Bedienungsanleitung

RY-LGSP28-10
RY-LGSP28-28
RY-LGSP28-52/xxx (EOL)

RY-LGSO38-10
RY-LGSP38-28
RY-LGSPTR38-52/740

19"-Switche:
RY-Switche der 28er- und der 38er-Serie
Firmware-Release ab v8.40.1589
Hardware-Version ab v1.02
Maschinenversion ab v1.01
PoE Firmware-Version ab 208-211

Herausgeber:

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

Erscheinungsdatum: Januar 2025
Version: 1.2

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
- Vertrautheit mit Computersystemen
- Kenntnisse über Local Area Networks (LANs) und Basiswissen über IP-Kommunikation
- Umgang mit einem Webbrowser

1.1 Inhalt

Das Bedienungshandbuch ist in folgende Bereiche unterteilt:

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

1.2 Über uns

Überall dort, wo Videodaten in Netzwerken mit höchster Qualität prompt und sicher übertragen 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 für Multicast-Anwendungen.

1.3 Web-Seite

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 Funktionen für Layer 2/2+, unterschiedlicher Anzahl optischer und elektrischer Ports. Sie können verwaltet werden 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 Start des Switches können die einzelnen PoE-Ports zeitversetzt gestartet werden, um eine Überlastung der PoE-Netzteile zu verhindern.

- **Weitere nützliche Eigenschaften**

Jumbo Frames mit bis zu 9.600 Bytes werden bei 1 Gbit/s und auch bei 100 Mbit/s 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 (Frontseite) 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 auf alle 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 sich der PC/Laptop mit der IP-Adresse im gleichen Netzwerk-Segment befindet wie der Switch. Zum Bsp.: 192.168.1.111

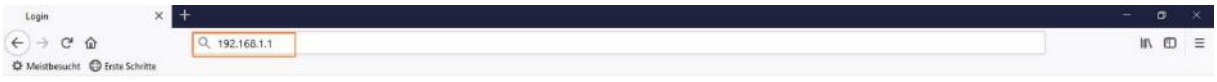
Alternativ können die Switche auch über CLI (Consolen-Port) konfiguriert werden. In dieser Dokumentation wird die Konfiguration des Switches mittels Webbrowser erklärt.

3.1 Werkeinstellung und Login

Ab Werk haben die Switche folgende Einstellungen:

IP-Adresse:	192.168.1.1
Subnetz-Maske:	255.255.255.0
Benutzer:	admin
Passwort:	admin

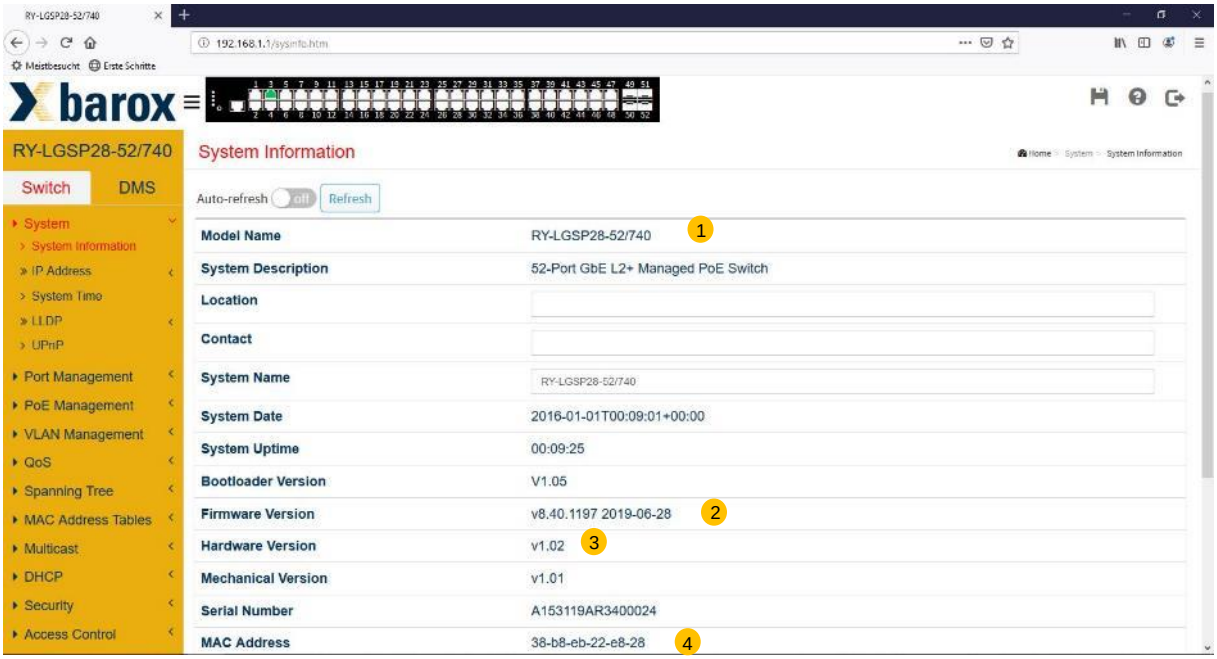
Durch Eingabe der IP-Adresse des Switches (192.168.1.1) direkt im Webbrowser wird die Verbindung zum Switch hergestellt. Die Anmeldung erfolgt mittels Eingabe des Benutzernamens und des Passworts.



Nach erfolgreichem Login wird automatisch die Seite „System Information“ angezeigt. Dort sind die wichtigsten Angaben zum Switch ersichtlich.

3.2 Systeminformation

Auf dieser Seite sind die wichtigsten Angaben zum Switch ersichtlich.

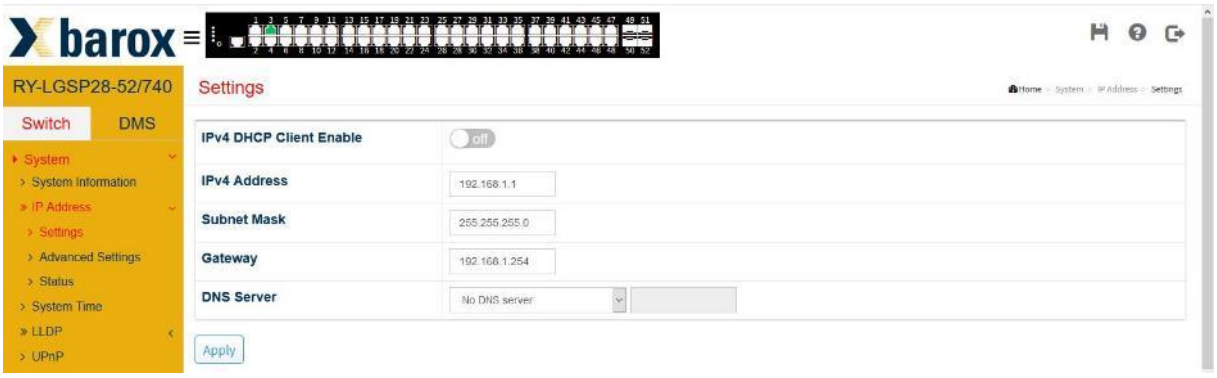


Legende:

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

3.3 Feste IP-Adresse vergeben oder DHCP

Im ersten Schritt muss dem Switch eine IP-Adresse zugewiesen werden. Hierfür wird in der Baumstruktur der Menüpunkt „Switch/System/IP Address/Settings“ gewählt.



Feste IP-Adresse

Im oberen Bild sieht man, dass der Switch die IP-Adresse 192.168.1.1, die Subnetzmaske 24 (255.255.255.0) und als Gateway die IP-Adresse 192.168.1.254 hat.

Soll dem Switch eine neue IP-Adresse zugewiesen werden, ist die bestehende IP-Adresse zu überschreiben und mit durch einen Klick auf die Schaltfläche „Apply“ zu bestätigen. Das Gleiche gilt, falls die Subnetzmaske oder Gateway-Adresse geändert werden muss.

DHCP

Wird der Switch in einem Netzwerk integriert, in dem ein DHCP-Server die IP-Adressen vergibt, muss der Schiebeschalter „IPv4 DHCP Client Enable“ auf „on“ umgestellt werden.

Der DHCP-Server im Netzwerk weist dem Switch eine IP-Adresse im vordefinierten Bereich zu.
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

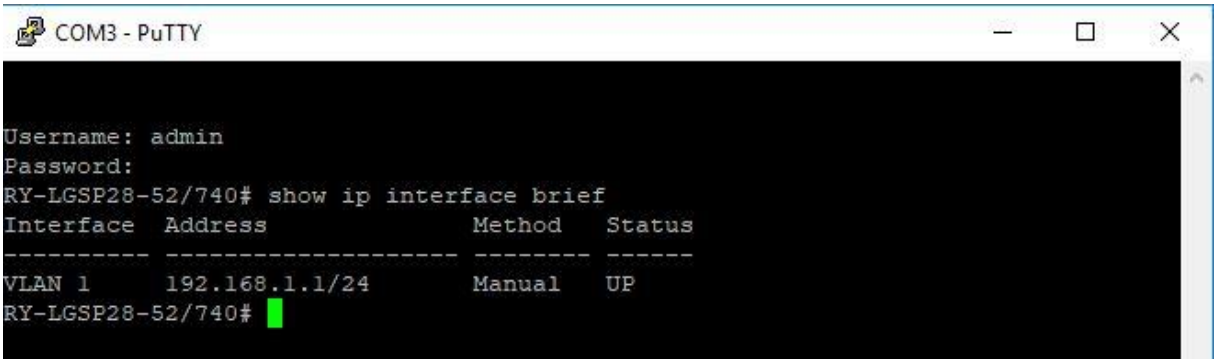
Hierfür kommt das mitgelieferte Konsolen-Kabel zum Einsatz. Der Konsolen-Port am Switch ist eine RS232-Schnittstelle. Es wird also ein PC/Laptop mit einer seriellen Schnittstelle oder einem USB–RS232-Wandler benötigt.
Als Software empfehlen wir „PuTTy“, um den Switch via CLI-Port zu konfigurieren.
http://www.chip.de/downloads/PuTTY_12997392.html

Die CLI-Schnittstelle hat ab Werk folgende Einstellung:

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

Ist die Verbindung über die serielle Schnittstelle hergestellt, ist eine Anmeldung mit Benutzernamen und Passwort erforderlich.

Mit nachfolgendem Befehl kann die IP-Adresse erfragt werden:
RY-LGSP28-52/740# ***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.

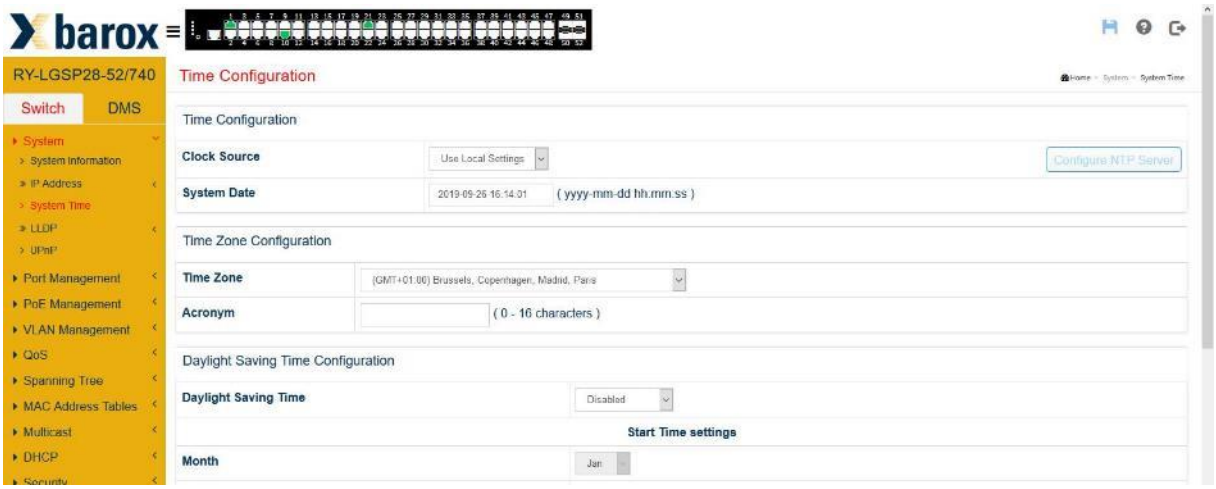
3.4 Uhrzeit einstellen

Die Systemuhrzeit der barox Switche kann manuell eingestellt oder mittels NTP-Server eingelesen 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.

3.4.1. Lokale Einstellungen

Im Menüpunkt „System/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 Schaltfläche „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.



3.4.2. NTP (Network Time Protocol)

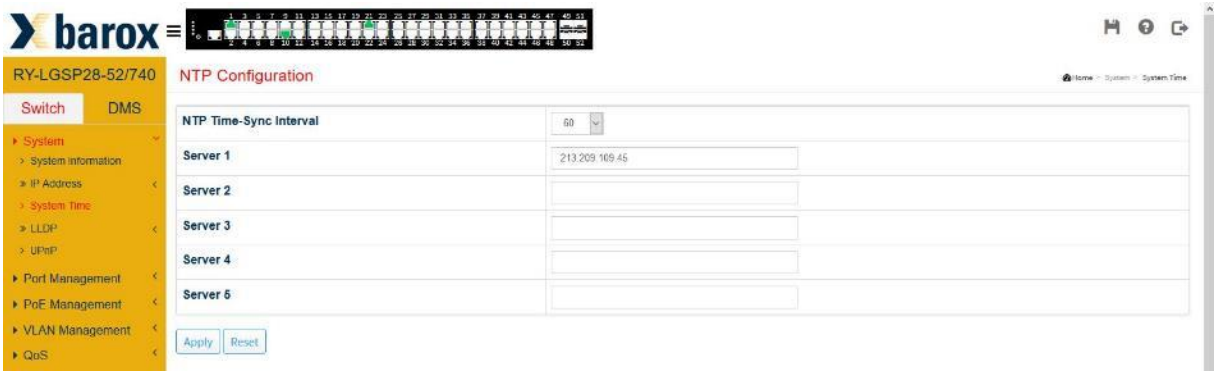
Das Network Time Protocol ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze.

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.

Die Konfiguration erfolgt in zwei Schritten.

Im ersten Schritt muss als Zeitquelle (Clock Source) „Use NTP Server“ gewählt werden. Somit wird das Icon rechts oben in der Maske „Configure NTP Server“ aktiv.

Mit einem Click auf dieses Symbol gelangt man zur Eingabemaske (2. Schritt).



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

Mit „NTP Time-Sync Interval“ wird definiert, in welchen Zeitabständen die Uhrzeit synchronisiert werden soll. Möglich sind 5, 10, 15, 30, 60 und 120 Minuten.

Falls im eigenen Netzwerk keine Zeitquelle zur Verfügung steht und eine externe Quelle 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/).

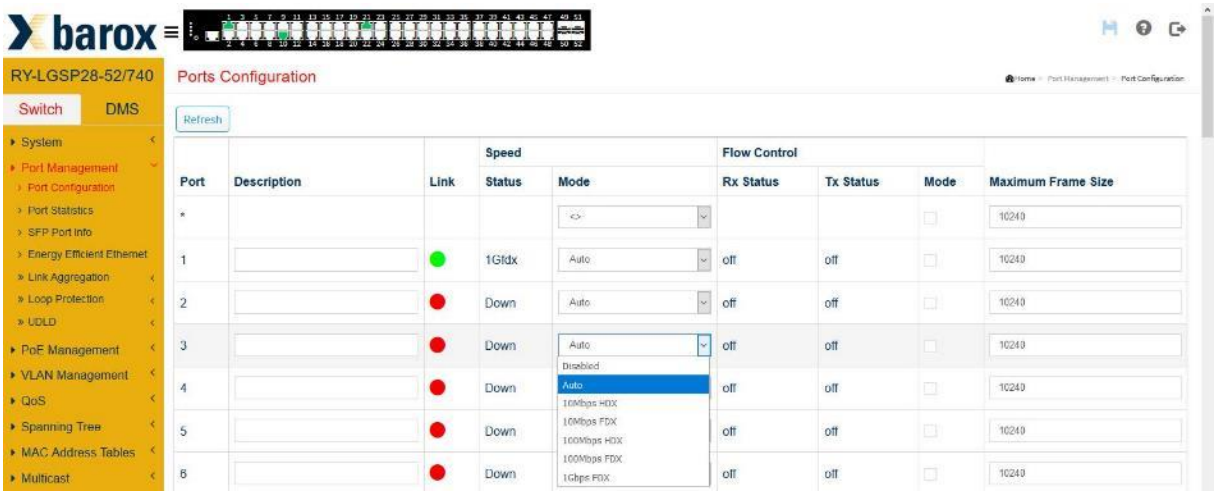
Sobald der Switch Uhrzeit und Datum beziehen kann, wird die korrekte Uhrzeit im Feld „System Date“ dargestellt.

3.5 Port-Konfiguration

Die Ports sind ab Werk auf 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 100 Mbit/s Interface vor. In diesen Fällen muss der Port manuell auf 100 Mbit/s eingestellt werden.

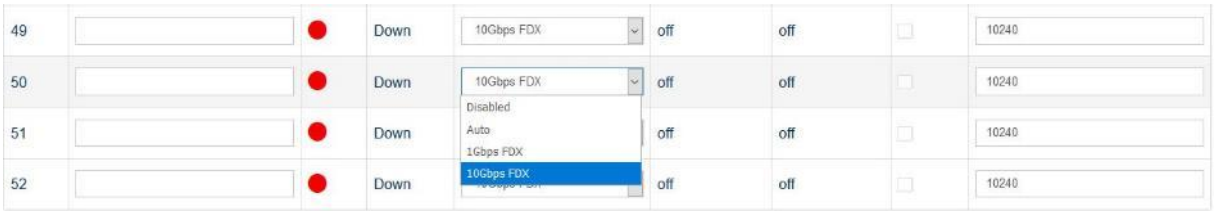
Soll ein Port aus Sicherheitsgründen nicht nutzbar sein, kann er auch ganz ausgeschaltet werden. Hierfür ist der Konfigurationsmodus auf „Disabled“ zu setzen.



3.5.1. 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 unterstützen nur Full-Duplex.

Es kann vorkommen, dass der Switch einen SFP-Transceiver nicht richtig erkennt (ob es eine 100M oder eine 1000M-Variante ist) und dieses 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.

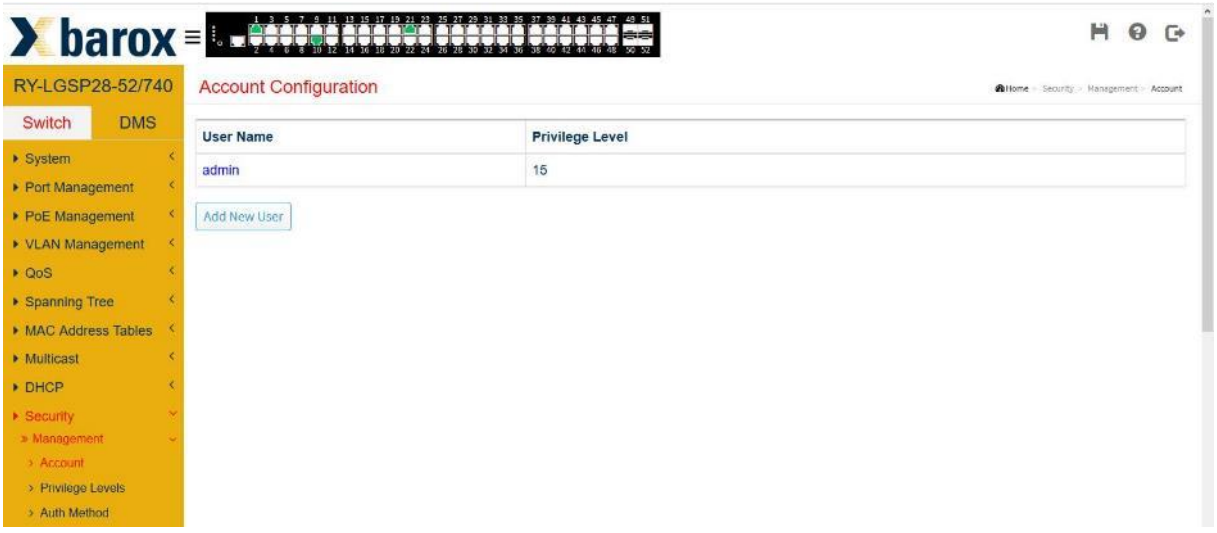
Das barox Sortiment umfasst SFPs für Multi- und Singlemode Fasern mit 100 Mbit/s, 1 Gbit/s oder 10 Gbit/s Übertragungsgeschwindigkeit. Die möglichen Distanzen variieren je nach Fasertyp und Übertragungsgeschwindigkeit zwischen 550 m und 120 km.

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

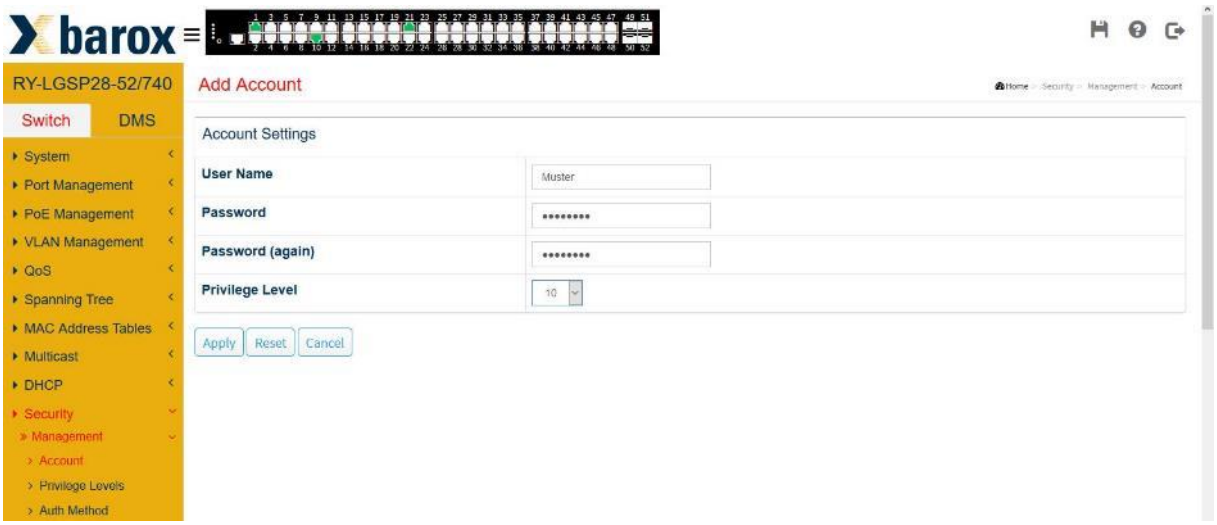
3.6 Benutzername und Passwort ändern

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.

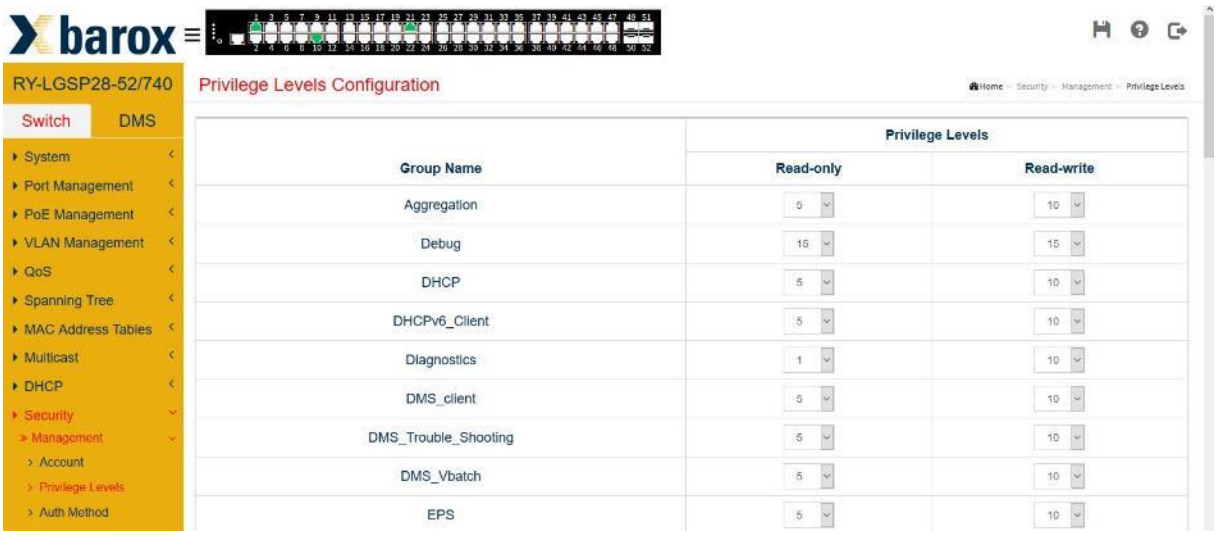


Mit „Add New User“ kann ein weiterer Benutzer generiert werden. Zu definieren sind der Name des Benutzers, das Passwort und das Berechtigungsniveau.



Im Menüpunkt „Privilege Levels“ kann nun die genaue Berechtigungsvielfalt des neuen Benutzers definiert werden.

Im nachfolgenden Beispiel hat der Benutzer „Muster“ 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 Benutzer definieren, der nur die MAC-Tabelle lesen darf.

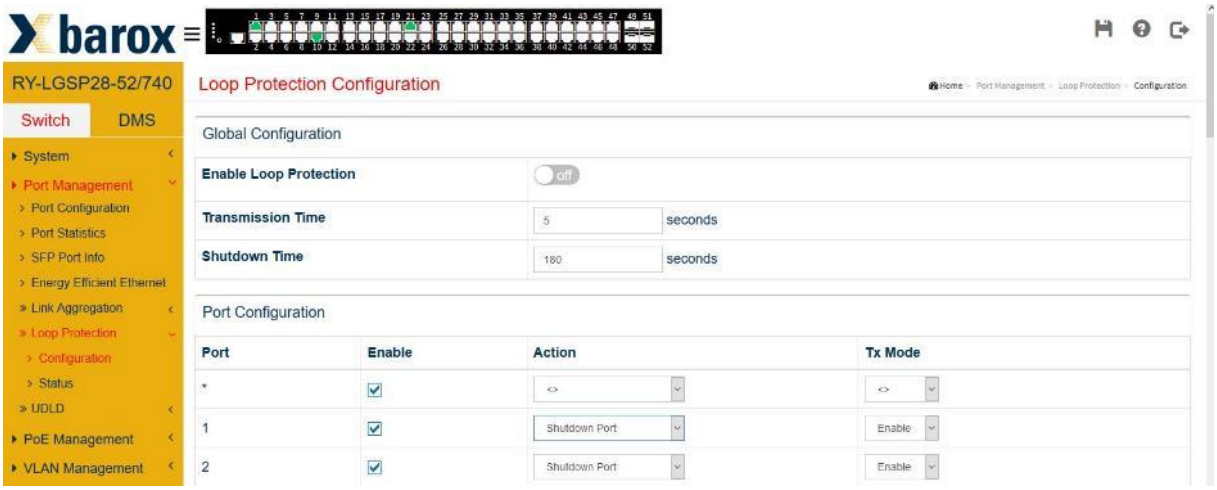
3.7 Loop Protection

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

In einer solchen Situation wird das Leistungsmerkmal „Loop Protection“ benötigt. Ist dieses 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 ein Loop detektiert wird. Mögliche Zeiteingabe: 0 – 604800 s (7 Tage). Bei Eingabe von „0“ bleibt der Port bis zu einem Neustart des Switches deaktiviert.



3.8 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.

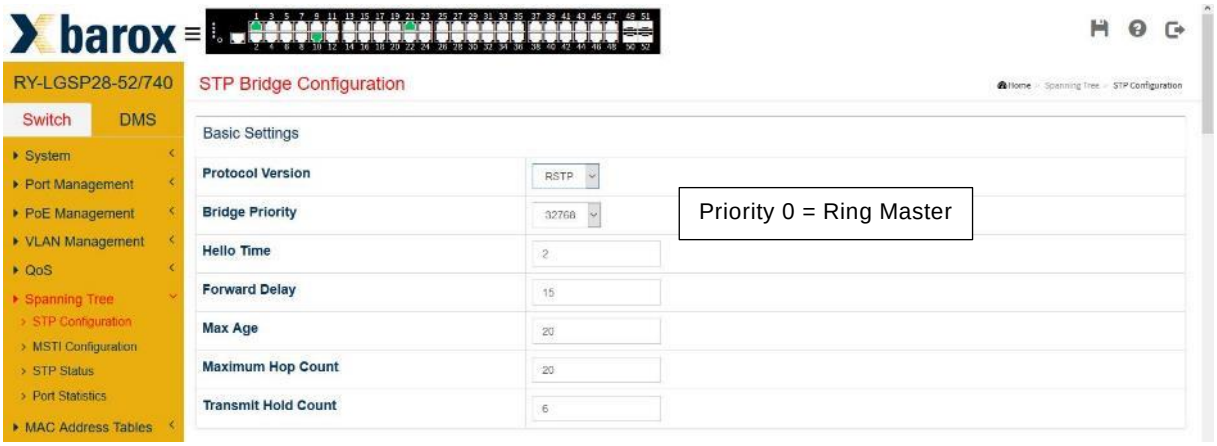
RSTP (Rapid Spanning Tree Protocol) ist eines der grundlegenden Protokolle in Ethernet-Netzwerken. Es sorgt dafür, dass in einem Netzwerksegment keine Netzwerkschleifen entstehen. Ethernet-Frames haben im Gegensatz zu IP-Paketen keine maximale Lebensdauer (Time to Live, TTL) und bewegen sich deshalb 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

3.8.1. Ring-Master

In einer Ring-Topologie muss ein Switch als Master, der die Ringüberwachung übernimmt, definiert werden. Bei einer möglichen Verbindungsunterbrechung 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 definierten Ring-Master der Switch mit der kleinsten MAC-Adresse automatisch Ring-Master wird.

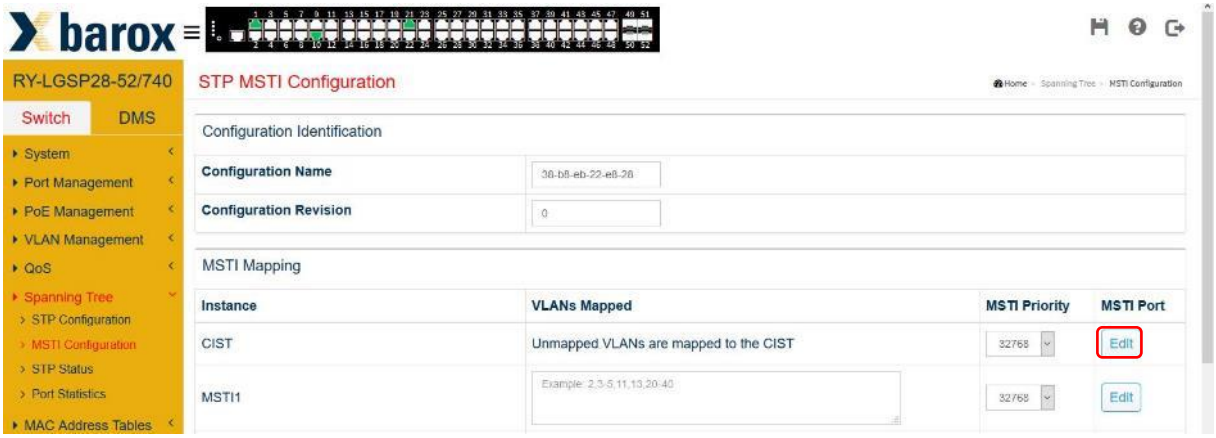


Im Menüpunkt „Spanning Tree / STP Configuration“ muss die gewünschte Protokollversion gewählt werden. RSTP wird von allen Switch-Herstellern unterstützt und ist somit kompatibel zu Dritt-Herstellern.

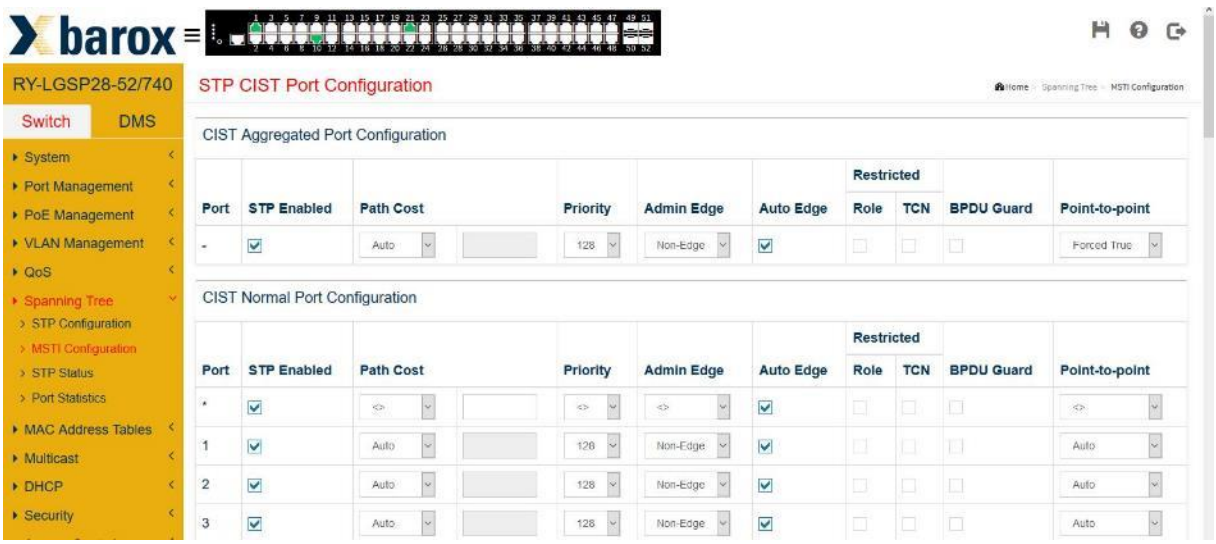
Per Default haben die Switche die „Bridge Priority“ 32768. Soll der Switch als Master fungieren, muss die Bridge Priority auf „0“ gesetzt werden. Alle anderen Werte können so belassen werden wie sie sind.

3.8.2. Port-Konfiguration

Zur Definition der Ports, welche im Ring eingebunden sind, ist im Menü „MSTI Configuration“ der Menüpunkt „CIST“ zu editieren.

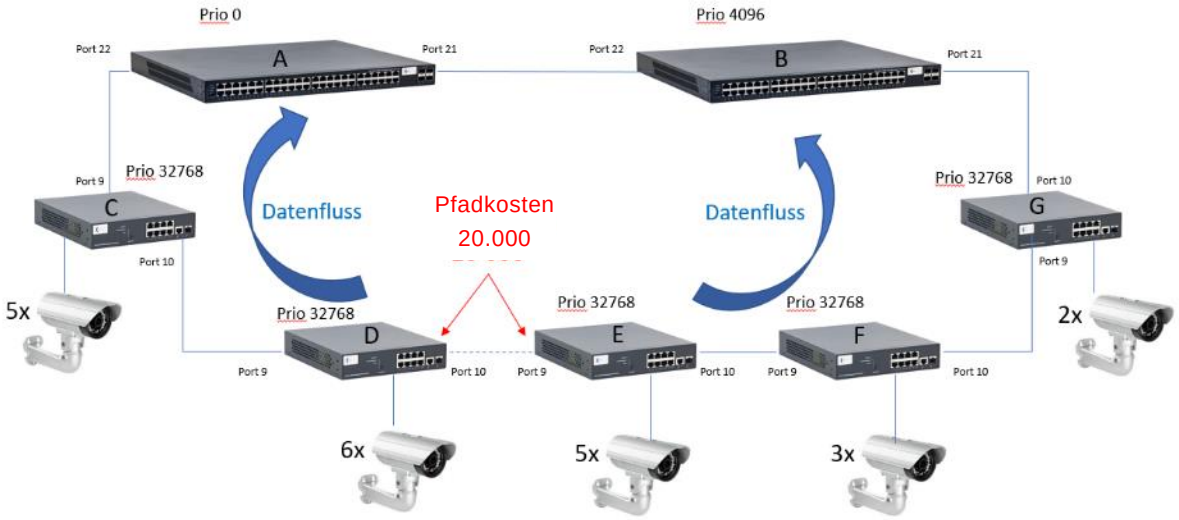


Ab Werk ist bei allen Ports „STP Enabled“ aktiv. Somit kann der Ring theoretisch an einem beliebigen Port gebildet werden. Zur optimalen Lastverteilung im Netzwerk kann der Datenpaketfluss per Definition mittels Pfadkosten gelenkt werden. Der Begriff „Pfadkosten“ stammt aus der Zeit, als Mietleitungen 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 5 Mbit/s Videodaten liefern. Insgesamt also über 100 Mbit/s Daten.

<u>Szenario 1:</u> 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 einer Unterbrechung kann die Umschaltzeit etwas länger dauern, da der kleine Switch die Daten nicht so schnell verarbeiten kann.

<u>Szenario 2:</u> 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. Bei einem Ausfall 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.

<u>Szenario 3:</u> 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 höher sind als bei allen anderen Ports im Ring, wird diese Strecke nur bei einer Unterbrechung im Netzwerk aktiv geschaltet.

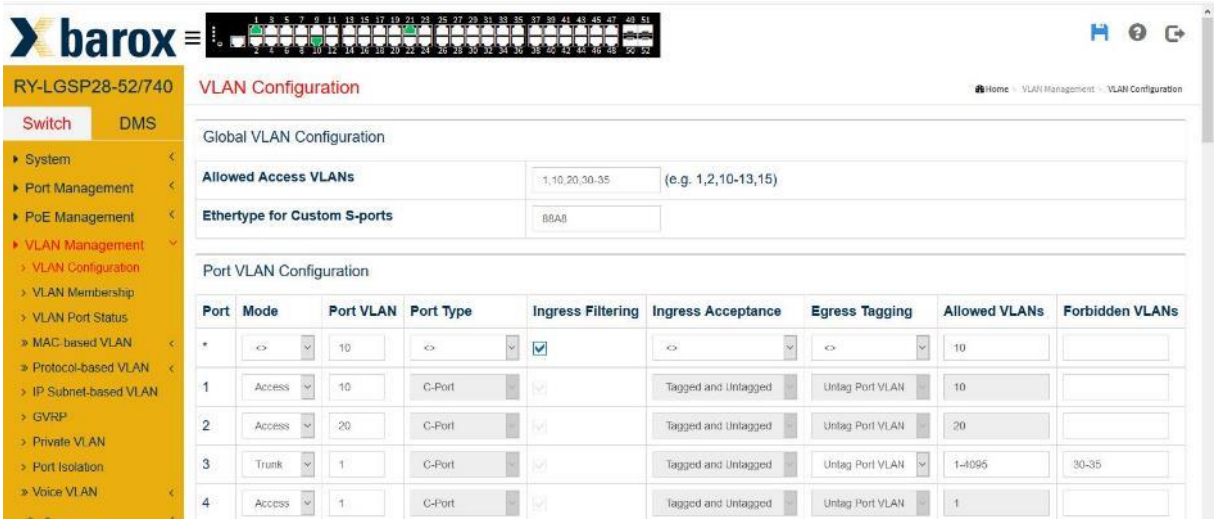
Pfadkosten Werkeinstellung:

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 1 Gbit/s-Uplink zum gleichen Ziel, der 100 Mbit/s Link würde daher als redundanter Pfad geblockt werden. Die Pfadkosten sind nach IEEE-Vorgaben genormt. Sie können jedoch manuell abweichend festgelegt werden, beispielsweise, um bei gleicher Geschwindigkeit einen bevorzugten Uplink auszuwählen, um so die realen Kosten von Standleitungen widerzuspiegeln.

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

3.9 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.

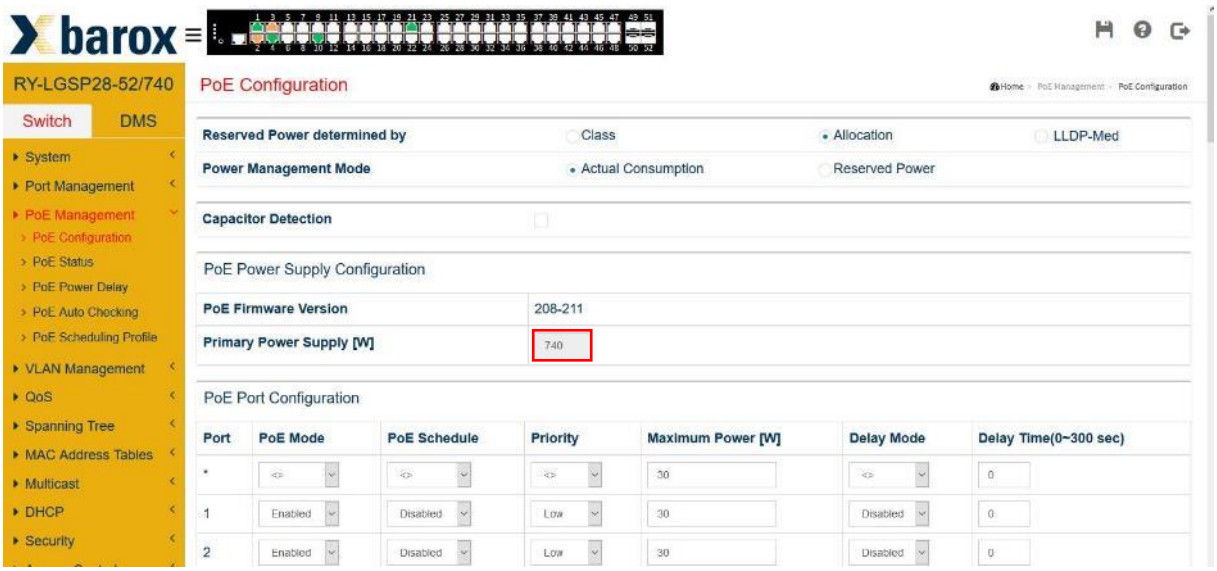
Modus	VLAN	Funktion
Access	Nr	an diesem Port wird ein Endgerät angeschlossen.
Trunk	---	Verbindung zwischen zwei Switchen
Hybrid	---	Verbindung zwischen zwei Switchen oder zu einem Endgerät

Sowohl im Trunk- als auch im Hybridmodus kann in der Spalte „Allowed VLANs“ definiert werden, welche VLANs erlaubt sind und in der Spalte „Forbidden VLANs“, welche VLAN nicht erlaubt sind.

3.10 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.

3.10.1. 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 diesem Beispiel, einem RY-LGSP28-52 Switch mit 24 PoE+-Ports, stehen max. 740 W zur Verfügung. Das bedeutet, dass es unmöglich ist, an allen 48 Ports jeweils ein 30 W Endgerät anzuschließen, da dafür 1.440 W 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. Leistungs-bereitstellung 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 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.

3.10.2. PoE Power-Delay

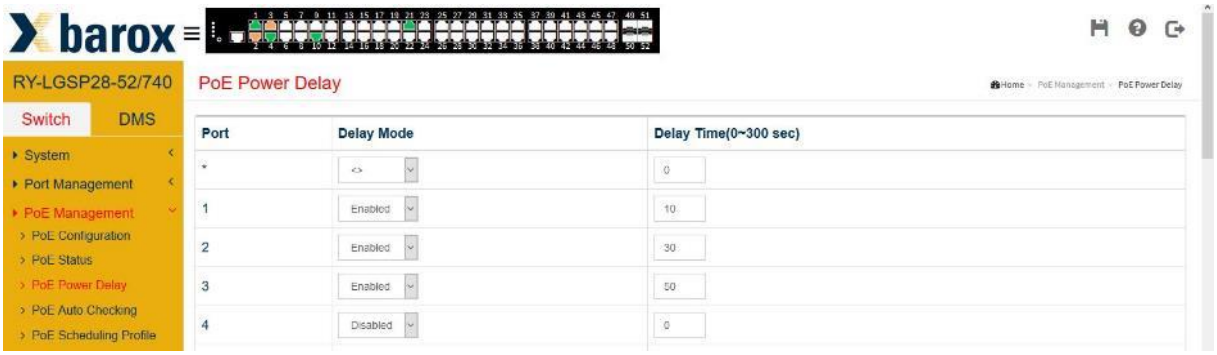
Wie bereits erwähnt kann der Switch eine begrenzte Leistung zur Verfügung stellen.

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 oder Zuschaltung von Heizungen oder IR-Strahlern usw. benötigen Kameras wesentlich mehr Strom (= Leistungsspitzen) 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 Switch-Leistung überschritten wird. Die Leistungsüberschreitung führt dazu, dass sich der Switch sofort wieder abmeldet und das Netzteil bei häufigen Fehlversuchen Schaden nimmt.

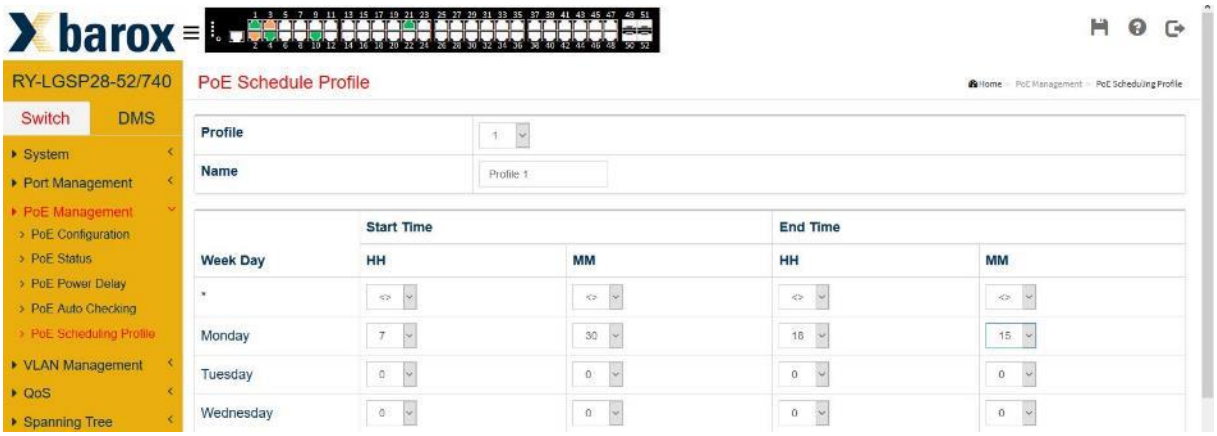
Um diese Problematik zu umgehen, kann im folgenden Menü ein zeitversetzter Start jedes einzelnen Ports konfiguriert werden. Im nachfolgenden Beispiel wird Port 1 nach 10 Sekunden aktiviert und die Ports 2 und 3 in Abständen von 20 Sekunden.



3.10.3. 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 nachfolgenden Beispiel wird die Kamera respektive Strom am PoE-Port im Profil 1 nur am Montag zwischen 07:30 Uhr und 18:15 Uhr eingeschaltet.

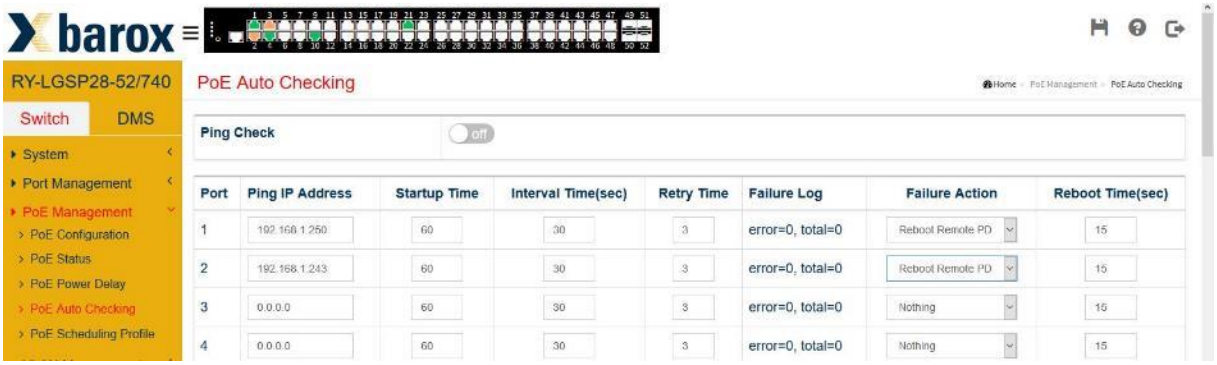


3.10.4. PoE Auto-Checking

„PoE Auto Checking“ dient der Funktionsüberwachung. Mittels Ping wird zum Beispiel alle 30 Sekunden die am Port 1 angeschlossene Kamera mit der IP-Adresse 192.168.1.250 auf deren Erreichbarkeit hin geprüft.

Nach 3 fehlerhaften Versuchen wird PoE am Port 1 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.

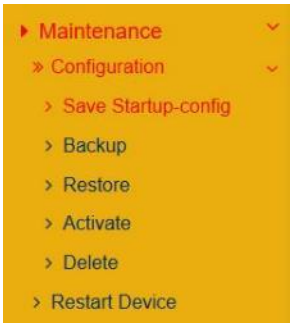


3.11 Speichern und Laden der Konfiguration

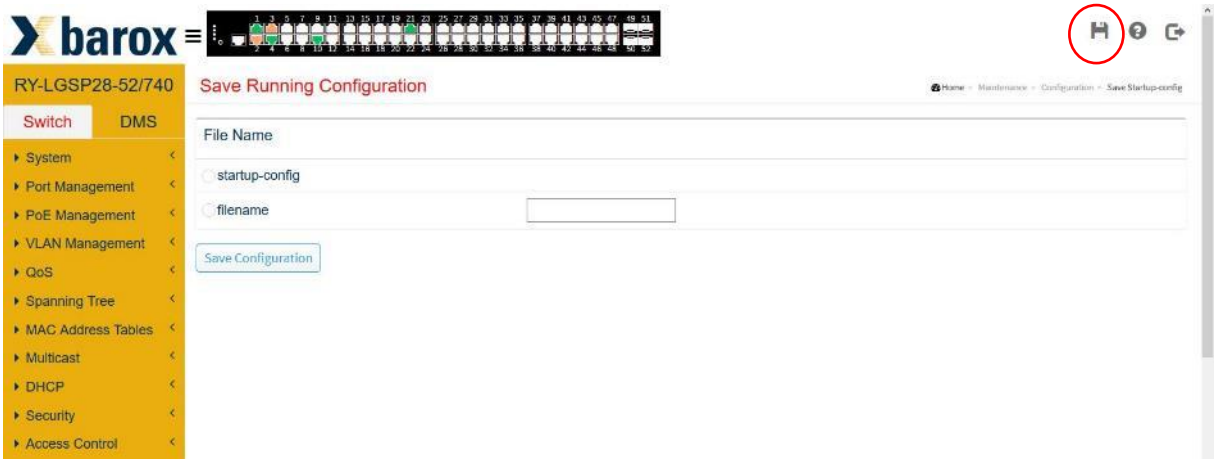
Jede Änderung muss gespeichert werden. Durch „Apply“ wird die Änderung in den Arbeitsspeicher geschrieben. Bei einem Neustart leert sich der Arbeitsspeicher und die Änderungen gehen alle verloren. Die Änderungen müssen daher definitiv gespeichert werden.

Es gibt zwei Möglichkeiten:

- Im Menü „Maintenance/Configuration/Save startup-config“



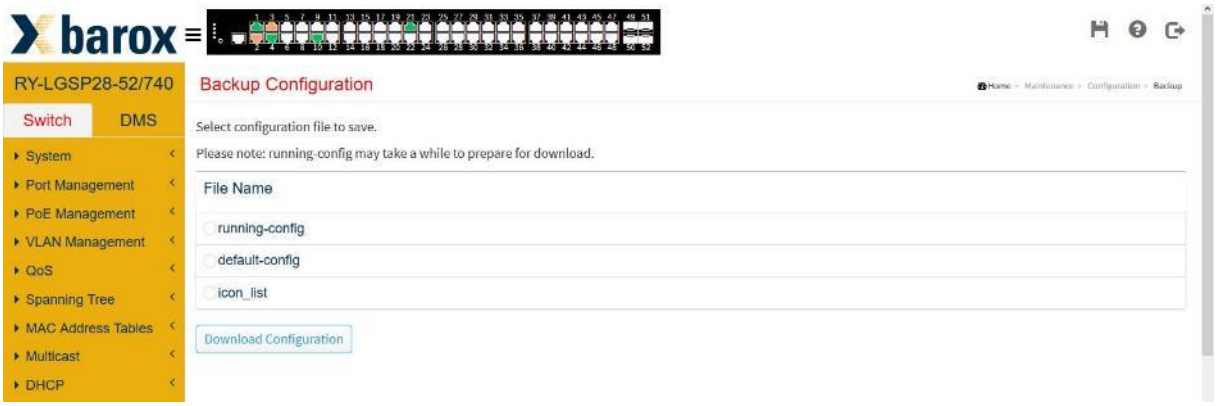
- Diskettensymbol in jeder Maske



3.11.1. Download der Konfiguration

Die aktuelle Switch-Konfiguration kann heruntergeladen und separat gespeichert werden. Die generierte Konfigurationsdatei kann bei einem Austausch des Switches eingespielt oder verwendet werden, wenn mehrere Switche identisch konfiguriert werden müssen und sich nur die IP-Adresse ändert.

Das erspart viel Zeit. Wir empfehlen ausdrücklich, das „startup-config File“ zu speichern.



3.11.2. Einspielen der Konfiguration (Upload)

Die umgekehrte Variante ist das Einspielen einer Konfigurationsdatei in den Switch. Hierfür wird der Pfad der hinterlegten Datei angegeben und als „running-config“ abgelegt. Funktioniert alles wunschgemäß, muss die Datei wie oben beschrieben danach als „startup-config –File“ gespeichert werden.

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 „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. ein Service-Laptop, 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.

Das DMS kann bei sehr hoher Netzwerklast bei den am niedrigsten frequentierten Switch 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.

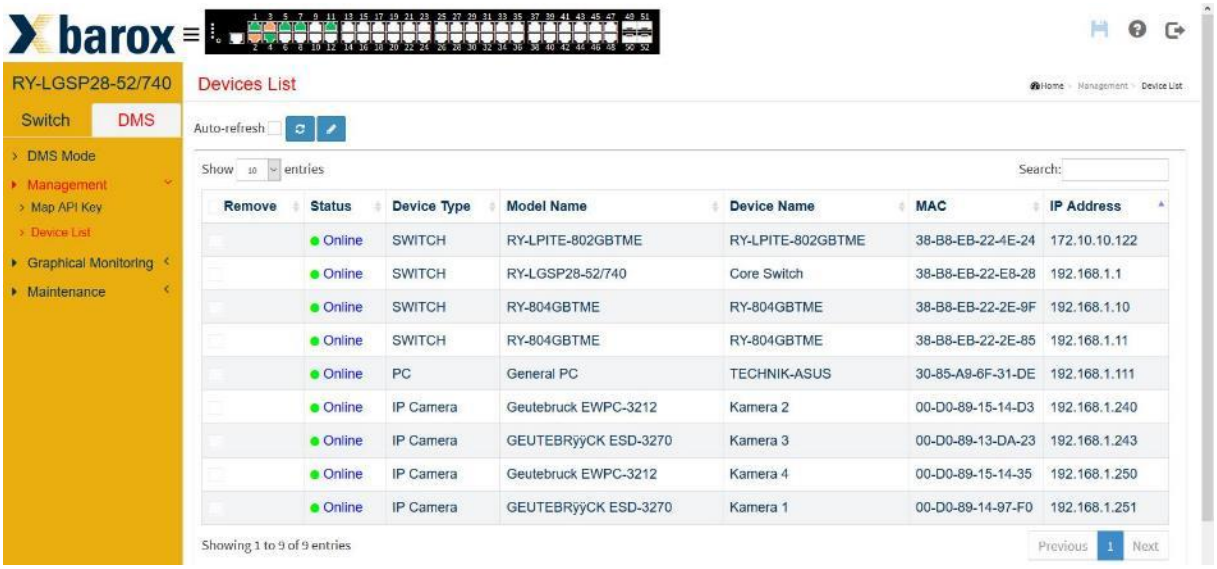
In der Zeile „Controller IP“ wird mittels IP-Adresse angezeigt, welcher Switch der Master ist.

Geräteliste (Devices List)

Auf dieser Seite werden alle Geräte aufgeführt, die im Netz on- oder offline sind. In tabellarischer Form wird der Gerätetyp, der Status, der Gerätename sowie MAC- und IP-Adresse aufgelistet.

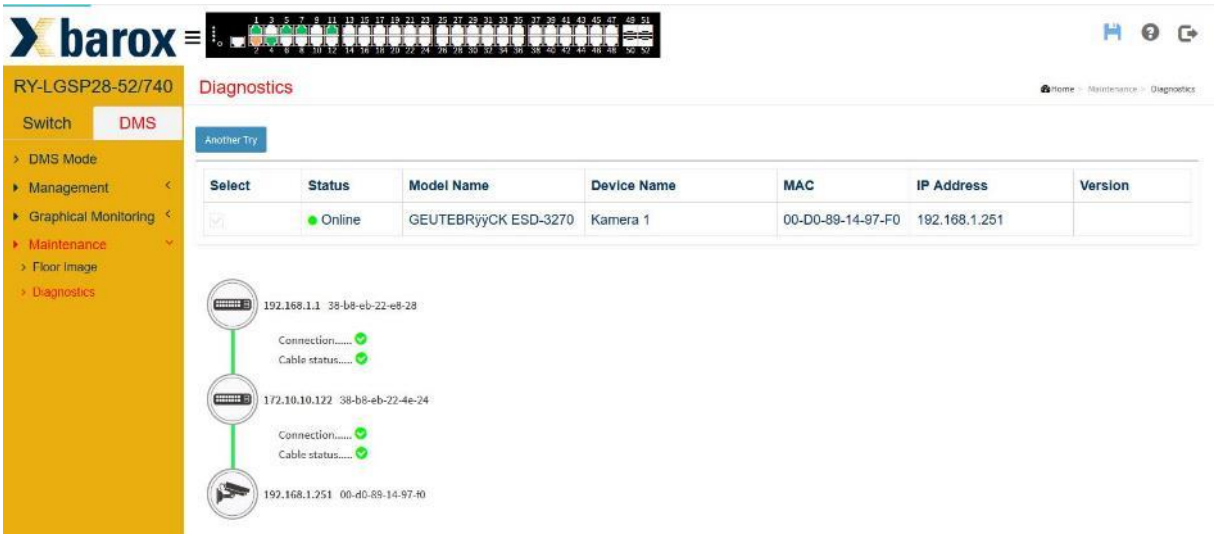
Es werden sämtliche Geräte − auch die, deren IP-Adresse in einem anderen Netz-Segment angesiedelt ist − aufgeführt.

Diese nützliche Funktion hilft, wenn bspw. ein nicht konfiguriertes Gerät in das 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. Eventuelle Unterbrechungen in der Verbindungskette sind erkennbar.

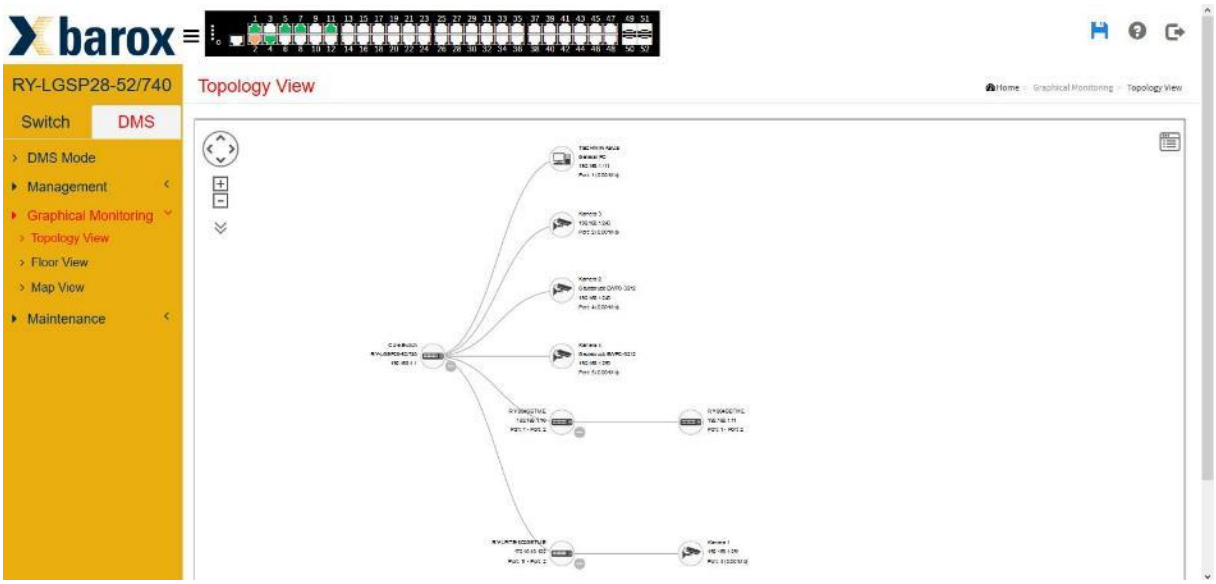
Die gleiche Überprüfung kann auch im Menü „Maintenance/Diagnostics“ ausgeführt werden.



4.2 Grafische Überwachung

Topologiesicht (Topology View)

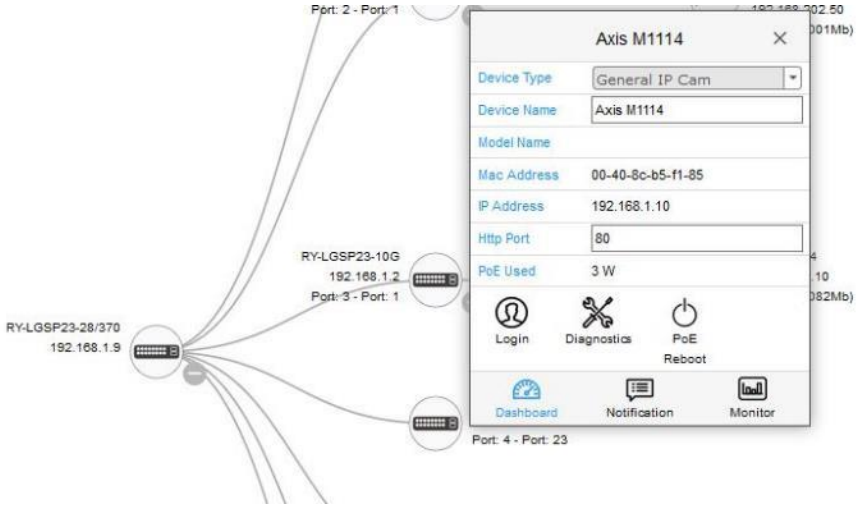
In der Topologiesicht (Topology View) wird das Netzwerk inkl. aller angeschlossenen IP-Endgeräte automatisch grafisch dargestellt. Wird das Endgerät richtig erkannt, wird das entsprechende Symbol (Kamera, Switch, Access Point etc.) dargestellt. Sämtliche Informationen, wie Gerätename, IP-Adresse, Datenrate 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 Gerätetyp und -Name definiert und MAC- und IP-Adressen sowie der in Echtzeit dargestellte PoE-Bedarf abgelesen werden, sofern es sich um einen PoE-Verbraucher handelt.

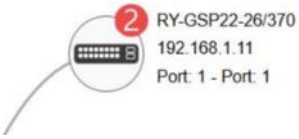
Zudem kann mittels „Login“ direkt auf das Gerät zugegriffen oder eine Verbindungsdiagnose ausgeführt werden. Mit Klick auf die „PoE Reboot“-Schaltfläche ist ein Neustart des PoE-Verbrauchers problemlos möglich.



War ein Gerät

- kurzzeitig nicht erreichbar (Kabelfehler, Ausstecken 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 Menü „Notification“ können die Meldungen gelesen und editiert werden.



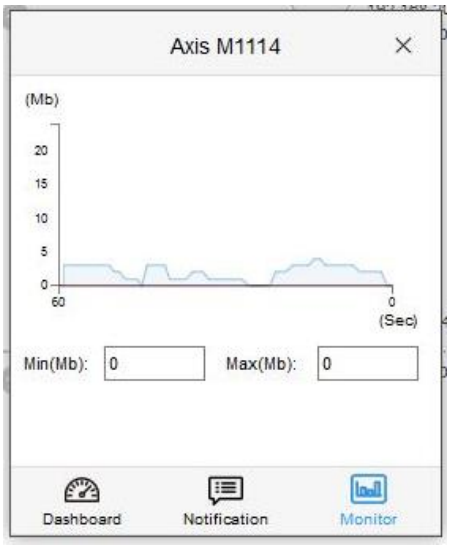
Ist ein Gerät im Netzwerk nicht mehr vorhanden, wird es in der Topologiesicht rot dargestellt und im „Dashboard“ das „Remove“-Symbol zur Verfügung gestellt. Mit einem Klick auf „Remove“ wird das Gerät aus der Topologiesicht endgültig entfernt.

„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 Kombination von IP- und MAC-Adresse 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“.

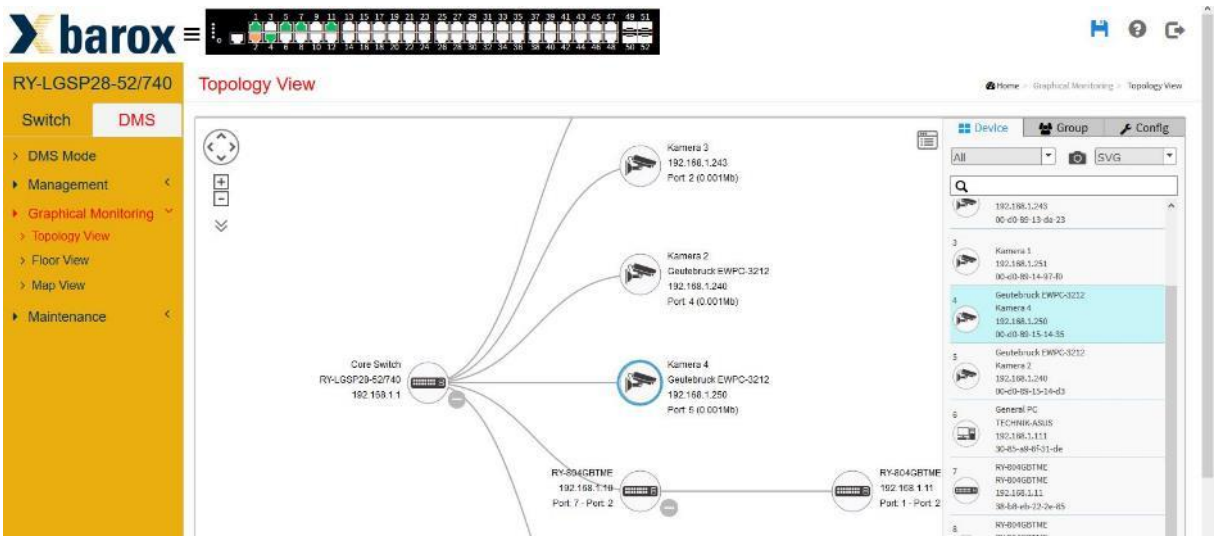
Hier wird der Datenfluss (z. B. von einer Kamera) in Echtzeit angezeigt.

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 alles in Ordnung ist.



Oben rechts in der Topologiesicht befindet sich ein Symbol, mit dem alle Geräte aufgelistet werden.

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



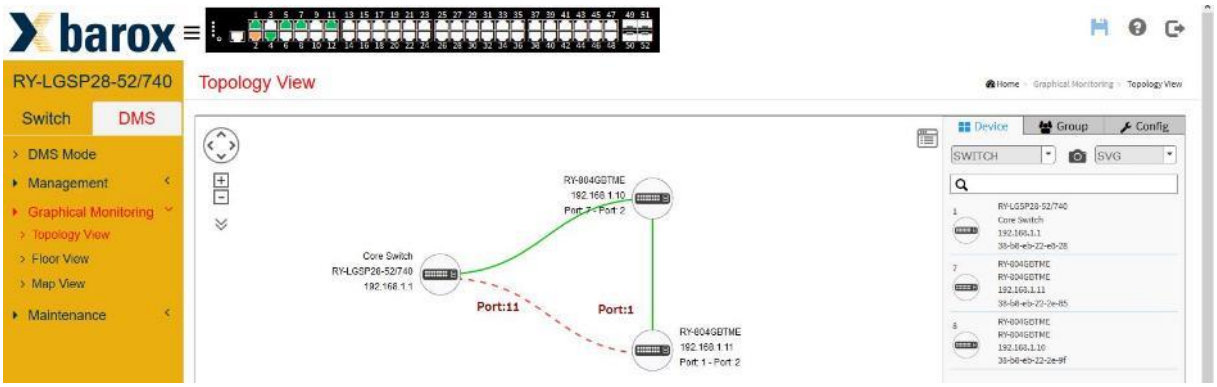
Das Tool bietet auch die Möglichkeit, den Netzwerkplan im Format SVG, PNG oder als PDF direkt aus der Topologiesicht auszudrucken. Hierfür muss das Format gewählt und danach das Kamerasymbol angeklickt werden.

Die Topologiesicht bietet auch die Möglichkeit, die Ringkonstellation darzustellen. Hierfür muss im Register „Device“ die Auflistung „Switche“ gewählt werden. Es wird sodann der Ring dargestellt. Eine rot gestrichelte zeigt an, 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-Switchen, die DMS unterstützen



Lageplan (Floor View)

Im Lageplan (Floor View) können hochgeladene bzw. importierte Gebäude-, Stockwerk- und/oder Umgebungspläne betrachtet werden. Diese dienen als Grundlage bzw. Hintergrundbild, um das Netzwerk abzubilden. Diese Funktion bietet eine gute Orientierungshilfe bei Vor-Ort-Einsätzen und kann wie zuvor beschrieben auch als Dokumentation ausgedruckt werden.

Zum Eintrag der Kamera oder des Switches im Plan ist nur das entsprechende Gerät in der Liste per Mausklick anzuwählen und im Plan zu platzieren, fertig.

Kartensicht (Map View)

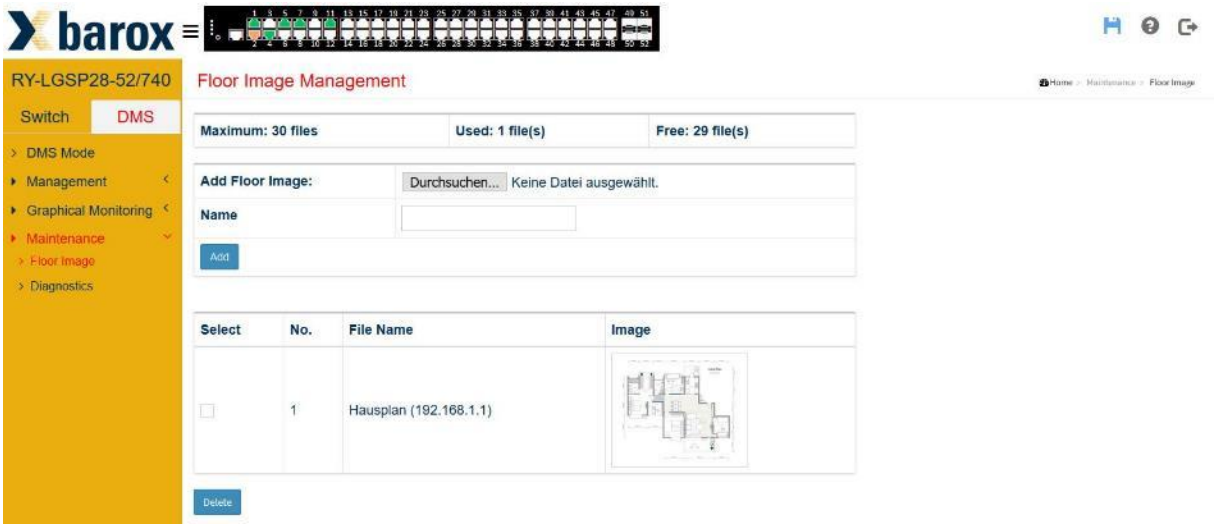
Die gleiche Funktion ist mit der Kartensicht (Map View) möglich. Hier wird gleich mittels Google Maps das Hintergrundbild generiert. Dies erfordert jedoch eine Internetverbindung und Google-Lizenzen, um den Dienst nutzen zu können.

4.3 Wartung (Maintenance)

Um einen Plan als Hintergrundbild zu nutzen, muss in das Menü „Maintenance“ gewechselt werden.

Im Menü „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 30 Dateien gespeichert werden.



Diagnose (Diagnostic)

Diese Funktion wurde auf der Seite 22 beim Thema „Device List“ beschrieben und erklärt.

5 Switch Management im Fokus der Security

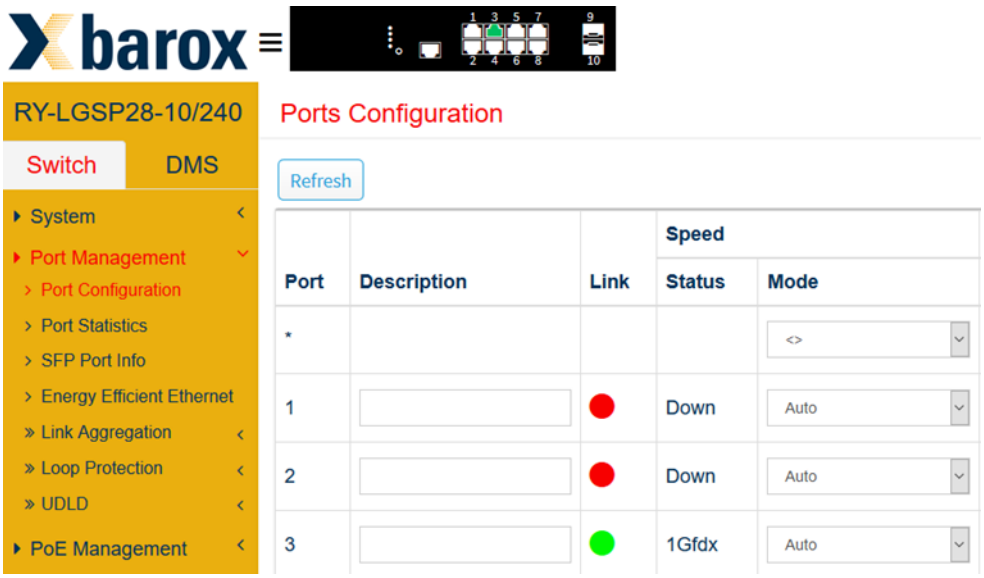
Folgende Themen sollen Aufschluss über Inhalte und Konfiguration der erweiterten Netzwerk-einstellungen und der Absicherung geben. Grundvoraussetzungen zur Konfiguration sind die Kenntnisse und Fertigkeiten der Themen aus Inbetriebnahme wie IP-Konfiguration, Login und VLAN-Konfiguration.

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

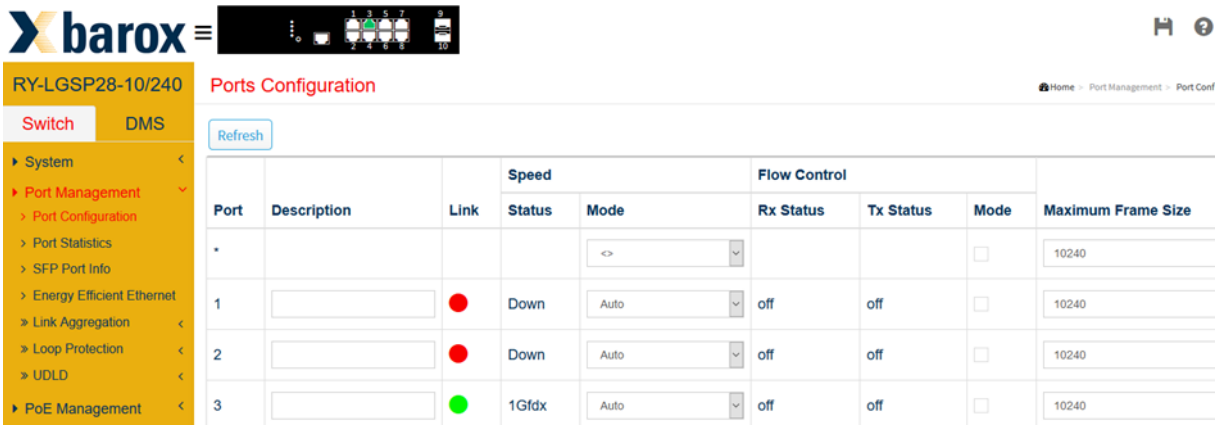
5.1.1. Bandbreiten-Einstellungen und Beschränkungen

Port-basierte Ethernet-Einstellung

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 bestimmter Einsatzbedingungen eine Herabstufung des ETH-Standards benötigen. Nachfolgend kann die Einstellung 10/100/1000/10000 FDX/HDX (ETH-Standard Modell-abhängig) selektiv je Port über das Web GUI angepasst werden.



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



! Wichtig, bei der Einstellung der Framegröße 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 dem 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 Leistung der Backplane des Switchmodells -> 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 Bezug auf VLAN und Port benötigen. Zudem kann mit der manuellen Zuweisung eine grundlegende Absicherung, bzw. Zugangsbeschränkung skaliert werden.

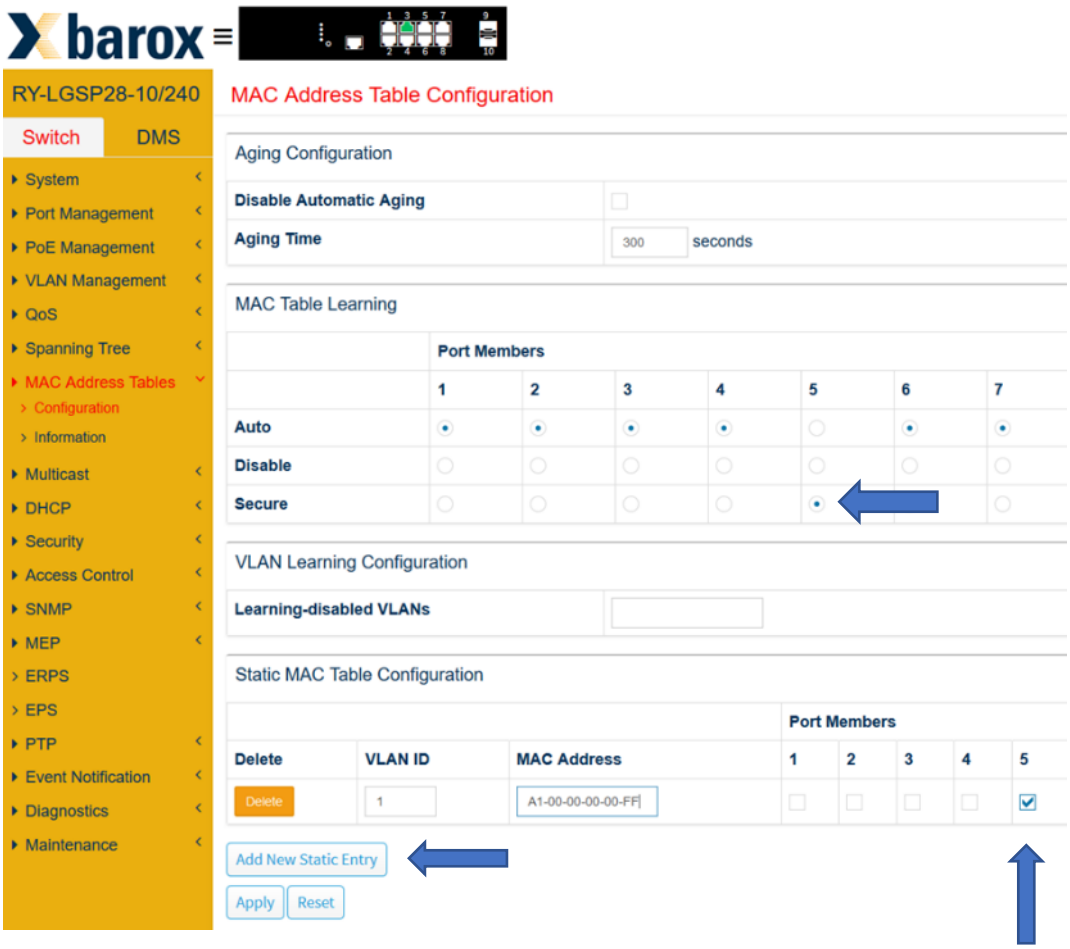
MAC-Filterung und Portkonfiguration

Beispiel der Konfiguration einer statischen MAC-Tabelle:

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 Menü „Switch -> Configuration -> MAC Table”
2. Eingabe der VLAN ID, MAC-Adresse 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“.

Portabsicherung mit ACL beginnend im Layer 2

Regelbasierte Absicherung von Ports mit MAC-Adressüberprüfung per ACL

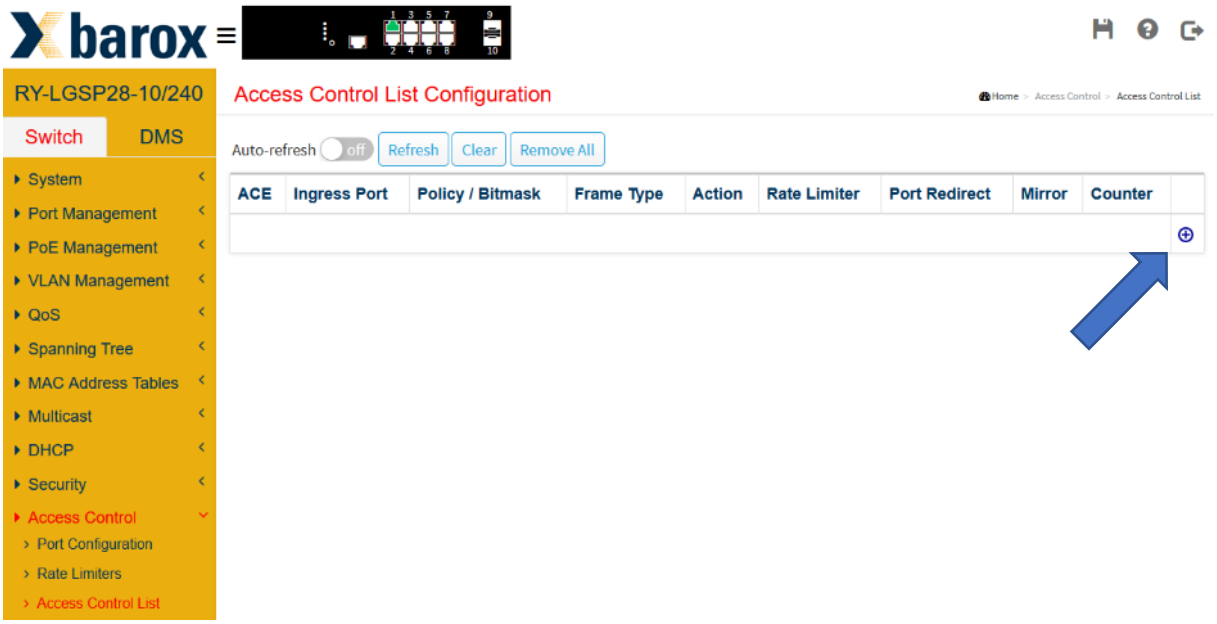
Vorbetrachtung:

Am Beispiel wird die Absicherung eines Ports mit einer physikalischen Ethernet-Adresse am barox Switch beschrieben.

Die ACL-Funktion ist ähnlich einer Netzwerkfirewall, welche Regeln bzw. Bedingungen in einer Abfolge überprüft und je nach Eintreffen der Bedingung die Regel und die damit verbundenen Aktionen auslöst. Am konkreten Beispiel ist dies die Überprüfung, ob an einem bestimmten Port des Switches eine bestimmte MAC-Adresse bzw. Endgerät angeschlossen ist. Sollte dies nicht übereinstimmen, so soll der Port administrativ und physisch abgeschaltet werden (Shutdown). Darüber hinaus können mit ACL auch die höheren Netzwerkschichten, mit Regeln für TCP/ IP bis hin zur Datenflusskontrolle, realisiert werden.

Konfiguration:

Das Anlegen von ACLs/ACEs erfolgen im Menü unter „*Access Control* > *Access Control List*“. Eine neue Regel wird durch Klick auf das „+“-Symbol wie nachfolgend abgebildet erzeugt.

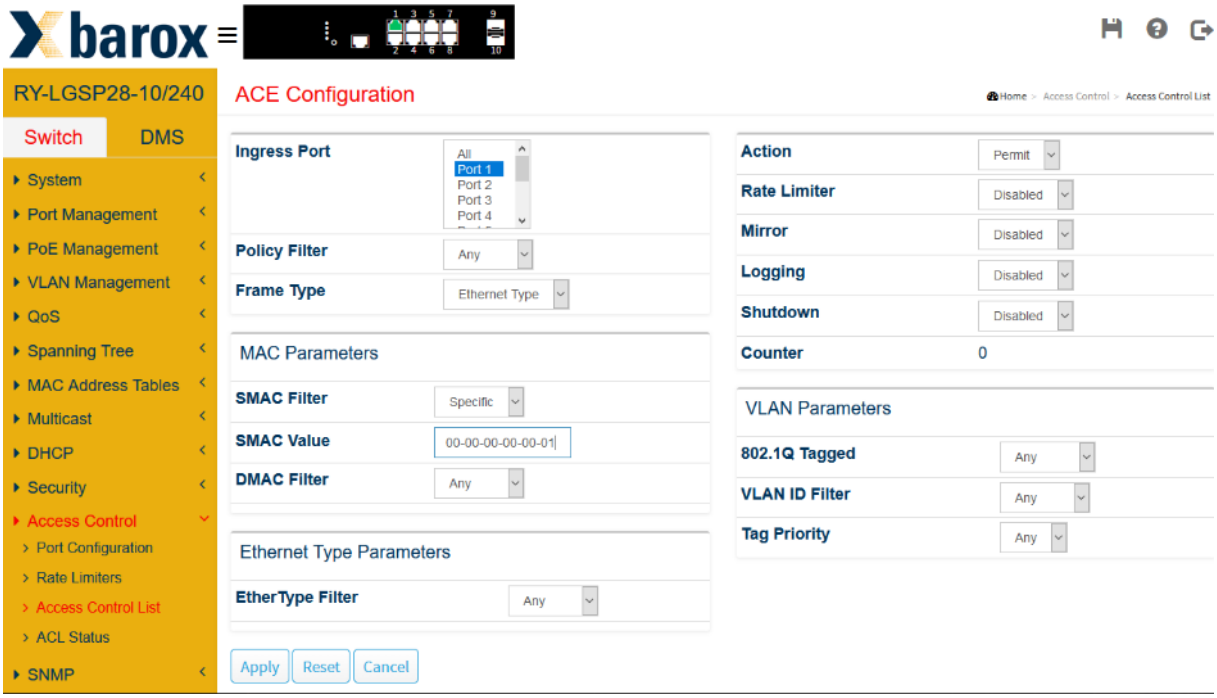


Für das Beispiel wird für Port 1 erlaubt eine spezifische MAC-Adressregel erzeugt.

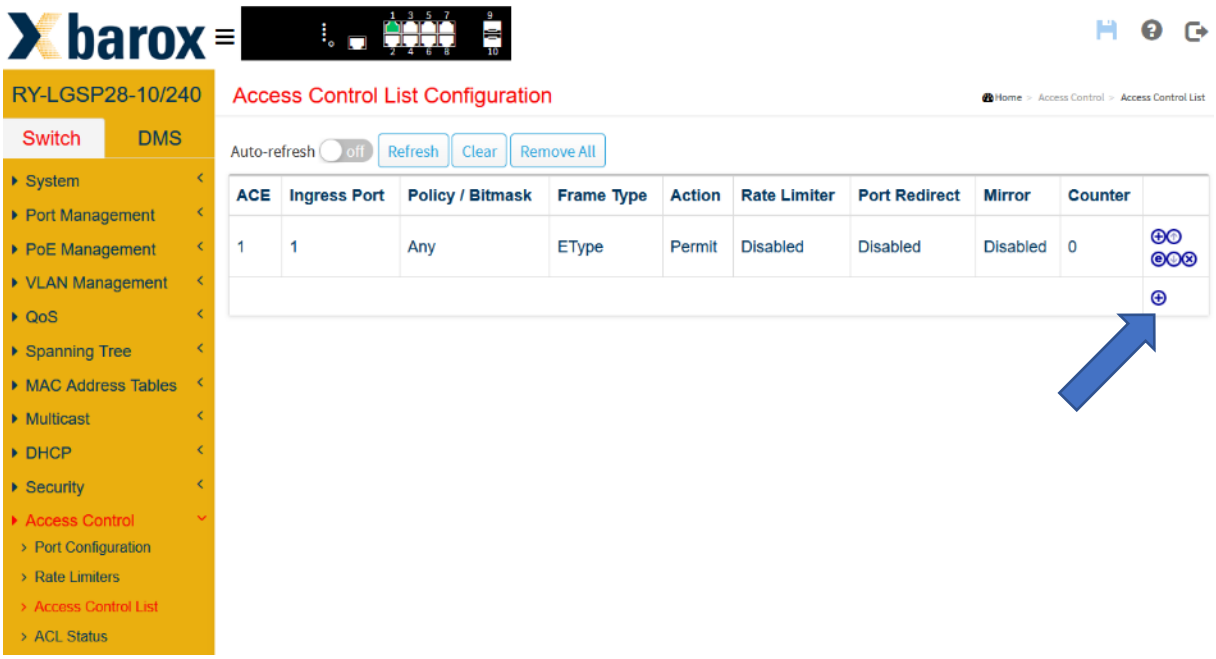
Einstellungen:

Ingress Port: Port 1
Policy Filter: Any
Frame Type: Ethernet-Typ
SMAC Filter: Specific
SMAC Value: „MAC-Adresse des Endgeräts“
DMAC Filter: Any
Ether Type Filter: Any
Action: Permit

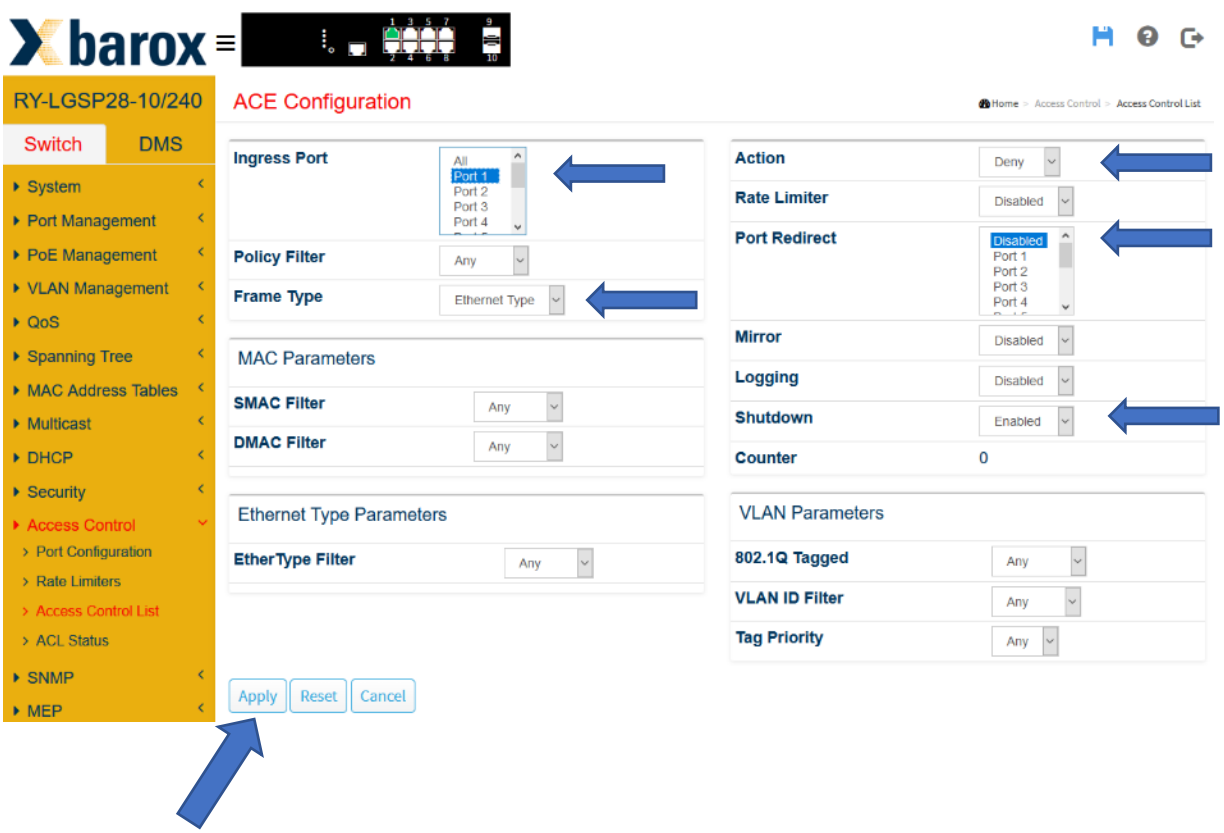
Weitere Einstellungen können der nachfolgenden Abbildung entnommen werden. Nach Setzen der Parameter werden diese mit einem Klick auf „Apply“ bestätigt.



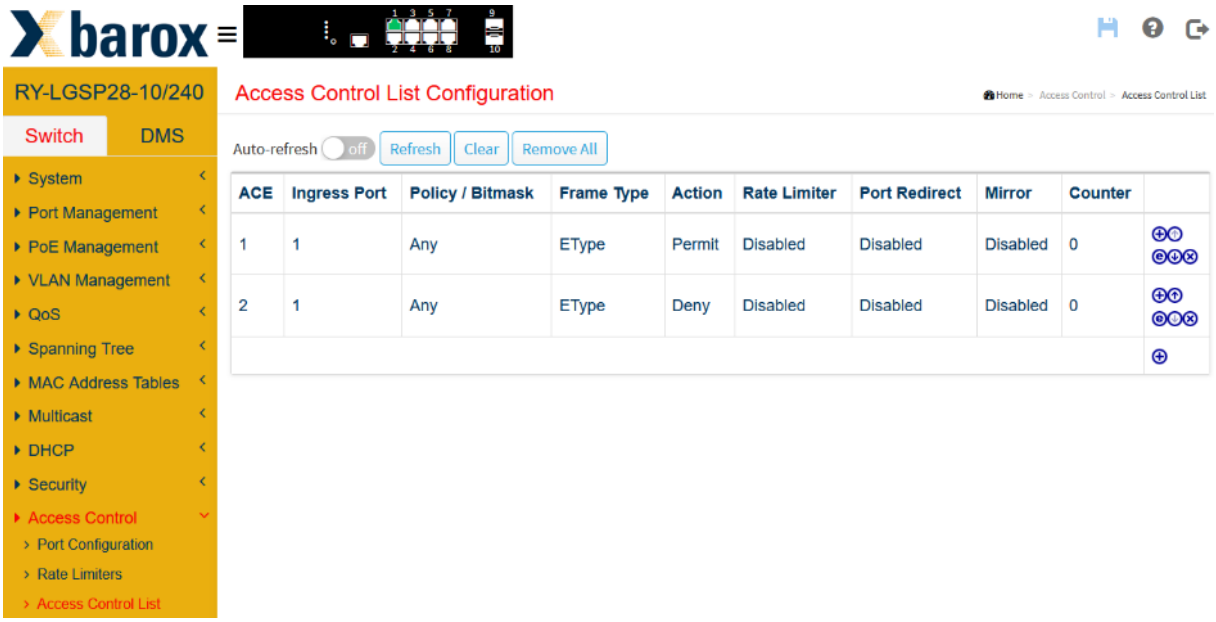
Nach Anlegen der ersten Regel wird eine zweite Regel benötigt. Diese wird durch Klick auf „+“ hinzugefügt.



Nachfolgende Regel steuert, dass keine weitere MAC-Adresse am Port 1 erlaubt ist. Sinngemäß wird jede weitere MAC-Adresse abgelehnt. Die Einstellungen können wie nachfolgend abgebildet übernommen werden.

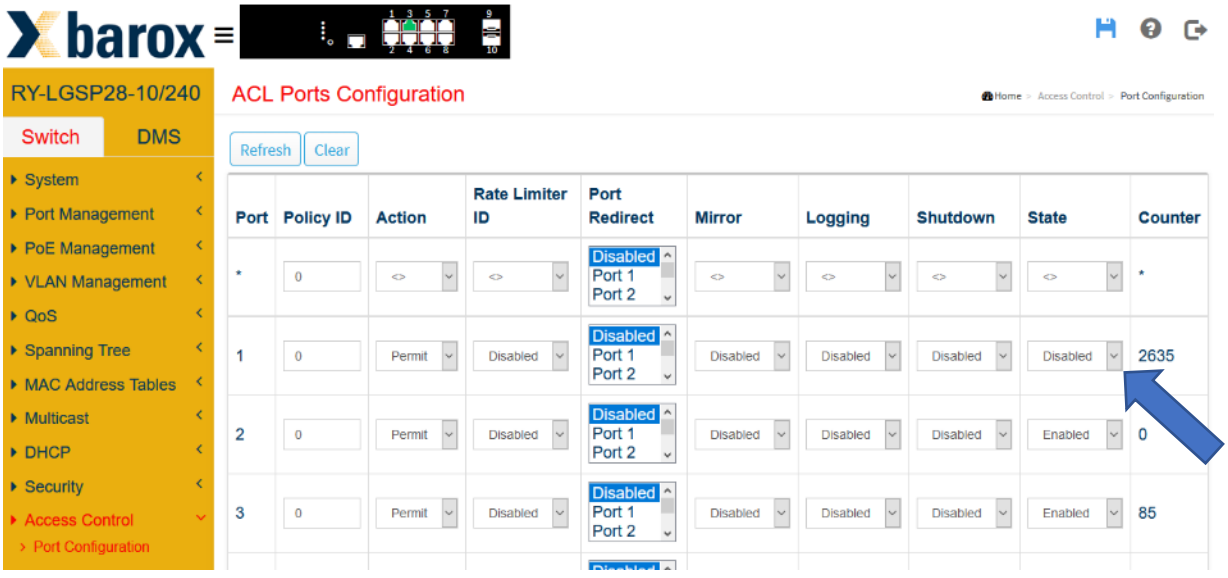


Nach Abschluss der Konfiguration sollten die Regeln wie folgt aufgezeigt sein.



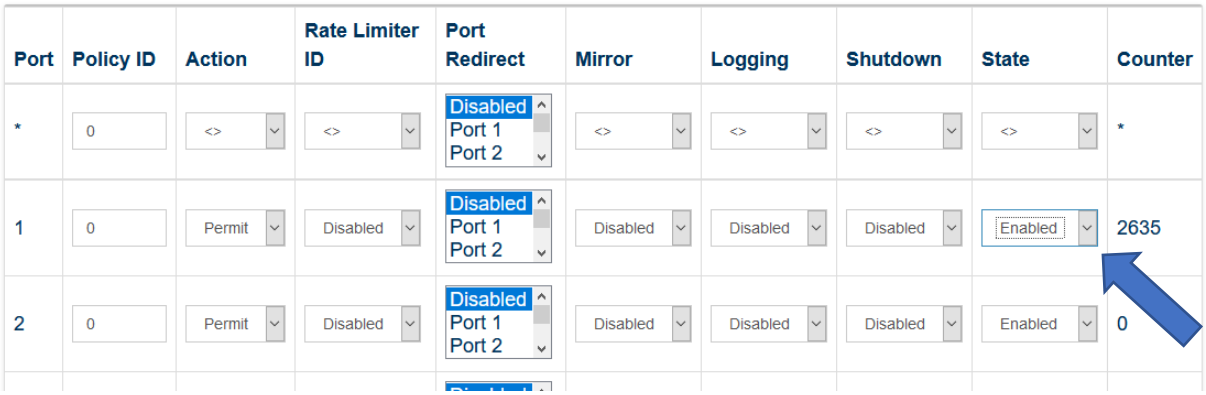
Wird ein Endgerät mit der erlaubten MAC-Adresse angeschlossen, so wird der Switch die Kommunikation mit dem Netzwerk zulassen. Wird ein Endgerät mit einer anderen als der festgelegten MAC-Adresse angeschlossen, so wird der Port 1 abgeschaltet.

Indikationen für den Anschluss eines nicht erlaubten Endgerätes findet man zum einen in der Port-Übersicht der Kopfzeile und im Menü „Access Control > Port Configuration“ im Status „Disabled“, wie weiter aufgezeigt.



Reaktivierung des Ports

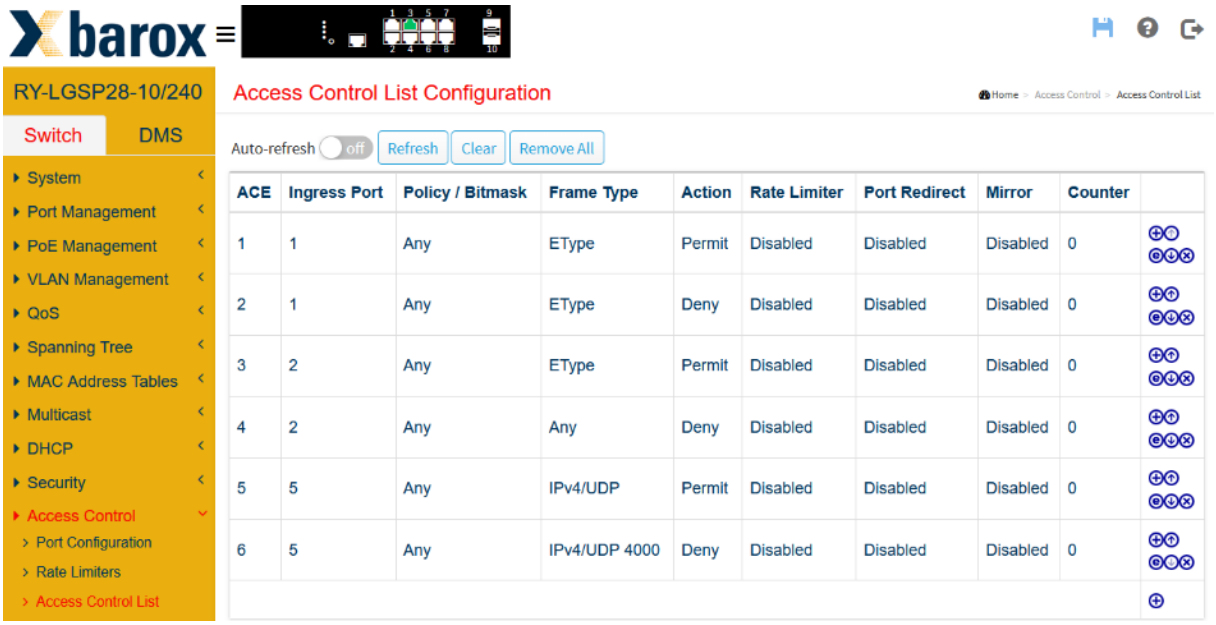
Um den Port wieder einzuschalten, muss an selbiger Stelle im Menü der Status wieder auf „Enabled“ gesetzt und abschließend mit einem Klick auf „Apply“ bestätigt werden.



Dabei ist zu beachten, dass entweder das Endgerät mit der passenden MAC-Adresse oder kein Gerät am Port verbunden ist.

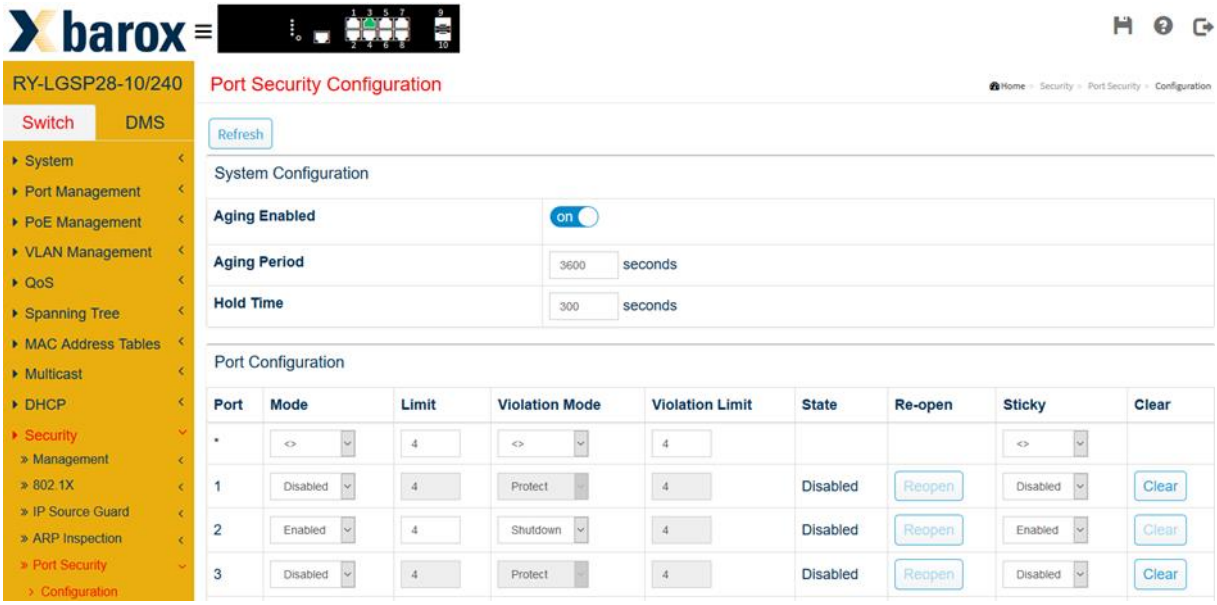
Hinweise zum Erstellen mehrerer Port-Regeln:

Die ACL-Erstellung für MAC-Adressen bietet sich bei einer geringen Anzahl an Ports an. Für jeden Port muss jeweils eine Regel für das Erlauben der spezifischen MAC-Adresse und eine Regel für das Ablehnen anderer MAC-Adressen erstellt werden. Dabei ist zu beachten, dass der Switch jeweils alle Regeln von oben nach unten prüft und die Reihenfolge bei der Konfiguration genau eingehalten werden muss. Siehe folgendes Beispiel:



5.1.4. Port-Security mit Limit-Control − Einstellungen

Werden am barox Switch nicht-gemanagte Switche mit Endgeräten angeschlossen, so empfiehlt es sich der Einsatz der Limit-Control. Grundlegend ermöglicht diese Funktion, dass weiteren nicht erwünschten IP/ Ethernet-Endgeräte an freien Ports der nicht-gemanagten Switche der Zutritt zur Netzwerkkommunikation verweigert 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 physisch mit dem barox Switch am zu konfigurierenden Port angeschlossen sind. Eine Veranschaulichung zu den Einstellungen ist nachfolgend aufgezeigt.



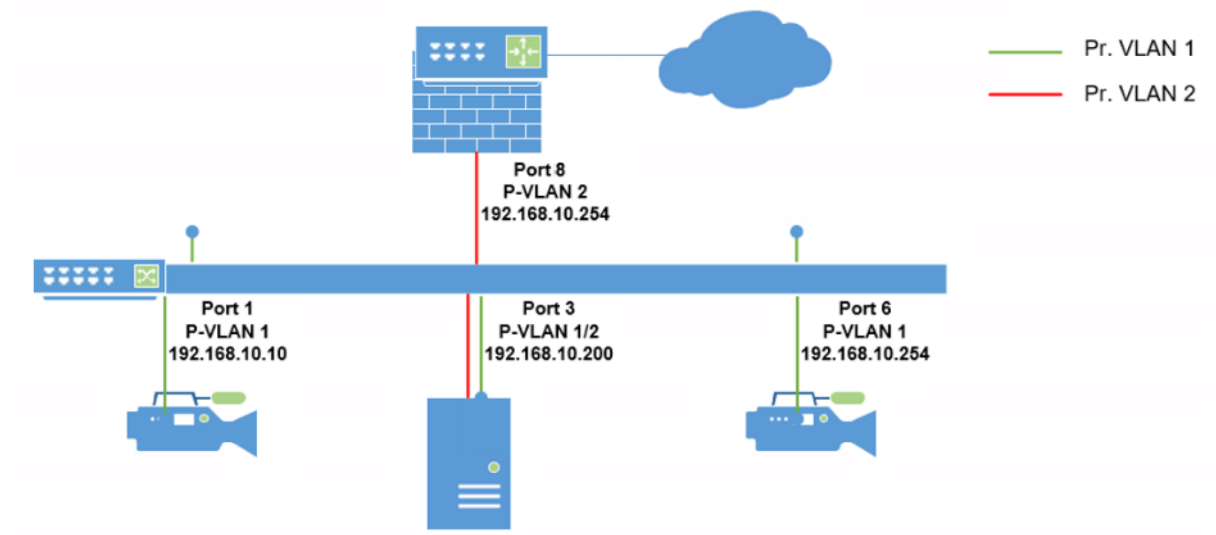
5.1.5. Privates VLAN mit Port-Isolation

Der Einsatz von Port-Isolation und privatem VLAN eignet sich z.B. für die Trennung von Endgeräten im selben VLAN. Sie verhindert ein Lockup beginnend auf Layer 2 und ermöglicht die Kommunikation eines weiteren Subnetzes im gleichen VLAN. Bei einem flachen Netzdesign können ausgewählte Ports mit weiteren Netzwerken, z.B. über eine WAN Verbindung für Remotezugriffe, kommunizieren.

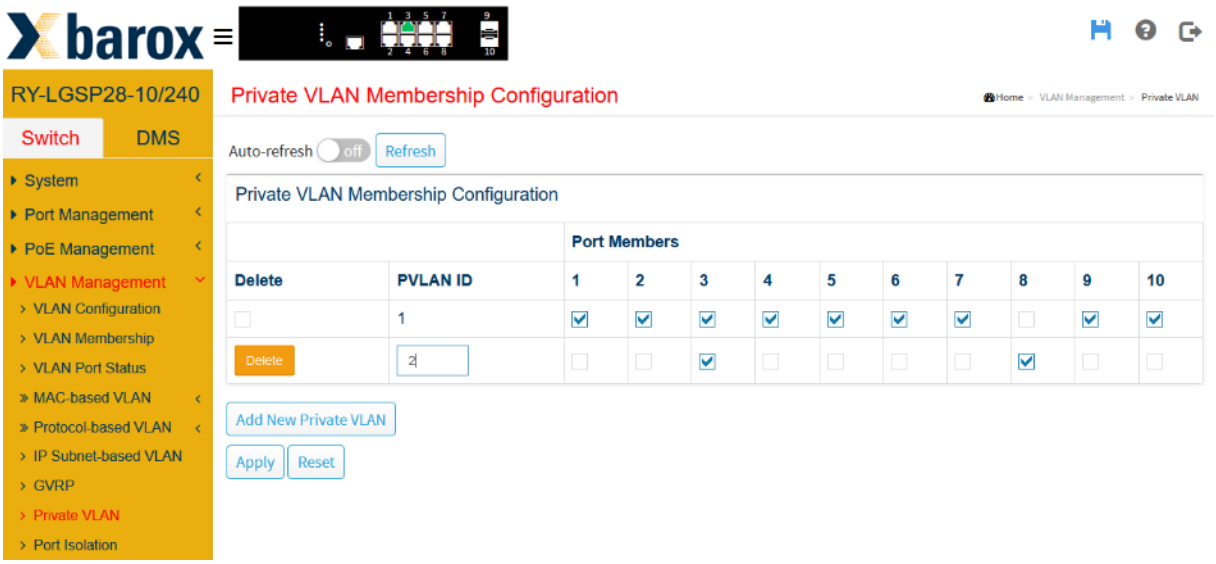
Hinweise zur Planung des Einsatzes:

- Aufzeichnen welche Komponenten miteinander kommunizieren
- Der Dokumentation die logische Trennung (Private VLAN) der Komponenten sowie IP- Adressen hinzufügen

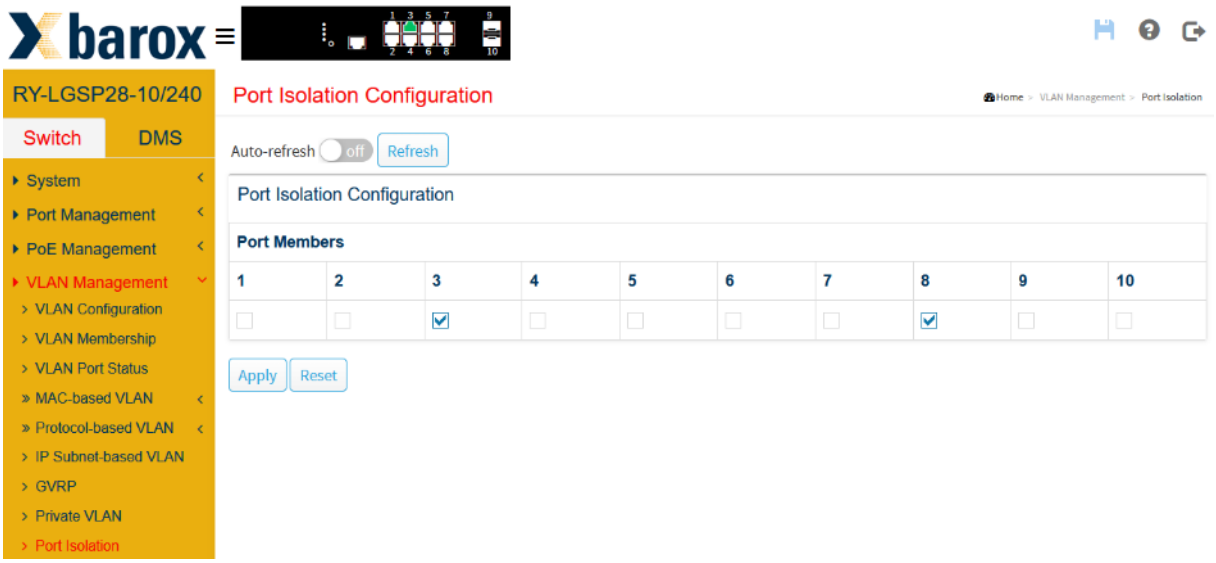
Beispielkonfiguration:



Schritt 1:



Schritt 2:



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

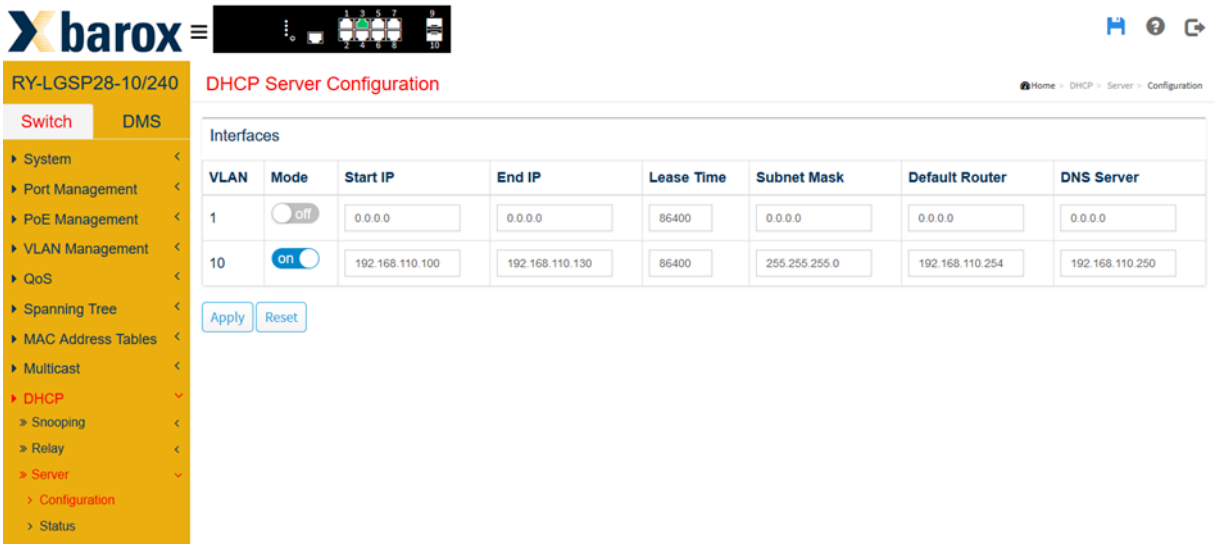
5.2.1. DHCP-Server

Hinweise zum Einsatz von DHCP-Servern in Videonetzwerken

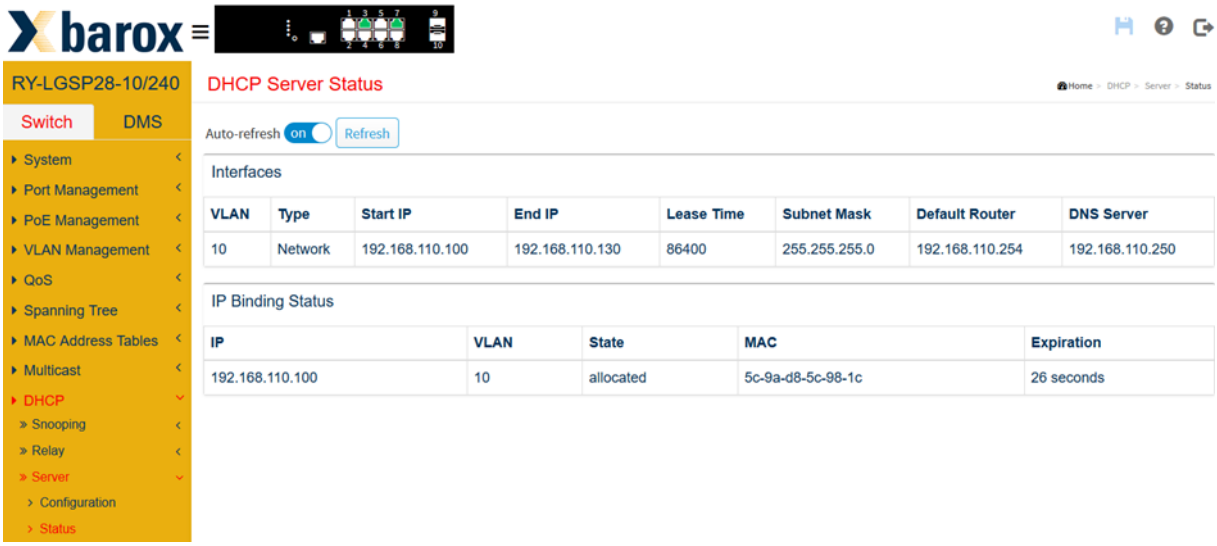
Es gilt zu prüfen, ob der Einsatz eines DHCP-Servers generell vom Netzdesign her erforderlich ist. Dieser Dienst bietet neben den Vorteilen der automatisierten Netzwerkinformationsverteilung auch verschiedenste Angriffspunkte

Grundlegende Konfiguration und Inbetriebnahme des DHCP-Dienstes am Beispiel

Beginnend wird das VLAN des Dienstes und die Größe des DHCP-Pools durch Angabe der Start- und Endadresse und weitere Informationen wie die Lease Time in Sekunden, die Netzwerkmaske, das Gateway und den DNS-Server zur Clientübermittlung festgelegt. Der Dienst wird generell im Modus mit der Einstellung „*On*“ aktiviert, wie weiter aufgezeigt.



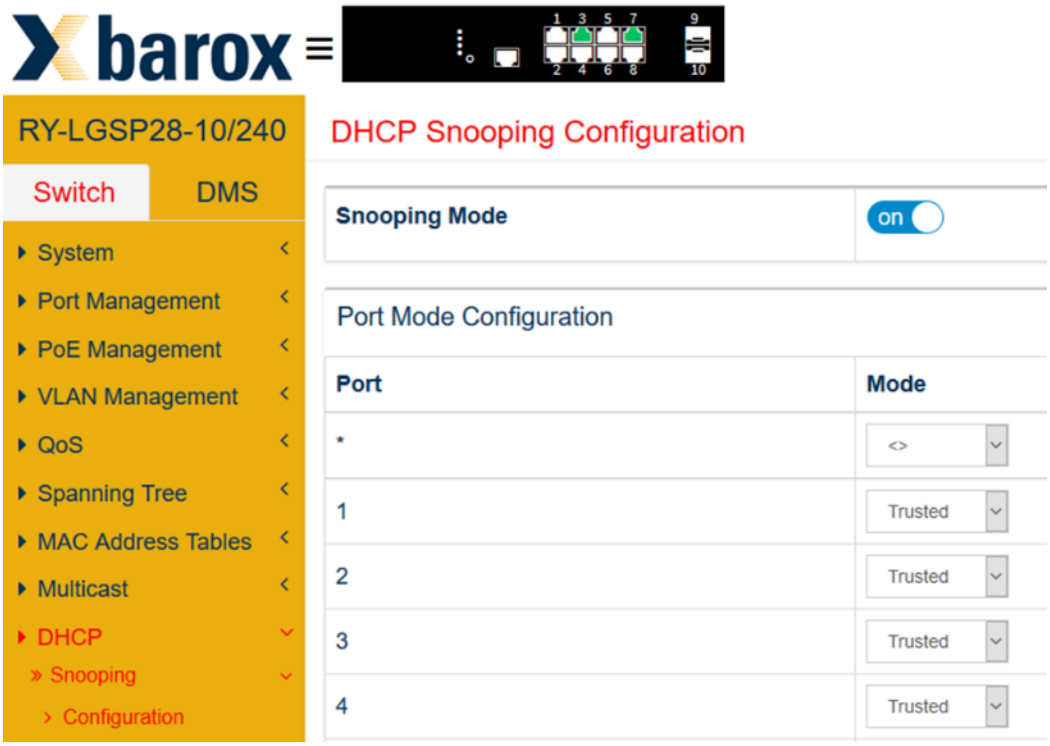
Eine Übersicht des Dienststatus bzw. über die vergebenen Clientadressen ist wie folgt zu finden:



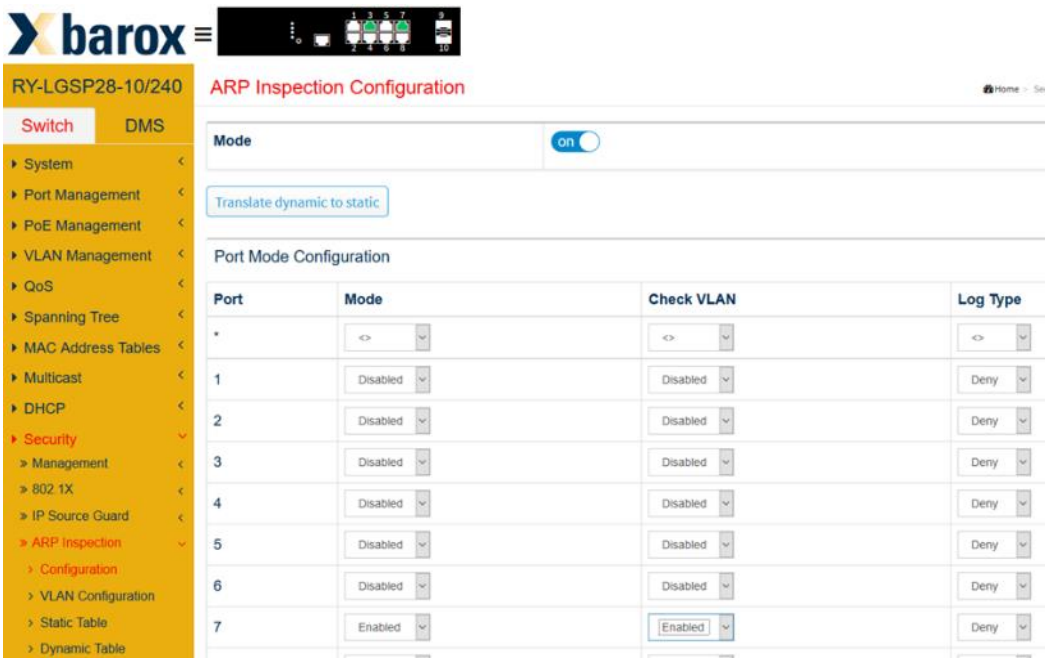
5.2.2. Absicherung des DHCP-Dienstes durch ARP-Inspection

Die Absicherung vor unerwünschten DHCP-Clients, bzw. der Schutz vor Manipulation des ARP-Caches, kann mit der ARP-Inspection realisiert werden. Nachdem der Aktivierung der Funktionen können die DHCP-Clients statisch als Rezipienten in einer Tabelle eingetragen werden. Grund-voraussetzung für die höchste Sicherheit ist, dass die Größe des DHCP-Adresspools mit der Anzahl von Clients eingestellt wird.

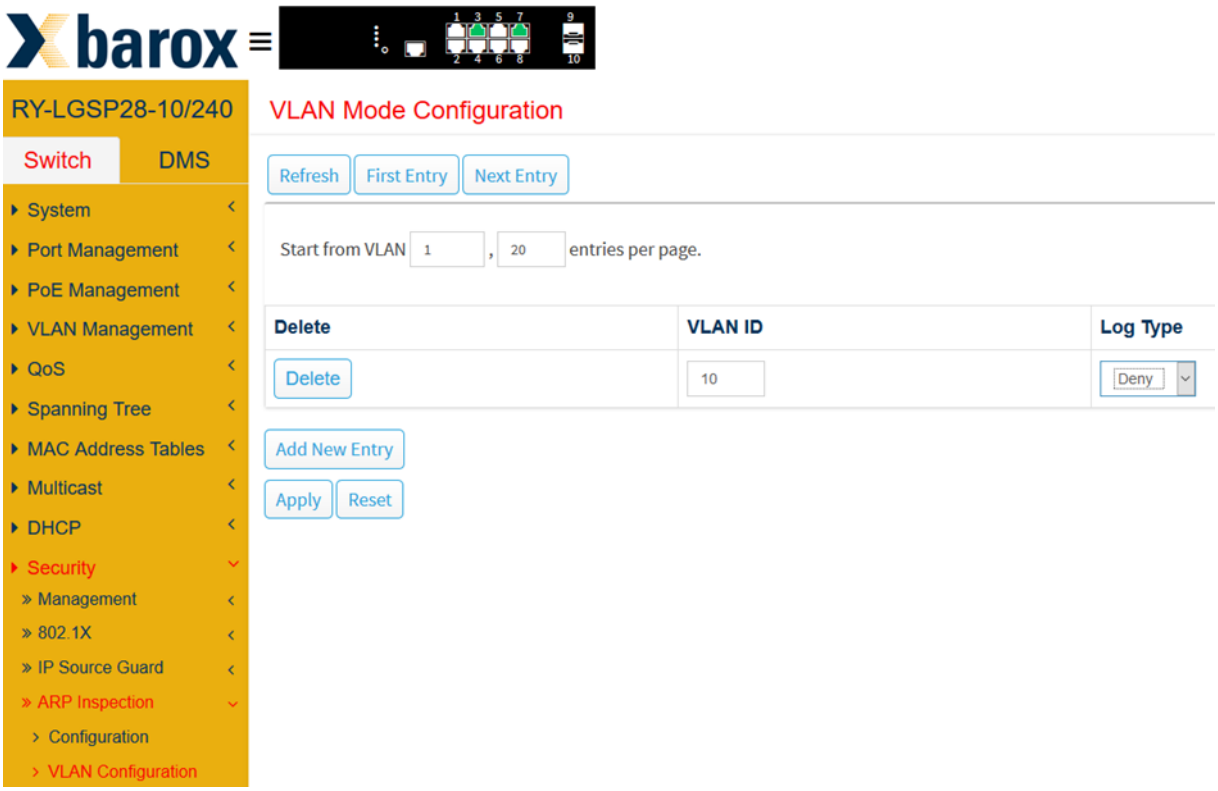
Zunächst wird die Snooping-Funktion unter „Snooping Mode“ generell aktiviert, wie nachfolgend abgebildet. Weiter können für die Ports des Switches die Vertrauensstellungen ausgewählt werden. Für die Funktion der „Inspection“ muss der Modus auf „Trusted“ gesetzt sein.



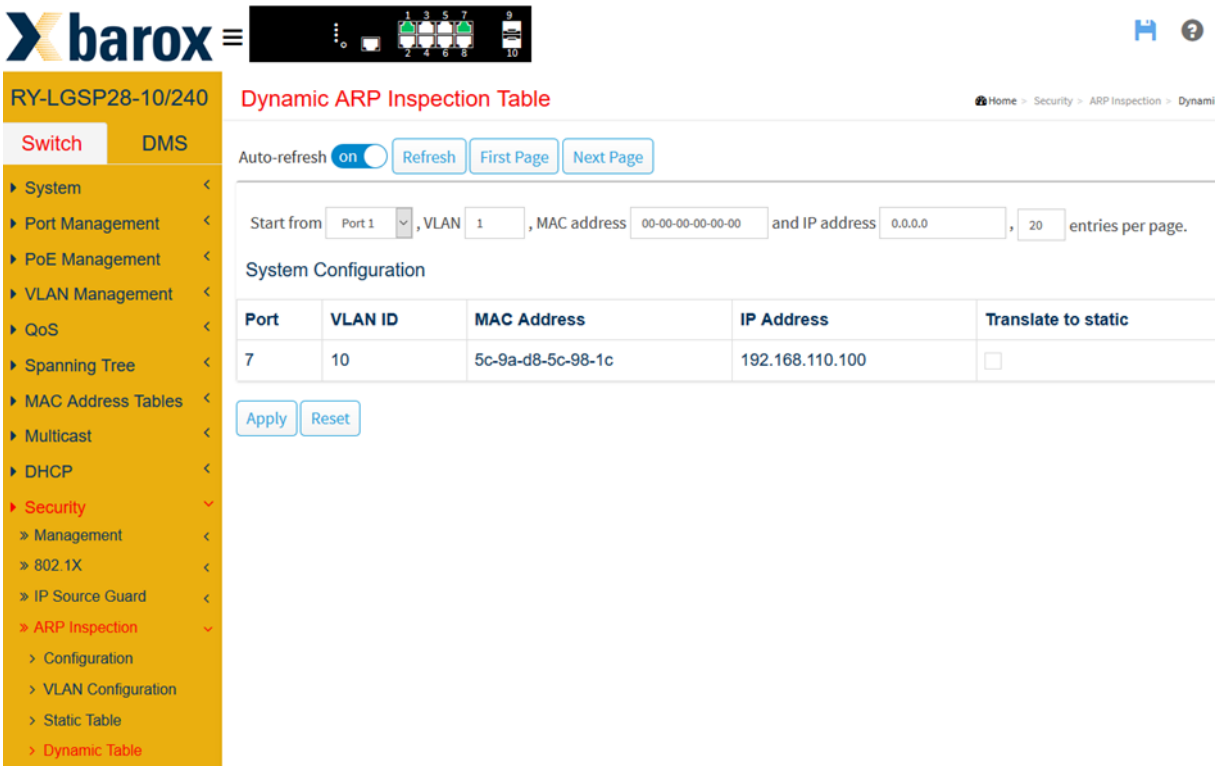
Weiter werden die Parameter für die Ports aktiviert und konfiguriert. Im folgenden Beispiel wird die ARP-Inspection für den Port 7 aktiviert, die Überprüfung des VLANs aktiviert und der Log-Typ eingestellt.



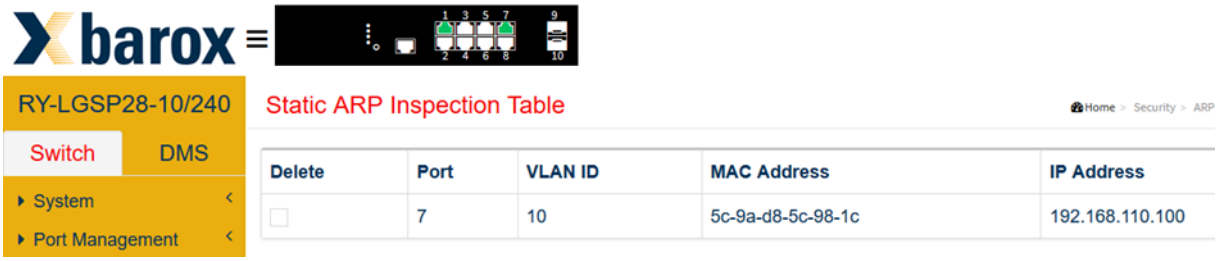
Im Anschluss werden die VLANs festgelegt, die in der Überprüfung berücksichtigt werden sollen, und der Log-Typ (Vertrauensstellung) festgelegt.



Nach erfolgten Einstellungen können die DHCP-Clients angeschlossen werden. Nachdem der DHCP-Dienst IP-Adressen verteilt, werden die Clients mit ihren Eigenschaften für Layer 2 und 3 in der dynamischen ARP-Inspection-Tabelle sichtbar und können anschließend in die statische ARP-Inspection-Tabelle übersetzt werden.



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

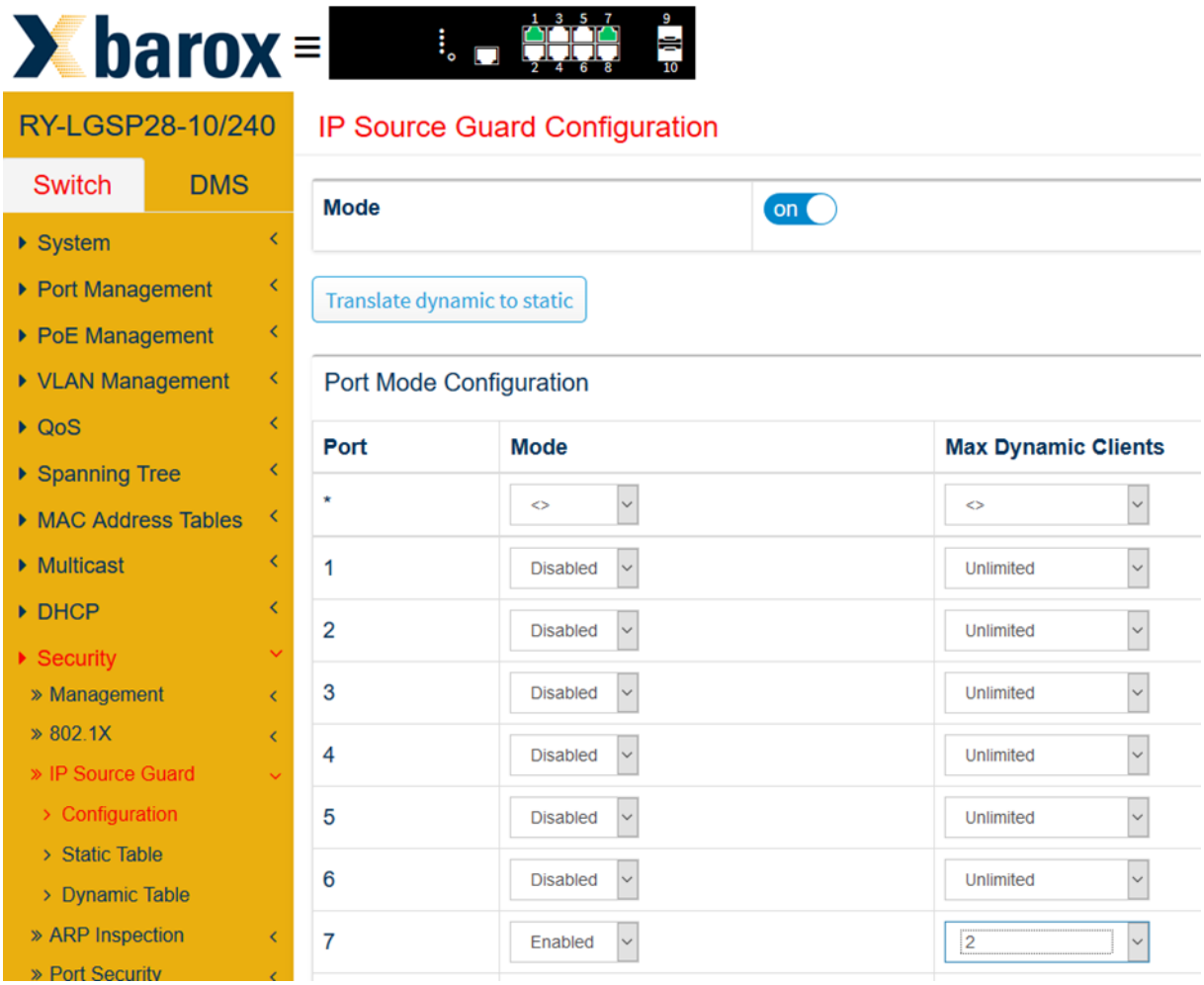


5.2.3. IP Source Guard

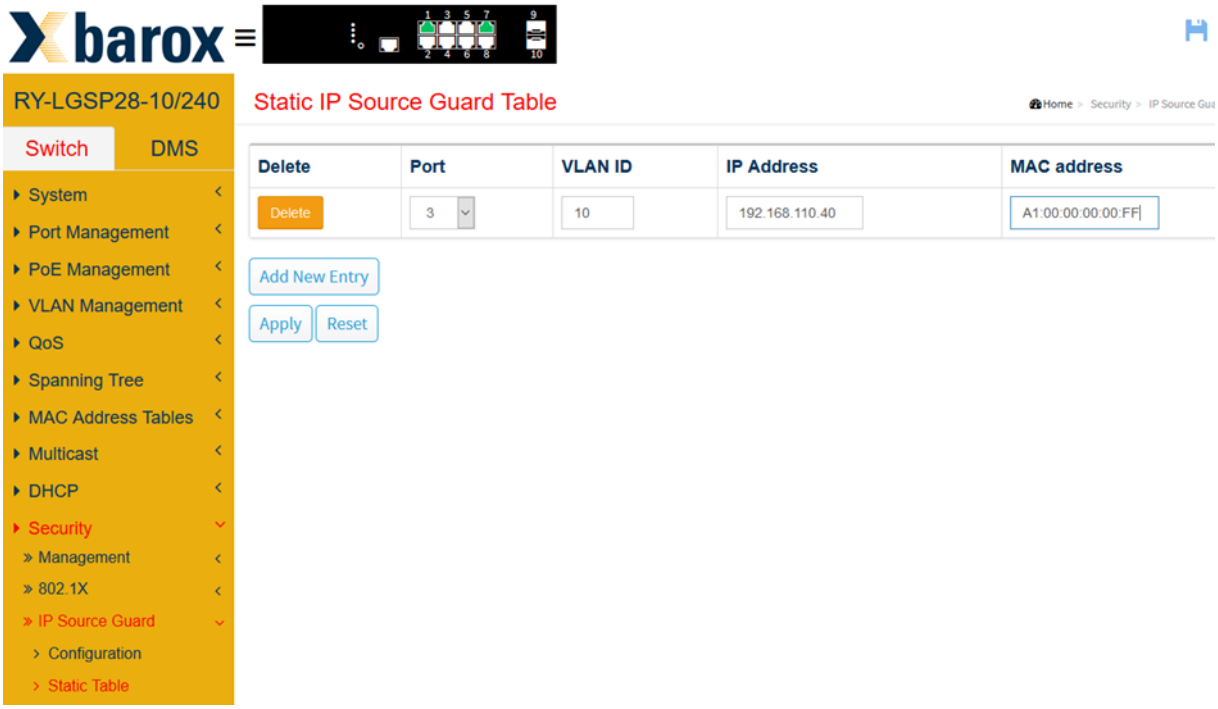
Einsatz und Konfiguration:

Eine erweiterte Funktion zur Absicherung von Endgerät- Seite stellt der Einsatz der Funktion „IP Source Guard“ dar. Diese verknüpft neben der Untersuchung der MAC-Adresse des Endgeräts zudem auch die vorgegebene statische IP-Adresse der angeschlossenen Geräte. Sie bietet beispielsweise den Schutz vor sogenanntem „IP-Spoofing“.

Wie nachfolgend aufgezeigt wird diese Funktion generell aktiviert und kann weiter, je Port granuliert, eingestellt werden.

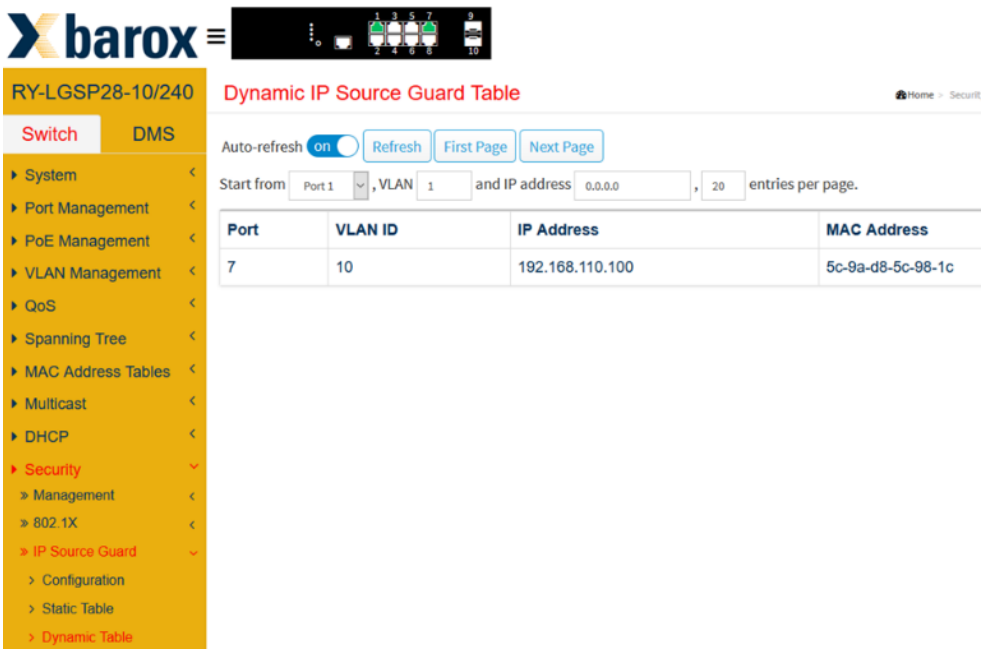


Nach dem Einschalten der Funktion kann die Konfiguration, mit statischen Einträgen − wie weiterführend abgebildet − erfolgen.



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, wo statische MAC-Adresseinträge je Port einen möglichen Angriff verhindern sollen, bietet der „IP Source Guard“ mit statischen Einträgen zusätzlich die Bedingung, die IP-Adresse des angeschlossenen Gerätes 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, dass der Angreifer die MAC-Adresse und die IP-Adresse des Geräts kennen muss, um sich Zugang zum Netzwerk zu verschaffen.

Der „IP Source Guard“ stellt auch eine weitere Möglichkeit zur Absicherung eines auf dem Switch konfigurierten DHCP bereit. Bei dieser Art der Verwendung wird die Funtkion „DHCP Snooping“ benötigt, die unter „*Switch* > *DHCP* > *Snooping* > *Configuration*“ aktiviert wird. Die geschützten Clients können wie im folgenden Bild in der dynamischen Tabelle betrachtet werden.

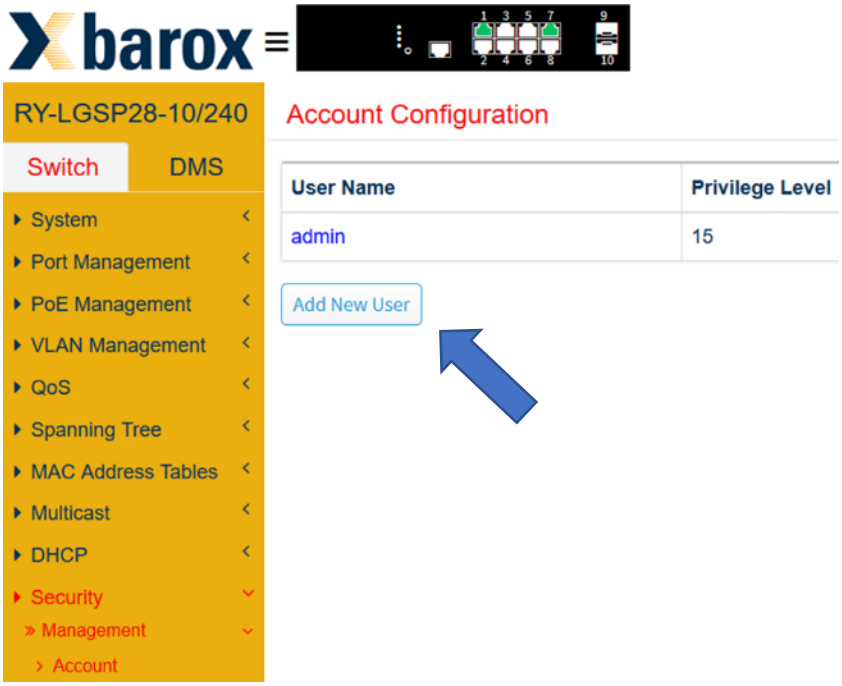


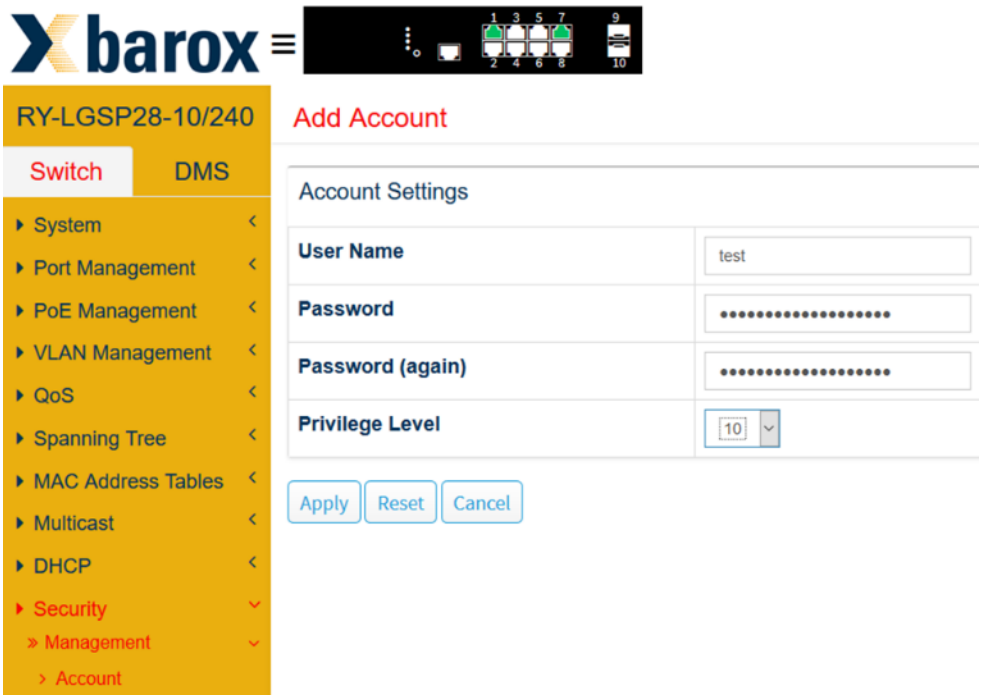
5.3 Absicherung von Switch-Management und Netzwerkadministration (Layer 3 – 7)

5.3.1. Benutzerverwaltung und Konfiguration

Anlegen eines Benutzers:

Nachfolgend ist ein Beispiel für die Anlage eines weiteren Benutzers aufgeführt:

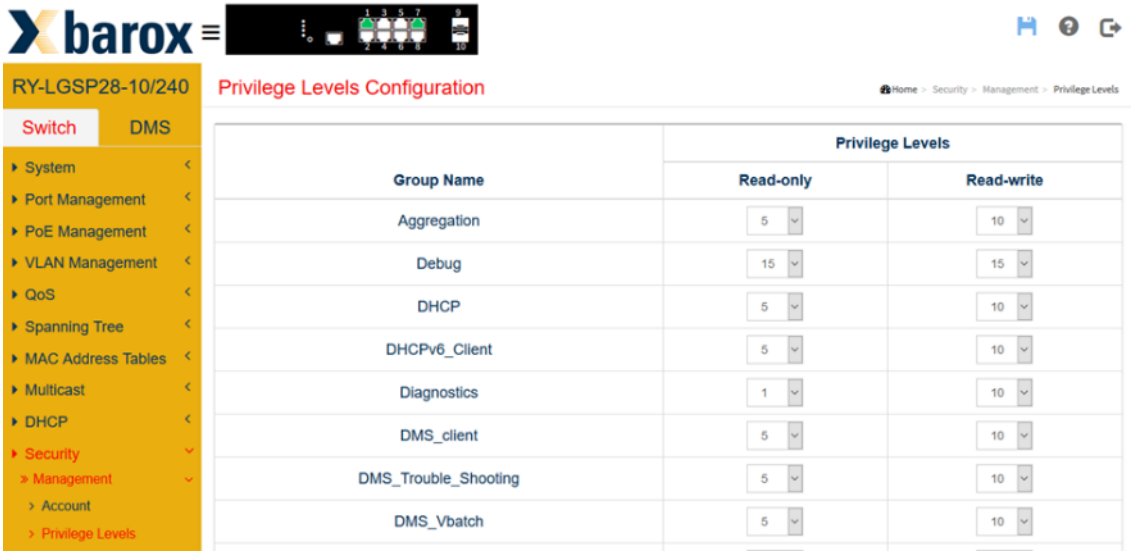




Grundlegende Einstellungen der Nutzerrichtlinien und Privilegien:

- Die Privilegien-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 diese bei dem Anlegen neuer Nutzer zu vergeben.

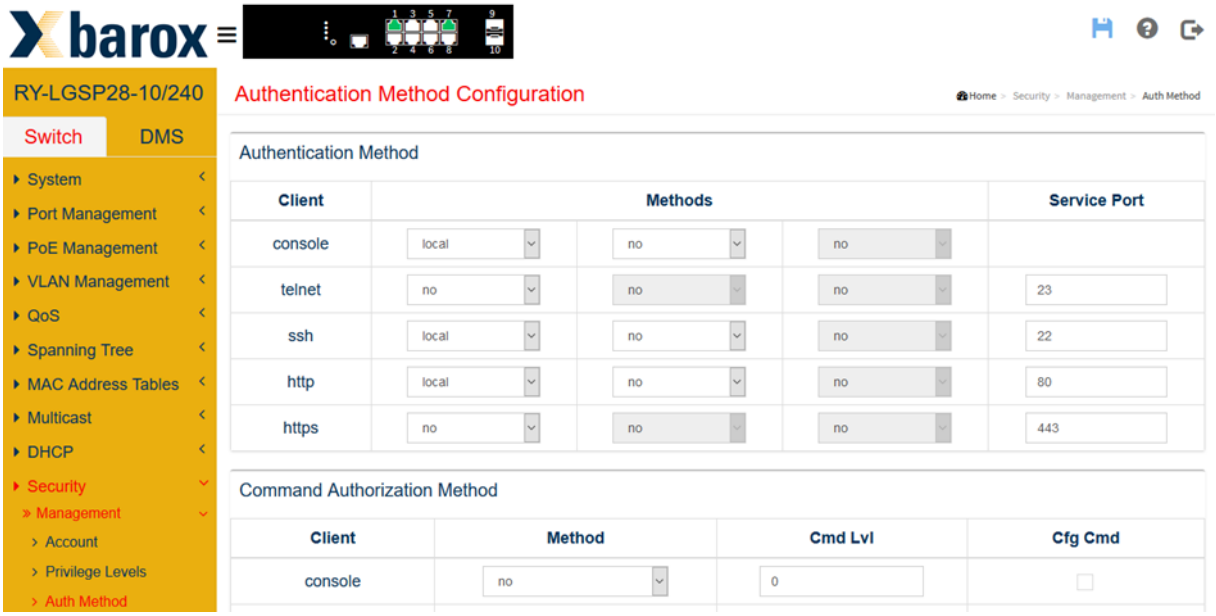
- Hinweis: Es ist hilfreich, die Rechte für einen weiteren Nutzer nach Befugnissen und Kompetenzen zu skalieren.



5.3.2. Einsatz und Einstellungen der Authentisierung am Switch-Management

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

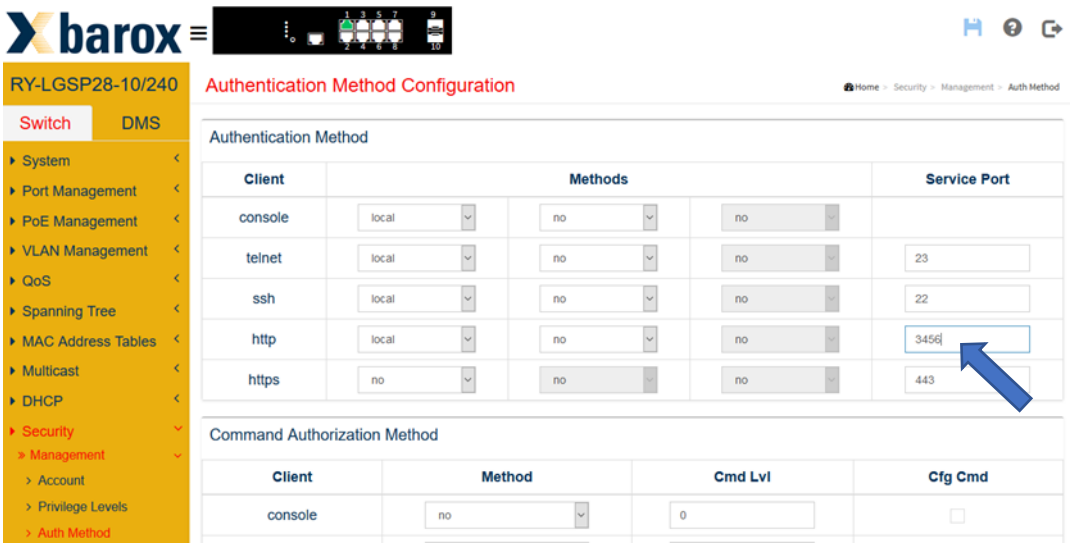
Wie nachfolgend abgebildet können die Zugriffsmethodik eingestellt bzw. nicht benötigte Funktionen abgestellt werden. Es ist zu empfehlen, sofern das Netzwerkdesign es zulässt, die Telnet Zugangsfunktion generell abzuschalten. Die Konfigurationsmethoden können wie folgt eingestellt werden:



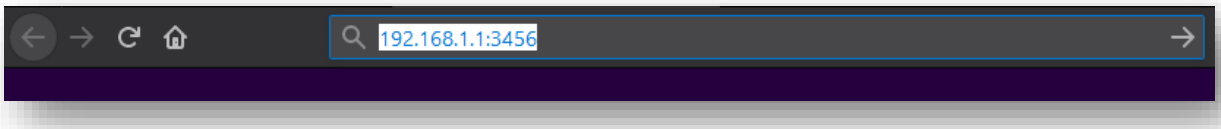
- Es empfiehlt sich, für die Kommandozeilen-basierte Verwaltung (CLI) das SSH-Protokoll zu nutzen, da diese Methode eine verschlüsselte Verbindung bietet.

Verwaltung des Zugriffs auf die Weboberfläche (GUI) mit HTTP:

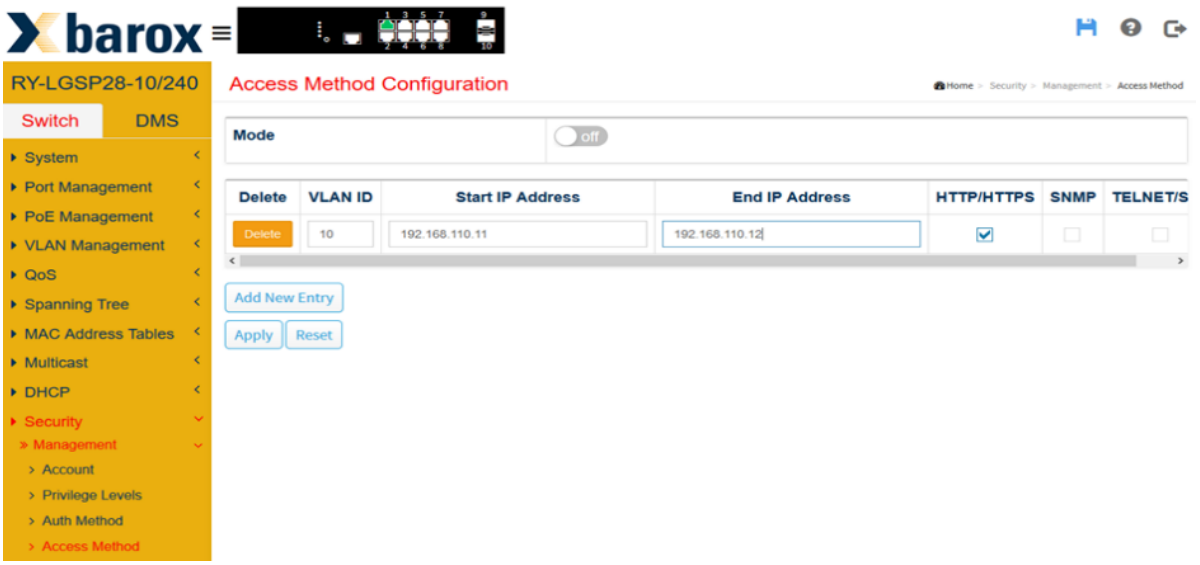
- Es empfiehlt sich, einen separaten Nutzer für HTTP anlegen
- Port 80 verändern, Hinweis: Portangabe bei Zugriff im Browser beachten!
- Der HTTPS Zugriff bietet den höchsten Schutz, da die Verbindung verschlüsselt wird



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



Der Managementzugriff und dessen Methoden kann auf bestimmte IP-Adressbereiche und VLANs eingeschränkt werden. Dies kann im Access-Management, wie weiter unten beispielhaft dargestellt, erfolgen.

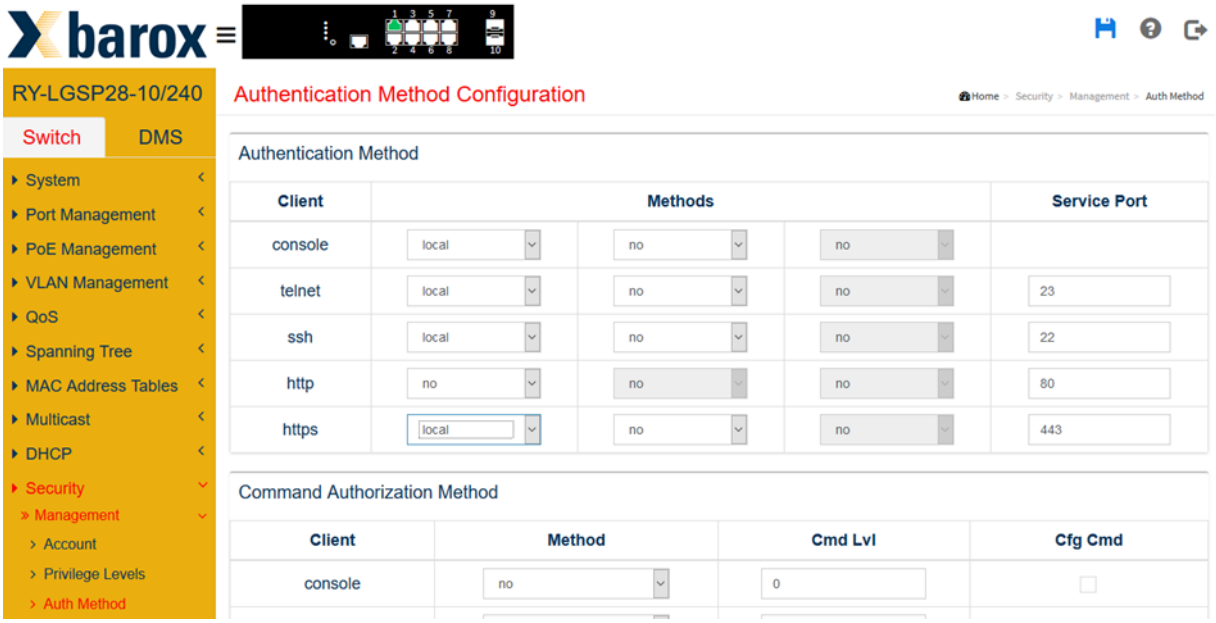


! Achtung !

Es ist zwingend erforderlich, dass für jeden Eintrag eine Methode ausgewählt ist. Sollte die jeweilige Methode dennoch generell ausgeschaltet sein, so ist der Switch in diesem VLAN nicht mehr verwaltbar bzw. der Zugang zum Management ist ausgeschlossen. Durch einen Neustart des Gerätes kann die „Falschkonfiguration“ rückgängig gemacht werden.

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 dieser Modus aktiviert ist, dann sollte die NTTP-Option ausgeschaltet werden. Der Aufruf der Switch-GUI erfolgt im Browser über die HTTPS-Protokollphrase 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

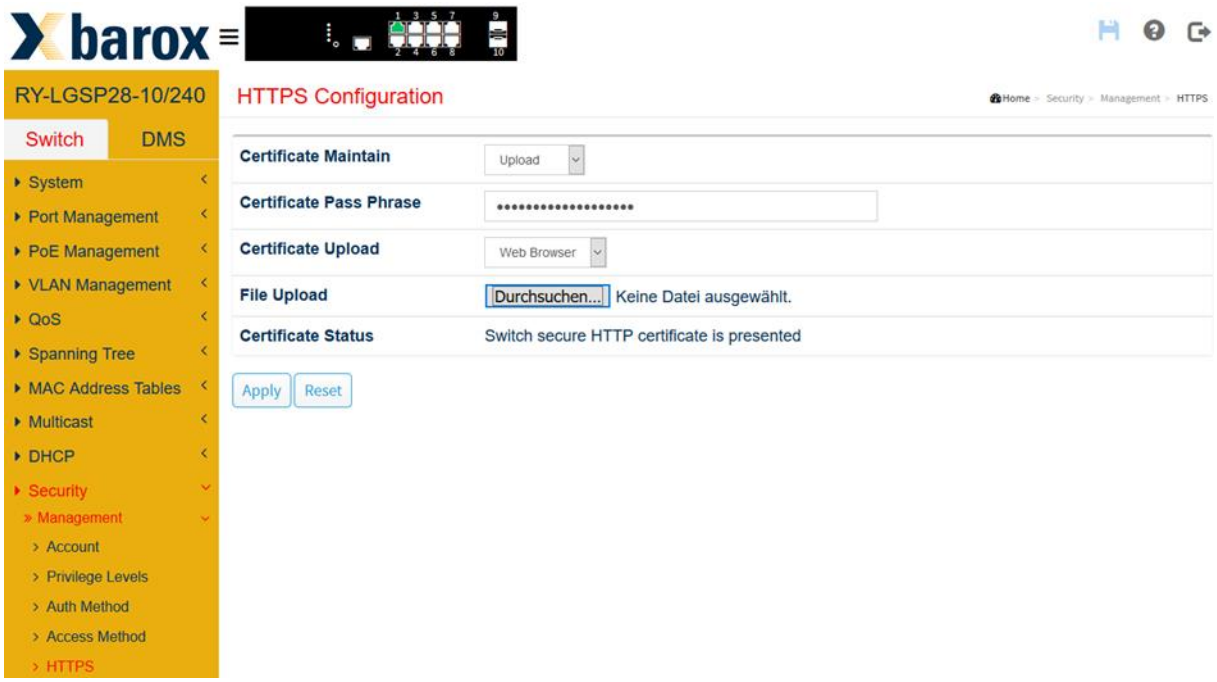
Kurzer Hinweis zur Verwendung von Zertifikaten:

Eine zertifikatsbasierte Anbindung ermöglicht eine der aktuell 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.

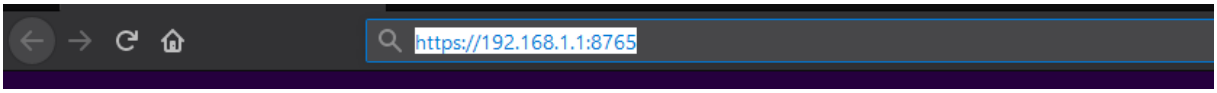
Nachfolgend sind die Einstellmöglichkeiten, bzw. der Methoden aufgezeigt:

- Generierung des Zertifikates zur späteren Verwendung, das 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

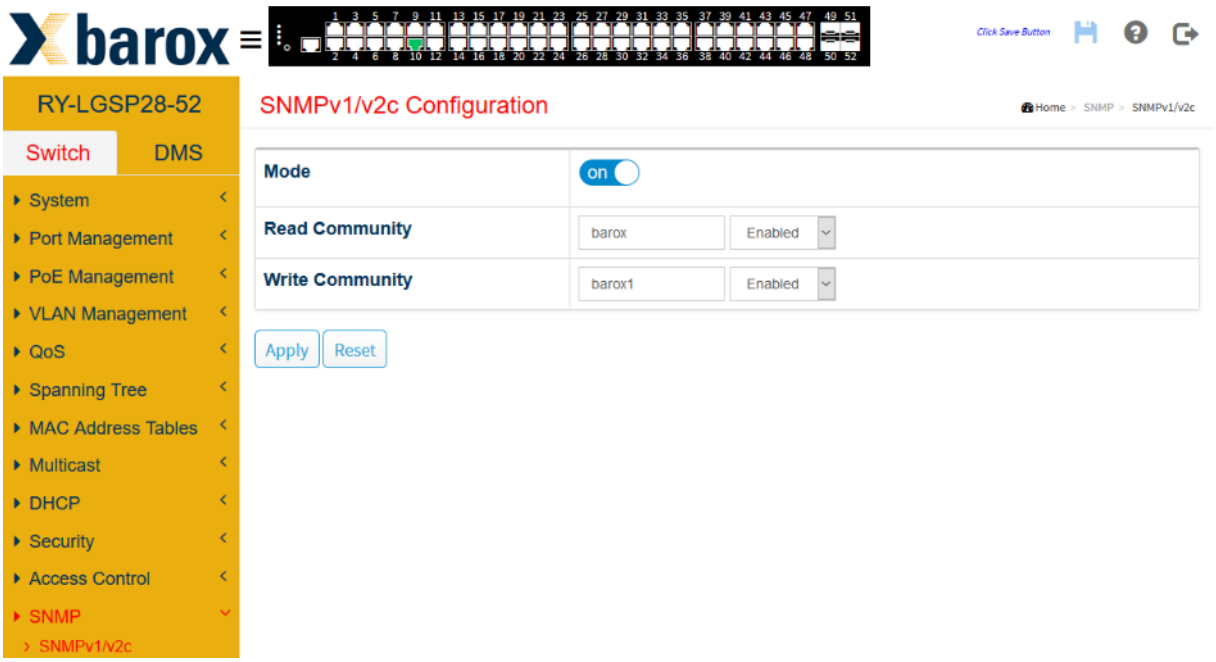
SNMP wurde von der IETF (Internet Engineering Task Force) entwickelt und dient als Protokoll zur Überwachung, Steuerung und Konfiguration von Netzwerkelementen.

5.4.1. Konfiguration von „SNMP v2c“

Im Weiteren wird eine grundlegende Konfiguration von „SNMP v2“ 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 Funktion „SNMP v2“

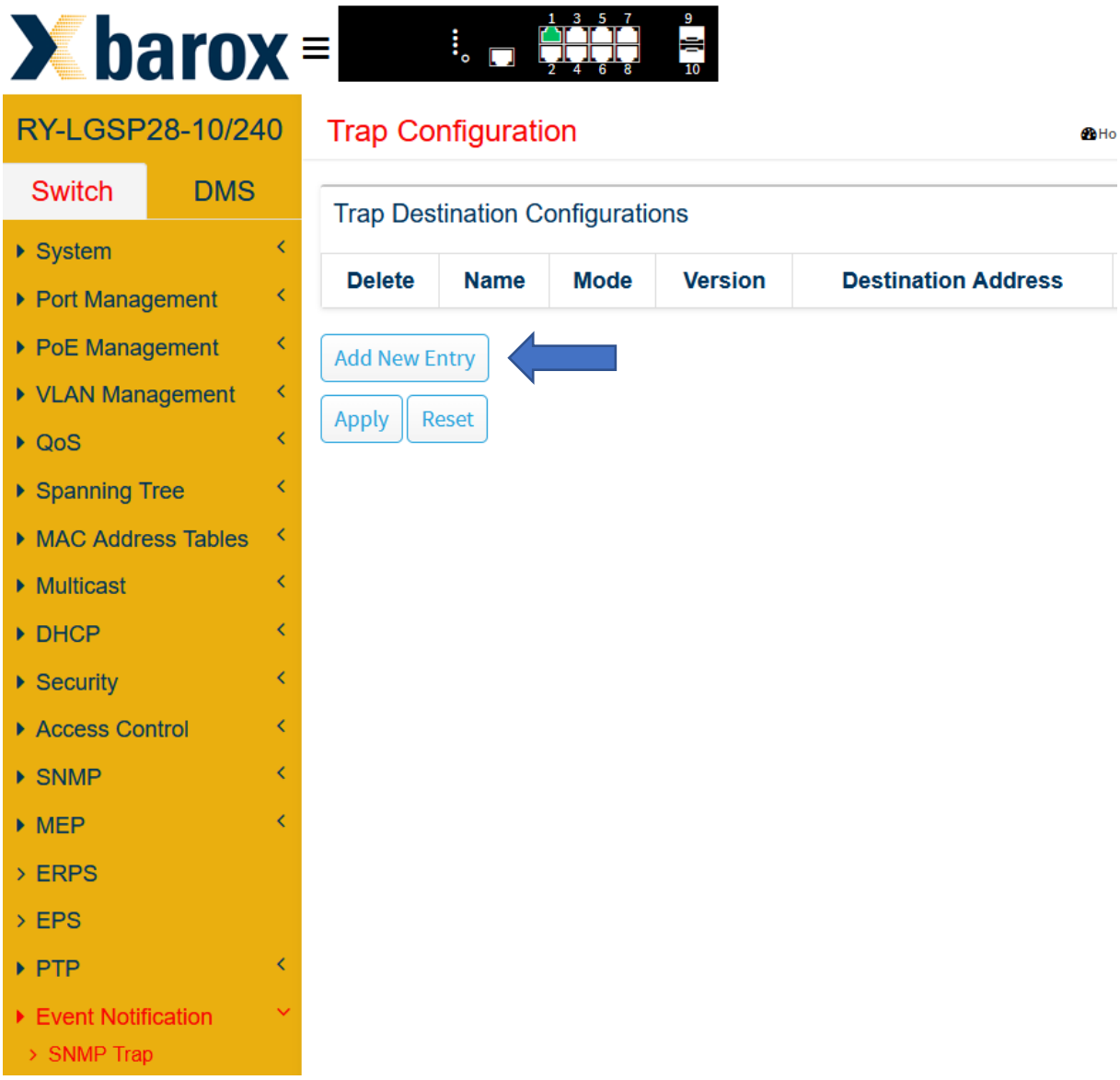
Grundlegend ist der Modus zu aktivieren. Weiter werden die Namen für die Read- und Write- Communities festgelegt und die Write-Community aktiviert.



Abschließend sind die Änderungen in die Startup-Konfiguration zu speichern und der Switch neu zu starten.

5.4.2. Konfiguration der SNMP-Traps

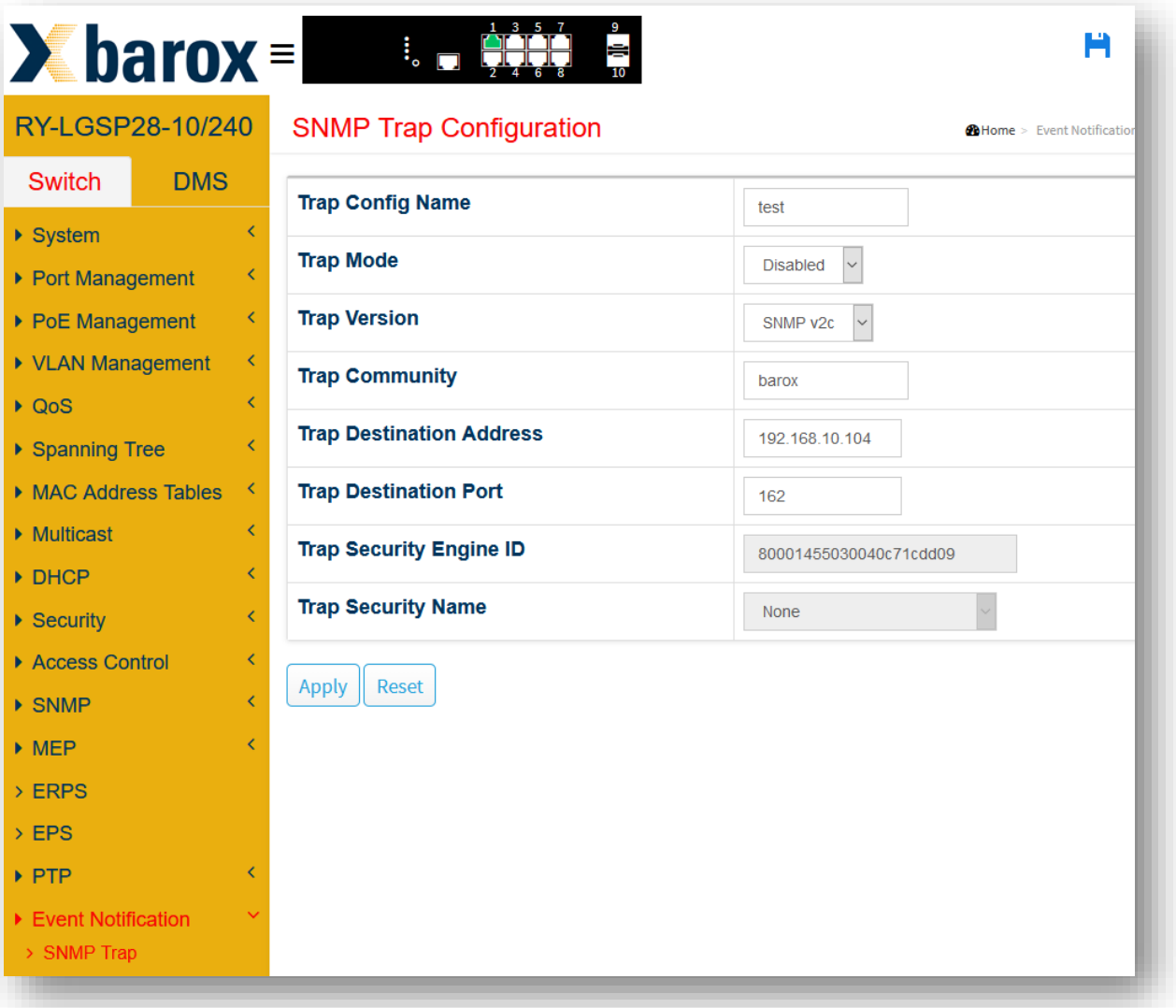
Für den Empfang von SNMP-Trap-Nachrichten sind zu einem die benötigten Parameter für die Verbindung zum Zielempfänger festzulegen. Dies ist mit dem Anlegen einer Konfiguration einzuleiten.



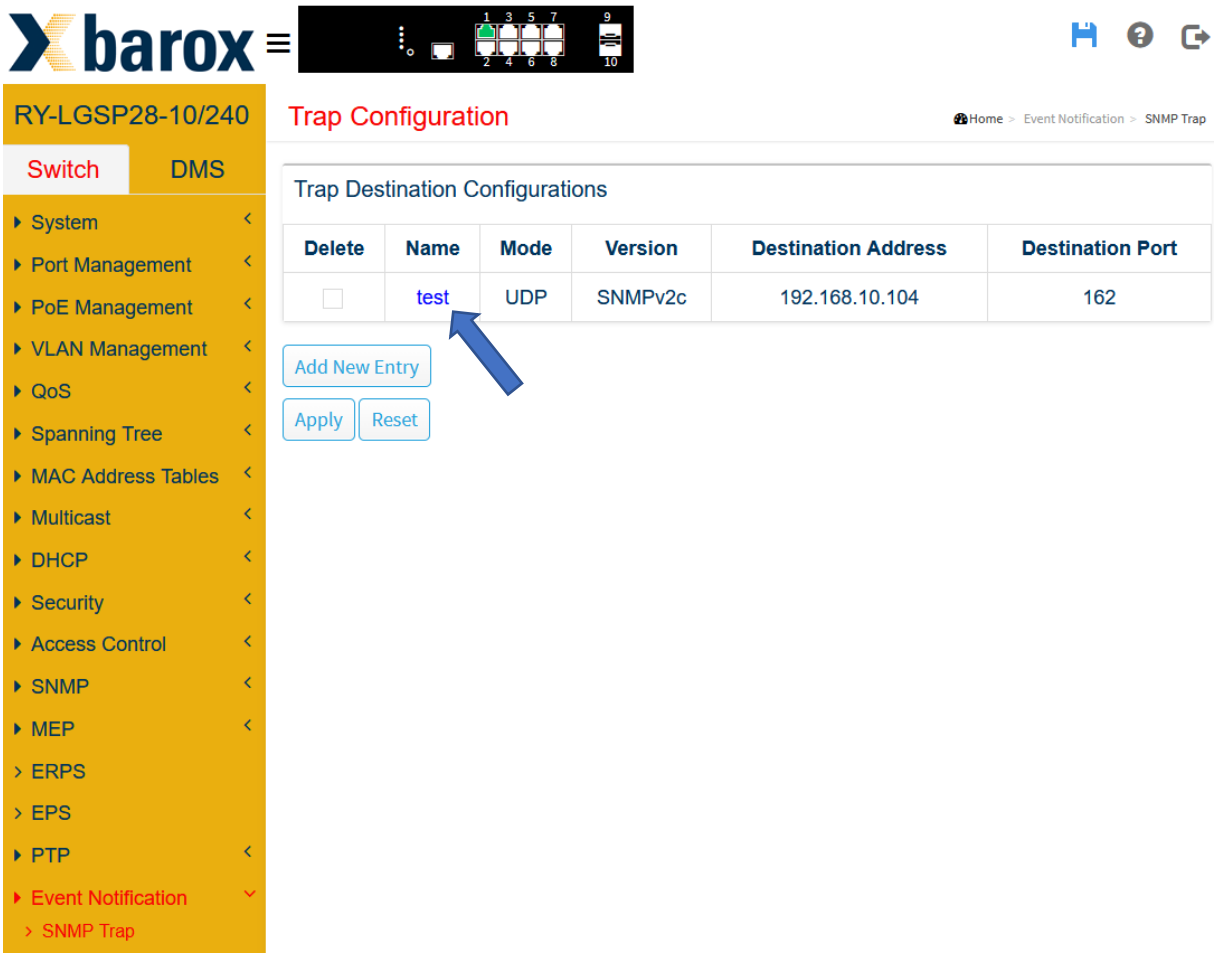
Am Beispiel nachfolgend sind folgende Werte für eine neue Konfiguration einzustellen:

- Trap Config Name -> Ein Name soll vergeben werden
- Trap Mode -> UDP oder TCP – für den Anfang wie gebräuchlich UDP
- Trap Version -> Auswahl von SNMP v2c
- Trap Community -> der vorher angelegte Community-Name muss eingetragen werden
- Trap Destination Address -> Angabe IP-Adresse des Trap-Empfängers
- Trap Destination Port -> Angabe des Ports für den Empfänger
- Weitere Einstellungen können zunächst den vorgegebenen übernommen werden

Anschließend werden die Einstellungen mit „Apply“ bestätigt.

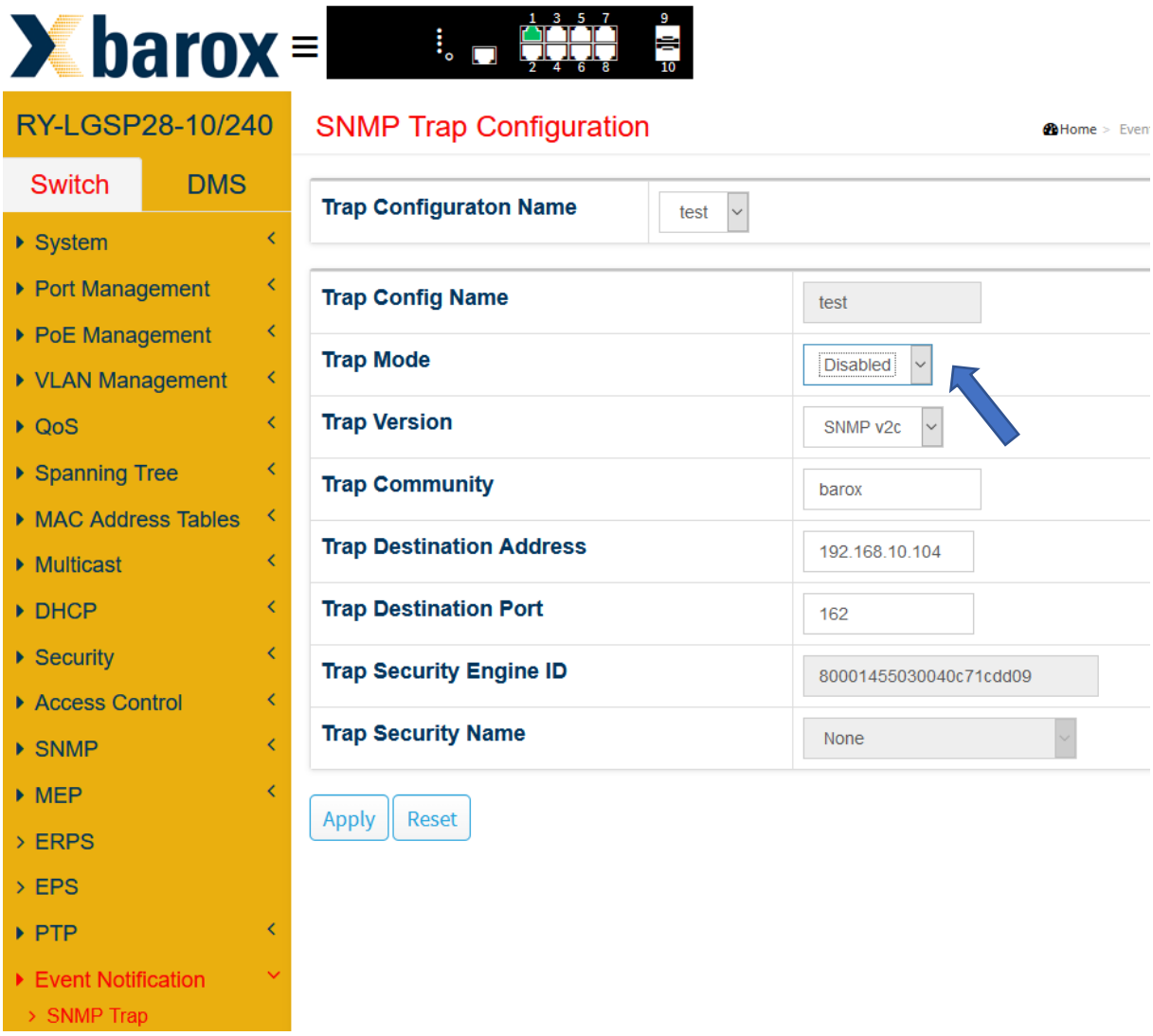


Nach dem Anlegen der neuen Konfiguration erscheint diese in der übergeordneten Ebene. Die Konfiguration kann durch Auswahl des Namens geöffnet werden.



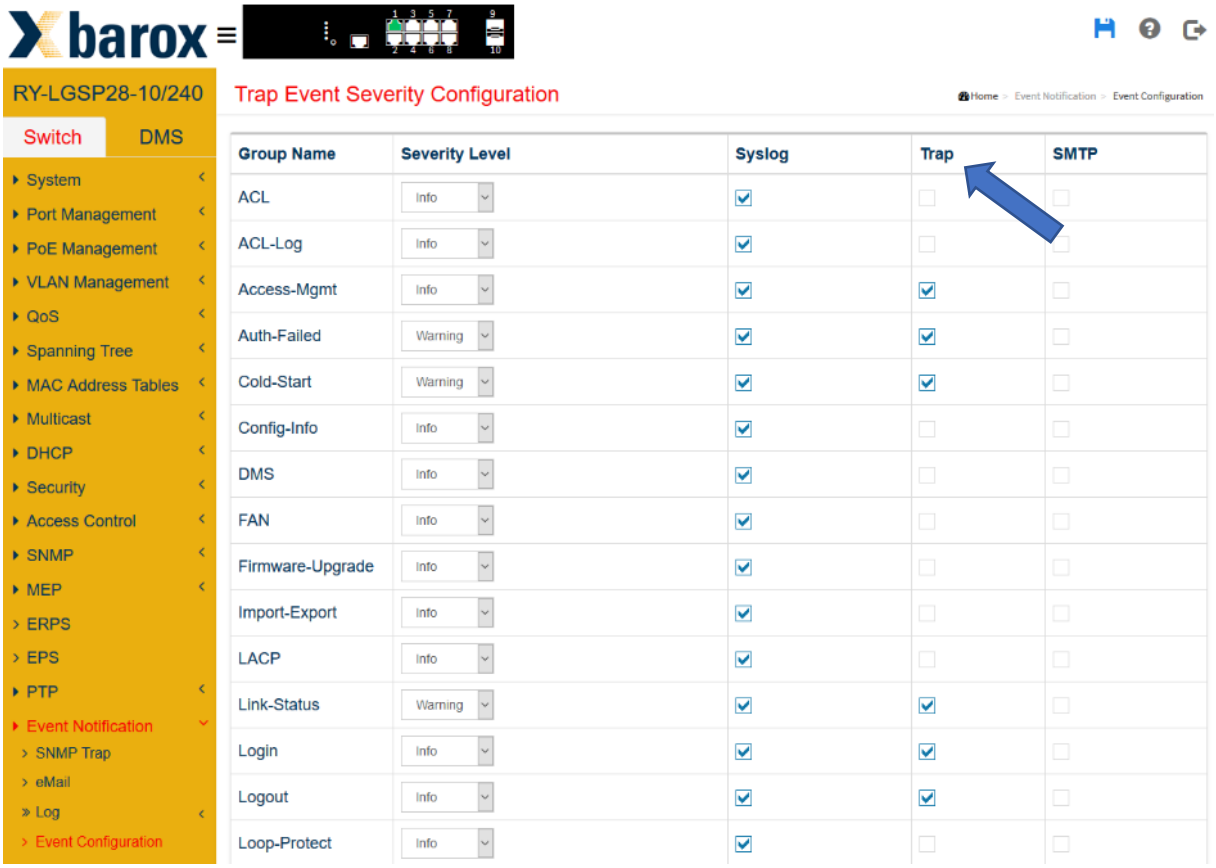
Deaktivierung der SNMP-Trap-Funktion

Die Deaktivierung kann auf zwei Wegen erfolgen. Zum einem kann sie durch das Löschen der Konfiguration deaktiviert werden. Sollte der Trap-Versand nur sporadisch verwendet werden müssen, so empfiehlt es sich, die Funktion in der Konfiguration auf „Disabled“ zu setzen.


barox
RY-LGSP28-10/240
Switch
DMS
System
Port Management
PoE Management
VLAN Management
QoS
Spanning Tree
MAC Address Tables
Multicast
DHCP
Security
Access Control
SNMP
MEP
ERPS
EPS
PTP
Event Notification
SNMP Trap
SNMP Trap Configuration
Home
Trap Configuraton Name
test
Trap Config Name
test
Trap Mode
Disabled
Trap Version
SNMP v2c
Trap Community
barox
Trap Destination Address
192.168.10.104
Trap Destination Port
162
Trap Security Engine ID
80001455030040c71cdd09
Trap Security Name
None
Apply
Reset

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 Konfigurationsmenü 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.



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

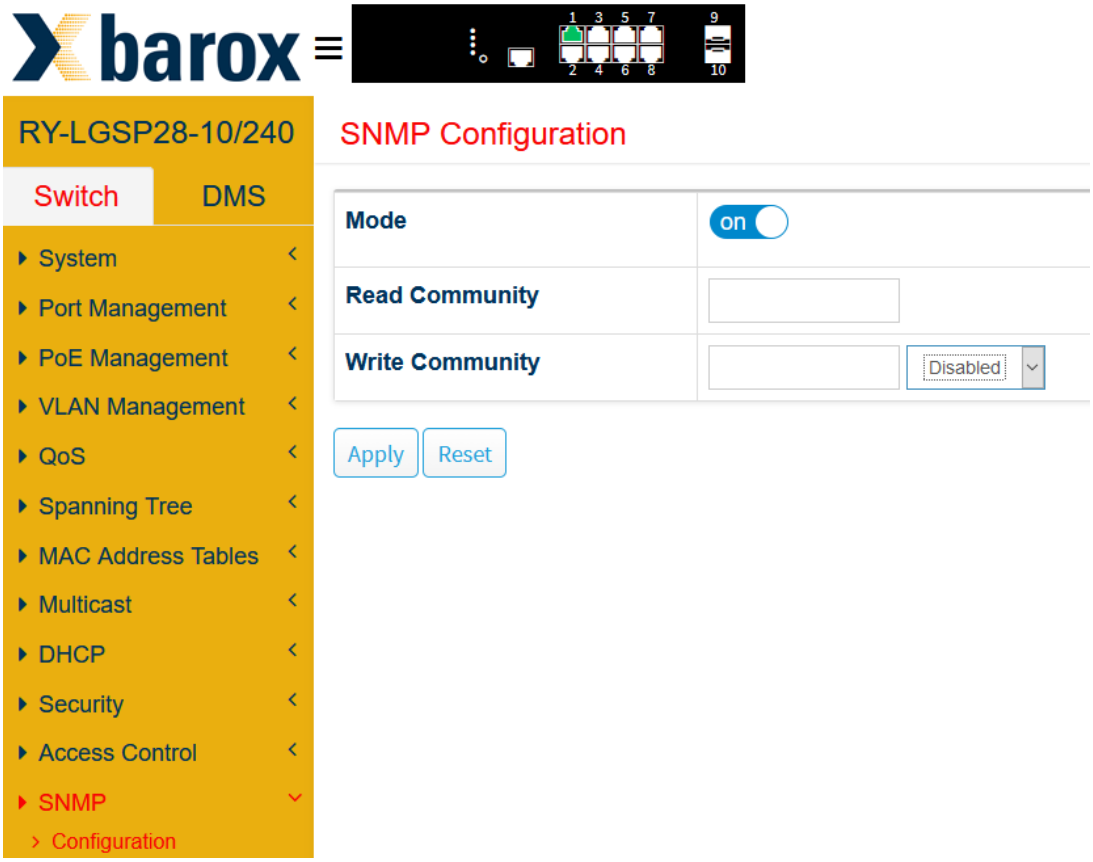
5.5 Konfiguration von „SNMP v3“

Ausgangslage:

Der gestiegene Sicherheitsbedarf im Netzwerk bedingt auch steigende Anforderungen an die Administration und die Überwachung der Netzwerkkomponenten. Dies kann z.B. durch den Einsatz von SNMP in Version 3 mit Authentifizierung erfolgen. Im Weiteren wird eine grundlegende Konfiguration von „SNMP v3“ 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.

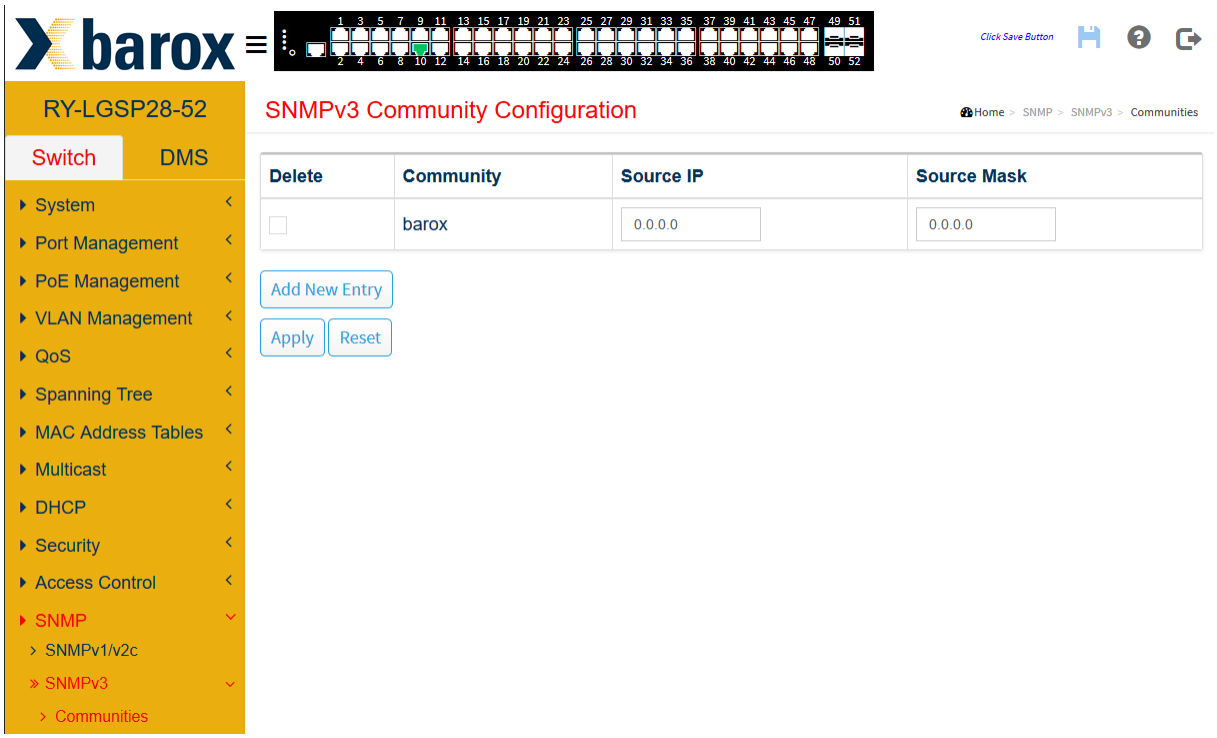
5.5.1. Aktivierung der „SNMP v3“-Funktion

Grundlegend ist der SNMP Modus zu aktivieren. Die Texteinträge der Read- und Write-Community (standard „public“ und „private“) müssen zudem gelöscht und die Write-Community auf den Status „Disabled“ gesetzt sein.



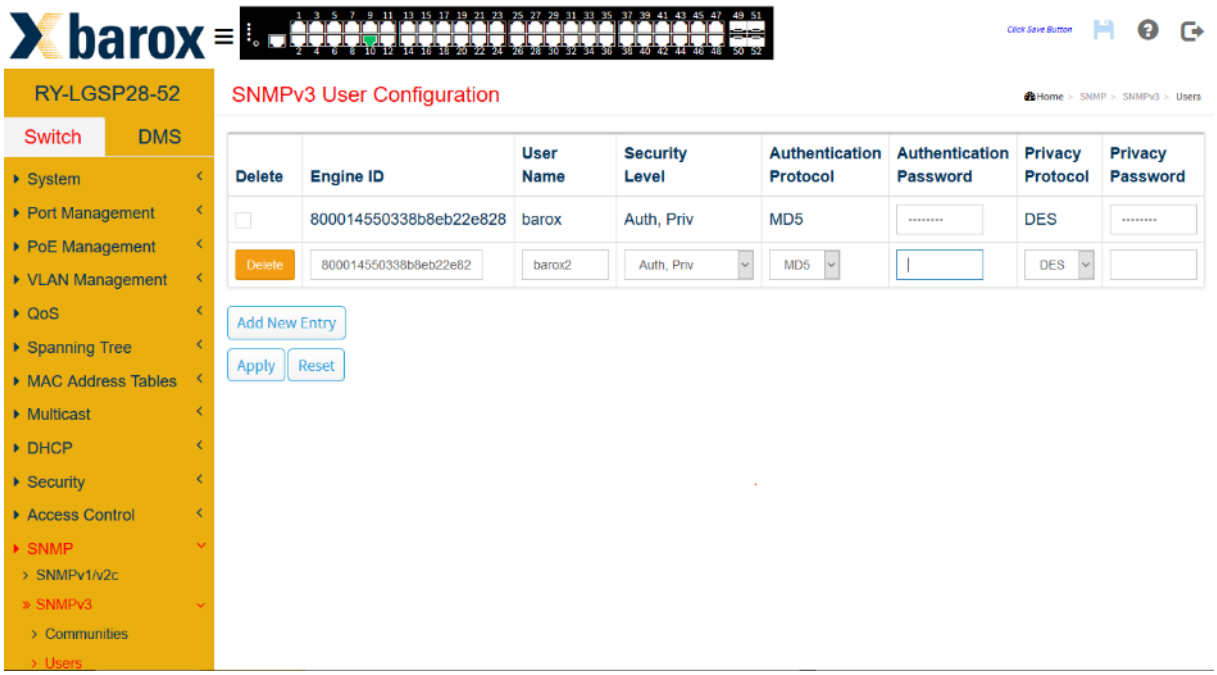
Erstellen einer dedizierten Community

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



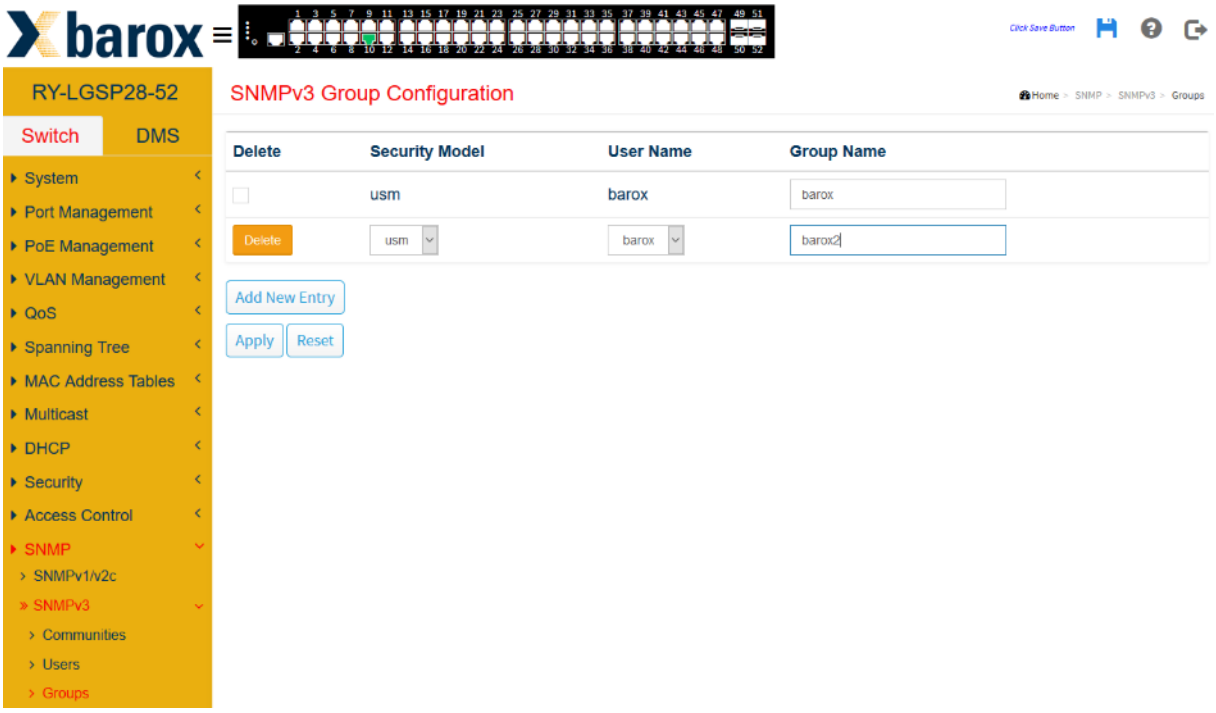
Anlegen eines neuen Benutzers

Bei der Konfiguration des neuen Benutzers ist zu beachten, dass dem neuem Benutzerobjekt die Engine-ID automatisch hinzugefügt wird. Neben der Festlegung des Benutzernamens soll der Sicherheitsgrad, hier im Beispiel *„Auth, Priv“* eingestellt werden. In der Auswahl des Authentifizierungs- „MD5“ und des Privacy-Protokolls DES ist zu beachten, dass beide Passwörter mindestens 8 Zeichen (Ziffern und Buchstabenkombinationen) lang sein müssen.



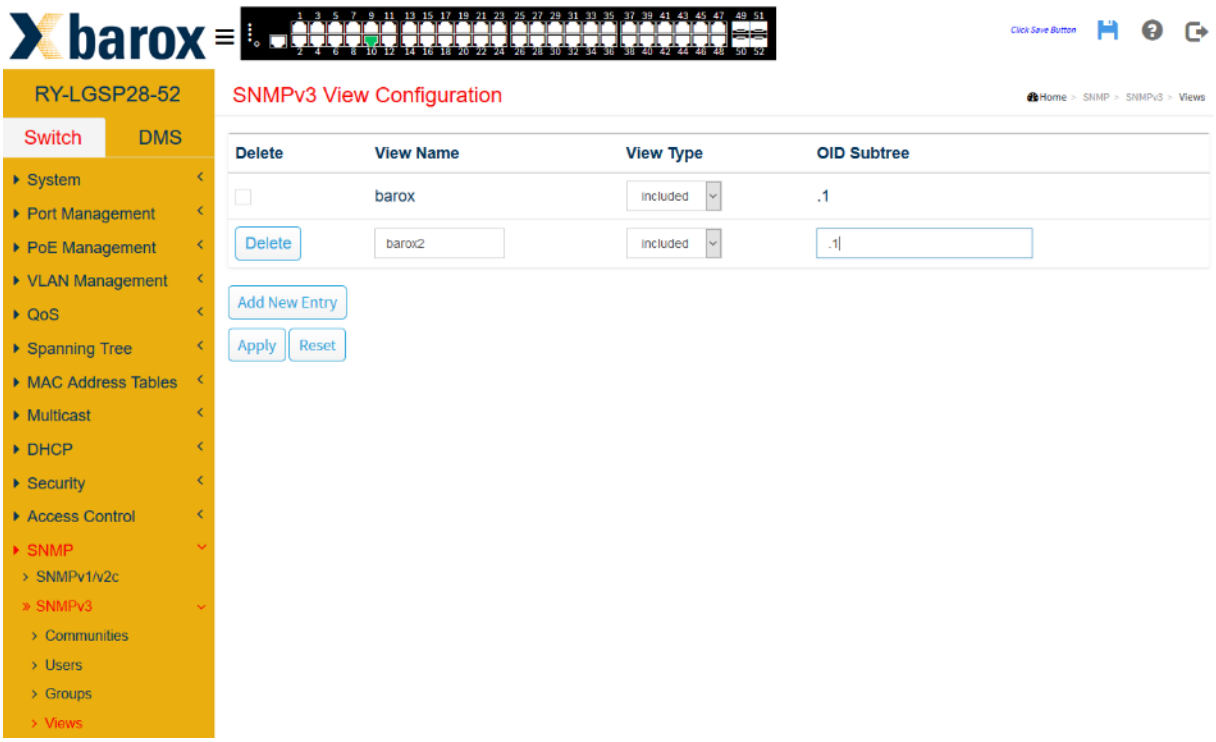
Anlegen einer Gruppe

Zur Konfiguration einer neuen Gruppe im SNMP v3 soll als Sicherheitsmodell *„usm“* ausgewählt werden. Der vorher erstellte Benutzername ist als *„Security Name“* auszuwählen. Anschließend muss ein Gruppennamen vergeben werden.



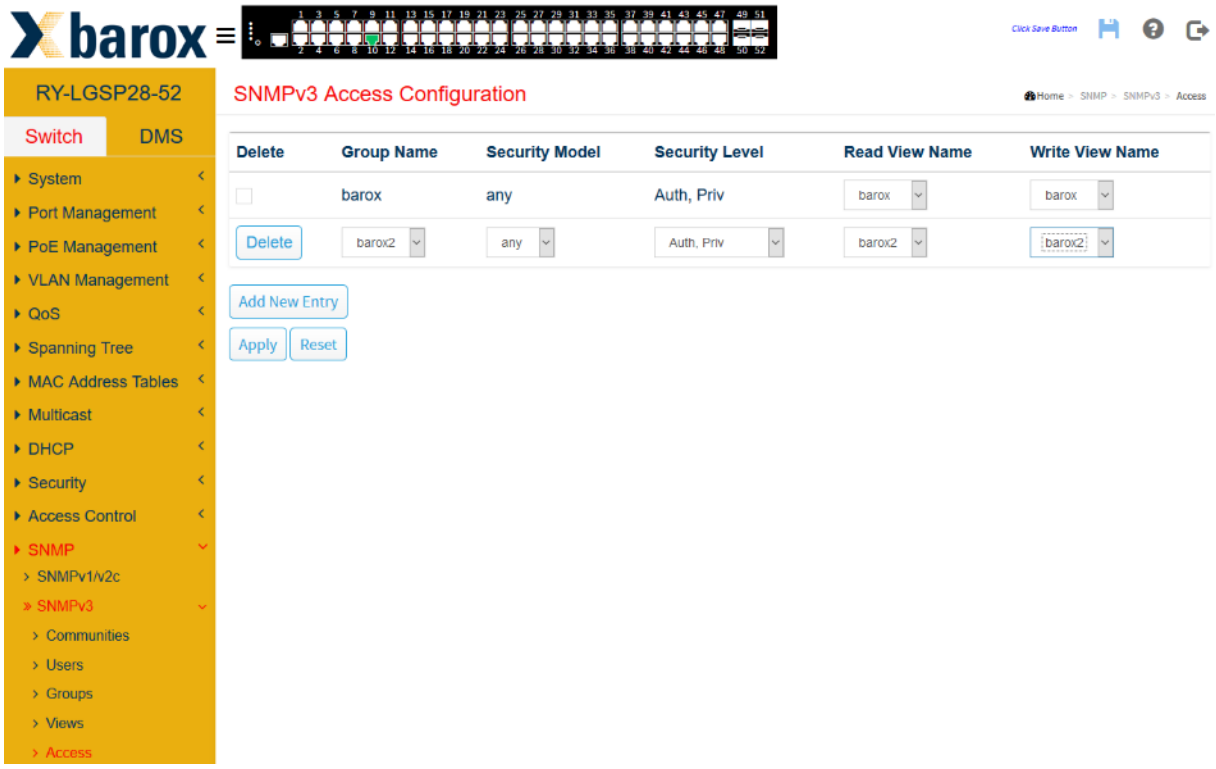
Einstellen der View-Konfiguration

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

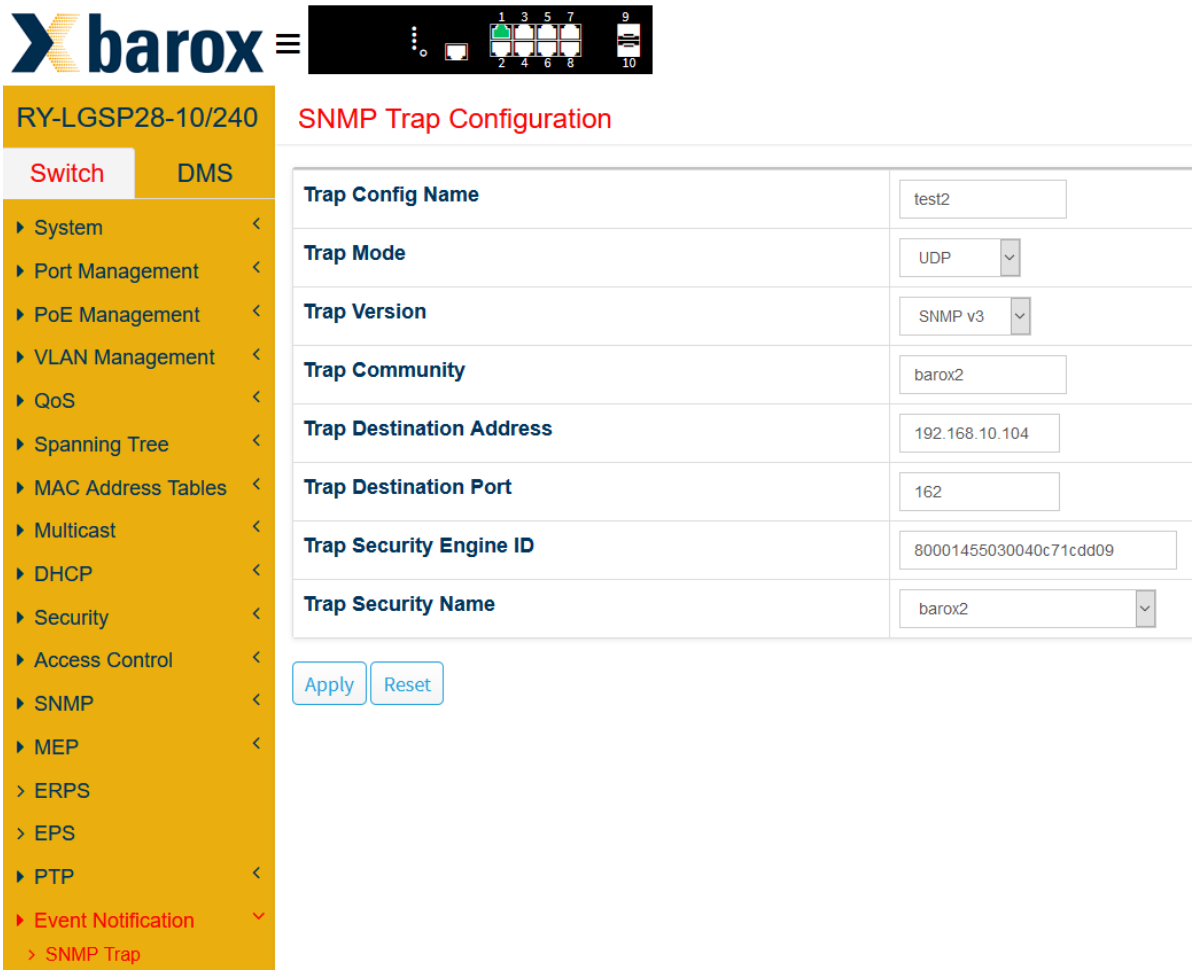
Hierzu soll ein neuer Eintrag mit der Authentifizierungs- und Privatisierungsmethode generiert werden. Zunächst ist die zuvor erstellte Gruppe unter „Group Name“ auszuwählen. Weiter wird der Gruppe das *„Security Model“* – **„usm“** und dem *„Security Level“* – **„Auth, Priv“** zugewiesen. Letztens werden für das Lesen und Schreiben die vorher erstellten Views, unter „Read View Name“ und „Write View Name“ ausgewählt.



5.5.2. Konfiguration der SNMP-Traps

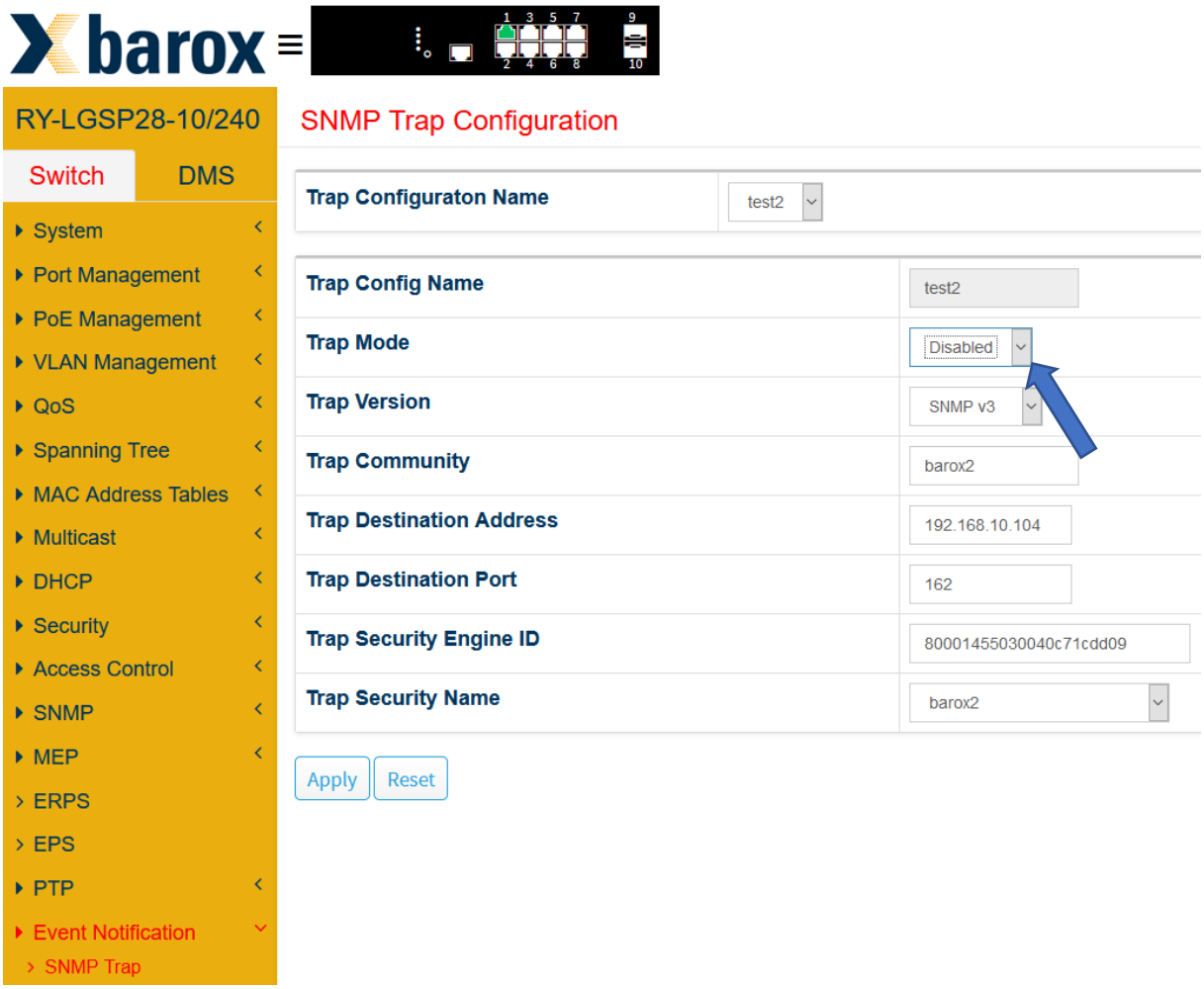
Am Beispiel nachfolgend sind folgende Werte für eine neue Konfiguration einzustellen:

- Trap Config Name -> Ein Name soll vergeben werden
- UDP oder TCP – für den Anfang wie gebräuchlich UDP
- Trap Version -> Auswahl von SNMP v3
- Trap Community -> der vorher angelegte Community Name muss eingetragen werden
- Trap Destination Address -> Angabe der IP-Adresse des Trap-Empfängers
- Trap Destination Port -> Angabe des Ports für den Empfänger
- Trap Security Engine ID -> hier ist die Engine-ID eingetragen
- Trap Security Name -> Auswahl des jeweiligen USM-Users
- Anschließend werden die Einstellungen mit „Apply“ bestätigt



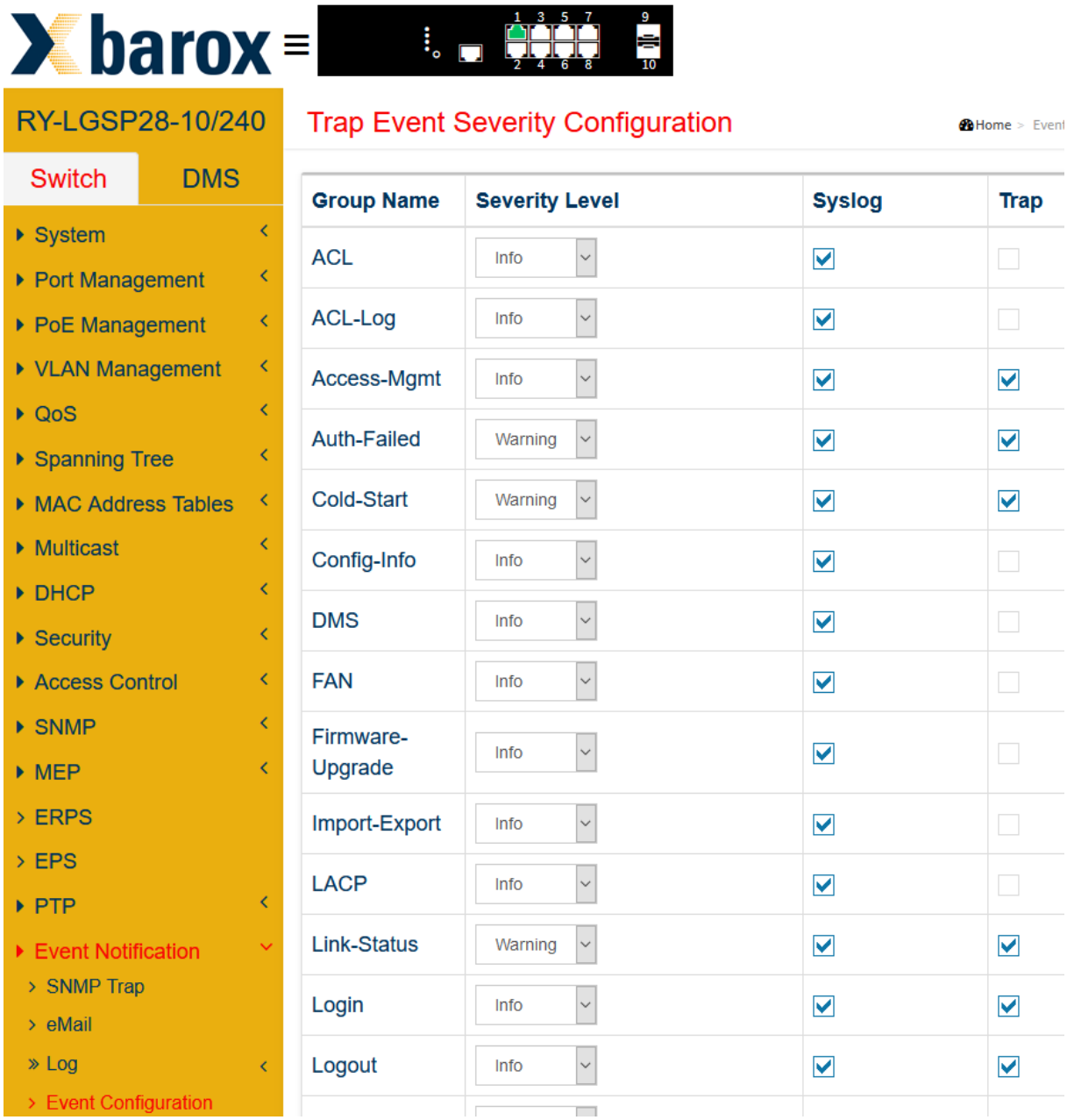
Deaktivierung der SNMP-Trap-Funktion

Die Deaktivierung kann auf zwei Wegen erfolgen. Zu einem kann Sie durch das Löschen der Konfiguration deaktiviert werden. Sollte der Trap-Versand nur sporadisch verwendet werden müssen, so empfiehlt es sich, die Funktion in der Konfiguration auf „Disabled“ zu setzen.



5.5.3. Ergänzende Hinweise zum Senden von SNMP-Traps

Vergewissern Sie sich, dass die Ereignisse, die den SNMP-Trap-Versand auslösen, entsprechend konfiguriert sind. Diese Einstellungen können im Konfigurationsmenü 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.



5.6 Auslesen von SNMP-Traps

Über das SNMP-Protokoll lassen sich verschiedenste Konfigurationsparameter der barox Switche auslesen, bzw. einstellen. Grundlegend werden dafür sogenannte „SNMP/MIB-Browser“ benötigt. Aber auch Netzwerk-Mitschnitt- bzw. Sniffer-Software kann für das Lesen von SNMP-Übertragungen verwendet werden.

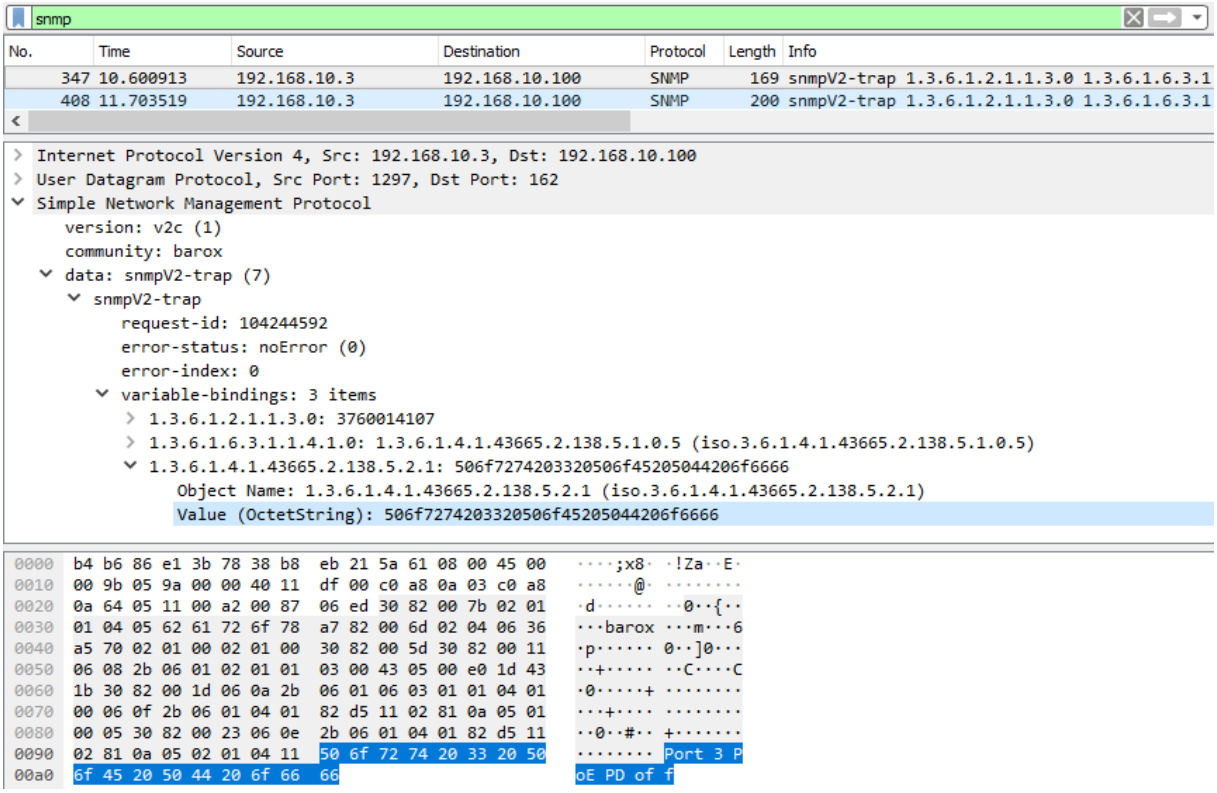
Das Auslesen einer SNMP v2-Trap wird im folgenden Beispiel kurz erläutert:

Ausgangslage:

Eine PoE-Kamera wird vom Ethernet-Port 3 des Switches 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 ***„iReasoning MIB Browser“ (http://www.ireasoning.com/mibbrowser.shtml) verwendet.

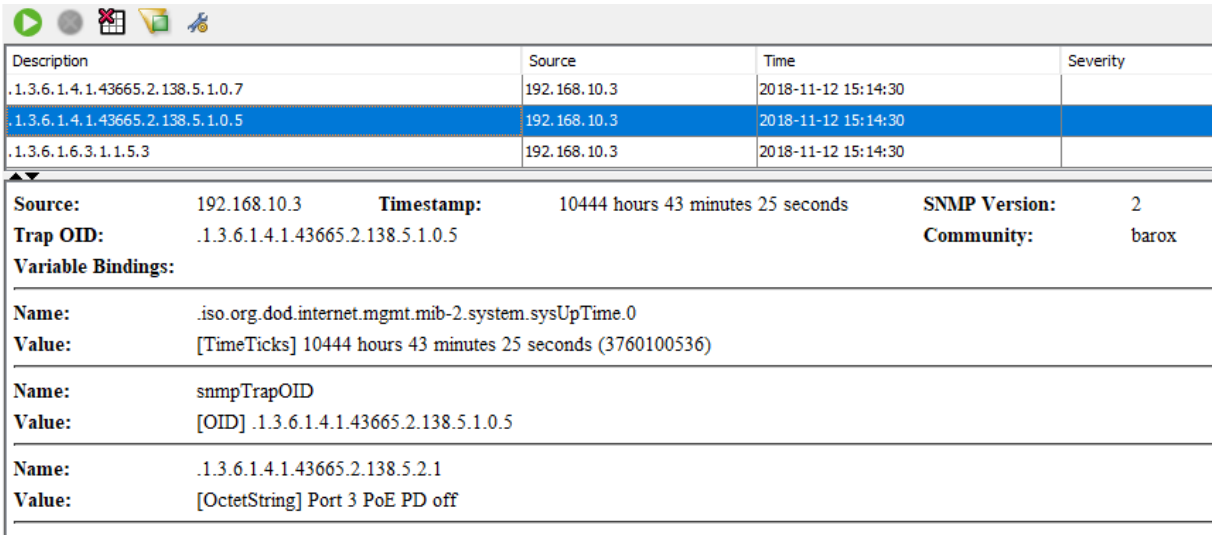
PoE-Kamera wird getrennt/ PD-Gerät offline:

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:



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:

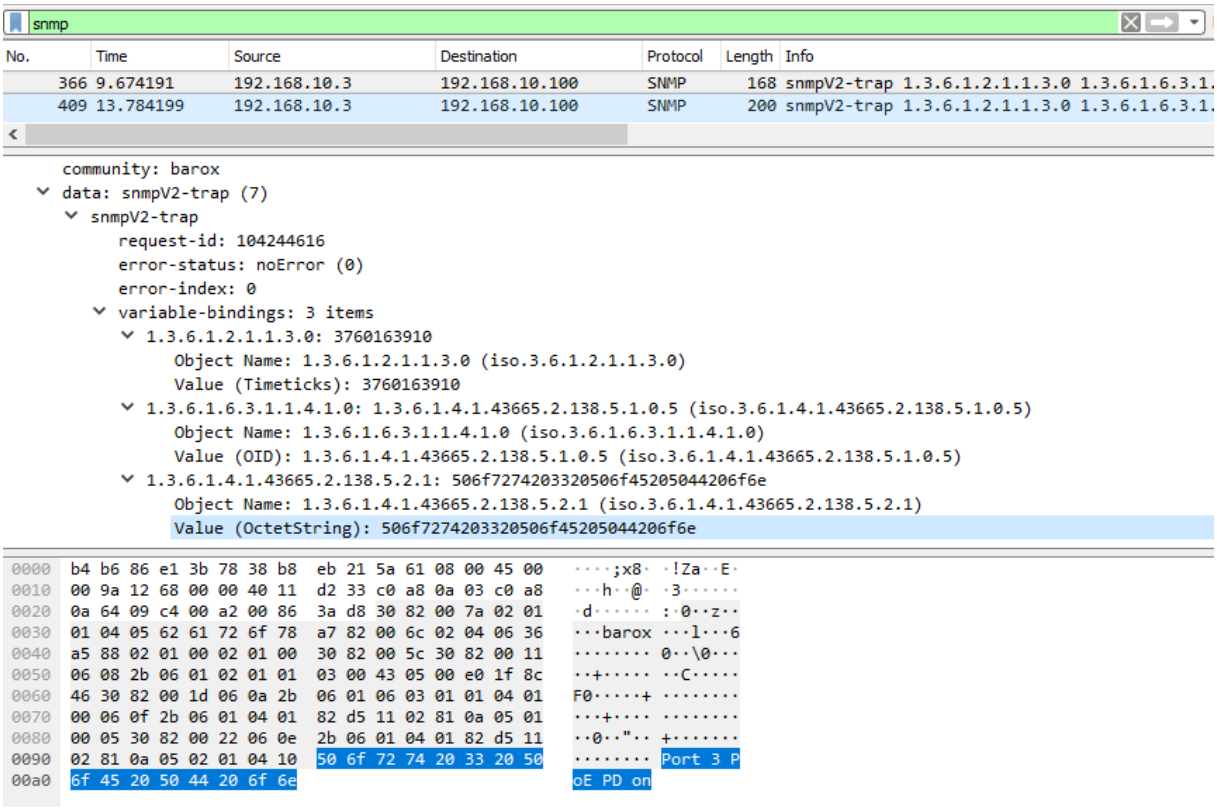
Name: .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0
Value: [TimeTicks] 10444 hours 43 minutes 25 seconds (3760100536)

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-Kamera wird wieder verbunden/ PD-Gerät online:

Mitschnitt der Informationen, welche vom Switch gesendet werden:



snmp

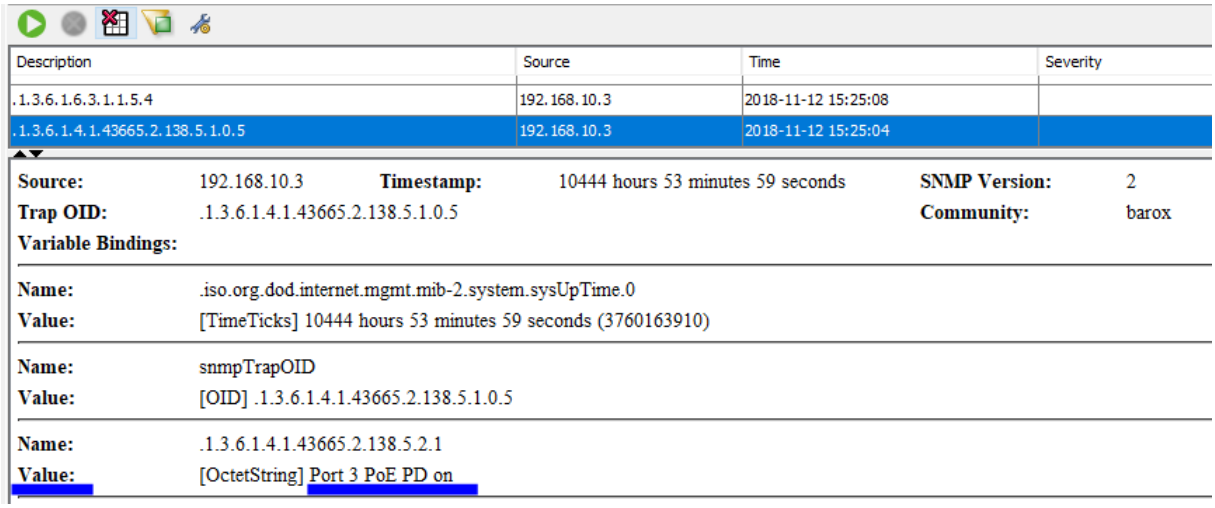
No.	Time	Source	Destination	Protocol	Length	Info
366	9.674191	192.168.10.3	192.168.10.100	SNMP	168	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.
409	13.784199	192.168.10.3	192.168.10.100	SNMP	200	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.

```
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
```

Ansicht der Information im SNMP-Browser:

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



Description	Source	Time	Severity
.1.3.6.1.6.3.1.1.5.4	192.168.10.3	2018-11-12 15:25:08	
.1.3.6.1.4.1.43665.2.138.5.1.0.5	192.168.10.3	2018-11-12 15:25:04	

Source: 192.168.10.3 **Timestamp:** 10444 hours 53 minutes 59 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 53 minutes 59 seconds (3760163910)

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 on

5.7 Verwendung von MIB-Dateien zum Auslesen und zur Steuerung der Switche

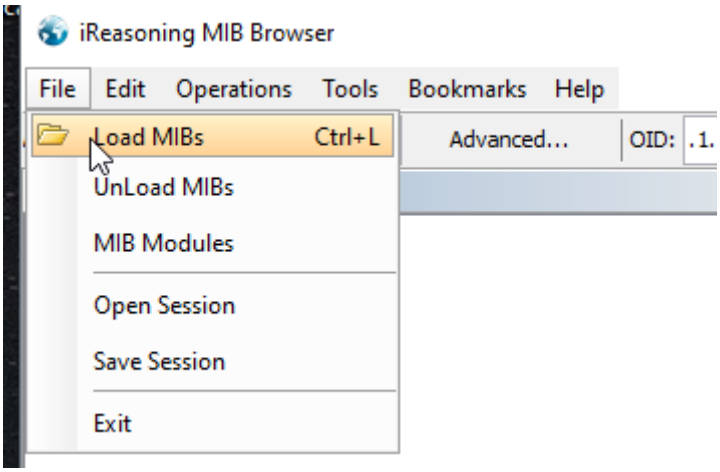
Grundsätzlich können Statusabfragen im Netzwerk bei verwaltbaren Geräten wie Switchen, Router oder Server meist über die SNMP-Funktionalität erfolgen. Oftmals werden aus sicherheitstechnischen oder herstellerspezifischen Aspekten sogenannte MIB-Dateien (MIB-Files) für die Abfrage der Geräte benötigt. Diese Dateien enthalten die Informationen über die Identifikationskennzahlen der Funktionen.

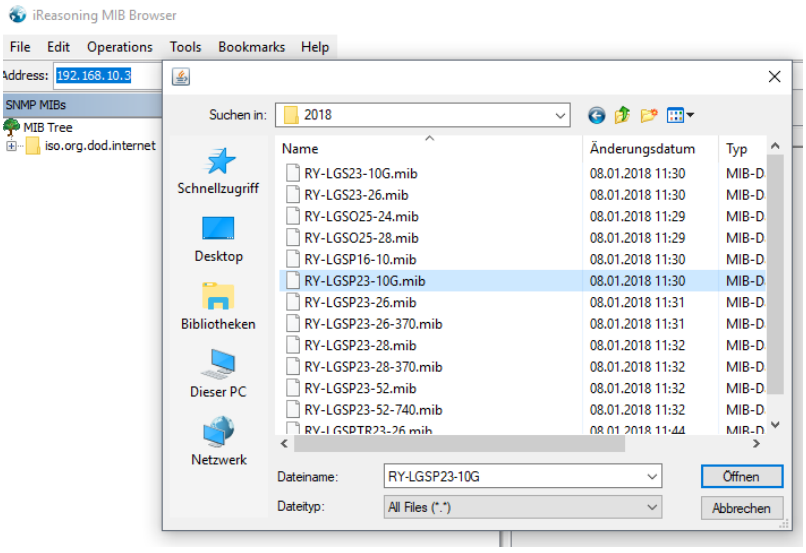
Abfrage der Switch-Statusfunktionen über SNMP (unter Verwendung von MIB-Dateien)

Zur Einführung empfiehlt sich grundlegend der Einsatz eines MIB-Browsers. Im folgenden Beispiel wird der *„iReasoning 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 der MIB-Datei

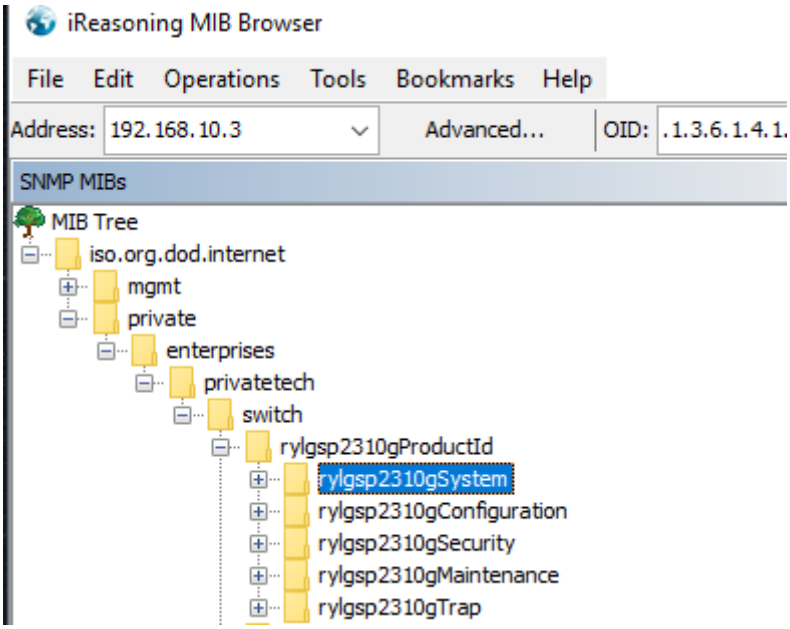
Beim Import ist darauf zu achten, dass die passende MIB-Datei für den entsprechenden Switch ausgewählt wird. Die erforderlichen MIB-Dateien sind am *„.mib“* Postfix zu erkennen.





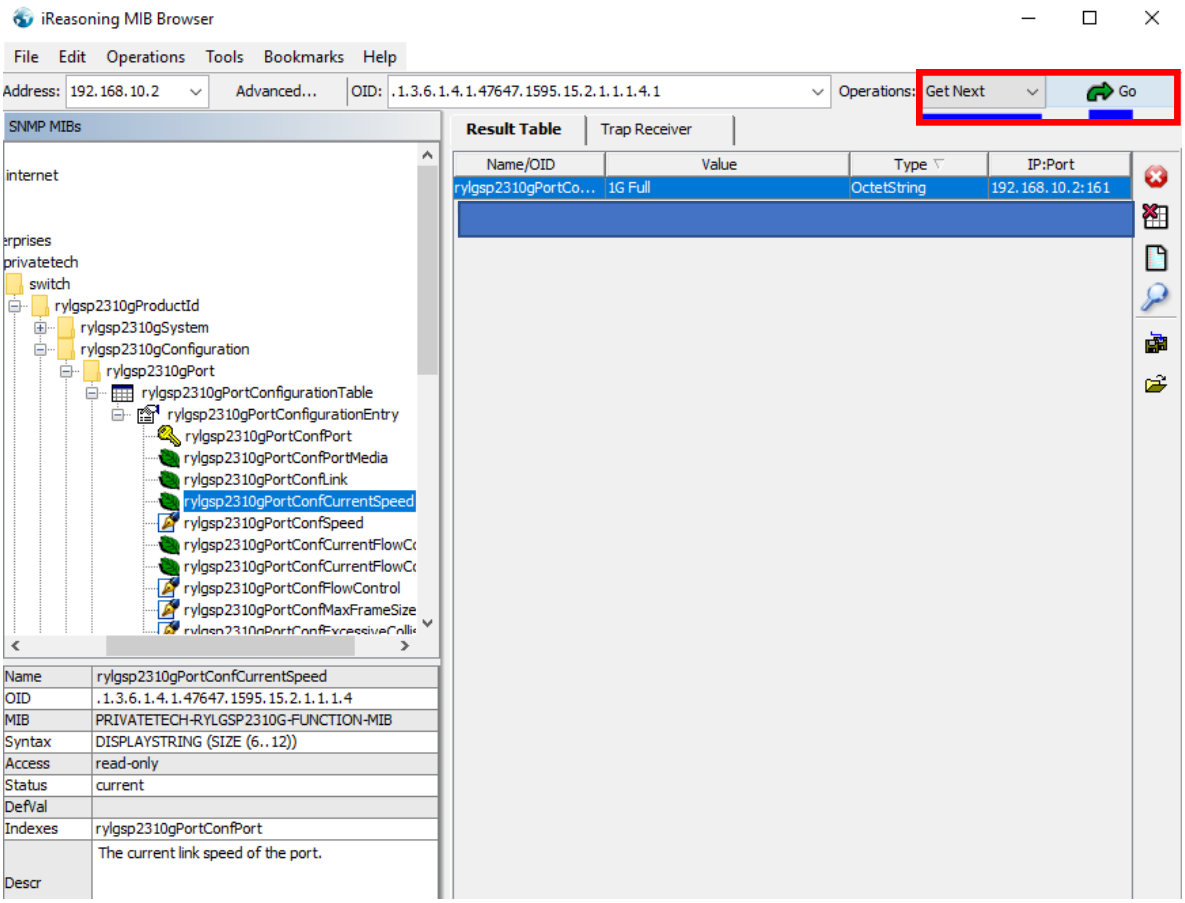
* Bitte beachten Sie bei Verwendung der Software die jeweiligen Lizenzbestimmungen der Softwareanbieter!

Nach dem erfolgreichem Import sind die MIB-Strukturen wie nachfolgend abgebildet ersichtlich:



Schritt 2: Abfragen generieren

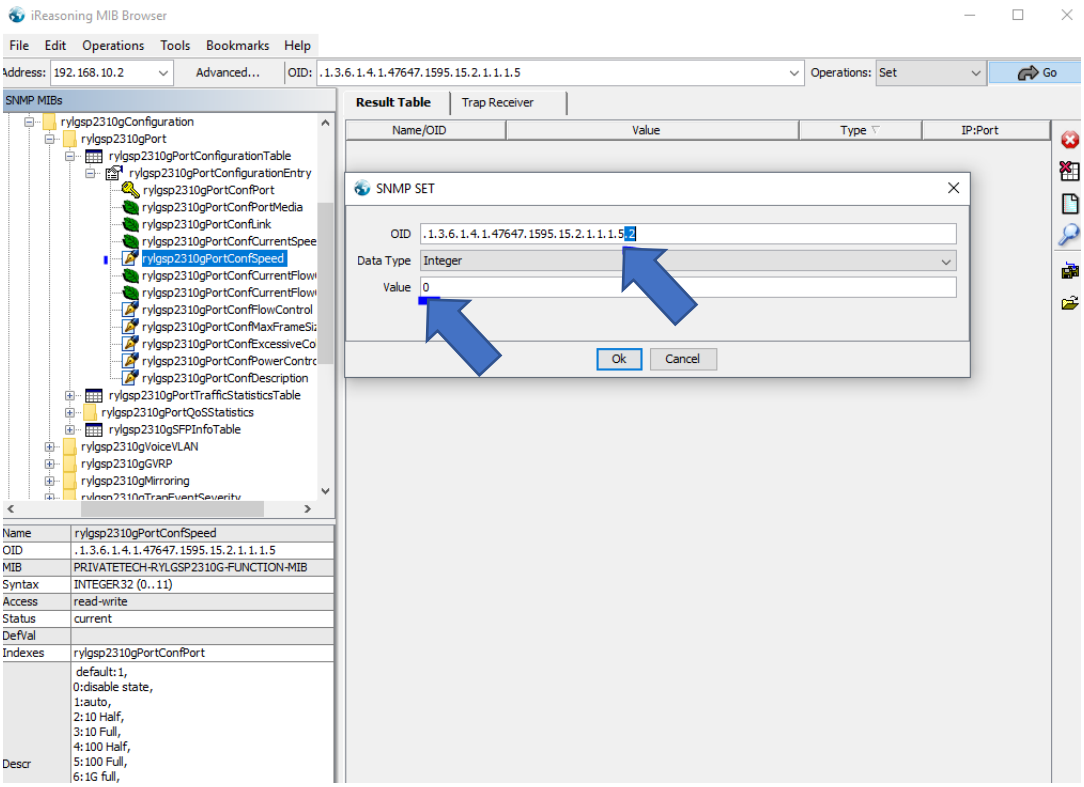
Zur Erzeugung einer Abfrage wird zunächst der gewünschte Status ausgewählt und dann mit der *„Get Next“*-Operation und dem Klick auf *„Go“* die Abfrage generiert. Nach erfolgreicher Abfrage erscheinen die Informationen zum Status in der Resultatstabelle, wie im folgenden Beispiel abgebildet:



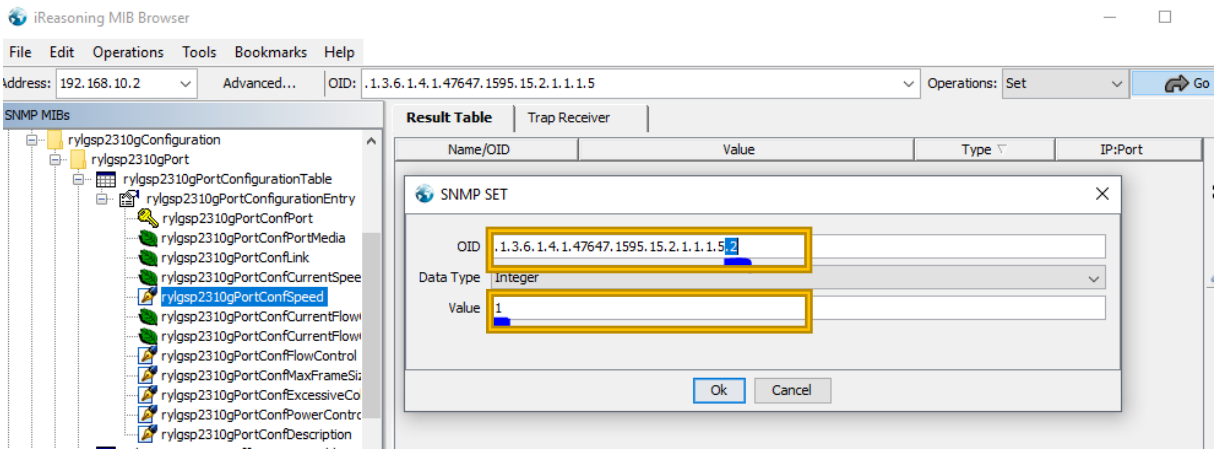
5.8 Switch-Funktionen über SNMP und MIB mit der „SET“-Operation steuern

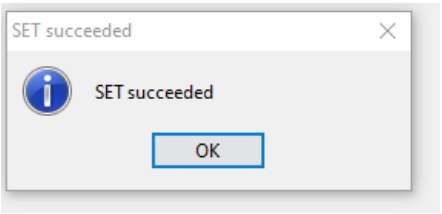
Als weitere Methode zur Steuerung der barox Switche kann die Operation „SET“ über das SNMP-Protokoll erfolgen. Voraussetzungen sind die grundlegende SNMP-Konfigurationen am Switch und des MIB-Browsers. Nachfolgend ist ein Beispiel mit dem Einsatz der SET-Operation aufgeführt, welches eine Portabschaltung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

Zur Deaktivierung des Ports 2 am Switch 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 eine entsprechende Erfolgsmeldung generiert.



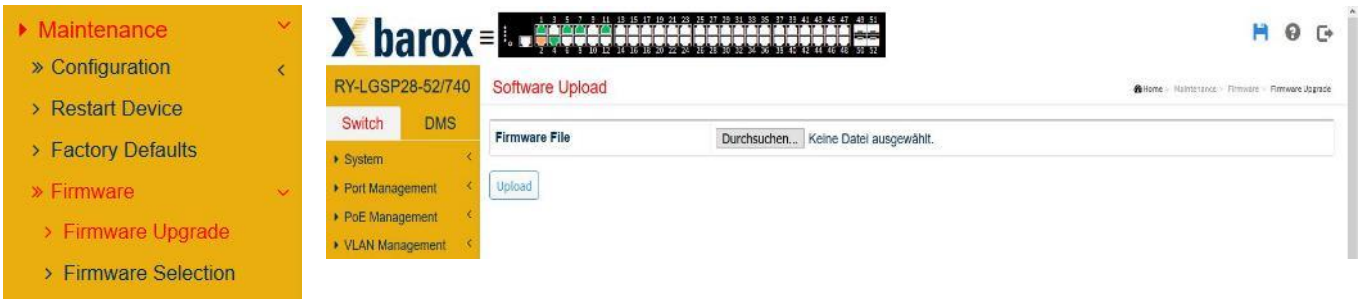
Zur Aktivierung des Ports 2 am Switch wird die Portkonfiguration im MIB-Verzeichnis gesucht. Dabei ist zu beachten, dass der zugehörige Informationsblog mit Schreibfunktion ausgewählt ist. Die Set-Operation wird durch den Klick auf *„Go“* geöffnet und der OID-Eintrag mit *„.2 “* (Kennzeichnung des Ports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



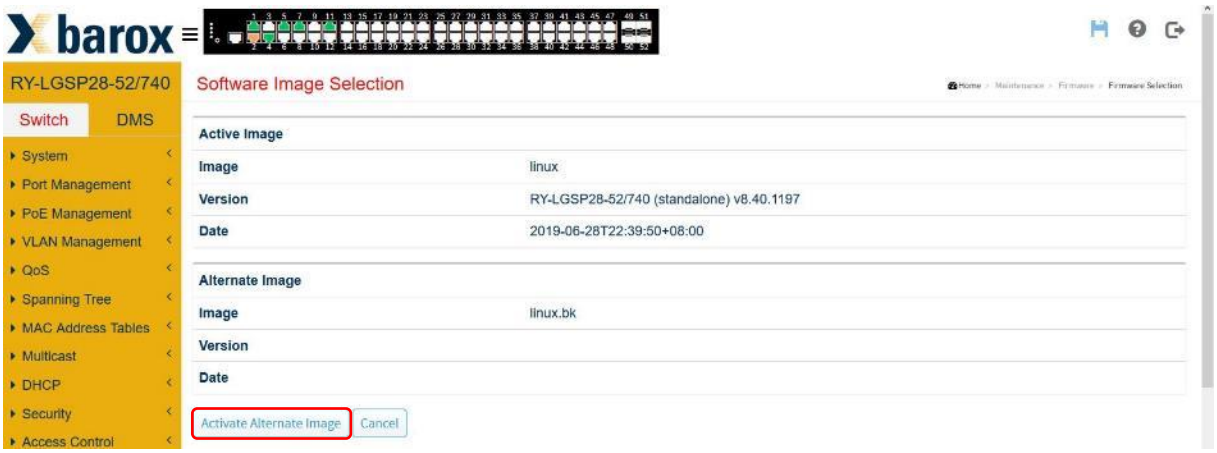


6 Firmware-Upgrade

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 Menüpunkt „Firmware Selection“ reaktiviert werden.



7 Werkeinstellung

Die Switche können jederzeit wieder auf die Werkseinstellung zurückgesetzt werden.

Entweder per Software im 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 Werkseinstellung zurückgesetzt.

8 GARANTIE

barox Kommunikation gewährleistet, dass das Produkt für die Dauer der landes-spezifischen 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.