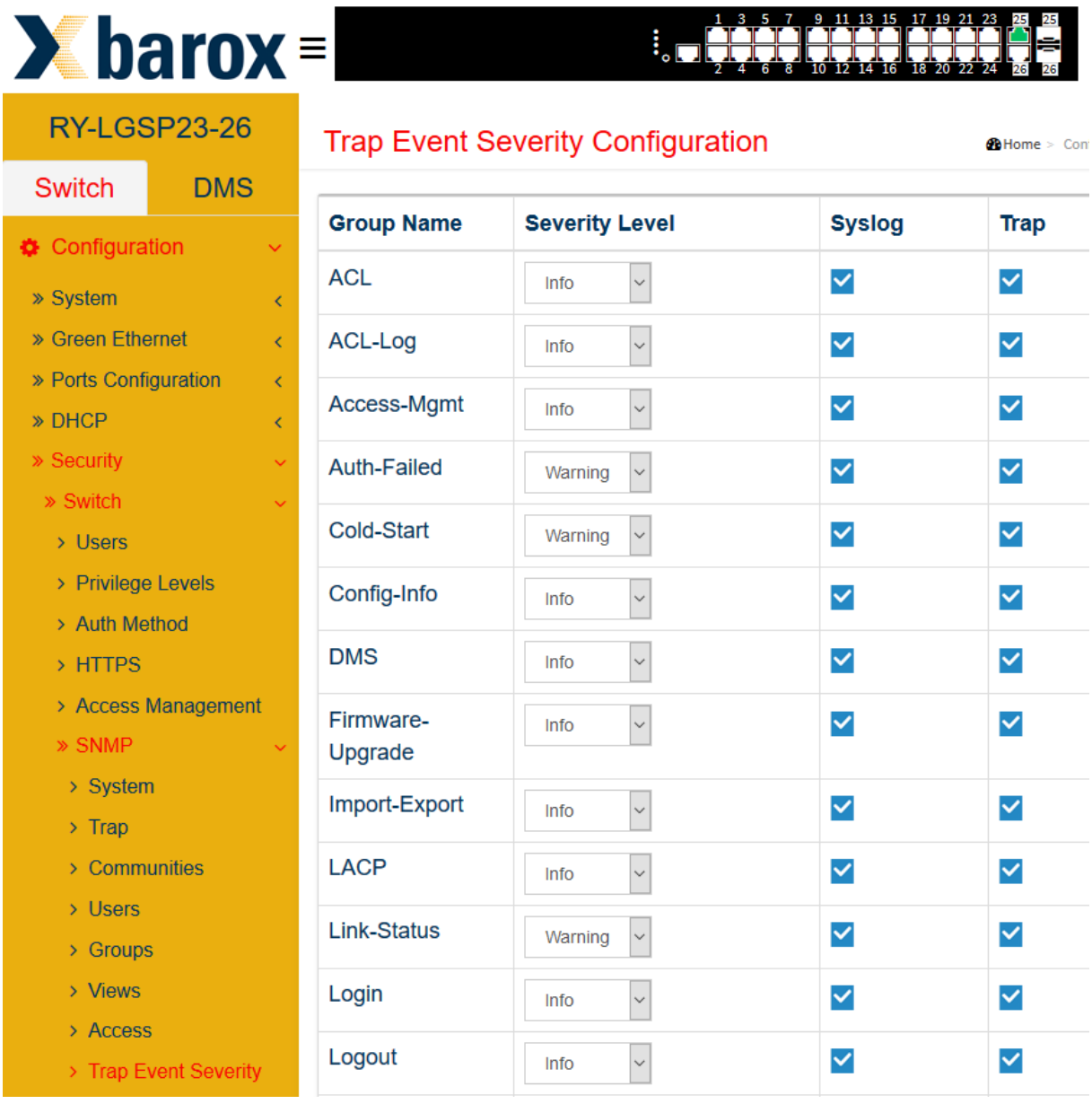

**Aktivierung der SNMP Trap Funktion**

Nach Abschluss der Trap Konfiguration ist der generelle Modus zu aktivieren.



### 5.4.3. Ergänzende Hinweise zum Senden von SNMP Traps

Vergewissern Sie sich, dass die Ereignisse welche eine Trap auslösen entsprechend konfiguriert sind. Diese Einstellungen können im Konfigurationsmenu an anderer Stelle, wie weiter dargestellt, je nach Endgerät Konfiguriert werden. Einige Ereignisse wie z.B. Port Events müssen auch entsprechend in der Portkonfiguration eingestellt werden.




**ACHTUNG: Bei den Industrie-Switchen ist diese Einstellung unter Configuration/System/Alarm Notification zu finden.**

Weiterführende Informationen zum Auslesen und testen der Konfiguration sind unter „5.6 SNMP Traps auslesen“ zu finden.

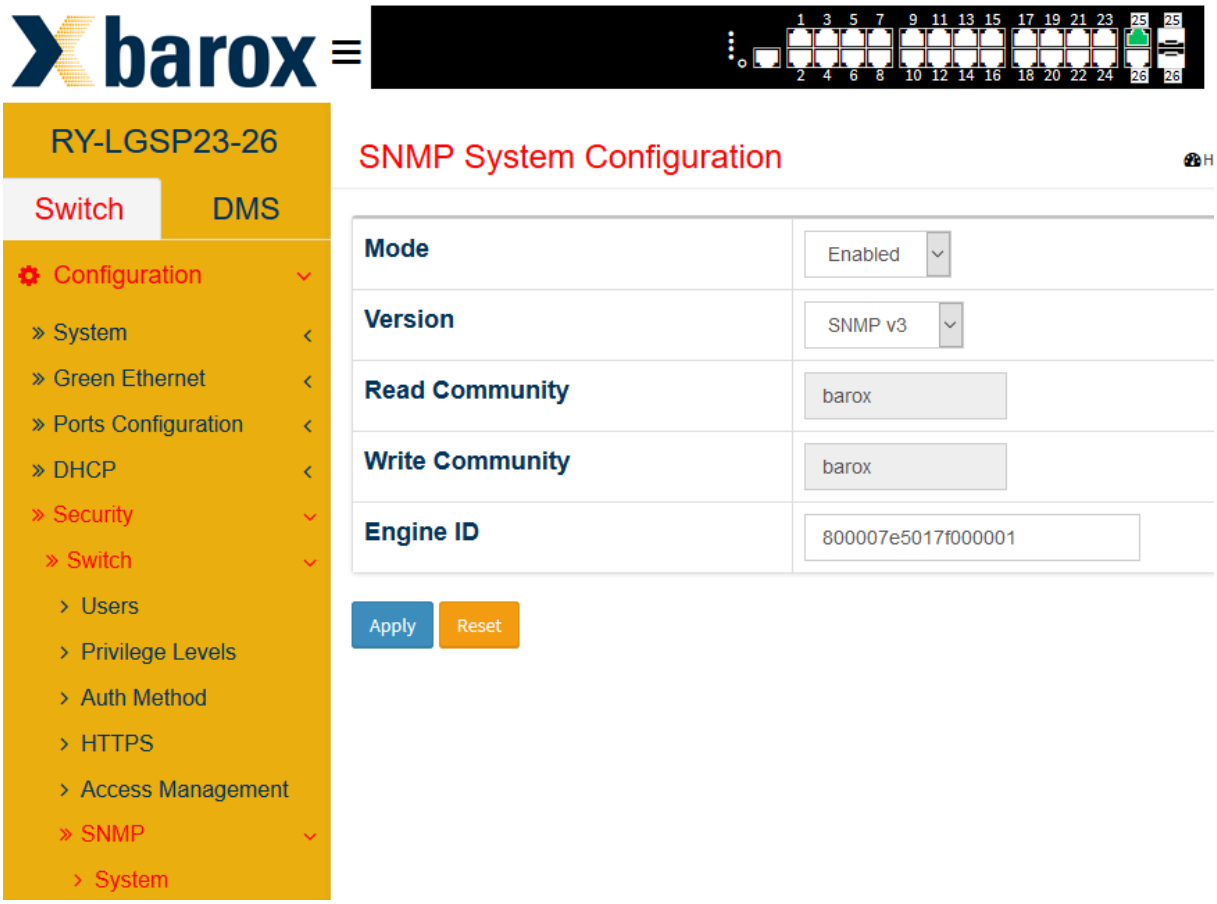
## 5.5 SNMP v3 Konfiguration

**Ausgangslage:**

Der gestiegene Sicherheitsbedarf im Netzwerk bedingt auch die gestiegenen Anforderungen an die Administration und das Monitoring der Netzwerkkomponenten. Dies kann z.B. durch den Einsatz von SNMP in Version 3 mit Authentifizierung erfolgen. Im Weiteren wird eine grundlegende SNMP v3 Konfiguration zur Systemstatusabfrage oder dem Versenden von Systemevents über SNMP Traps an einem Beispiel beschrieben. Die nachfolgenden Schritte sollen die Verwendung von Authentifizierung und Passwortabsicherung aufzeigen.

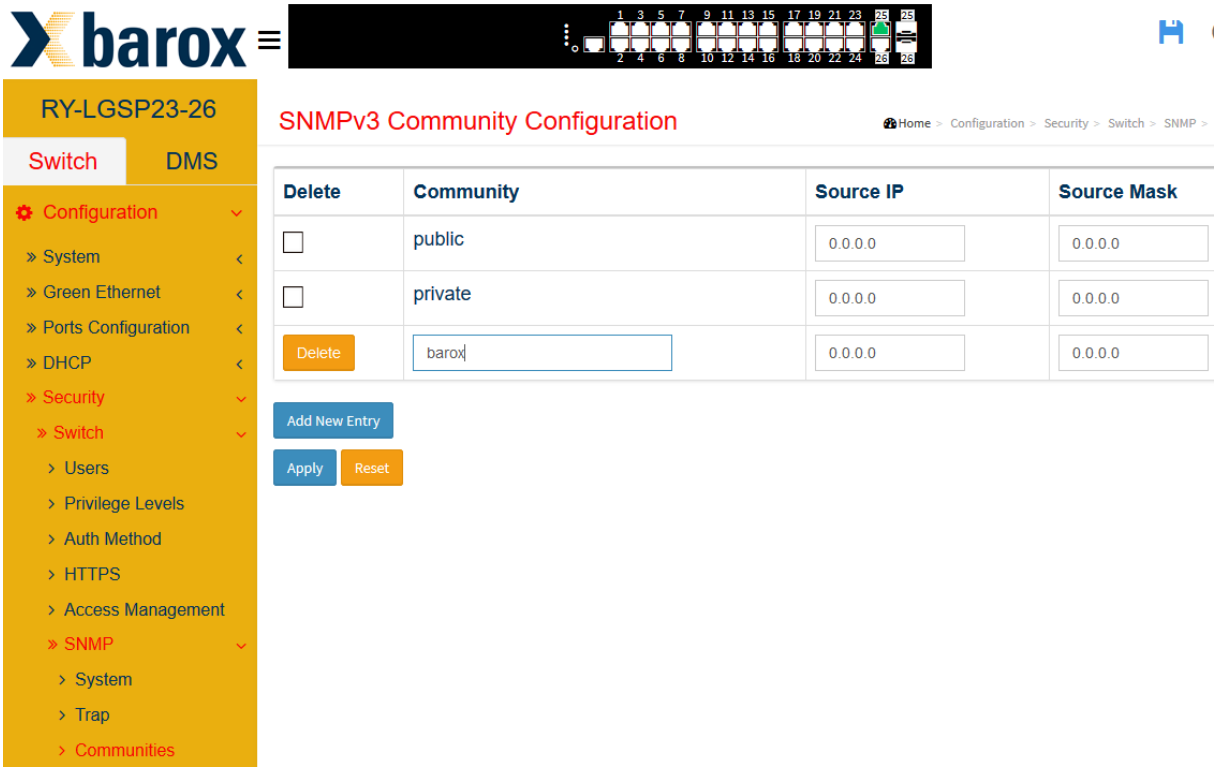
### 5.5.1. Aktivierung der SNMP v3 Funktion

Grundlegend ist der Modus zu aktivieren und die Version SNMP v3 in der SNMP Konfiguration auszuwählen.



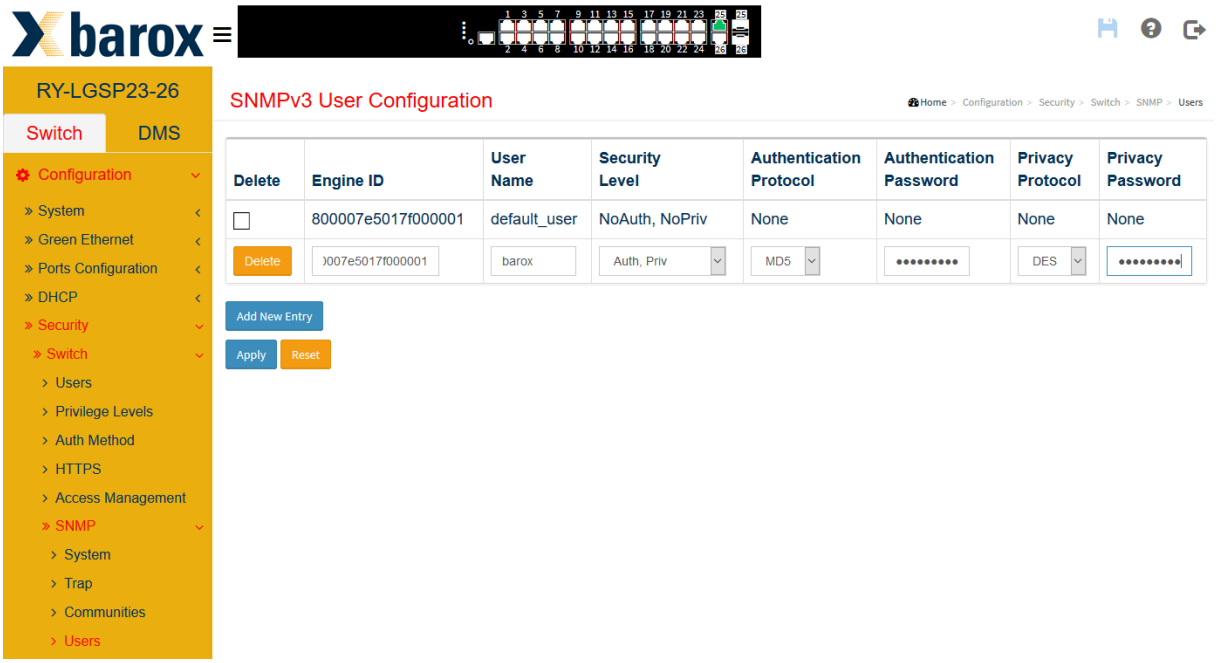

**Erstellen einer dedizierten Community**

Bei der Generierung der Community kann die Quell- IP und Maske jeweils auf 0.0.0.0 gesetzt bleiben. Dies bewerkstelligt, dass auch über mehrere Teilnetze das Versenden und Empfangen von SNMP Nachrichten möglich ist.



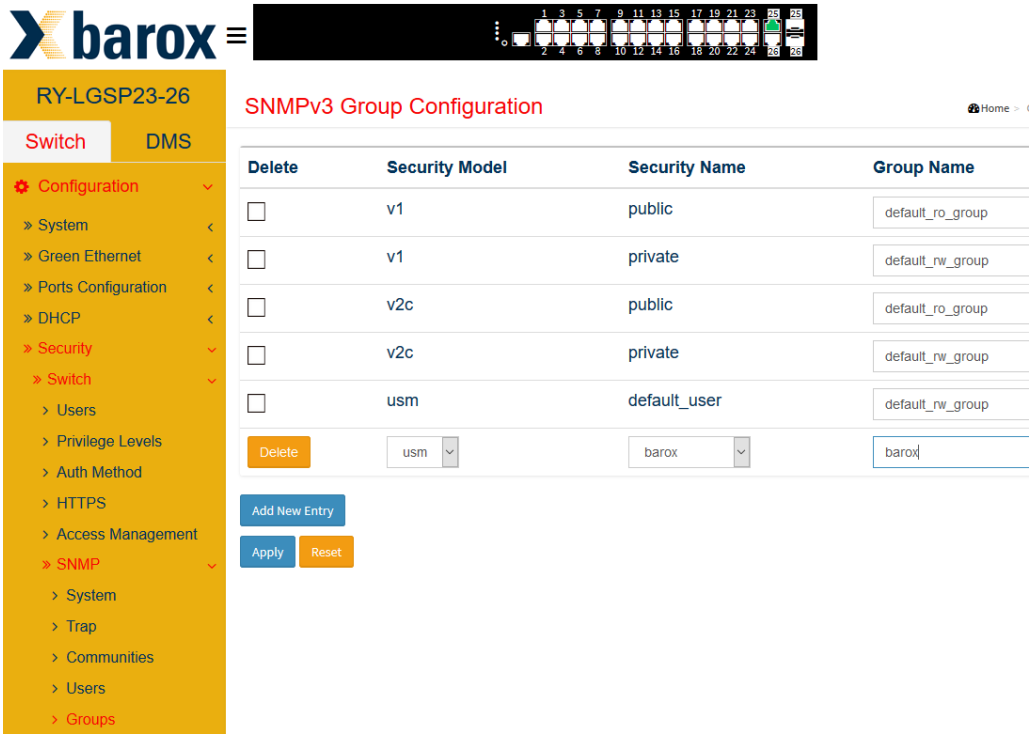

**Anlegen eines neuen Benutzers**

Bei der Konfiguration des neuen Nutzers ist zu beachten, dass dem neuem Nutzerobjekts unbedingt die Engine ID hinzugefügt wird. Diese kann einfach aus dem *„default_user“* Eintrag kopiert und eingefügt werden. Neben dem festlegen des Nutzernamens soll der Sicherheitsgrad, hier im Beispiel *„Auth, Priv“* eingestellt werden. In der Auswahl der Authentifizierungs- „MD5“ und dem Privacy Protokoll DES ist zu beachten, dass beide Passwörter mindestens 8 Zeichen (Ziffern und Buchstabenkombinationen) lang sein müssen.



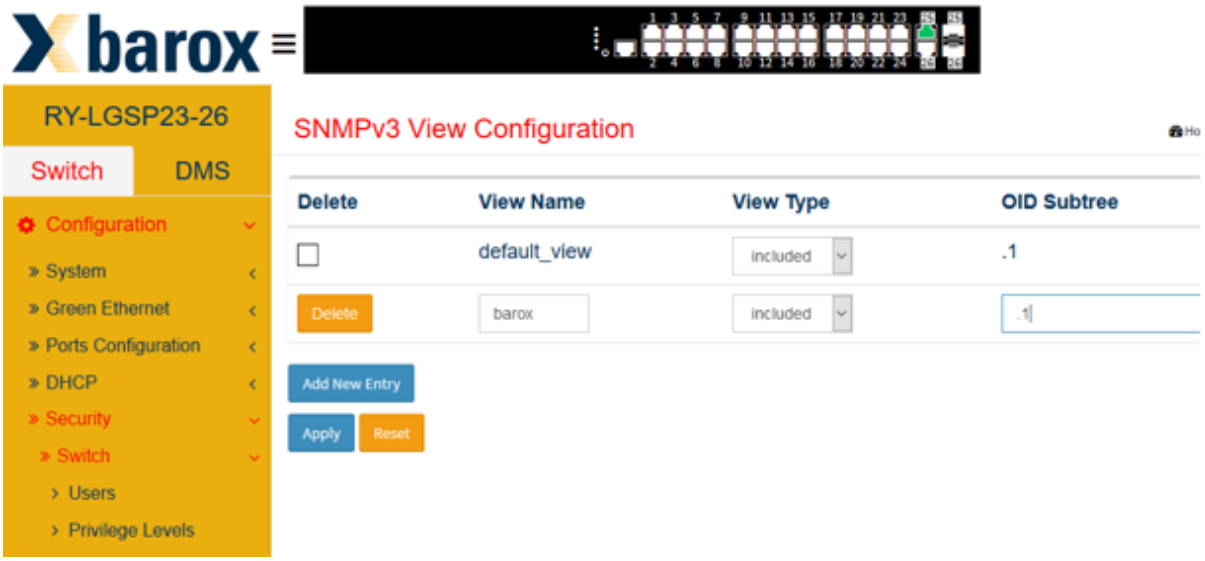
### Anlegen einer Gruppe

Zur Konfiguration einer neuen Gruppe im SNMP v3 soll als Sicherheitsmodell *„usm“* ausgewählt werden. Der vorher erstellte Nutzername ist als *„Security Name“* auszuwählen und anschließend einen Gruppennamen zu vergeben.




### Einstellen der View Configuration

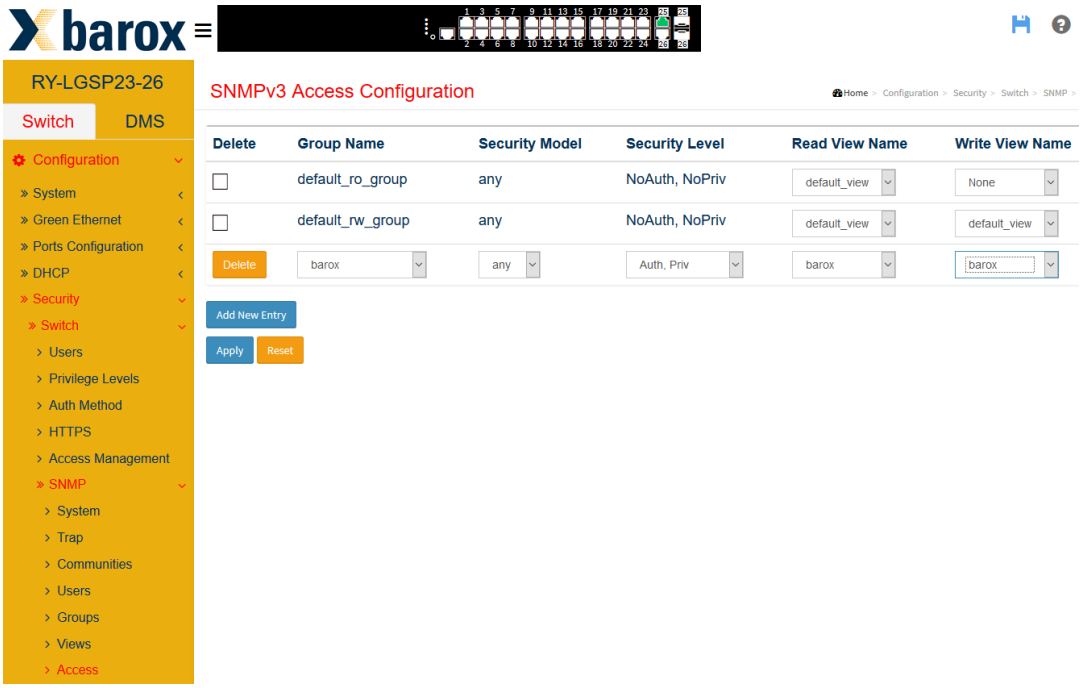
Zunächst wird der View Name festgelegt. Es empfiehlt sich, sofern alle SNMP relevanten Nachrichten einzusehen sind, den OID auf den Wert „.1“ zu setzen. Dies ermöglicht die gesamte Sicht auf alle verzweigten OIDs.




### Konfiguration der Zugriffsmethode

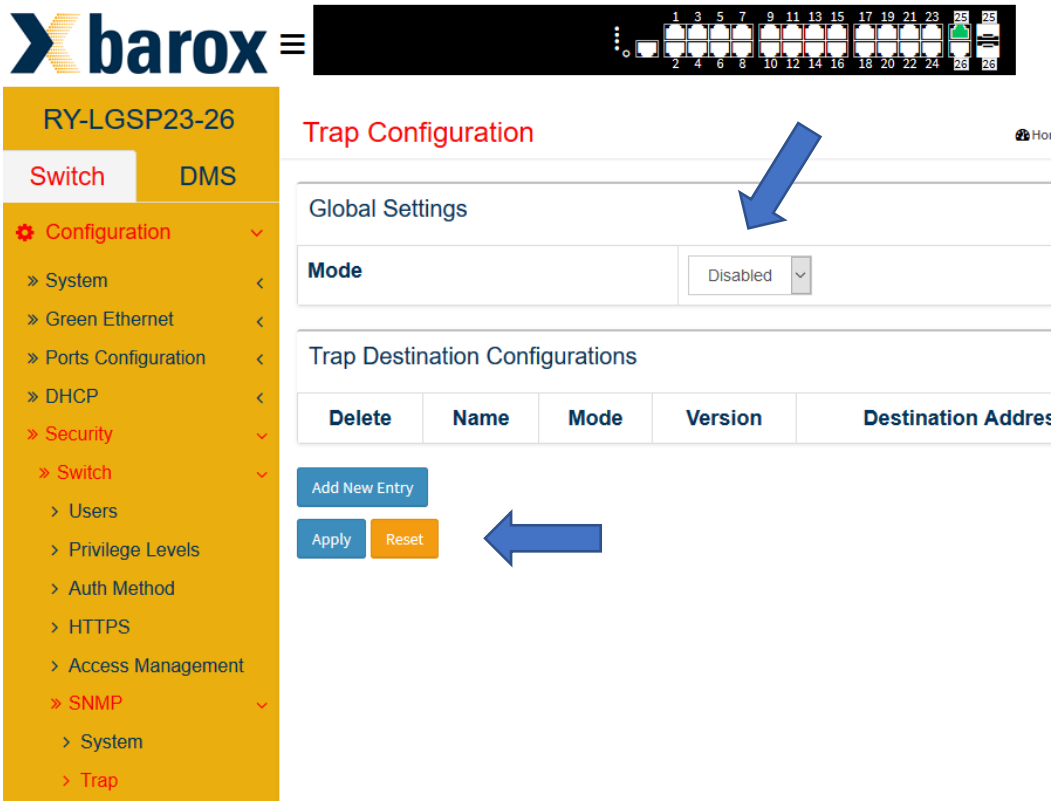
Hierzu soll ein neuer Eintrag mit der Authentifizierungs- und Privatisierungsmethode generiert werden. Zunächst ist die zuvor erstellte Gruppe unter „Group Name“ auszuwählen. Weiter wird der

Gruppe das *„Security Model“* – **„usm“**, dem *„Security Level“* – **„Auth, Priv“** zugewiesen. Letztens werden für das lesen und schreiben die vorher erstellten Views, unter „Read View Name“ und „Write View Name“ ausgewählt.




### 5.5.2. Konfiguration der SNMP Trap

Vor der Konfiguration der neuen Trap Einstellungen ist darauf zu achten, dass die globale Einstellung des Trap- Modus deaktiviert ist.



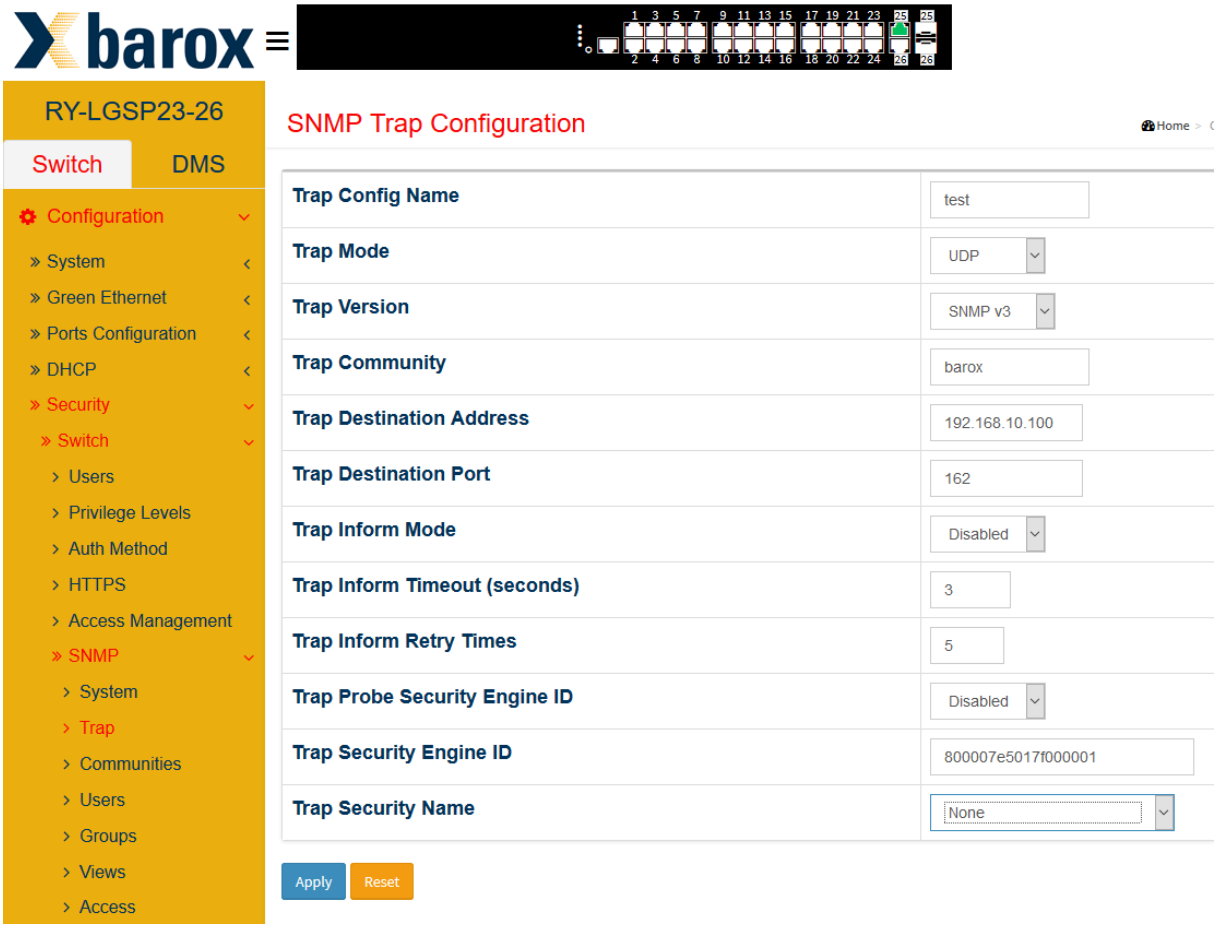
Die Neukonfiguration erfolgt in 2 Schritten:

**Schritt 1:**

Am Beispiel nachfolgend sind folgende Werte für eine neue Konfiguration einzustellen:

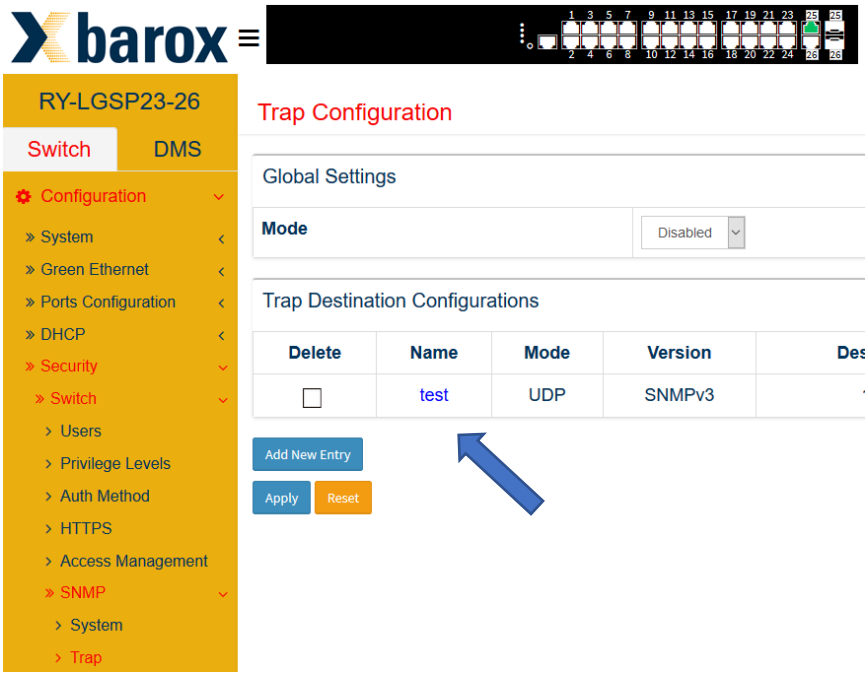
- Trap Config Name -> Ein Name soll vergeben werden
- UDP oder TCP – für den Anfang wie gebräuchlich UDP
- Trap Version -> auswählen von SNMP v3
- Trap Community -> der vorher angelegte Community Name muss eingetragen werden
- Trap Destination Address -> Angabe der Trap Empfänger IP Adresse
- Trap Destination Port -> Angabe des Ports für den Empfänger
- Trap Inform Mode -> Hier im Beispiel auf deaktiviert
- Trap Inform Timeout (seconds) -> 3 eingetragen (Standard)
- Trap Inform Retry Times -> 5 (Standard)
- Trap Probe Security Engine ID -> soll deaktiviert werden
- Trap Security Engine ID -> hier muss die Engine ID des Benutzers eingetragen werden
- Trap Security Name -> es kann vorerst nur „None“ ausgewählt werden“

Anschließend werden die Einstellungen mit „Apply“ bestätigt

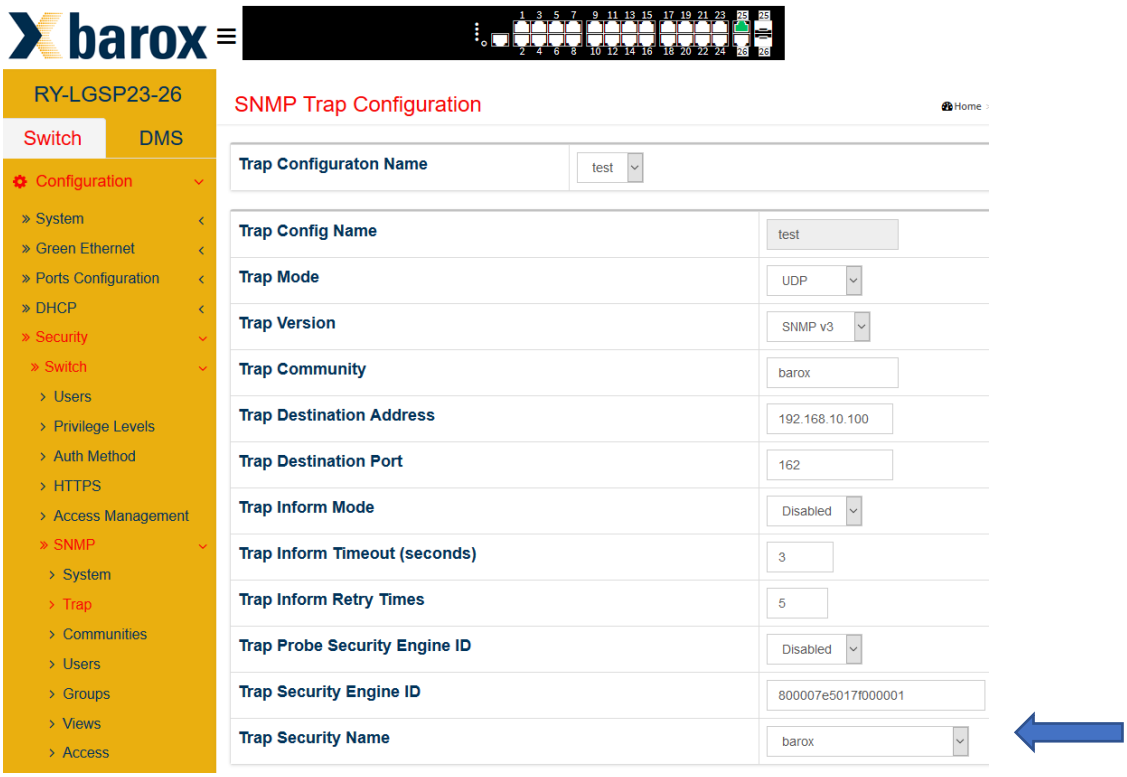



Nach bestätigen der Konfiguration erfolgt noch ein Hinweis, dass ein entsprechender Security Name noch eingestellt werden sollte. Dies wird im 2. Schritt konfiguriert.
**Schritt 2**:

Nach dem Anlegen der neuen Konfiguration wird die Konfiguration durch auswählen des Namens geöffnet.

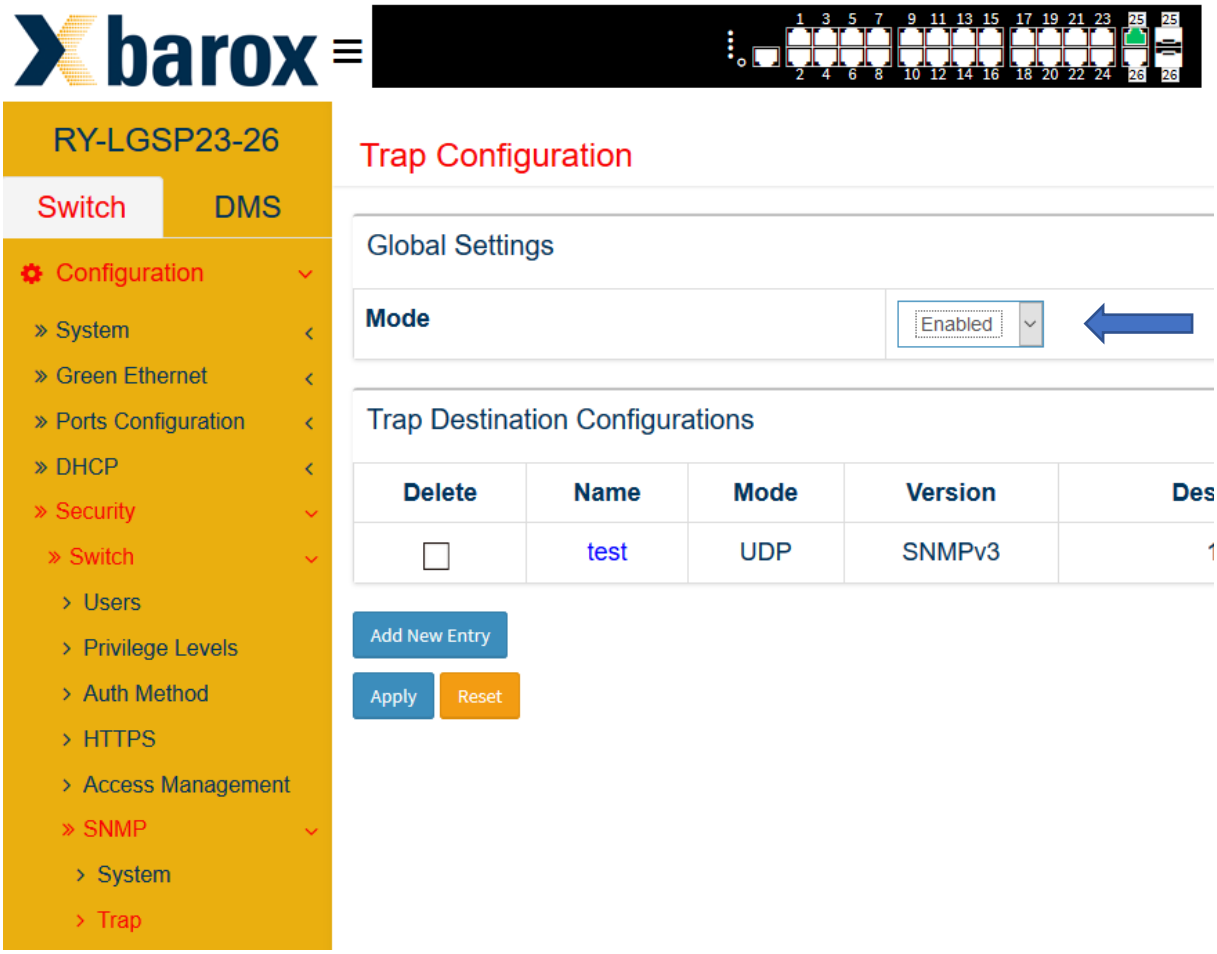



Nun kann der Eintrag „Trap Security Name“ auf den SNMP User eingestellt werden.



**Aktivierung der SNMP Trap Funktion**

Nach Abschluss der Trap Konfiguration ist der generelle Modus zu aktivieren.




### 5.5.3. Ergänzende Hinweise zum Senden von SNMP Traps

Vergewissern Sie sich, dass die Ereignisse, welche eine Trap auslösen entsprechend konfiguriert sind. Diese Einstellungen können im Konfigurationsmenu an anderer Stelle, wie weiter dargestellt, je nach Endgerät, konfiguriert werden. Einige Ereignisse wie z.B. Port Events müssen auch entsprechend in der Portkonfiguration eingestellt werden.


**ACHTUNG: Bei den Industrie-Switchen ist diese Einstellung unter Configuration/System/Alarm Notification zu finden.**

Weiterführende Informationen zum Auslesen und testen der Konfiguration sind unter „5.6 SNMP Traps auslesen“ zu finden.

### 5.6 SNMP Traps auslesen

Über das SNMP Protokoll lassen sich verschiedenste Parameter der barox Switch-Konfigurationen auslesen, bzw. einstellen. Grundlegend werden dafür sogenannte „SNMP/ MIB Browser“ benötigt. Aber auch Netzwerk- Mitschnitt/ Sniffer Software können für das lesen von SNMP Übertragungen verwendet werden.

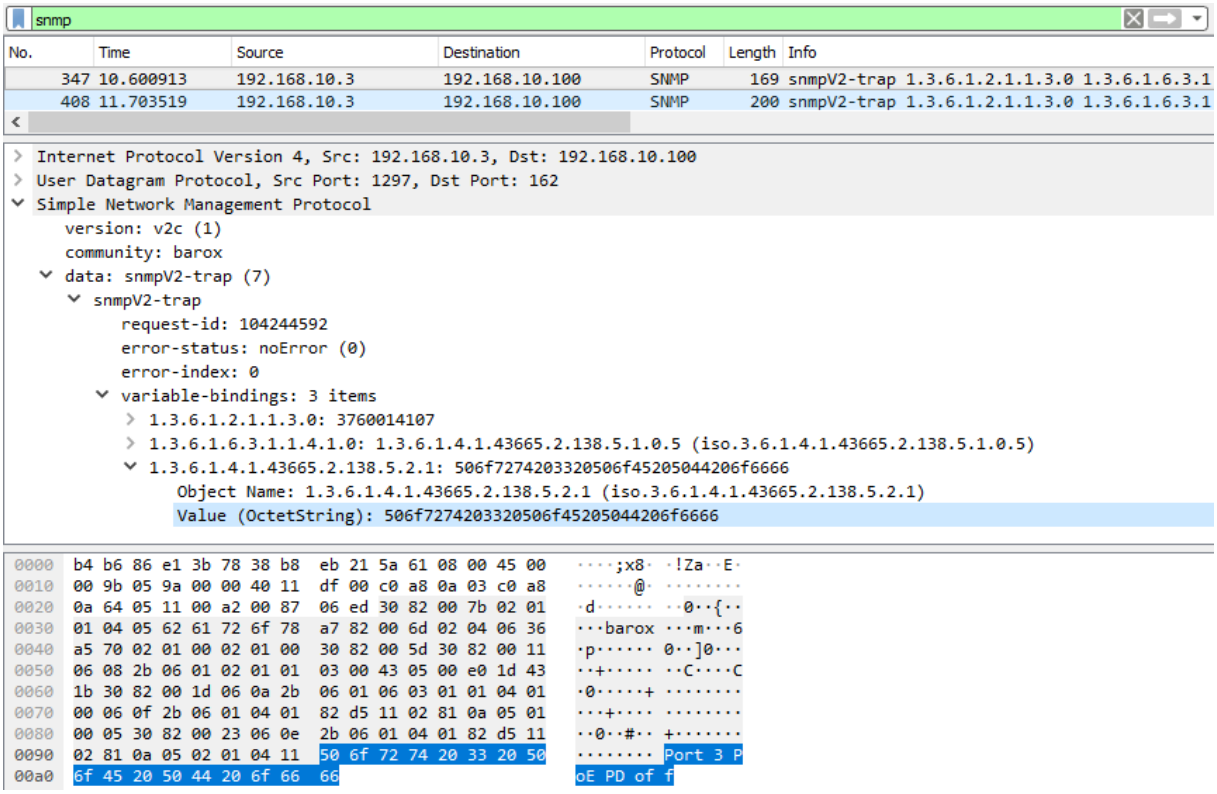
Das Auslesen einer SNMP v2 Trap soll am folgenden Beispiel dies kurz erläutern:

**Ausgangslage:**

Eine PoE Kamera wird am Ethernet Port 3 am Switch getrennt und wieder eingesteckt. Ein PC im Netzwerk ist für das Empfangen der SNMP Traps konfiguriert. Zum Auslesen werden die Software Wireshark (https://www.wireshark.org) und zur benutzerfreundlichen Ansicht der *„iReasonning MIB Browser“ (http://www.ireasoning.com/mibbrowser.shtml) verwendet.

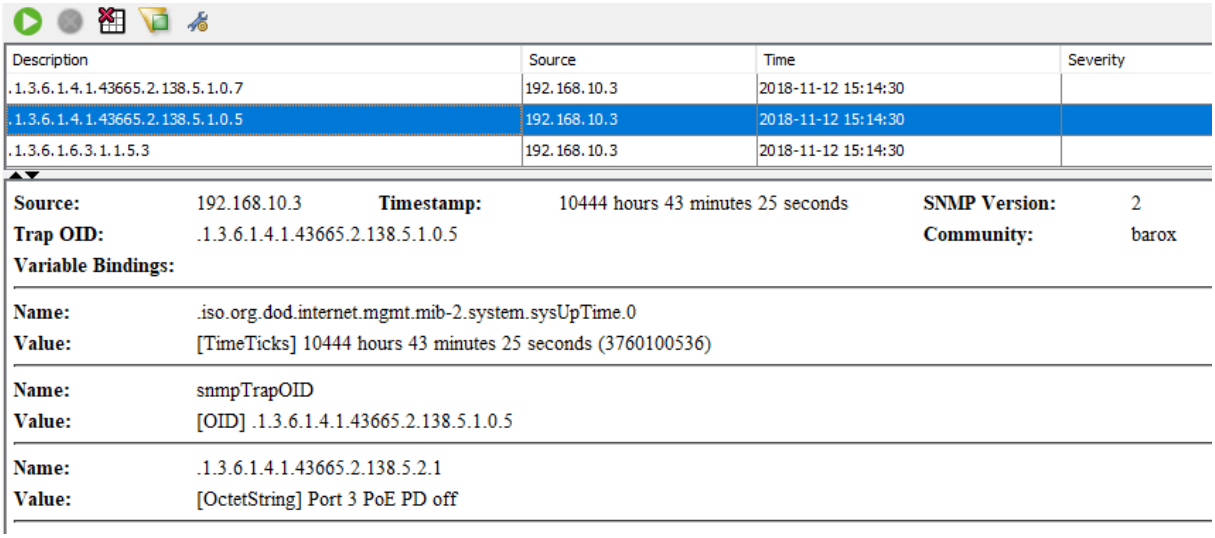
**PoE Kamera wird getrennt/ PD Gerät offline:**

Mitschnitt der Informationen welche vom Switch gesendet werden:



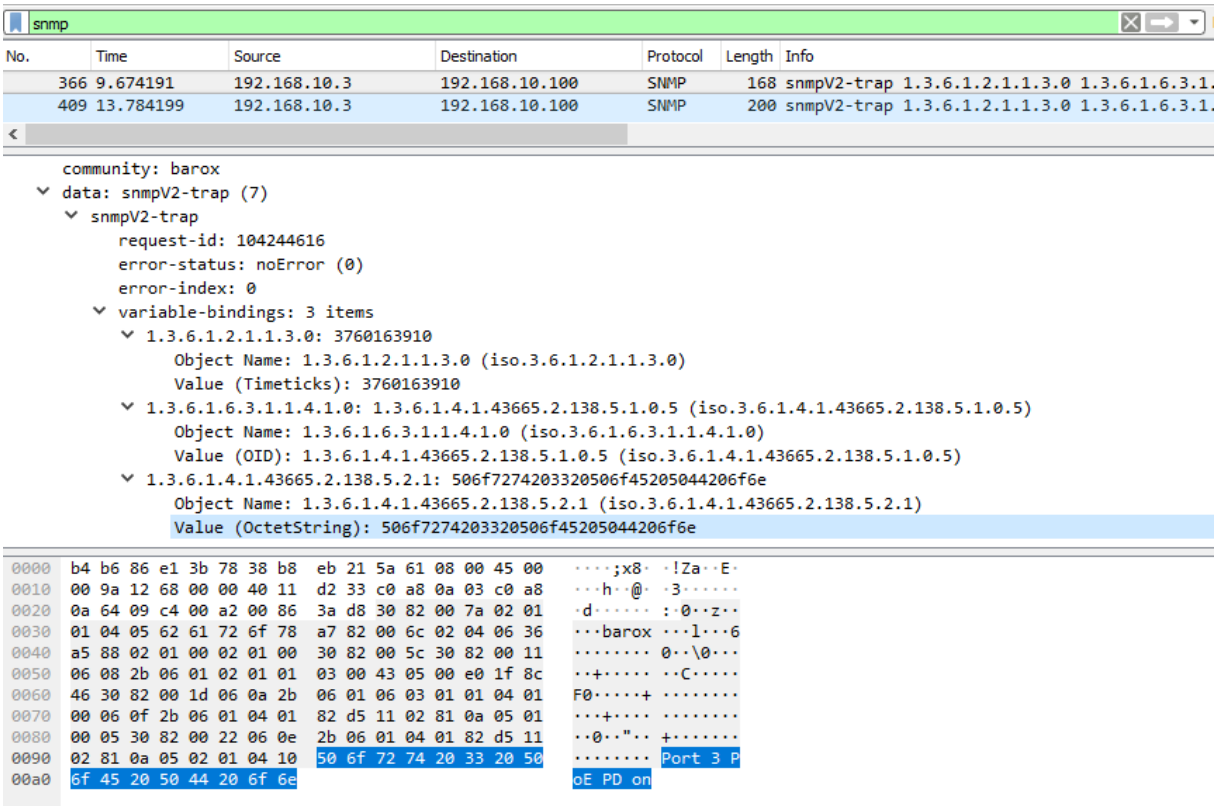

* Bitte beachten Sie bei Verwendung der Software die jeweiligen Lizenzbestimmungen der Softwareanbieter.

Ansicht der Information im SNMP Browser:



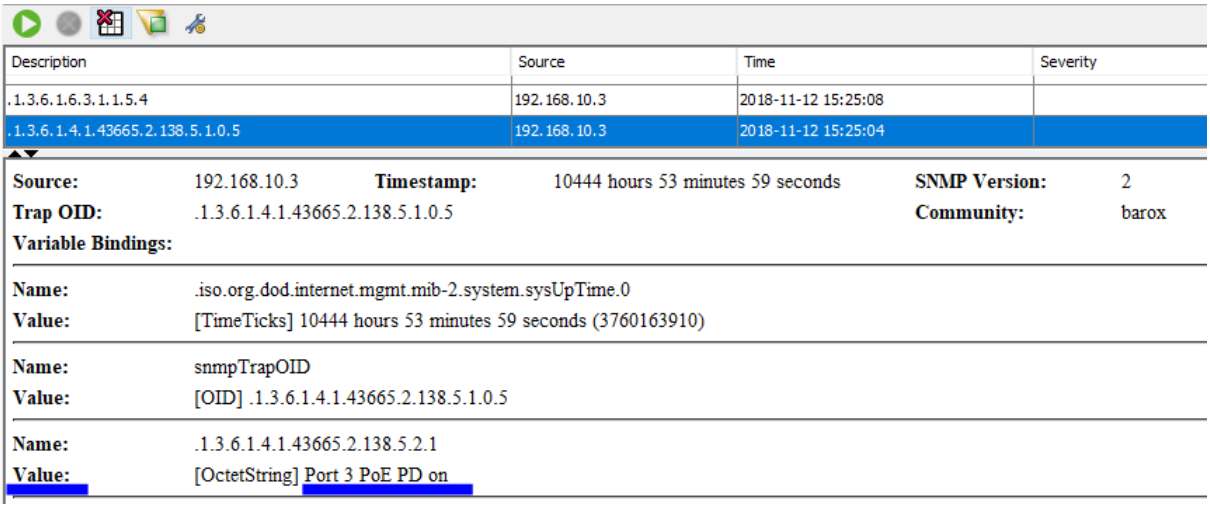
**PoE Kamera wird wieder verbunden/ PD Gerät online:**

Mitschnitt der Informationen welche vom Switch gesendet werden:




Ansicht der Information im SNMP Browser:

Zumeist werden neben den zugehörigen OIDs (Objekt Kennzeichnungen für Informationseinheiten) der Traps auch ein Wert zum Ablesen, bzw. Deuten des Status/ Nachricht der SNMP Nachricht hinzugefügt. In diesem Beispiel ist die letzte Zeile zur Veranschaulichung gekennzeichnet.



## 5.7 Verwendung von MIB Files zum Auslesen und Steuerung der Switche

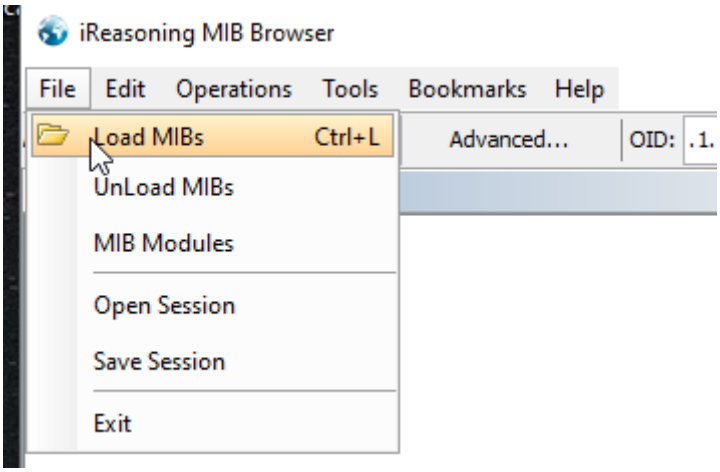
Grundsätzlich können im Netzwerk bei managebaren Geräten wie Switches, Router oder Server meist über die SNMP Funktionalität Statusabfragen erfolgen. Oftmals werden aus sicherheitstechnischen oder Herstellerspezifischen Aspekten sogenannte MIB Files für die Abfragen der Geräte benötigt. Diese Dateien enthalten die Informationen über die Identifikationskennzahlen der Funktionen.

### Switch Status Funktionen abfragen über SNMP unter Verwendung von MIB Files

Zur Einführung empfiehlt sich grundlegend der Einsatz eines MIB Browsers. Im Beispiel zur benutzerfreundlichen Ansicht wird der *„iReasonning MIB Browser“ (http://www.ireasoning.com/mibbrowser.shtml) verwendet. Weiter muss der Browser auch mit den entsprechenden SNMP Parametern zur Verbindung mit dem jeweiligen Switch konfiguriert sein.

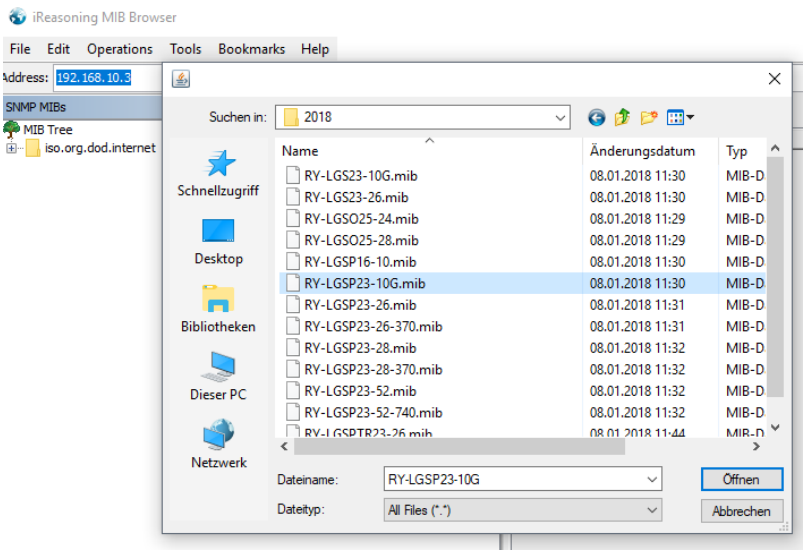
### Schritt 1 Import des MIB Files

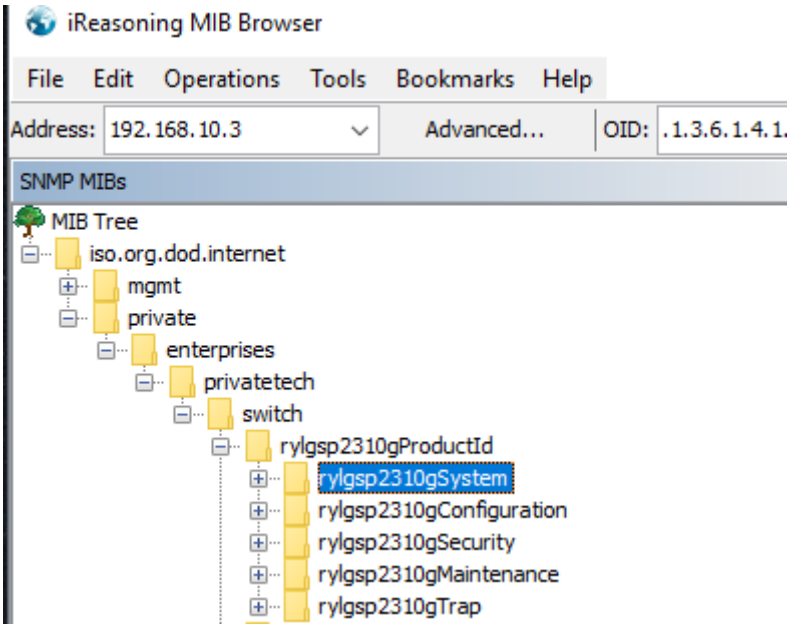
Beim Import ist darauf zu achten, dass die passende MIB Datei für den entsprechenden Switch ausgewählt wird. Die erforderlichen MIB Dateien sind am *„.mib“* Präfix zu erkennen.




* Bitte beachten Sie bei Verwendung der Software die jeweiligen Lizenzbestimmungen der Softwareanbieter!

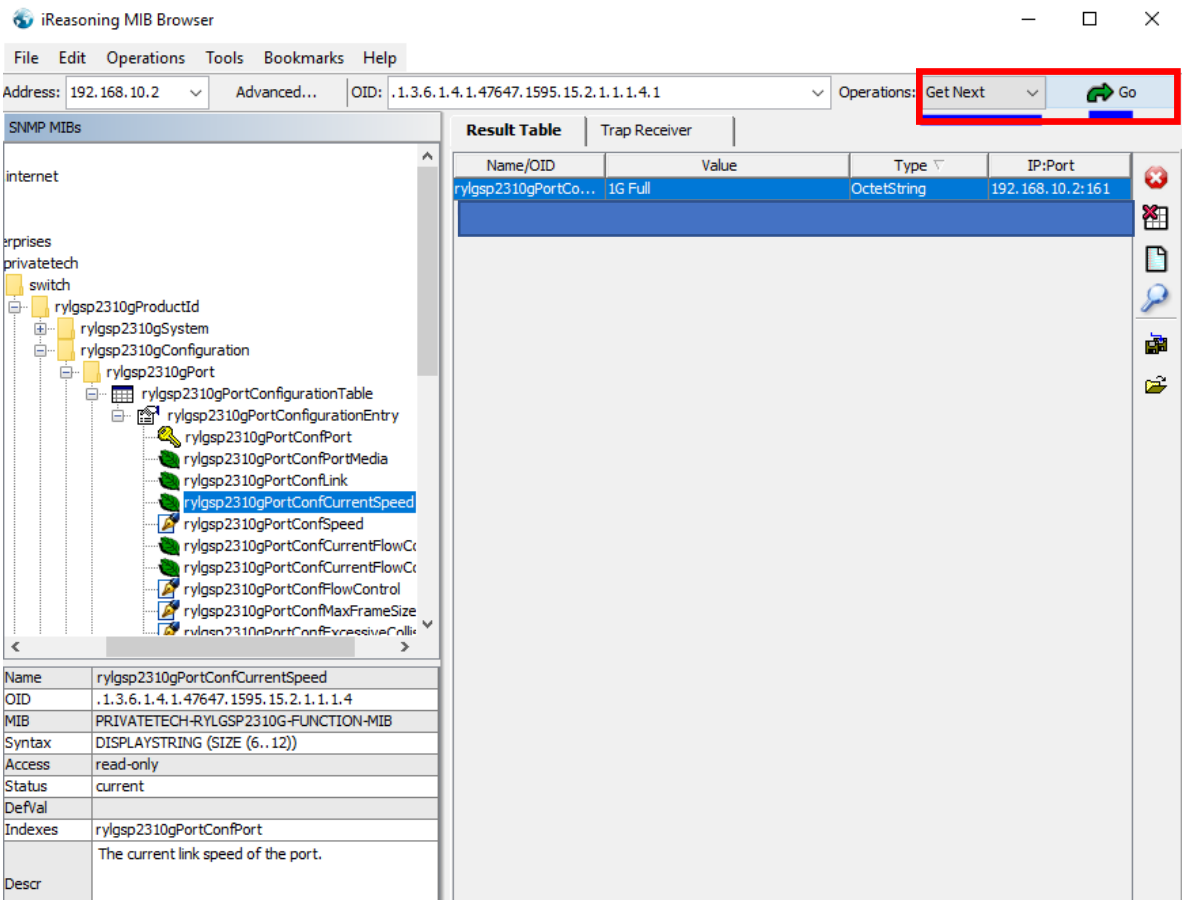
Nach erfolgreichem Import sind die MIB Strukturen wie folgend abgebildet ersichtlich.






**Schritt 2 Abfragen generieren**

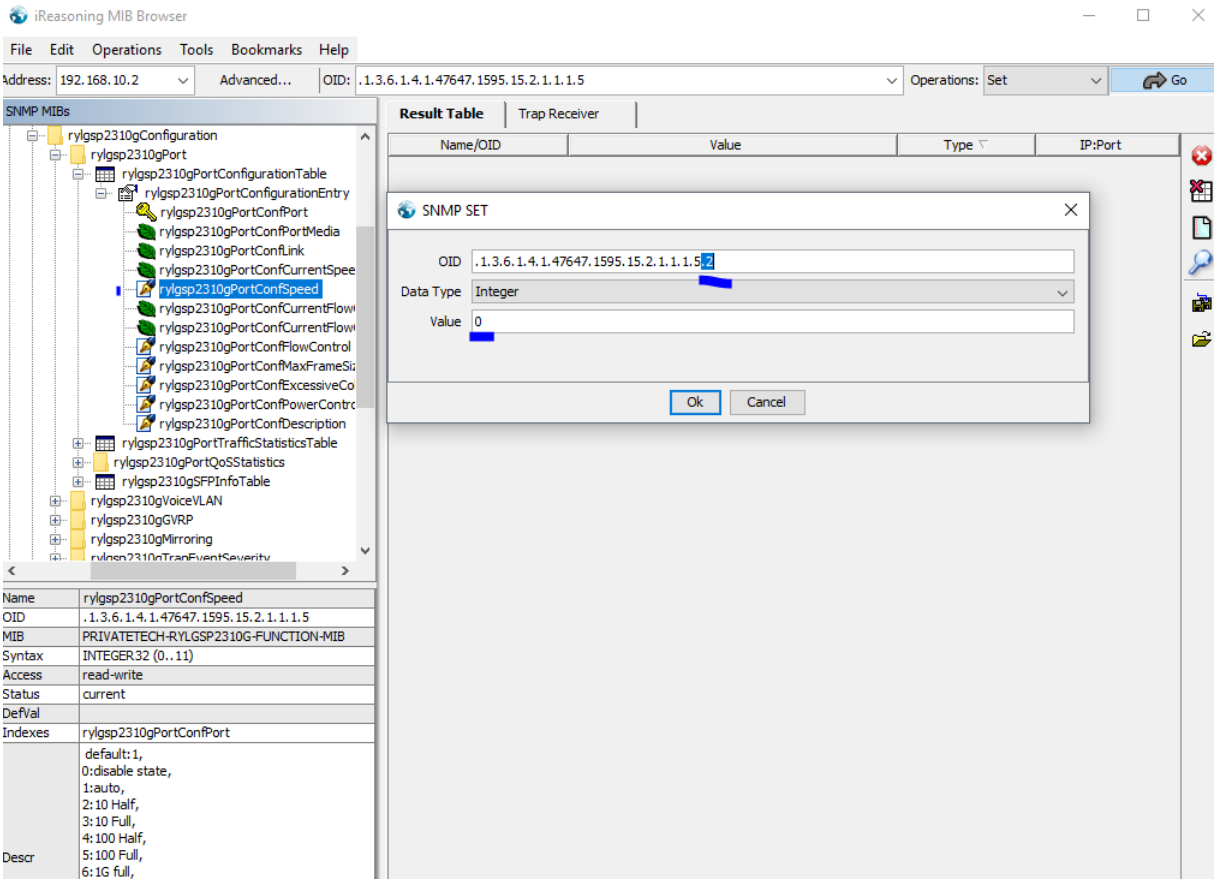
Um eine Abfrage zu generieren wird zunächst der gewünschte Status ausgewählt und mit *„Get Next“* Operation und dem Klick auf *„Go“* die Abfrage generiert. Nach erfolgreicher Abfrage erscheinen die Informationen zum Status in der Resultatstabelle wie im Beispiel, folgend, abgebildet.

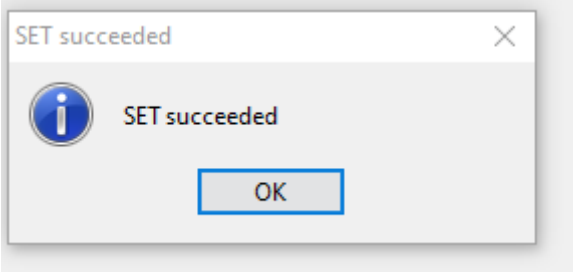


## 5.8 Switch Funktionen steuern über SNMP und MIB unter Verwendung der „SET“ Operation

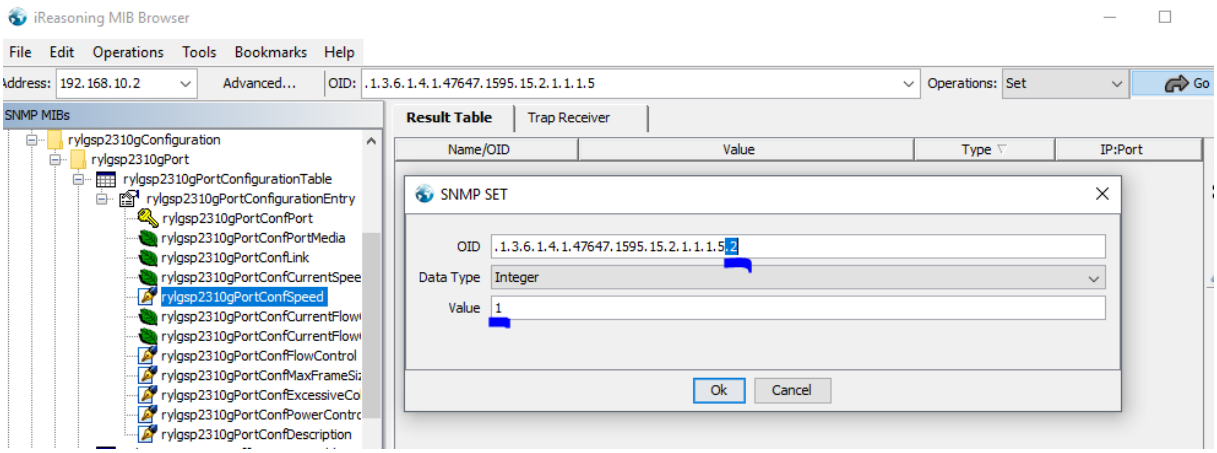
Als weitere Methode zur Steuerung der barox Switche kann die Operation „SET“ über das SNMP Protokoll erfolgen. Voraussetzungen sind die grundlegende SNMP Konfigurationen am Switch und des MIB Browsers. Nachfolgend ist ein Beispiel mit dem Einsatz der SET Operation aufgeführt, welches eine Portabschaltung und Wiederanschaltung am Switch auslöst.

Um den Port 2 am Switch zu deaktivieren wird die Portkonfiguration im MIB Verzeichnis gesucht. Dabei ist zu beachten, dass der richtige Informationsblock mit Schreibfunktion ausgewählt ist. Die Set Operation wird durch den Klick auf *„Go“* geöffnet und der OID Eintrag mit *„ .2 “* (Kennzeichnung des Ports 2) ergänzt. Zudem wird der Wert *„0“* (für deaktivieren) eingetragen und mit „OK“ bestätigt. Nach erfolgreicher Operation wird dementsprechend eine Erfolgsmeldung generiert.



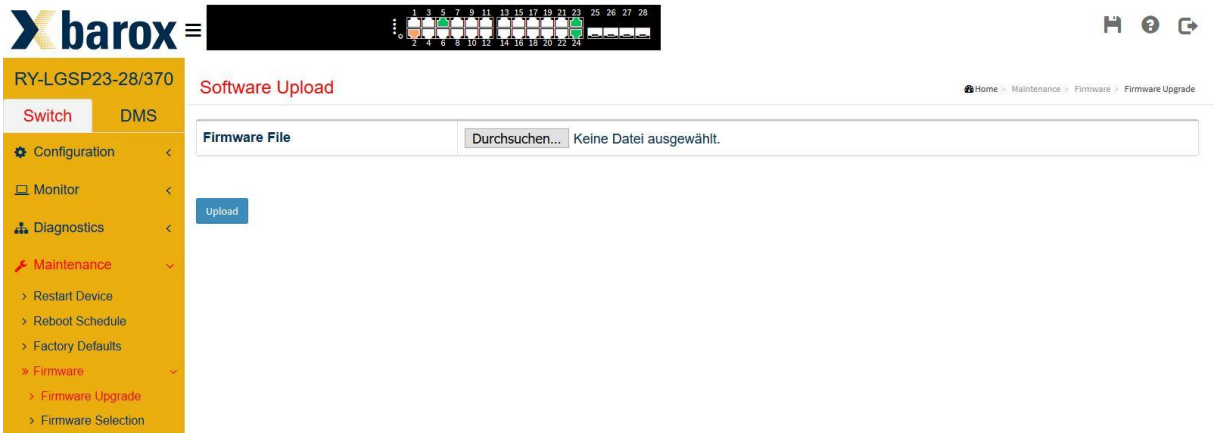



Um den Port 2 am Switch zu aktivieren wird die Portkonfiguration im MIB Verzeichnis gesucht. Dabei ist zu beachten, dass der zugehörige Informationsblog mit Schreibfunktion ausgewählt ist. Die Set Operation wird durch den Klick auf *„Go“* geöffnet und der OID Eintrag mit *„ .2 “* (Kennzeichnung des Ports 2) ergänzt. Zudem wird der Wert *„1“* (für aktivieren) eingetragen und mit „OK“ bestätigt. Nach erfolgreicher Operation wird dementsprechend eine Erfolgsmeldung generiert.

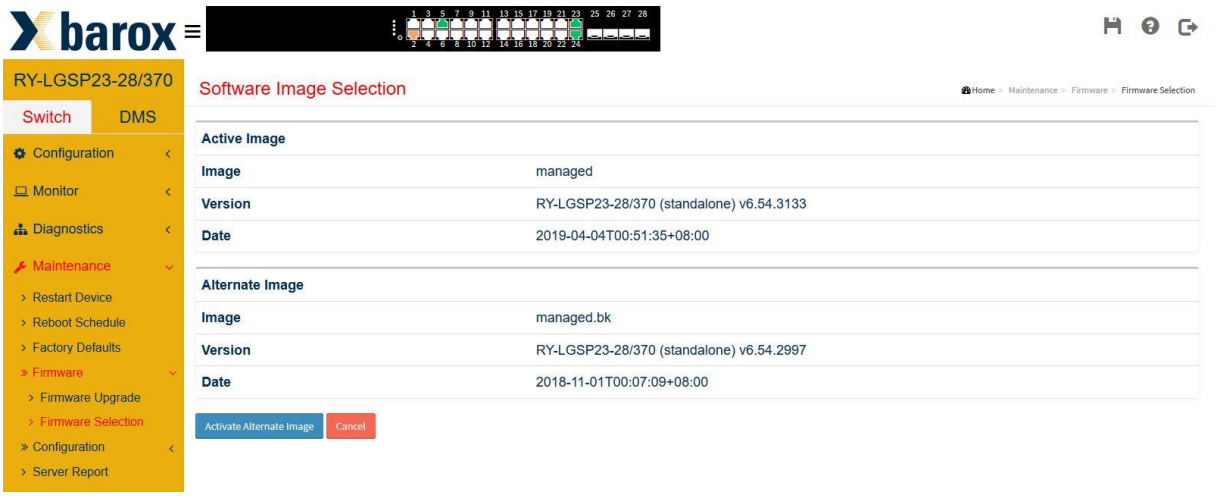



## 6 Firmware Upgrade

Aufgrund regelmäßiger Softwareupdates zur Fehlerbehebung und Einführung neuer Leistungsmerkmale empfiehlt es sich, die Firmware sporadisch zu aktualisieren.




Nach dem Upgrade steht die neue Firmware gleich zur Verfügung. Sollte aus irgendeinem Grund wieder die alte Firmware aufgespielt werden, kann dies ganz einfach im Menupunkt "Firmware Selection" reaktiviert werden.

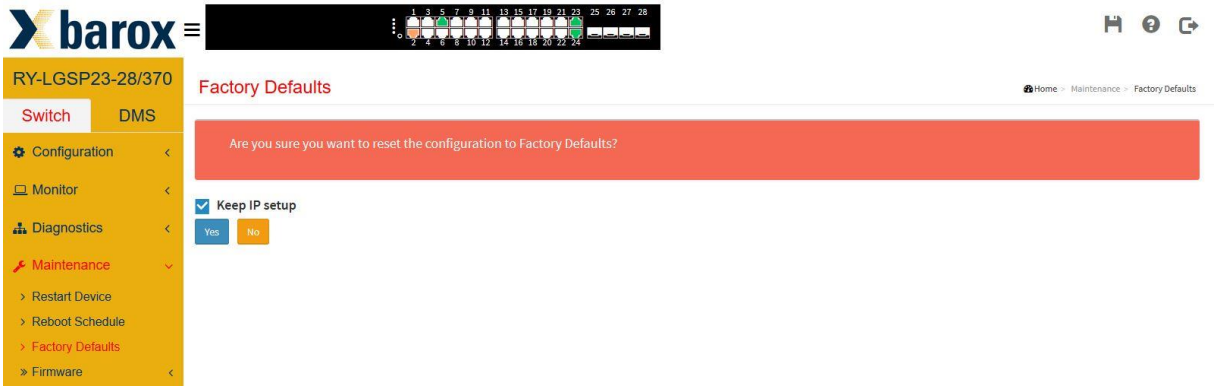



## 7 Werkeinstellung

Die Switche können jederzeit wieder in die Werkeinstellung zurückgesetzt werden.

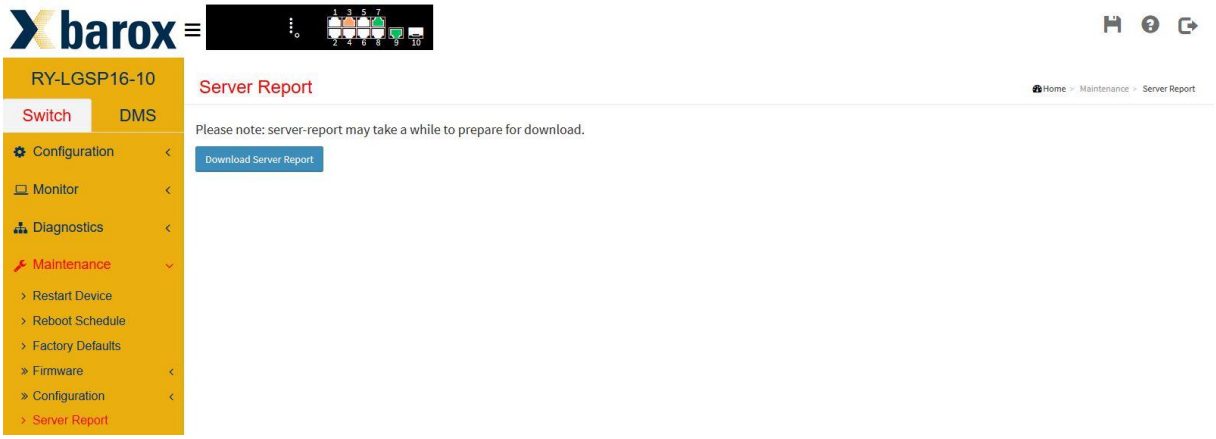
Entweder per Software via Menü "Maintenance/Factory Defaults" oder per Druck des Reset-Knopfes auf der Frontseite (länger als 10 Sekunden).

Mit dem "Häkchen" bei "Keep IP setup" behält der Switch die konfigurierte IP-Adresse, alles andere wird auf Werkeinstellung zurückgesetzt.

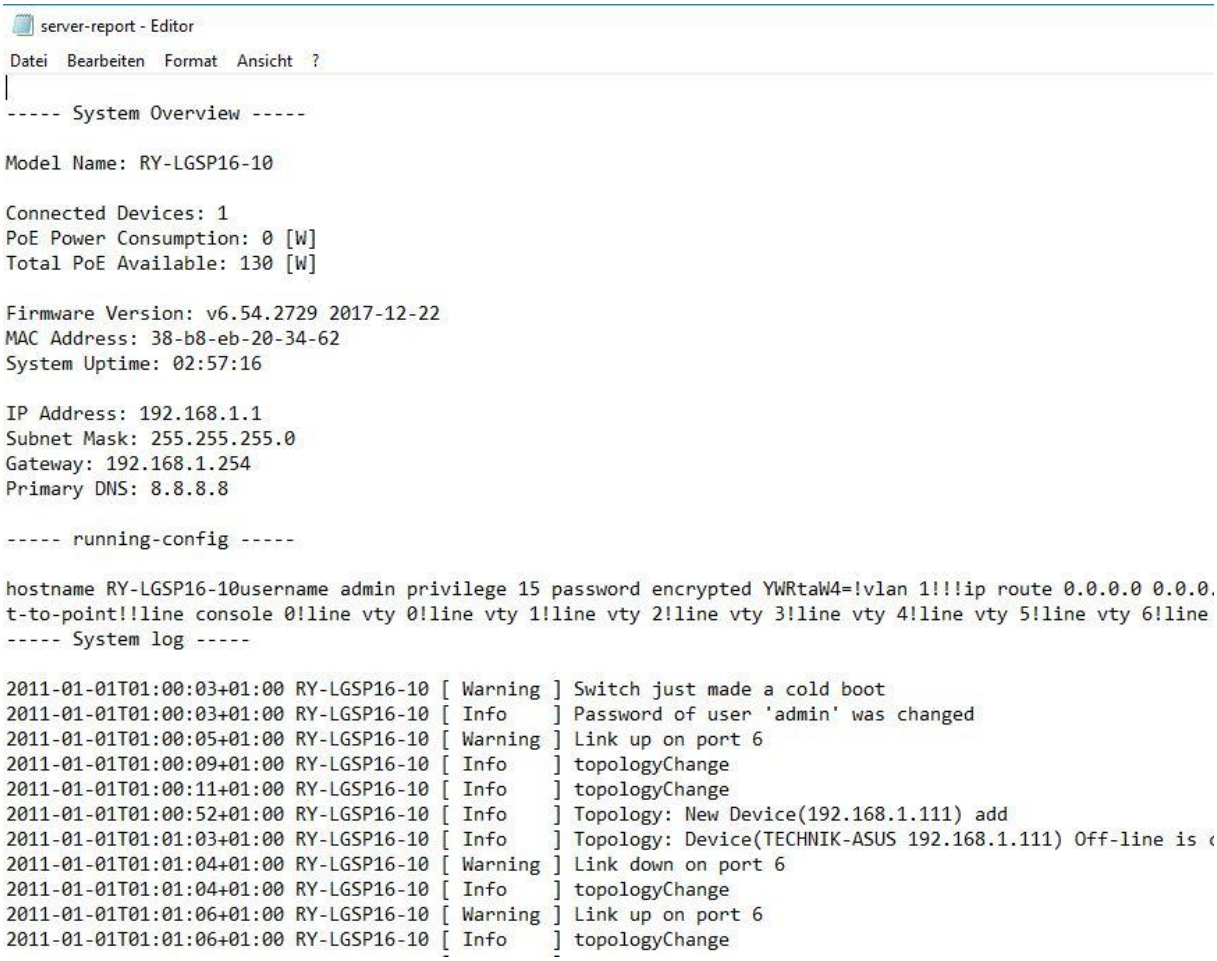



## 8 Server Report

Bei Supportanfragen sollte der Server Report mitgesendet werden. Er enthält die Darstellung der gesamten Konfiguration sowie weitere nützliche Informationen für den Support-Techniker.



**Auszug eines Server Reports**



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 GARANTIE

barox Kommunikation gewährleistet, dass das Produkt für die Dauer der landesspezifischen Garantiedauer frei von Fehlern in Material und Verarbeitung ist. Die barox Kommunikation Garantie ist unabhängig von der Gewährleistungsverpflichtung des Verkäufers aus dem Kaufvertrag mit dem Endkunden und lässt diese unberührt.

barox Kommunikation behebt unentgeltlich Mängel am Produkt, die auf einem Material- und / oder Verarbeitungsfehler beruhen und der barox Kommunikation innerhalb der Garantiedauer angezeigt werden. barox Kommunikation entscheidet nach eigenem Ermessen über die Massnahme zur Behebung des Mangels. Die Garantie hinsichtlich der reparierten oder ersetzten Teile wird für die verbleibende Zeit der Garantiedauer übernommen.

Das Garantieprogramm gilt nicht für Produkte, an denen die Seriennummer entfernt, unkenntlich gemacht oder geändert wurde. Die Garantie umfasst auch nicht die folgenden Schäden:

1. Schäden durch Unfall oder missbräuchlichen oder unsachgemässen Betrieb, insbesondere bei Missachtung der Gebrauchsanweisung für das Produkt.
2. Schäden durch den Einsatz von Teilen, die nicht von barox Kommunikation gefertigt oder vertrieben wurden.
3. Schäden durch vorgenommene Änderungen, die von barox Kommunikation nicht zuvor schriftlich genehmigt wurden.
4. Schäden infolge von Serviceleistungen, die nicht von barox Kommunikation oder ermächtigten Vertretern von barox Kommunikation erbracht wurden.
5. Schäden, die durch Transport, Unachtsamkeit, Schwankungen oder Ausfall der Energieversorgung, höhere Gewalt oder die Betriebsumgebung verursacht wurden.
6. Schäden infolge von normaler Abnutzung und üblichem Verschleiss.
7. Schäden durch Computerviren und andere Software.
8. Schäden durch die Festlegung bzw. Neukonfiguration von Kennwörtern.

Für von barox Kommunikation erbrachte Serviceleistungen im Zusammenhang mit dem Beheben solcher Mängel oder Schäden, die auf einen der oben aufgeführten Ausschlussgründe zurückzuführen sind, fallen zusätzliche Gebühren für Arbeitsleistung, Transport und Teile an. Für die Neuinstallation der ursprünglichen Software werden zusätzliche Gebühren in Rechnung gestellt.