



Mode d'emploi

RY-LGSP28-10

RY-LGSP28-28

RY-LGSP28-52/xxx (EOL)

RY-LGS038-10

RY-LGSP38-28

RY-LGSPTR38-52/740



Switches 19" :

switches RY de la série 28 et de la série 38

Version du firmware à partir de la v8.40.1589

Version du hardware à partir de la v1.02

Version mécanique à partir de la v1.01

Version du firmware PoE à partir de la v208-211

Copyright © barox Kommunikation

Tous droits réservés. Toute reproduction sous quelque forme ou par quelque moyen que ce soit est interdite sans l'autorisation de barox Kommunikation.

Protection de la marque

barox® est une marque déposée de barox Kommunikation.

Toutes les autres marques de commerce ou marques déposées mentionnées dans ce manuel sont la propriété de leurs propriétaires respectifs.

Responsabilité

Les informations contenues dans ce document sont sujettes à modification sans préavis barox Kommunikation se réserve le droit d'apporter des modifications aux appareils et/ou au manuel sans préavis.

Notre produit peut contenir des erreurs techniques et/ou typographiques involontaires.

Des changements sont régulièrement apportés pour améliorer notre produit.

Le mode d'emploi actuel est toujours disponible sur notre site Internet.

www.barox.ch

www.barox.ch/fr

Éditeur :

barox Kommunikation AG

Im Grund 15

CH-5405 Baden-Daettwil

Suisse

www.barox.ch

Date de publication : Janvier 2025

Version : 1.2

TABLE DES MATIÈRES

1	INTRODUCTION	5
1.1	Contenu	5
1.2	À propos de nous	5
1.3	Site Internet	5
1.4	Assistance	5
2	Description sommaire	5
2.1	Particularités des réseaux vidéo	5
2.2	DMS (Device Management System)	6
3	Mise en service	6
3.1	Réglages d'usine et login	6
3.2	System Information	7
3.3	Attribuer une adresse IP fixe ou DHCP	7
3.4	Réglage de l'heure	9
3.4.1.	Paramètres locaux	9
3.4.2.	NTP (Network Time Protocol)	9
3.5	Configuration des ports	10
3.5.1.	Port SFP	11
3.6	Changer le nom d'utilisateur et le mot de passe	11
3.7	Loop Protection	12
3.8	Configuration en anneau	13
3.8.1.	Ring Master	13
3.8.2.	Configuration des ports	14
3.9	Configuration VLAN	16
3.10	Power over Ethernet (PoE)	16
3.10.1.	Configuration PoE	17
3.10.2.	PoE Power Delay	18
3.10.3.	PoE Schedule	18
3.10.4.	PoE Auto Checking	19
3.11	Sauvegarde et chargement de la configuration	19
3.11.1.	Téléchargement de la configuration	20
3.11.2.	Importer la configuration (upload)	20
4	DMS Device Management System	21
4.1	Gestion	21
4.2	Surveillance graphique	23
4.3	Maintenance	27
5	La gestion des switches au cœur de la sécurité	28
5.1	Gestion et protection au niveau du switch (Layer 1 et 2)	28
5.1.1.	Paramètres et limites de la bande passante	28
5.1.2.	Notes sur la prise en compte générale des besoins en bande passante	29
5.1.3.	Protection des ports via les paramètres de configuration MAC	29
5.1.4.	Sécurité des ports avec paramètres de Limit Control	35
5.1.5.	Private VLAN avec Port Isolation	36
5.2	Utilisation et protection des fonctions IP (Layer 3)	37
5.2.1.	Serveur DHCP	37
5.2.2.	Protection du DHCP par inspection ARP	39
5.2.3.	IP Source Guard	42
5.3	Protection de la gestion des switches et administration réseau (layer 3 – 7)	44
5.3.1.	Administration et configuration des utilisateurs	44
5.3.2.	Utilisation et paramétrage de l'authentification au niveau de la gestion des switches	46
5.3.3.	Gestion des accès et utilisation de HTTPS	48
5.3.4.	Configuration et déploiement de l'accès à la gestion basé sur les certificats	49
5.4	SNMP - Fonction de surveillance et d'administration	50
5.4.1.	Configuration SNMP v2c	50
5.4.2.	Configuration de la Trap SNMP	51

5.4.3. Informations supplémentaires pour l'envoi de Traps SNMP	55
5.5 Configuration SNMP v3	56
5.5.1. Activation de la fonction SNMP v3	56
5.5.2. Configuration de la Trap SNMP	60
5.6 Lecture des Traps SNMP	63
5.7 Utilisation de fichiers MIB pour la lecture et le contrôle des switches	66
5.8 Commande des fonctions du switch via SNMP et MIB en utilisant l'opération "SET"	68
6 Mise à niveau du firmware	70
7 Réglages d'usine	70
8 GARANTIE	71

1 INTRODUCTION

Ce mode d'emploi décrit la mise en service des switches et la configuration des principales fonctions de base.

L'utilisateur de ce manuel doit avoir les connaissances suivantes :

- Connaissance de l'installation et de la manipulation de dispositifs électroniques
- Familiarité avec les systèmes informatiques
- Connaissance des Local Area Networks (LAN) et connaissances de base en communication IP
- Savoir utiliser un navigateur Web

1.1 Contenu

La notice d'utilisation est divisée en chapitres suivants :

- 1.Introduction
- 2.Mise en service des switches
- 3.Options de diagnostic et mise à niveau du firmware

1.2 À propos de nous

Partout où les réseaux doivent être transportés rapidement et en toute sécurité pour une transmission vidéo de la plus haute qualité, barox Kommunikation assure, avec ses switches POWERHAUS, des connexions révolutionnaires.

barox planifie, coordonne et fournit des connexions point à point simples ainsi que des réseaux étendus avec des applications multicast.

1.3 Site Internet

Des informations sur l'ensemble de la gamme de produits Switch ainsi que des liens pour télécharger les fiches techniques, la documentation et le firmware actuel sont à votre disposition sur notre site Internet <http://www.barox.ch/fr/fr>.

1.4 Assistance

Nos partenaires POWERHAUS sont à votre disposition pour d'éventuels problèmes ou questions concernant la configuration des switches.

2 Description sommaire

Tous les switches RY sont des commutateurs IP Full-Gigabit avec fonctions Layer 2/2+, équipés de différents nombres de ports optiques et électriques, pouvant être gérer et supportant jusqu'à PoE++ selon le modèle.

2.1 Particularités des réseaux vidéo

• Surveillance active de la caméra

Les caméras alimentées par le switch via PoE sont surveillées en permanence. En cas de panne de la caméra, le switch redémarre automatiquement la caméra. En cas d'échec, le switch envoie un message d'alerte via SNMP.

• Surveillance active de l'alimentation PoE

Si, par exemple, une caméra défectueuse nécessite trop de puissance de la part du switch, ce dernier émet une alerte via SNMP.

• Gestion active de la puissance PoE

Lorsque le switch démarre, les ports PoE individuels peuvent être démarrés avec une temporisation pour éviter une surcharge des blocs d'alimentation PoE.

- **Autres caractéristiques utiles**

Les trames Jumbo jusqu'à 9600 octets sont prises en charge à 1 Gbits et également à 100 Mbits. Sécurité des ports par restriction d'adresse MAC et détection IP.

Lisibilité ou fourniture de certificats.

Performances Backplane très élevées pour une transmission vidéo fluide lors d'occupation totale des ports

Possibilité de voir quels ports reçoivent PoE en appuyant sur un bouton (panneau avant).

2.2 DMS (Device Management System)

Le switch dispose d'un système intégré de surveillance et de contrôle du réseau qui donne à l'utilisateur une vue d'ensemble très simple de la totalité du réseau.

L'aperçu de la topologie du réseau permet une vue d'ensemble rapide de tous les switches et terminaux disponibles sur le réseau, tels que les caméras IP ou les serveurs, avec des détails sur l'adresse IP, le type de périphérique et le nom du périphérique. Les plans d'étage et les plans d'environnement peuvent être stockés sous forme d'images d'arrière-plan, avec lesquelles l'utilisateur peut accéder rapidement à certains périphériques réseau même sans connaître la structure IP. Les plans finis peuvent être exportés à nouveau et il est possible d'y joindre des documents.

3 Mise en service

Les switches peuvent être configurés à l'aide d'un navigateur Web. Pour cela, le PC/ordinateur portable peut être connecté à n'importe quel port RJ45. Veuillez faire attention à ce que le PC/ordinateur portable avec l'adresse IP se trouve dans le même segment de réseau que le switch. Par exemple : 192.168.1.111

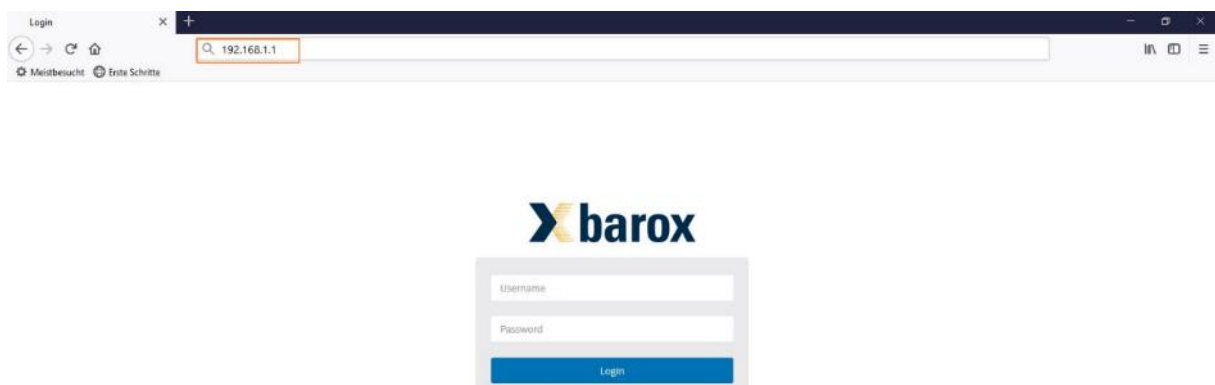
Sinon, les switches peuvent également être configurés via CLI (port console). Cette documentation explique comment configurer le switch à l'aide d'un navigateur Web.

3.1 Réglages d'usine et login

Les switches ont les réglages d'usine suivants :

Adresse IP :	192.168.1.1
Masque de sous-réseau :	255.255.255.0
Utilisateur :	admin
Mot de passe :	admin

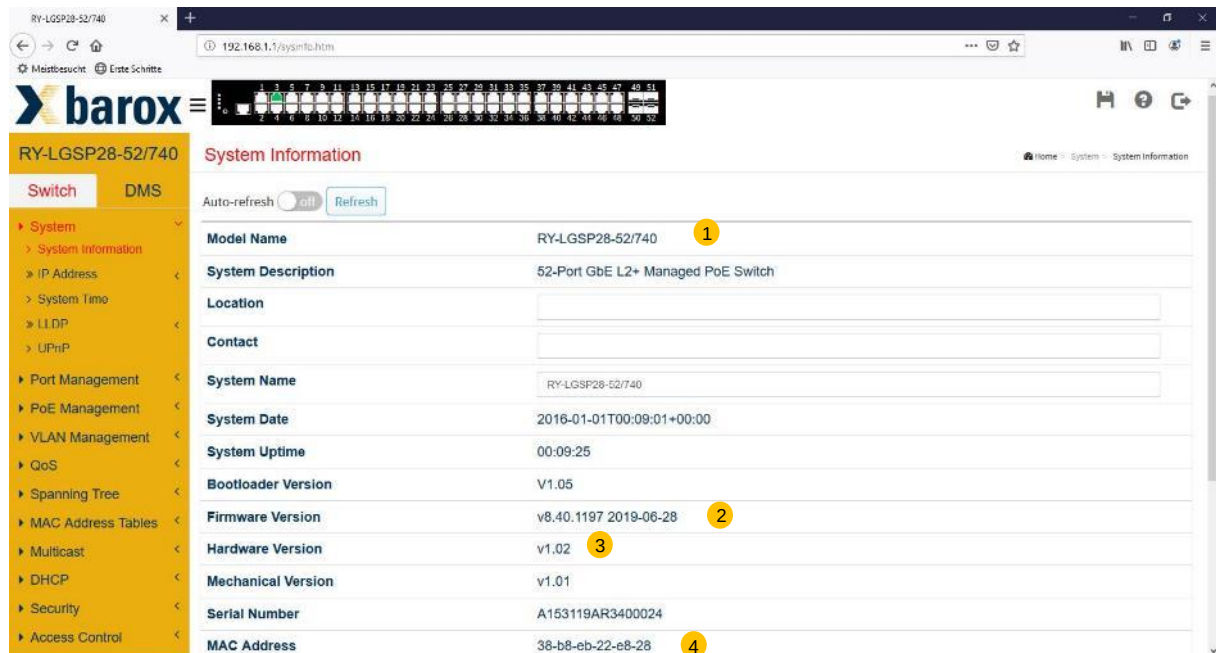
En entrant l'adresse IP du switch (192.168.1.1) directement dans le navigateur Web, la connexion au switch s'établit. L'identification s'effectue en saisissant le nom d'utilisateur et le mot de passe.



Une fois la connexion réussie, la page "System Information" s'affiche automatiquement et présente les principales informations concernant le switch.

3.2 System Information

Cette page permet de voir les principales informations concernant le switch.

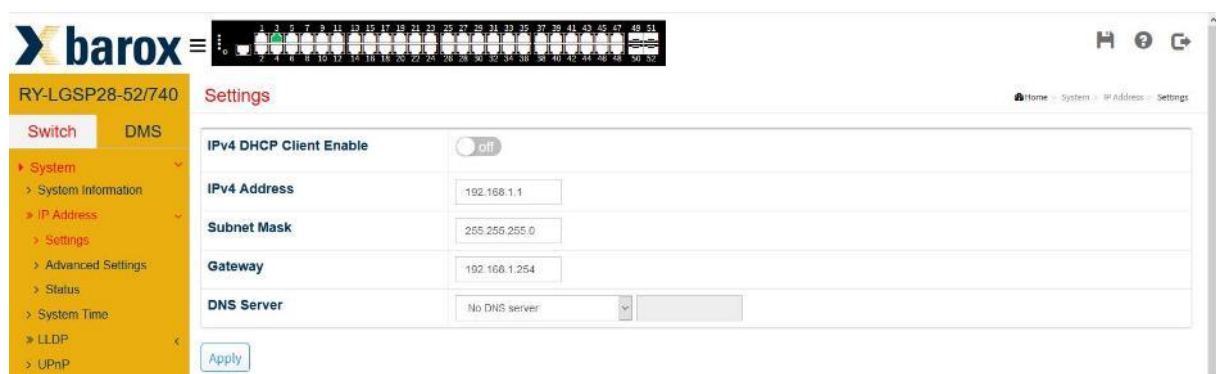


Légende :

1. Nom du modèle du switch
2. Version du firmware
3. Version du matériel
4. Adresse MAC

3.3 Attribuer une adresse IP fixe ou DHCP

La première étape consiste à attribuer une adresse IP au switch. Pour ce faire, sélectionnez le point de menu "Switch/System/IP Address/Settings" dans l'arborescence.



Adresse IP fixe

L'image ci-dessus montre que le switch possède l'adresse IP 192.168.1.1, le masque de sous-réseau 24 (255.255.255.0) et l'adresse IP 192.168.1.254 comme passerelle.

Si une nouvelle adresse IP doit être attribuée au switch, l'adresse IP existante doit être écrasée et confirmée par l'icône "Apply". Il en va de même si le masque de sous-réseau ou l'adresse passerelle doivent être modifiés.

DHCP

Si le switch est intégré dans un réseau dans lequel un serveur DHCP attribue les adresses IP, l'interrupteur à coulisse "IPv4 DHCP Client Enable" doit être positionné sur "on".

Le serveur DHCP dans le réseau attribue au switch une adresse IP dans la plage prédéfinie. Il y a deux façons de trouver l'adresse IP reçue.

a) Outil logiciel, par exemple : SoftPerfect Network Scanner

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

b) Port console

On utilise à cet effet le câble de console fourni. Le port console du switch est une interface RS232. Il faut alors un PC/ordinateur portable équipé d'une interface de série ou un convertisseur USB-RS232.

En ce qui concerne le logiciel, nous recommandons "PuTTY" pour configurer le switch via le port CLI.

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

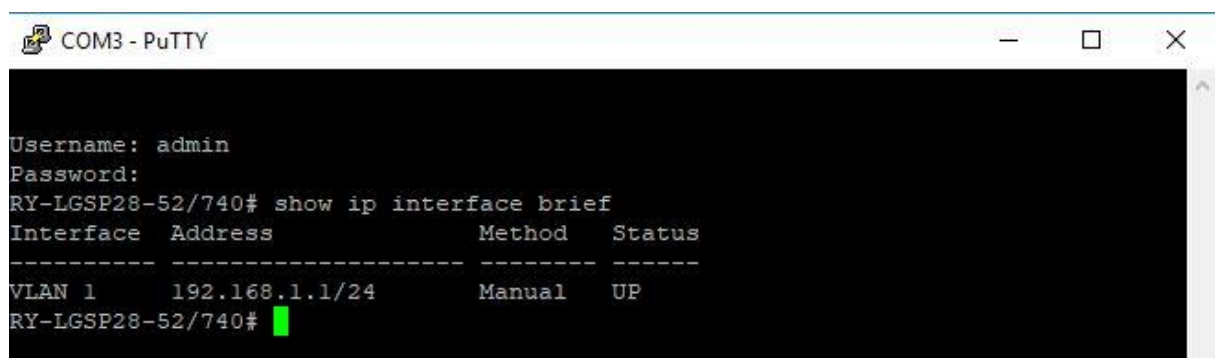
L'interface CLI est réglée en usine comme suit :

Bitrate :	115'200
Bits de données :	8
Parité :	aucune
Bits d'arrêt :	1
Contrôle de flux :	aucun

Une fois la connexion à l'interface de série établie, un login à l'aide d'un nom d'utilisateur et d'un mot de passe est nécessaire.

L'adresse IP peut être interrogée avec la commande suivante :

RY-LGSP28-52/740# **show ip interface brief**



```
COM3 - PuTTY
Username: admin
Password:
RY-LGSP28-52/740# show ip interface brief
Interface  Address                Method  Status
-----
VLAN 1     192.168.1.1/24         Manual  UP
RY-LGSP28-52/740#
```

➔ Important : la modification doit maintenant être sauvegardée définitivement.

Pour ce faire, accédez au switch via un navigateur Web avec la nouvelle adresse IP et cliquez sur le symbole de la disquette dans le coin supérieur droit.

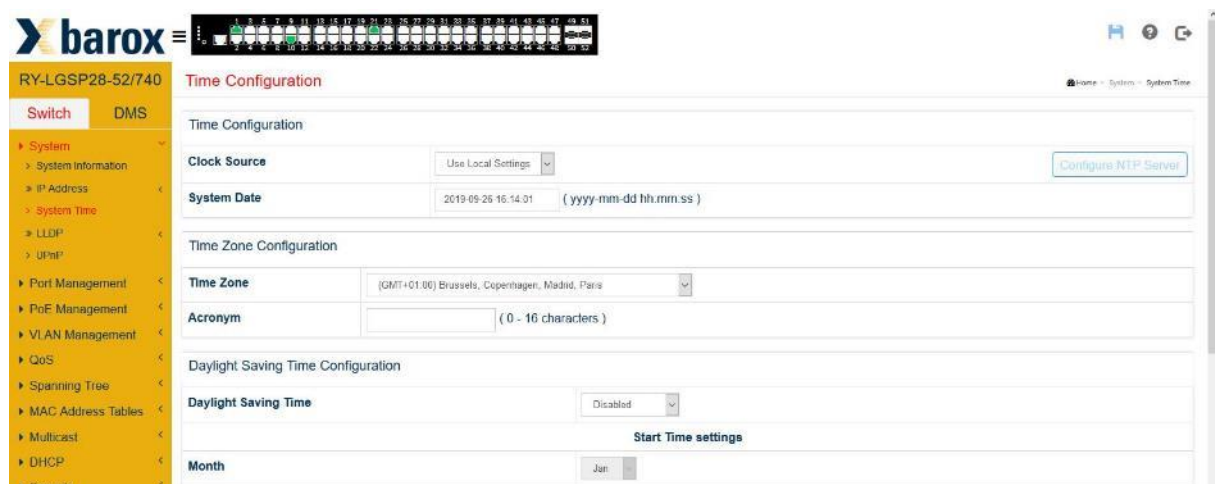
3.4 Réglage de l'heure

L'heure système des switches barox peut être enregistrée manuellement ou via un serveur NTP. La définition de l'heure sert au fichier journal. En cas de message d'erreur, l'entrée dans le fichier journal est complétée par un horodatage afin de consigner avec précision les dysfonctionnements et les temps d'erreur et de localiser les causes possibles.

3.4.1. Paramètres locaux

Dans le menu "System/System/Time", sélectionner "Use Local Settings" comme "Clock Source". Dans le champ en dessous de "System Date", entrer ensuite la date et l'heure manuellement selon le format voulu et confirmer avec la touche "Apply".

➔ Si le switch est redémarré, l'heure est perdue et doit être reconfigurée car le switch n'a pas de batterie de secours.



3.4.2. NTP (Network Time Protocol)

Le Network Time Protocol est un standard pour la synchronisation des horloges dans les systèmes informatiques via des réseaux de communication par paquets.

Comme les serveurs d'heure donnent généralement l'heure moyenne de Greenwich, la "Time Zone" doit être sélectionnée en conséquence pour que a) l'heure soit correcte et b) l'heure d'été/d'hiver soit réglée correctement.

La configuration s'effectue en deux étapes.

Lors de la première étape, sélectionner "Use NTP Server" comme "Clock Source". Cela active l'icône dans le coin supérieur droit du masque "Configure NTP Server".

En cliquant sur cette icône, vous accédez au masque de saisie, qui constitue l'étape 2.



Si l'heure doit être obtenue à partir d'une source spécifique, par exemple un serveur de temps, un serveur NTP ou un pare-feu etc., l'adresse IP correspondante doit être saisie dans le champ "Server 1". C'est la seule façon de s'assurer que le switch peut atteindre l'adresse IP. Il est possible de définir jusqu'à 5 sources.

Avec NTP Time-Sync Interval, vous définissez les intervalles dans lesquels le temps doit être synchronisé. Il est possible de choisir entre 5, 10, 15, 30, 60 et 120 minutes.

Si aucune source de temps n'est disponible dans votre propre réseau et qu'une source doit être obtenue de l'extérieur via Internet, un serveur NTP externe peut également être saisi directement, par exemple 213.209.109.45 de <https://www.ntppool.org/fr/>.

Dès que le switch peut obtenir l'heure et la date, l'heure correcte est affichée dans le champ "System Date".

3.5 Configuration des ports

Les ports sont réglés en usine en mode Auto. L'autonégociation est une procédure qui permet à deux ports Ethernet interconnectés de négocier et de configurer automatiquement la vitesse de transmission maximale possible et la procédure duplex. Cette procédure ne s'applique qu'aux câbles à paires torsadées et non aux connexions par fibre optique.

Néanmoins, il peut arriver que le terminal final ne soit pas reconnu correctement. Cela se produit de temps en temps avec les caméras ayant une interface 100 Mbit/s. Dans ces cas, le port doit être réglé manuellement sur 100 Mbit/s.

Si un port n'est pas utilisable pour des raisons de sécurité, il peut également être complètement désactivé. Pour cela, le mode de configuration doit être réglé sur "Disabled".

Port	Description	Link	Speed		Flow Control			Maximum Frame Size
			Status	Mode	Rx Status	Tx Status	Mode	
*				<>				10240
1		●	Up	Auto	off	off		10240
2		●	Down	Auto	off	off		10240
3		●	Down	Auto	off	off		10240
4		●	Down	Auto	off	off		10240
5		●	Down	Auto	off	off		10240
6		●	Down	Auto	off	off		10240

3.5.1. Port SFP

Les ports SFP disposent également d'un mode automatique. Celui-ci diffère de l'auto-négociation des ports en cuivre. Avec l'auto-négociation, les ports SFP ne peuvent détecter que la vitesse de transmission et ne prennent en charge que le full-duplex.

Il peut arriver que le switch ne reconnaisse pas correctement un SFP, qu'il s'agisse d'un SFP de 100 Mbit/s ou de 1000 Mbit/s et qu'il ne fonctionne donc pas. Dans ce cas, le débit de données sur le port doit être configuré manuellement.

49		●	Down	10Gbps FDX	off	off	☐	10240
50		●	Down	10Gbps FDX	off	off	☐	10240
51		●	Down	Disabled	off	off	☐	10240
52		●	Down	Auto	off	off	☐	10240
				1Gbps FDX				
				10Gbps FDX	off	off	☐	10240

Les ports SFP des switches ne sont pas codés. Cela signifie que les SFP d'autres fabricants peuvent également être utilisés, toutefois sans garantie de fonctionnement.

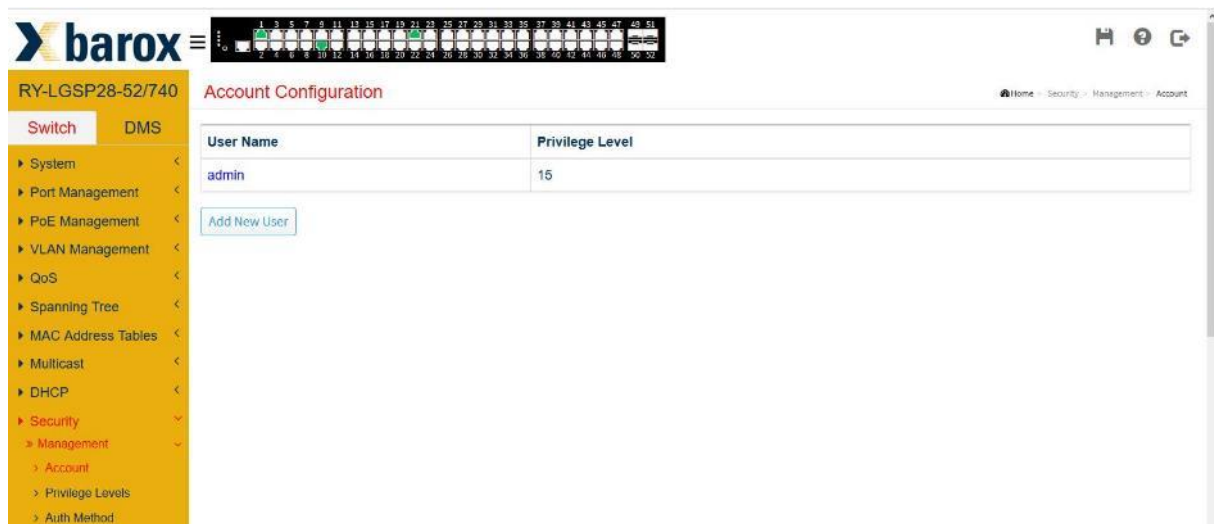
La gamme barox comprend des SFP pour fibres multimodes et monomodes avec des vitesses de transmission de 100 Mbit/s, 1 Gbit/s ou 10 Gbit/s. Les distances possibles varient en fonction du type de fibre et de la vitesse de transmission entre 550 m et 120 km.

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

3.6 Changer le nom d'utilisateur et le mot de passe

Les switches barox offrent la possibilité de générer plusieurs utilisateurs avec des droits différents. Il est possible de définir jusqu'à 15 niveaux différents.

Le niveau 15 est le niveau le plus élevé et est destiné aux administrateurs.



Un autre utilisateur peut être généré avec la fonction "Add New User". Vous devez définir le nom de l'utilisateur, le mot de passe et le niveau de droits.

barox RY-LGSP28-52/740

Add Account

Account Settings

User Name: Muster

Password: *****

Password (again): *****

Privilege Level: 10

Apply Reset Cancel

Le point de menu "Privilege Levels" permet ensuite de définir la diversité exacte des droits du nouvel utilisateur.

Dans l'exemple suivant, l'utilisateur "Exemple" possède le niveau de droits 10. Cela signifie qu'il peut tout configurer grâce à des droits de lecture et d'écriture. Pour le "Debug" il a cependant un niveau de droits trop bas, de sorte qu'il ne peut même pas lire "Debug".

barox RY-LGSP28-52/740

Privilege Levels Configuration

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5	10
Debug	15	15
DHCP	5	10
DHCPv6_Client	5	10
Diagnostics	1	10
DMS_client	5	10
DMS_Trouble_Shooting	5	10
DMS_Vbatch	5	10
EPS	5	10

Le tableau est très étendu et les droits peuvent être affectés de manière très détaillée. Par exemple, vous pouvez définir un utilisateur qui n'est autorisé à lire que la table des adresses MAC.

3.7 Loop Protection

Dans le cas de vastes réseaux, il peut arriver rapidement qu'une boucle soit physiquement branchée accidentellement ou involontairement. En l'absence d'un protocole anti-boucles actif (par ex. RSTP), l'ensemble du réseau s'arrête et devient inopérant.

La fonction "Loop Protection" sert à éviter ce genre de situation. Si cette option est activée, vous pouvez définir, pour la boucle créée par inadvertance, si le port doit être désactivé ou si seule une entrée doit être effectuée dans le fichier journal, ou bien les deux ("Shutdown and Log").

➔ Les ports qui sont déjà actifs avec RSTP ne doivent pas être surveillés en plus avec Loop Protection. Cela entraîne des perturbations massives dans le réseau.

Le "Shutdown Time" indique combien de temps un port doit rester désactivé si une boucle est détectée. Saisie des temps possible : 0 – 604800 s (7 jours). Si "0" est entré, le port reste désactivé jusqu'à ce que le switch soit redémarré.

barox RY-LGSP28-52/740

Loop Protection Configuration

Global Configuration

Enable Loop Protection: ☐ off

Transmission Time: 5 seconds

Shutdown Time: 180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
1	☒	Shutdown Port	Enable
2	☒	Shutdown Port	Enable

3.8 Configuration en anneau

Afin d'assurer la redondance dans le réseau, il est absolument nécessaire de mettre en place une topologie en anneau. Pour éviter que le réseau ne soit surchargé par un broadcast storm (tempête de diffusion), un mécanisme de protection est nécessaire.

RSTP (Rapid Spanning Tree Protocol) est l'un des protocoles de base des réseaux Ethernet. Il garantit qu'aucune boucle de réseau ne se produit dans un segment de réseau. Contrairement aux paquets IP, les trames Ethernet n'ont pas de durée de vie maximale (Time to Live, TTL) et peuvent donc tourner en rond pendant une durée infinie, ce qui peut surcharger le réseau et, dans le pire des cas, l'immobiliser.

Wikipedia explique en détail la fonction du Rapid Spanning Tree Protocol (RSTP)
https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol

3.8.1. Ring Master

Dans une topologie en anneau, un switch doit être défini comme le Master responsable de la surveillance de l'anneau. En cas d'interruption éventuelle de la connexion, il le signale à tous les switches de l'anneau afin que la connexion alternative soit activée. Le switch avec la priorité 0 est le Ring Master.

Le protocole RSTP est conçu de telle sorte que, sans Ring Master défini, le switch ayant la plus petite adresse MAC devient automatiquement le Ring Master.

barox RY-LGSP28-52/740

STP Bridge Configuration

Basic Settings

Protocol Version: RSTP

Bridge Priority: 32768

Hello Time: 2

Forward Delay: 15

Max Age: 20

Maximum Hop Count: 20

Transmit Hold Count: 6

Priority 0 = Ring Master

La version du protocole souhaitée doit être sélectionnée dans le menu "Spanning Tree / STP Configuration". RSTP est supporté par tous les fabricants de switches et est donc compatible avec les fabricants tiers.

Par défaut, les switches ont la "Bridge Priority" 32768. Si le commutateur doit agir en tant que Master, la Bridge Priority doit être réglée sur "0". Toutes les autres valeurs peuvent être laissées telles quelles.

3.8.2. Configuration des ports

Pour définir les ports qui sont inclus dans l'anneau, éditez l'élément de menu "CIST" dans le menu "MSTI Configuration".

Instance	VLANs Mapped	MSTI Priority	MSTI Port
CIST	Unmapped VLANs are mapped to the CIST	32768	Edit
MSTI1	Example: 2,3,5,11,13,20,40	32768	Edit

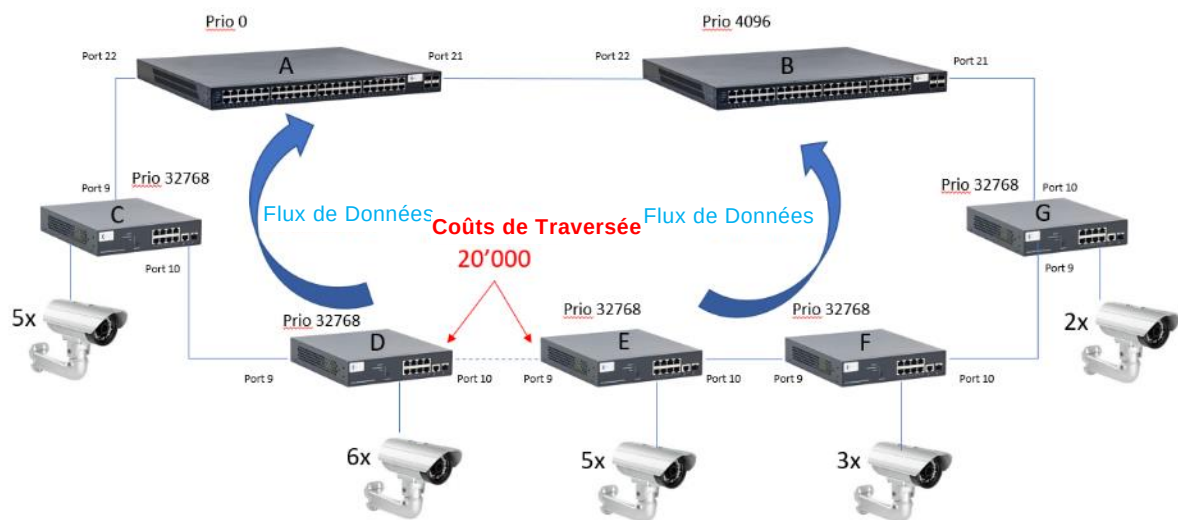
"STP Enabled" est actif pour tous les ports à la sortie de l'usine. Ainsi, l'anneau peut théoriquement être formée à n'importe quel port. Pour une répartition optimale de la charge dans le réseau, le flux de paquets de données peut être contrôlé par définition à l'aide des coûts de traversée. Le terme "coûts de traversée" vient de l'époque où les lignes étaient louées pour la connexion de A à B et étaient donc chères.

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted	TCN	BPDU Guard	Point-to-point
-	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Forced True

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted	TCN	BPDU Guard	Point-to-point
*	☒	<>	<>	<>	☒	☐	☐	☐	<>
1	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
2	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto
3	☒	Auto	128	Non-Edge	☒	☐	☐	☐	Auto

Exemple :

Dans le cas d'un anneau plus grande avec plusieurs terminaux et une plus grande quantité de données, il est judicieux de diriger le flux de données dans l'anneau de manière à ce que les switches soient chargés uniformément (répartition de la charge). Il faut pour cela définir les coûts de traversée.



Dans l'exemple illustré, le réseau se compose de deux switches centraux (A+B) et de 5 autres switches qui forment ensemble un anneau. Au total, 21 caméras sont installées, chacune fournissant 5 Mbit/s de données vidéo. Ce sont donc au total plus de 100 Mbit/s de données.

Scénario 1 : seul RSTP est actif sur tous les switches

Le switch avec l'adresse MAC la plus basse endosse la fonction de Master. Il se peut que ce soit le plus petit switch avec la puissance de processeur la plus faible de l'anneau. La direction du flux de données est inconnue.

En cas d'interruption, le temps de commutation peut être un peu plus long, car le petit switch ne peut pas traiter les données aussi rapidement.

Scénario 2 : RSTP actif sur tous les interrupteurs, switch-A Prio 0 et switch-B Prio 4096

Dans ce cas, Switch A endosse la fonction Master par définition. S'il subit une défaillance, le switch B hérite de la fonction Master. Switch A surveille l'anneau, et, en cas d'interruption du réseau, le processeur a suffisamment de puissance pour agir rapidement. Sur switch A, le port 21 peut être marqué comme "Blocked". Cela signifie que le flux de données de toutes les caméras vidéo passe par le port 22. Le petit Switch C doit traiter les données de toutes les caméras vidéo, ce qui crée goulot d'étranglement.

Scénario 3 : RTSP actif, Master défini et coûts de traversée définis

Cette configuration définit exactement le flux de données. La charge est répartie sur deux côtés. Aucun switch n'atteint ses limites. Étant donné que les coûts de traversée au niveau du Switch D, port 10 et du Switch E, port 9 sont plus élevés qu'à tous les autres ports de l'anneau, ce trajet n'est activé qu'en cas d'interruption dans le réseau.

Réglage d'usine des coûts de traversée :

Les coûts dépendent de la distance au Root Bridge (Master) et de la liaison montante disponible vers la destination. Une liaison montante à 100 Mbit/s a généralement des coûts de traversée plus élevés qu'une liaison montante à 1 Gbit/s vers la même destination, de sorte que la liaison à 100 Mbit/s serait bloquée car considérée comme un trajet redondant. Les coûts de traversée sont normalisés selon les spécifications IEEE, mais peuvent être réglés différemment manuellement, par exemple pour sélectionner une liaison montante préférée en cas de vitesse égale afin de refléter le coût réel des lignes dédiées.

➔ Dans la mesure du possible, la configuration doit être orientée telle qu'illustrée sur l'image.

3.9 Configuration VLAN

La configuration du VLAN se fait seulement d'un côté.

Dans le champ "Allowed Access VLANs", tous les numéros de VLAN à configurer doivent être indiqués.

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	10	<>	☒	<>	<>	10	
1	Access	10	C-Port	☒	Tagged and Untagged	Untag Port VLAN	10	
2	Access	20	C-Port	☒	Tagged and Untagged	Untag Port VLAN	20	
3	Trunk	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1-4095	30-35
4	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

Si les numéros VLAN sont listés, les différents ports peuvent maintenant être affectés à une fonction et à un VLAN.

Mode	VLAN	Fonction
Access	Nr	un terminal est connecté à ce port.
Trunk	---	raccordement entre deux switches
Hybrid	---	raccordement entre deux switches ou un terminal

Le mode Trunk ainsi que le mode Hybrid permettent de définir quels réseaux VLAN sont autorisés dans la colonne "Allowed VLANs" et quels réseaux VLAN ne sont pas autorisés dans la colonne "Forbidden VLANs".

3.10 Power over Ethernet (PoE)

Dans la zone PoE, le switch dispose de nombreuses options pour optimiser l'utilisation de PoE. L'alimentation peut être mise sous ou hors tension sous contrôle de temps ou d'événements. En outre, les appareils alimentés (par exemple les caméras PoE) peuvent être surveillés et redémarrés si nécessaire.

3.10.1. Configuration PoE

The screenshot shows the barox web interface for switch RY-LGSP28-52/740. The 'PoE Configuration' page is displayed, featuring a sidebar menu on the left with options like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, and Security. The main configuration area includes sections for 'Reserved Power determined by' (Class, Allocation, LLDP-Med), 'Power Management Mode' (Actual Consumption, Reserved Power), 'Capacitor Detection', 'PoE Power Supply Configuration' (PoE Firmware Version: 208-211, Primary Power Supply [W]: 740), and 'PoE Port Configuration'. The port configuration table shows ports 1 and 2, both with PoE Mode 'Enabled', PoE Schedule 'Disabled', Priority 'Low', Maximum Power [W] '30', Delay Mode 'Disabled', and Delay Time '0'.

Chaque switch a une capacité de performance définie. Celle-ci décrit la quantité d'énergie qui peut être fournie via les ports PoE. Elle dépend fortement de l'alimentation électrique intégrée dans le switch. Dans notre exemple, un switch RY-LGSP28-52 avec 24 ports PoE+ offre max. 740 W. Cela signifie qu'il est impossible de connecter un terminal de 30 W à chacun des 48 ports, car 1440 W seraient nécessaires. L'alimentation électrique intégrée ne peut pas fournir autant d'énergie.

Par conséquent, il faut prendre en compte l'allocation de puissance par port.

Les consommateurs de PoE sont divisés en différentes classes en fonction de leur consommation.

Classe	Puissance disponible sur l'appareil fourni	Signature de classification
0	0,44 – 12,96 W	0 à 4 mA
1	0,44 – 3,84 W	9 à 12 mA
2	3,84 – 6,49 W	17 à 20 mA
3	6,49 – 12,95 W	26 à 30 mA
4	12,95 – 25,50 W (only 802.3at/Type 2) ^[4]	36 à 44 mA

https://fr.wikipedia.org/wiki/Alimentation_%C3%A9lectrique_par_c%C3%A2ble_Ethernet

Reserved Power determined by

Sous Reserved Power determined, il est possible de définir comment l'alimentation max. doit être déterminée.

- Class = correspond à la classe à laquelle le terminal est identifié
- Allocation = selon les spécifications de la colonne "Maximum Power (W)"
- LLDP-Med = idem mode Class, obtient l'information via LLDP (si possible)

Si le terminal dépasse la puissance prédéfinie, le port éteint le PoE.

Power Management Mode

Cette section permet de définir le comportement du switch en cas de dépassement de la puissance maximale possible.

Actual Consumption

Si la puissance consommée par tous les appareils dépasse la puissance maximale que le switch peut fournir, le PoE est complètement éteint. Si un seul port dépasse la puissance, le PoE n'est désactivé que sur le port correspondant.

La colonne "Priority" définit quel port est important. Les ports portant la mention "low" seront immédiatement désactivés, tandis que les ports marqués "Critical" seront désactivés en dernier si la puissance totale est dépassée.

Reserved

Les ports portant la mention "reserved" ne sont désactivés que si la puissance réservée dans la colonne "Maximum Power (W)" est dépassée.

PoE Schedule

Chaque port peut être affecté à un horaire. Il est possible de créer un total de 16 horaires.

3.10.2. PoE Power Delay

Comme déjà mentionné, le switch peut fournir une puissance limitée.

Les caméras IP d'aujourd'hui ont besoin de plus en plus de puissance. Si on utilise une caméra panoramique inclinable avec chauffage intégré et spot infrarouge, la puissance requise augmente encore plus.

En particulier lors du redémarrage, du passage du jour à la nuit, de l'allumage de radiateurs ou de spots IR etc., les caméras ont besoin de beaucoup plus de courant (= pointes de puissance) qu'en fonctionnement continu.

Si plusieurs caméras sont maintenant connectées à un switch et que toutes les caméras se connectent en même temps, il est possible que la puissance maximale théorique du switch soit dépassée. En cas de dépassement de la puissance, le switch se déconnecte immédiatement et l'alimentation électrique subit des dommages si les pannes sont fréquentes.

Pour éviter ce problème, vous pouvez configurer un démarrage différé de chaque port dans le menu suivant. Dans l'exemple suivant, le port 1 est activé après 10 secondes et les ports 2 et 3 à intervalles de 20 secondes.

Port	Delay Mode	Delay Time(0~300 sec)
1	Enabled	10
2	Enabled	30
3	Enabled	50
4	Disabled	0

3.10.3. PoE Schedule

L'allumage et l'extinction du courant peuvent également être commandés selon un plan horaire hebdomadaire. Il est possible de créer jusqu'à 16 profils différents. Chaque port peut être affecté à un profil.

Dans l'exemple suivant, dans le profil 1, la caméra n'est allumée que le lundi entre 7h30 et 18h15, ou le port PoE est alimenté en électricité.







RY-LGSP28-52/740
PoE Schedule Profile

Switch
DMS

▶ System
 ▶ Port Management
 ▶ PoE Management
 ▶ PoE Configuration
 ▶ PoE Status
 ▶ PoE Power Delay
 ▶ PoE Auto Checking
 ▶ PoE Scheduling Profile
 ▶ VLAN Management
 ▶ QoS
 ▶ Spanning Tree

Profile
1

Name
Profile 1

Week Day	Start Time		End Time	
	HH	MM	HH	MM
*	<<>	<<>	<<>	<<>
Monday	7	30	16	15
Tuesday	0	0	0	0
Wednesday	0	0	0	0

3.10.4. PoE Auto Checking

PoE Auto Checking sert à la surveillance des fonctions. En utilisant ping, par exemple, l'accessibilité de la caméra connectée au port 1 avec l'adresse IP 192.168.1.250 est vérifiée toutes les 30 secondes.

Après 3 tentatives erronées, PoE est désactivé sur le port 1 et réactivé après 15 secondes. Ceci force le redémarrage de la caméra.

60 secondes après le redémarrage, la surveillance redémarre via ping.







RY-LGSP28-52/740
PoE Auto Checking

Switch
DMS

▶ System
 ▶ Port Management
 ▶ PoE Management
 ▶ PoE Configuration
 ▶ PoE Status
 ▶ PoE Power Delay
 ▶ PoE Auto Checking
 ▶ PoE Scheduling Profile

Ping Check
off

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	192.168.1.250	60	30	3	error=0, total=0	Reboot Remote PD	15
2	192.168.1.243	60	30	3	error=0, total=0	Reboot Remote PD	15
3	0.0.0.0	60	30	3	error=0, total=0	Nothing	15
4	0.0.0.0	60	30	3	error=0, total=0	Nothing	15

3.11 Sauvegarde et chargement de la configuration

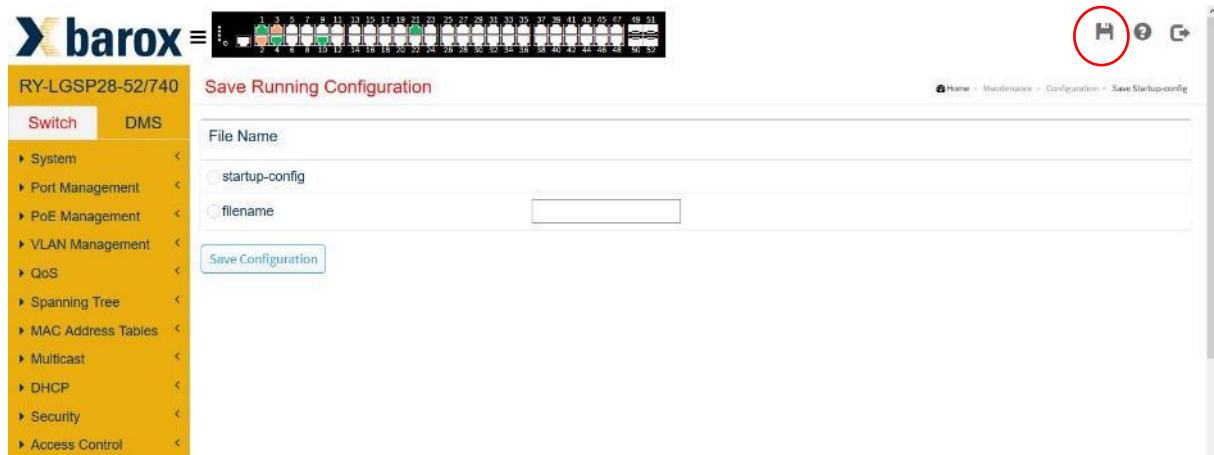
Chaque modification doit être sauvegardée. En sélectionnant "Apply", la modification est écrite dans la mémoire de travail. Un redémarrage efface la mémoire et tous les changements sont perdus. Les modifications doivent donc absolument être sauvegardées.

Il y a deux possibilités :

- Dans le menu Maintenance/Configuration/Save startup-config

▶ Maintenance
 » Configuration
 > Save Startup-config
 > Backup
 > Restore
 > Activate
 > Delete
 > Restart Device

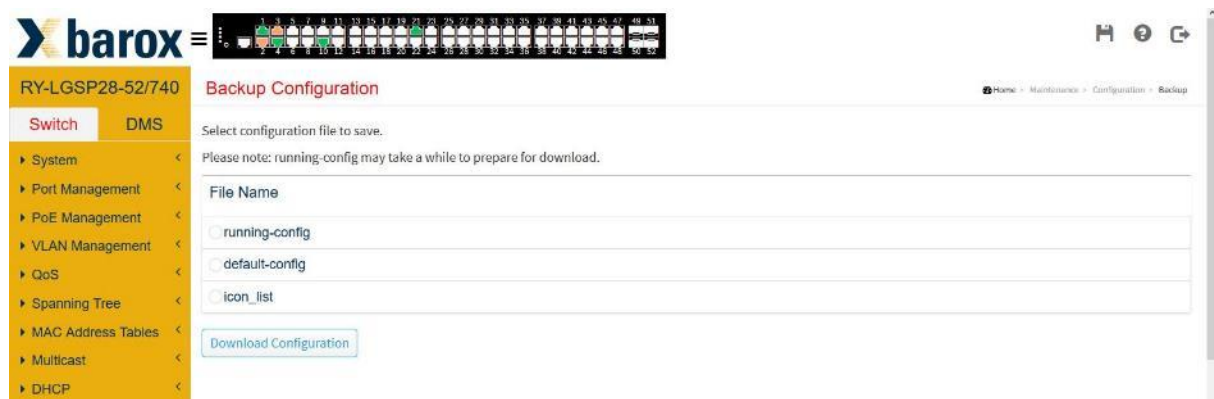
- Le symbole disquette dans chaque masque



3.11.1. Téléchargement de la configuration

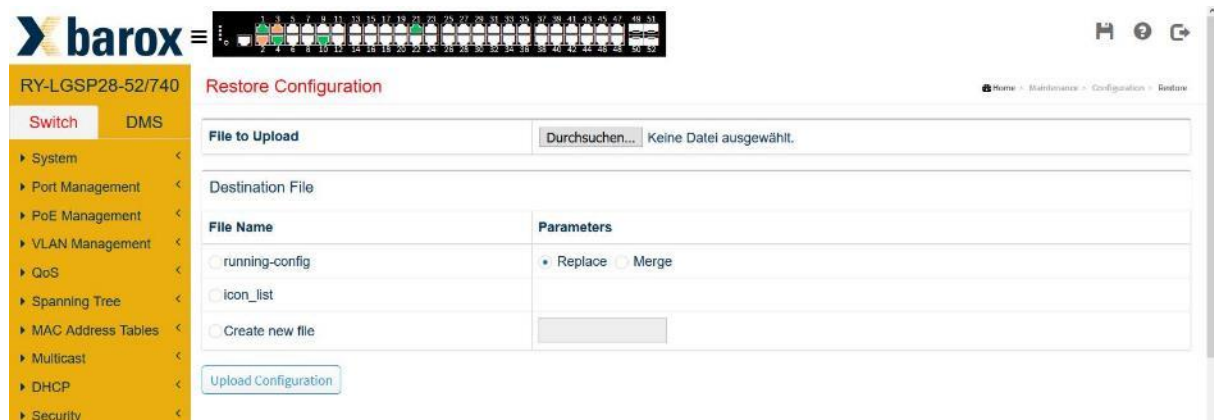
La configuration actuelle du switch peut être téléchargée et sauvegardée séparément. Le fichier de configuration généré peut être importé dans le cas du remplacement d'un switch ou utilisé si plusieurs switches doivent être configurés de manière identique et que seule l'adresse IP change.

Cela permet de gagner beaucoup de temps. Nous vous recommandons de n'enregistrer que le fichier "startup-config File".



3.11.2. Importer la configuration (upload)

La variante inverse consiste à importer un fichier de configuration dans le switch. Pour cela, il suffit d'indiquer le chemin du fichier enregistré et de le définir comme "running-config". Si tout fonctionne comme voulu, le fichier doit être enregistré sous la forme "startup-config -File" comme décrit ci-dessus.



4 DMS Device Management System

Le switch dispose d'un système intégré de surveillance et de contrôle du réseau qui donne à l'utilisateur une vue d'ensemble très simple de la totalité du réseau. L'aperçu de la topologie du réseau permet une vue d'ensemble rapide de tous les switches et terminaux disponibles sur le réseau, tels que les caméras IP ou les serveurs, avec des détails sur l'adresse IP, le type de périphérique et le nom du périphérique. Les plans d'étage et les plans d'environnement peuvent être stockés sous forme d'images d'arrière-plan, avec lesquelles l'utilisateur peut accéder rapidement à certains périphériques réseau même sans connaître l'infrastructure IP. Les plans finis peuvent être exportés à nouveau et il est possible d'y joindre des documents.

4.1 Gestion

Pour utiliser la fonction DMS, il faut passer à l'onglet "DMS". Le DMS est activé en usine. Sur la page d'information Mode DMS, il est possible de voir combien d'appareils ont été détectés dans le réseau, combien d'entre eux sont en ligne (actifs) ou hors ligne (inactifs).

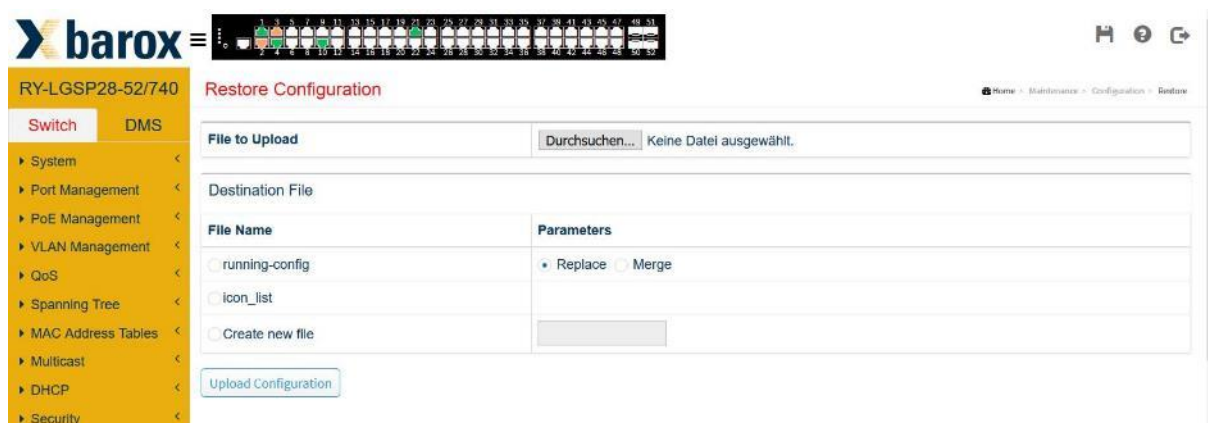
Les appareils hors ligne sont ceux qui ont été soit éteints, soit qui sont en panne (terminal défectueux) ou qui ne sont plus disponibles sur le réseau (par ex. l'ordinateur portable de service que l'installateur emporte chez lui après avoir terminé la configuration).

Pour pouvoir utiliser le DMS, un switch doit être défini comme Master dans le réseau. Ce switch recueille toutes les informations et les transmet à tous les switches compatibles DMS du réseau. Le champ "Controller IP" indique quel switch (adresse IP) possède la fonction Master.

Information	
Mode	Enabled
Controller Priority	High
Total Device	6
On-line Devices	6
Off-line Devices	0
Controller IP	192.168.1.1

Détermination du Master DMS :

Sur le switch qui doit être le Master, il faut choisir le mode "High" dans le champ "Controller Priority". Il est recommandé de définir le switch le plus puissant pour cette tâche, car le DMS nécessite de la capacité de calcul supplémentaire. Les autres switches du réseau peuvent être classés "Mid" ou "Low" en fonction de leurs performances. Pour qu'un switch ne devienne jamais Master DMS, la "Controller Priority" doit être réglée sur "Non".



Ou, si la charge du réseau est très élevée, le DMS peut être mis en marche sur le switch le moins fréquenté et désactivé sur les autres switches. Il est à noter que certaines fonctions sont limitées et que cette méthode est recommandée pour une structure homogène avec des switches barox.

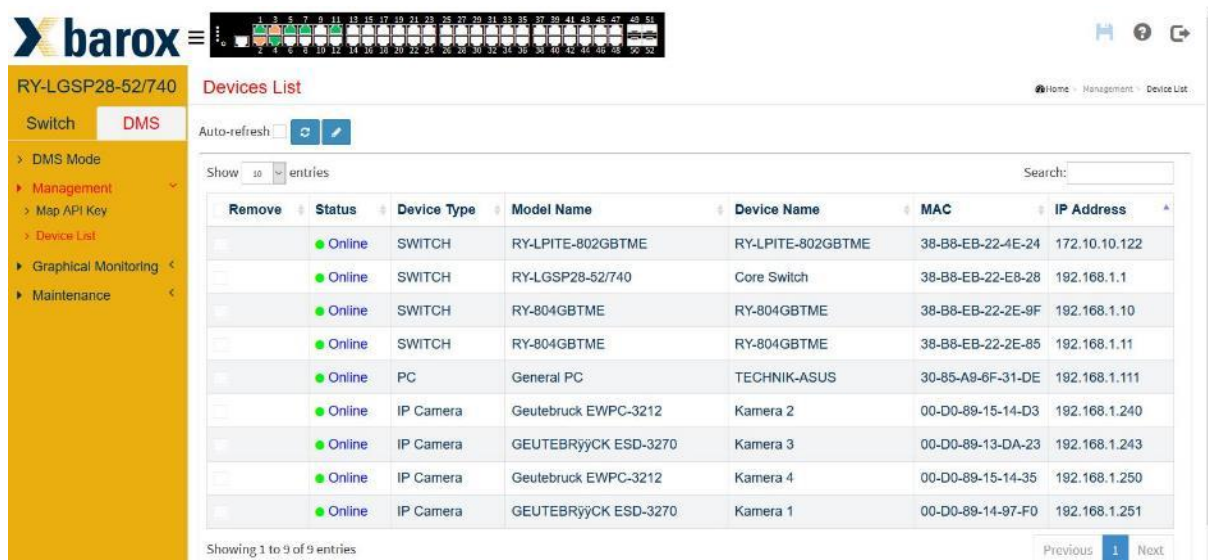
Sur la ligne "Controller IP", l'adresse IP indique quel switch est le Master.

Device List

Cette page répertorie tous les périphériques en ligne ou hors ligne du réseau. Le type d'appareil, l'état, le nom du périphérique ainsi que l'adresse MAC et l'adresse IP sont listés sous forme de tableau.

Tous les périphériques – y compris ceux dont les adresses IP sont situées dans un segment de réseau différent – sont répertoriés.

Cette fonction est particulièrement utile par ex. lorsqu'un périphérique non configuré est intégré dans le réseau et que l'adresse IP est inconnue.



En cliquant sur le symbole d'état "Online" ou "Offline", la connexion au périphérique peut être vérifiée – même lorsqu'elle passe par plusieurs switches. S'il y a une interruption dans la chaîne de connexion, vous pouvez le voir ici.

Le même contrôle peut être effectué dans le menu "Maintenance/Diagnostics".

barox RY-LGSP28-52/740

Switch **DMS**

Diagnostics

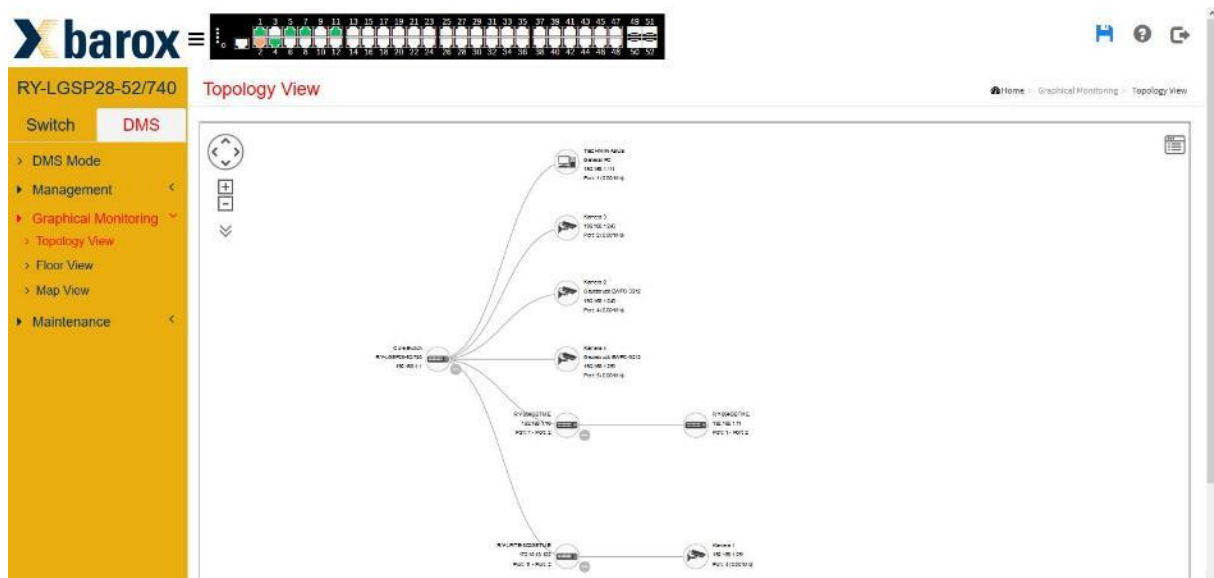
Select	Status	Model Name	Device Name	MAC	IP Address	Version
☐	Online	GEUTEBRyyCK ESD-3270	Kamera 1	00-D0-89-14-97-F0	192.168.1.251	

Graphical representation of the network topology showing connections between devices and their status (Connection, Cable status).

4.2 Surveillance graphique

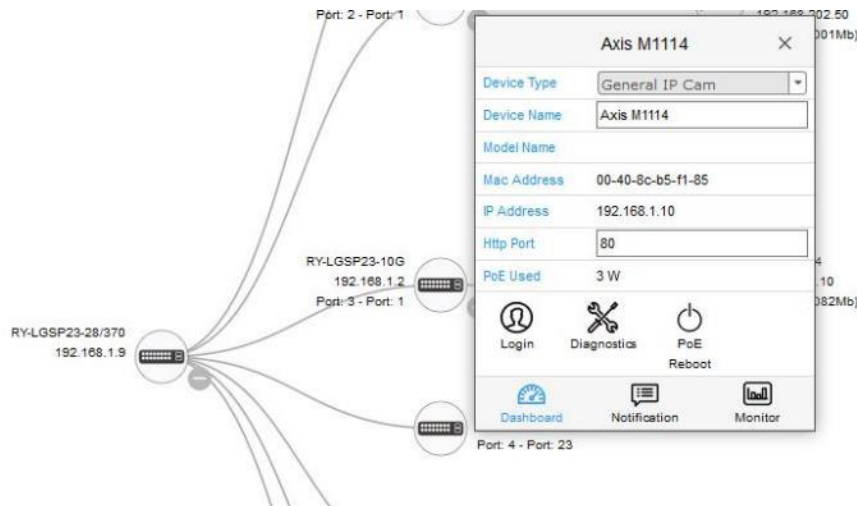
Topology View

Dans la vue topologique (Topology View), le réseau, y compris tous les terminaux IP connectés, est automatiquement affiché sous forme graphique. Si le terminal est reconnu correctement, le symbole correspondant (caméra, switch, point d'accès, etc.) s'affiche. Toutes les informations telles que le nom du périphérique, l'adresse IP, le débit de données, etc. apparaissent parallèlement au symbole. Tous les réglages peuvent également être configurés manuellement.



Un clic sur le symbole affiche le "Tableau de bord" (Dashboard) de l'appareil correspondant. Dans le "Dashboard", il est possible de définir le type et le nom du périphérique, les adresses MAC et IP ainsi que de consulter les exigences PoE affichées en temps réel, à condition qu'il s'agisse d'un consommateur PoE.

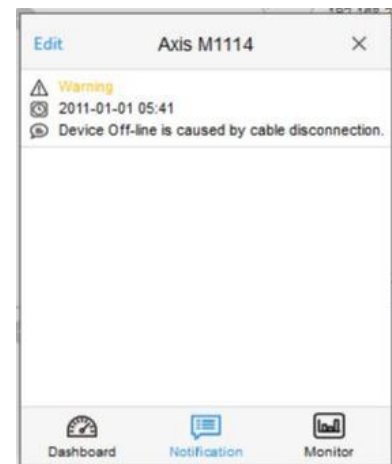
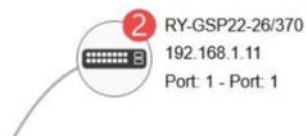
En outre, il est possible d'accéder directement au périphérique via "Login" ou d'effectuer un diagnostic de connexion. Le fait de cliquer sur l'icône "PoE Reboot" permet un redémarrage du consommateur PoE sans aucun problème.



Si un périphérique

- était temporairement indisponible (erreur de câble, déconnexion du consommateur, etc.),
- n'était pas immédiatement lisible via ONVIF
- avec une adresse IP déjà existante était connecté
- etc.

un numéro rouge apparaît à côté du symbole. Le chiffre rouge indique combien de messages sont disponibles pour ce périphérique. Les messages peuvent être lus et édités dans le menu "Notification".



Si un périphérique n'existe plus dans le réseau, il est affiché en rouge dans la vue topologique et le symbole "Remove" apparaît dans le "Dashboard". En cliquant sur "Remove", le périphérique est finalement retiré de la vue topologique.

Il faut impérativement cliquer sur "Remove" si, par exemple, une caméra défectueuse doit être remplacée par une nouvelle caméra avec la même adresse IP. Le switch stocke non seulement l'adresse IP mais aussi l'adresse MAC. Si l'ancienne adresse IP n'est pas supprimée via la fonction "Remove", le switch s'attend à ce que l'ancienne caméra soit réinitialisée avec la combinaison d'adresses IP et MAC d'origine et règle encore et toujours la nouvelle caméra sur l'adresse IP par défaut malgré une même adresse IP. Cela se produit parce que la nouvelle caméra a une adresse MAC différente.

Axis M1114

Device Type: General IP Cam

Device Name: Axis M1114

Model Name:

Mac Address: 00-40-8c-b5-f1-85

IP Address: 192.168.1.10

Http Port: 80

PoE Used: 0 W

Remove Diagnostics

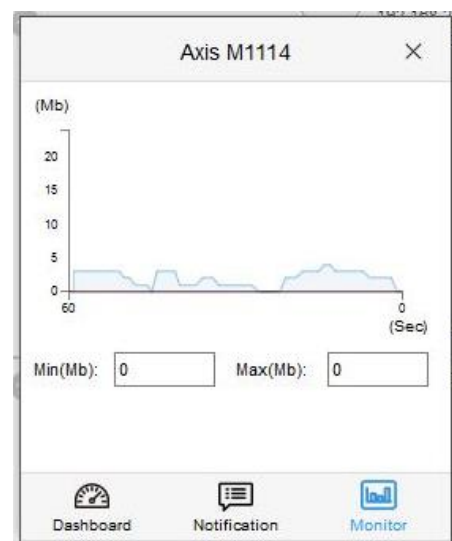
Dashboard Notification Monitor



Autre outil utile : la fonction "Monitor".

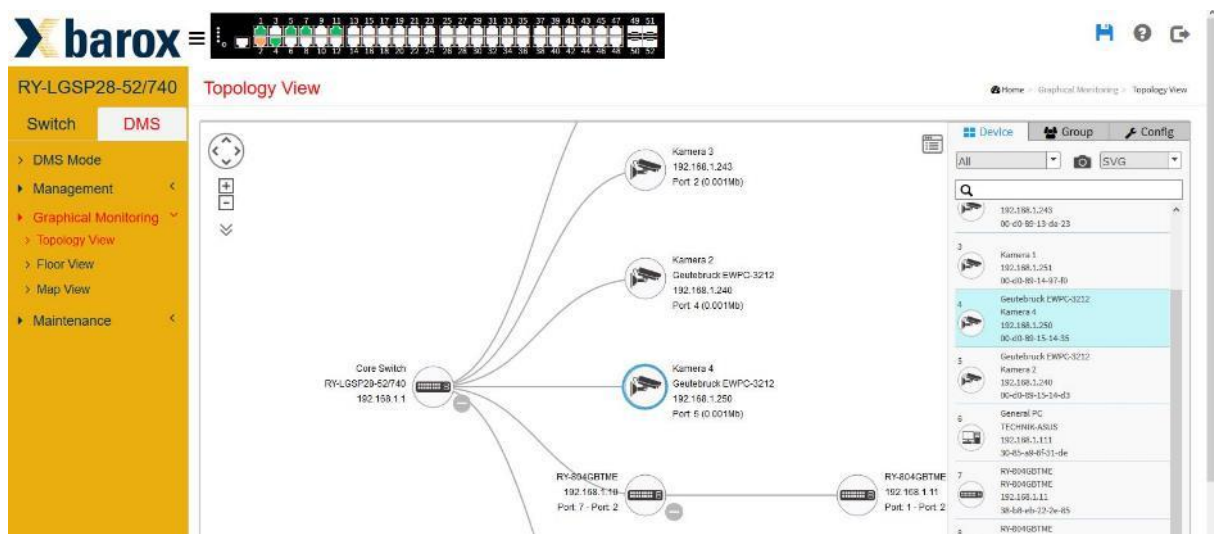
Ici, le flux de données (par ex. d'une caméra) est affiché en temps réel.

Min (Mb) et Max (Mb) peuvent être utilisés pour définir les seuils dans lesquels le flux de données doit se déplacer. Il est donc aisé de voir en un coup d'œil si tout fonctionne bien.



En haut à droite de la vue topologique se trouve une icône qui liste tous les périphériques "Device".

Si vous cliquez sur une entrée de la liste, le périphérique correspondant est marqué en bleu dans le diagramme de réseau.

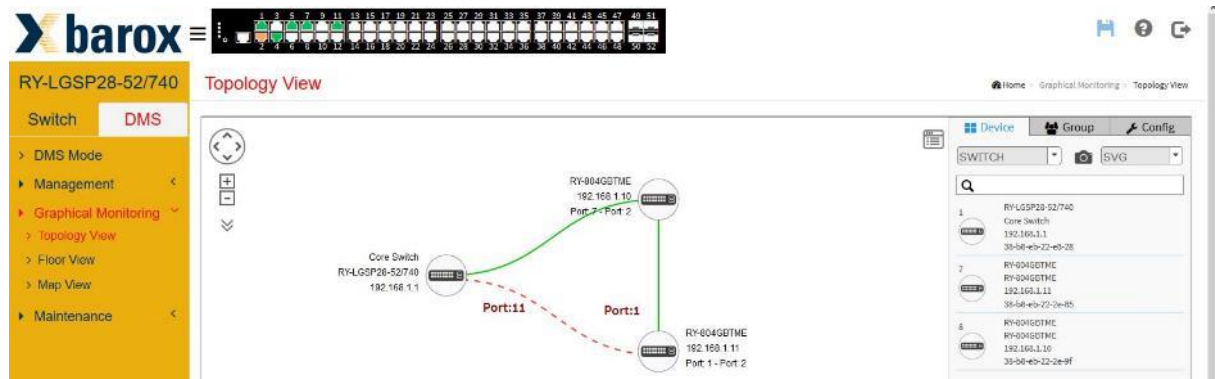


L'outil offre également la possibilité d'imprimer le plan de réseau au format SVG, PNG ou PDF directement depuis la "Topology View". Pour ce faire, il suffit de sélectionner le format désiré puis de cliquer sur l'icône de la caméra.

La "Topology View" offre également la possibilité d'afficher la constellation en anneau. Pour cela, il faut sélectionner la liste "Switch" dans le registre "Device". L'anneau est alors affiché et une ligne pointillée rouge indique quel itinéraire et quels ports sont définis comme ports alternatifs.

Deux conditions doivent être remplies pour cette représentation :

- RSTP en tant que protocole en anneau
- L'anneau se compose uniquement de switches RY qui supportent DMS



Plan de localisation (Floor View)

La Floor-View permet de visualiser les plans de bâtiment, d'étage et/ou d'environnement téléchargés ou importés. Ceux-ci servent de base ou d'image de fond pour cartographier le réseau. Cette fonction constitue une bonne aide à l'orientation pour les applications sur site et peut également être imprimée comme documentation, comme décrit ci-dessus.



Pour placer la caméra ou le switch sur le plan, il suffit de sélectionner l'appareil correspondant dans la liste avec un clic de souris et de le placer sur le plan. Rien de plus.

Vue cartographique (Map View)

La même fonction est possible avec la Map View. Ici, l'image de fond est générée avec Google Maps. Toutefois, une connexion Internet et des licences Google sont nécessaires pour utiliser le service.

4.3 Maintenance

Pour utiliser un plan comme image d'arrière-plan, il faut se rendre dans le menu "Maintenance". Dans le menu "Floor Image", il faut saisir le chemin d'accès et le nom du fichier et les télécharger en cliquant sur "Add".

barox RY-LGSP28-52/740

Switch DMS

> DMS Mode
> Management
> Graphical Monitoring
> Maintenance
 > Floor Image
> Diagnostics

Floor Image Management

Home > Maintenance > Floor Image

Maximum: 30 files Used: 1 file(s) Free: 29 file(s)

Add Floor Image: Durchsuchen... house-plan.png

Name Hausplan

Add

Les plans importés sont listés sur le bas de la page Web. Il est possible d'enregistrer jusqu'à 30 fichiers.

barox RY-LGSP28-52/740

Switch DMS

> DMS Mode
> Management
> Graphical Monitoring
> Maintenance
 > Floor Image
> Diagnostics

Floor Image Management

Home > Maintenance > Floor Image

Maximum: 30 files Used: 1 file(s) Free: 29 file(s)

Add Floor Image: Durchsuchen... Keine Datei ausgewählt.

Name

Add

Select	No.	File Name	Image
☐	1	Hausplan (192.168.1.1)	

Delete

Diagnostic

Cette fonction a été décrite et expliquée à la page 22 sous la rubrique "Device List".

5 La gestion des switches au cœur de la sécurité

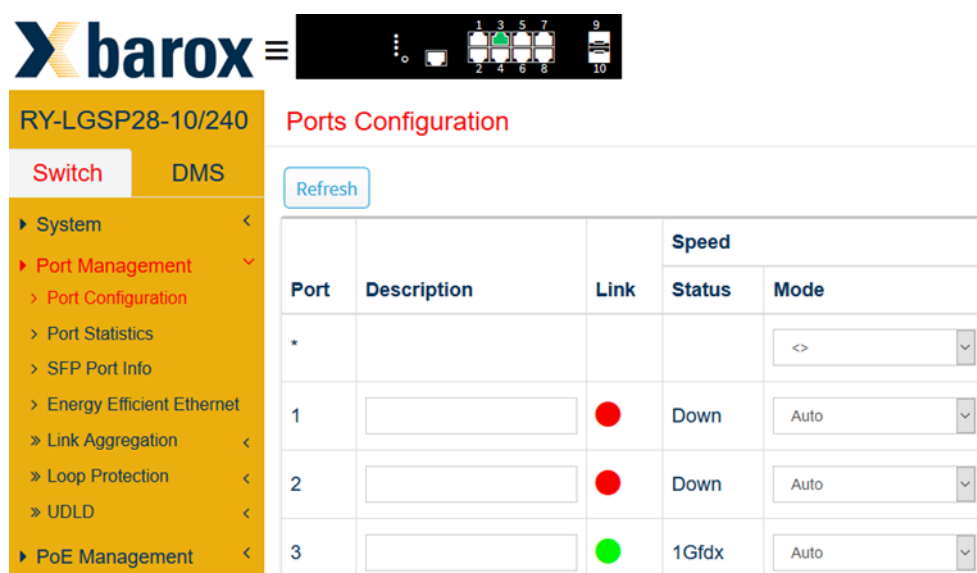
Les rubriques suivantes sont destinées à fournir des informations sur le contenu et la configuration des paramètres réseau avancés et la sécurité. Les prérequis de base pour la configuration sont les connaissances et les compétences en matière de mise en service telles que la configuration IP, la connexion et la configuration VLAN.

5.1 Gestion et protection au niveau du switch (Layer 1 et 2)

5.1.1 Paramètres et limites de la bande passante

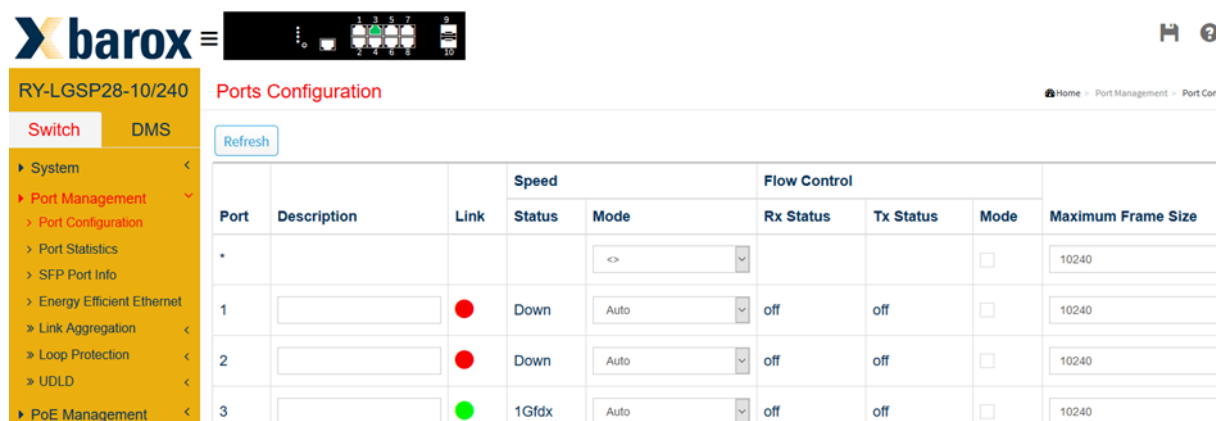
Réglage par port Ethernet

Dans certains cas, il est nécessaire de sélectionner manuellement la norme ETH requise. Par exemple, lors de la connexion de composants réseau qui ne permettent pas la négociation automatique de la norme ou qui nécessitent une révision à la baisse de la norme ETH en raison de certaines conditions de fonctionnement. Comme indiqué ci-dessous, les réglages 10/100/1000/10000 FDX/HDX (la norme ETH dépend du modèle), sélectionnables pour chaque port, peuvent être ajustés via le GUI Web.



Port	Description	Link	Speed	
			Status	Mode
*				<>
1		●	Down	Auto
2		●	Down	Auto
3		●	1Gfdx	Auto

Certaines applications nécessitent l'adaptation de la taille des trames Ethernet. Ceci peut également être fait dans le menu "Ports Configuration" dans le champ "Maximum Frame Size", comme dans la capture d'écran suivante.



Port	Description	Link	Speed		Flow Control			Maximum Frame Size
			Status	Mode	Rx Status	Tx Status	Mode	
*				<>				10240
1		●	Down	Auto	off	off		10240
2		●	Down	Auto	off	off		10240
3		●	1Gfdx	Auto	off	off		10240

! Il est important de respecter les valeurs exactes lors du réglage de la taille de la trame afin d'éviter les dysfonctionnements !

5.1.2. Notes sur la prise en compte générale des besoins en bande passante

Lors de la planification des besoins en largeurs de bande et de l'utilisation de switches barox appropriés, il est conseillé de prendre en compte les points suivants :

- Utilisation des normes Ethernet requises (10/100/1000/10000) en tenant compte d'éventuelles upgrades des terminaux.
- Planification de réserves, mises à l'échelle au niveau de la performance de commutation Backplane du modèle
-> on recommande souvent 30 %.
- Lors du calcul des besoins, tenez compte de la spécification Ethernet maximale par terminal.

5.1.3. Protection des ports via les paramètres de configuration MAC

La table MAC :

En principe, la table MAC peut être ajustée aussi bien manuellement qu'automatiquement. Ceci est généralement nécessaire si certains terminaux réseau requièrent une affectation statique par rapport au VLAN et au port. En outre, l'affectation manuelle peut être utilisée pour mettre à l'échelle une protection de base ou une restriction d'accès.

Filtrage MAC et configuration des ports

Exemple de configuration Table MAC statique :

L'appareil avec l'adresse MAC A1:00:00:00:00:FF ne doit pouvoir établir une connexion qu'au port 5 du VLAN 1.

1. Sélectionner "Add New Static Entry" dans le menu Switch -> Configuration -> MAC Table
2. Entrer l'ID VLAN, l'adresse MAC et régler l'élément de port 5 sous "MAC Table Learning" sur "Secure".
3. Confirmer les données saisies avec "Apply"

La capture d'écran suivante sert d'illustration.

barox 

RY-LGSP28-10/240

Switch **DMS**

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables**
 - Configuration
 - Information
- Multicast
- DHCP
- Security
- Access Control
- SNMP
- MEP
- ERPS
- EPS
- PTP
- Event Notification
- Diagnostics
- Maintenance

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging ☐

Aging Time seconds

MAC Table Learning

	Port Members						
	1	2	3	4	5	6	7
Auto	☒	☒	☒	☒	☐	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☒	☐	☐

VLAN Learning Configuration

Learning-disabled VLANs

Static MAC Table Configuration

	VLAN ID	MAC Address	Port Members				
Delete			1	2	3	4	5
Delete	1	A1-00-00-00-00-FF	☐	☐	☐	☐	☒

La protection par filtrage MAC offre une protection simple contre les accès indésirables au réseau. Néanmoins, elle ne protège pas contre l'attaque répandue du "MAC Spoofing", par exemple.

Protection du port avec ACL commençant à la layer 2

Protection des ports basée sur des règles avec vérification de l'adresse MAC via ACL

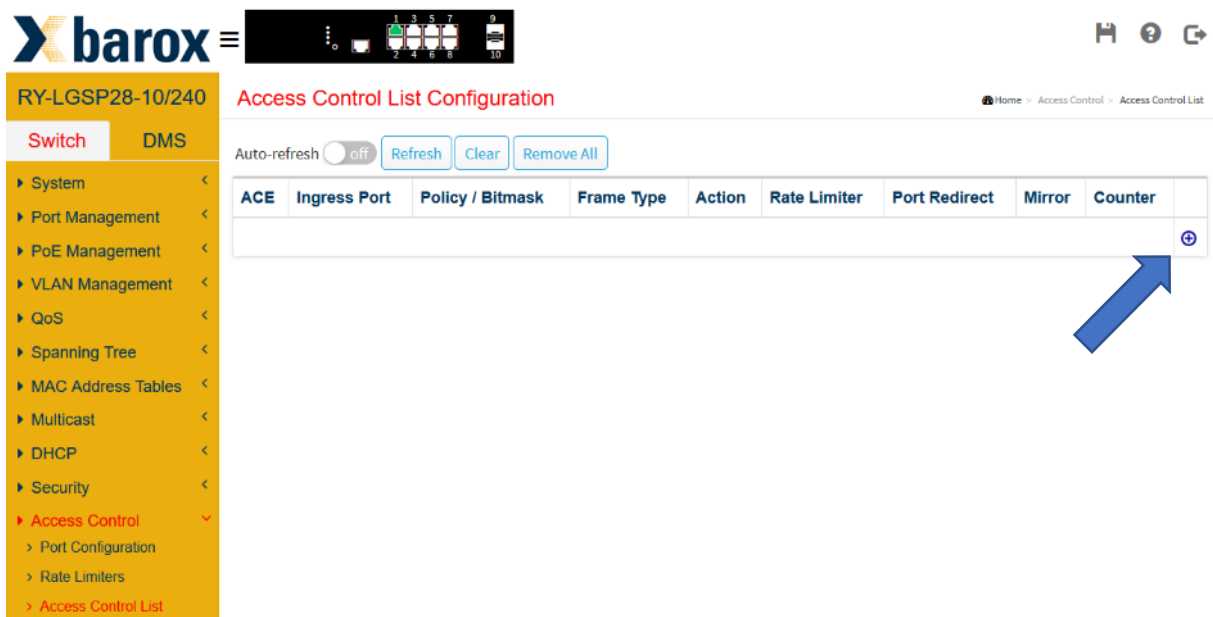
Considération préliminaire :

Cet exemple décrit la sécurisation d'un port avec l'adresse physique sur Ethernet sur le switch barox.

La fonction ACL est similaire à un pare-feu réseau qui vérifie les règles ou les conditions dans une séquence et déclenche la règle et les actions associées en fonction de la condition. L'exemple concret est de vérifier si une adresse MAC ou un terminal spécifique est connecté(e) à un port spécifique du switch. Si cela ne correspond pas, le port doit être fermé administrativement et physiquement (Shutdown). En outre, ACL peut également être utilisé pour mettre en œuvre les couches supérieures du réseau, avec des règles pour TCP/IP jusqu'au contrôle du flux de données.

Configuration :

Les ACL/ACE se créent dans le menu sous *Access Control > Access Control List*. Une nouvelle règle est créée en cliquant sur le signe "plus" comme sur l'image ci-dessous.

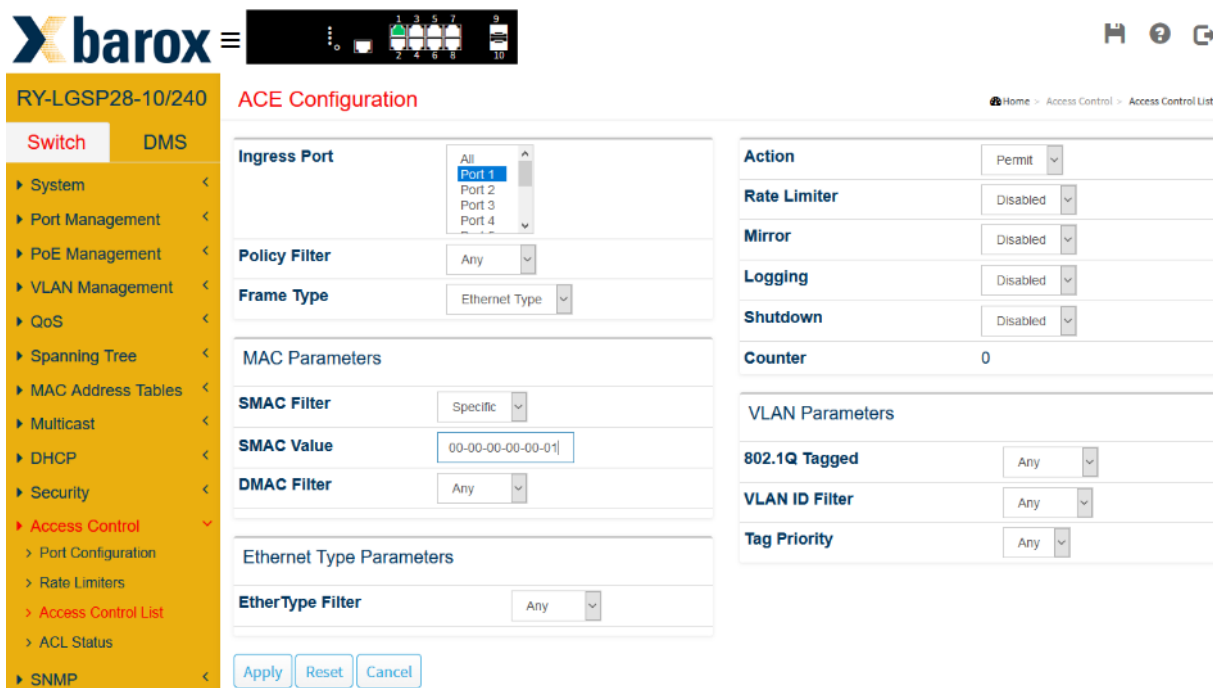


Pour cet exemple, une règle d'adresse MAC spécifique est créée pour le port 1 autorisé.

Paramètres :

Ingress Port: Port 1
 Policy Filter: Any
 Frame Type: Ethernet Type
 SMAC Filter: Specific
 SMAC Value: "Adresse MAC du terminal"
 DMAC Filter: Any
 Ether Type Filter: Any
 Action: Permit

D'autres réglages peuvent être effectués à partir de l'image suivante. Après avoir défini les paramètres, les entrées sont confirmées avec "Apply".



Après avoir créé la première règle, une deuxième est nécessaire. Vous pouvez l'ajouter en cliquant sur "plus".

barox RY-LGSP28-10/240 Access Control List Configuration

Auto-refresh ☐ off [Refresh](#) [Clear](#) [Remove All](#)

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	1	Any	EType	Permit	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊕ ⊖
+									

La règle suivante contrôle qu'aucune autre adresse MAC n'est autorisée sur le port 1. Ainsi, toute autre adresse MAC est rejetée. Les paramètres peuvent être adoptés comme le montre l'image ci-dessous.

barox RY-LGSP28-10/240 ACE Configuration

Ingress Port: All, Port 1, Port 2, Port 3, Port 4

Policy Filter: Any

Frame Type: Ethernet Type

MAC Parameters

SMAC Filter: Any

DMAC Filter: Any

Ethernet Type Parameters

EtherType Filter: Any

Action: Deny

Rate Limiter: Disabled

Port Redirect: Disabled, Port 1, Port 2, Port 3, Port 4

Mirror: Disabled

Logging: Disabled

Shutdown: Enabled

Counter: 0

VLAN Parameters

802.1Q Tagged: Any

VLAN ID Filter: Any

Tag Priority: Any

[Apply](#) [Reset](#) [Cancel](#)

Lorsque la configuration est terminée, les règles doivent être affichées comme suit.

barox RY-LGSP28-10/240 Access Control List Configuration

Switch DMS

Auto-refresh ☐ off Refresh Clear Remove All

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	1	Any	EType	Permit	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊕ ⊖
2	1	Any	EType	Deny	Disabled	Disabled	Disabled	0	⊕ ⊖ ⊕ ⊖

Home > Access Control > Access Control List

Si un terminal avec l'adresse MAC autorisée est connecté, le switch permettra de communiquer avec le réseau. Si un terminal avec un port différent de celui spécifié est connecté, le port 1 est désactivé.

Les indications pour la connexion d'un terminal non autorisé se trouvent dans l'aperçu des ports dans l'en-tête et dans le menu Access Control > Port Configuration, dans le statut "Disabled", comme indiqué ci-dessous.

barox RY-LGSP28-10/240 ACL Ports Configuration

Switch DMS

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	< >	< >	Disabled Port 1 Port 2	< >	< >	< >	< >	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Disabled	2635
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	85

Home > Access Control > Port Configuration

Réactivation du port

Pour réactiver le port, le statut doit être à nouveau réglé sur "Enabled" au même endroit du menu puis confirmé avec "Apply".

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	2635
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Veuillez vous assurer que le terminal est connecté à l'adresse MAC appropriée ou qu'aucun appareil n'est connecté au port.

Notes sur la création de règles de port multiples :

La création d'ACL pour les adresses MAC convient pour un petit nombre de ports. Pour chaque port, il faut créer une règle pour autoriser l'adresse MAC spécifique et une règle pour refuser d'autres adresses MAC. Il convient de noter que le switch vérifie à chaque fois toutes les règles de haut en bas et que la séquence doit être respectée scrupuleusement pendant la configuration. Voir l'exemple suivant :



Home > Access Control > Access Control List

RY-LGSP28-10/240

Switch DMS

▶ System
 ▶ Port Management
 ▶ PoE Management
 ▶ VLAN Management
 ▶ QoS
 ▶ Spanning Tree
 ▶ MAC Address Tables
 ▶ Multicast
 ▶ DHCP
 ▶ Security
 ▶ Access Control
 > Port Configuration
 > Rate Limiters
 > Access Control List

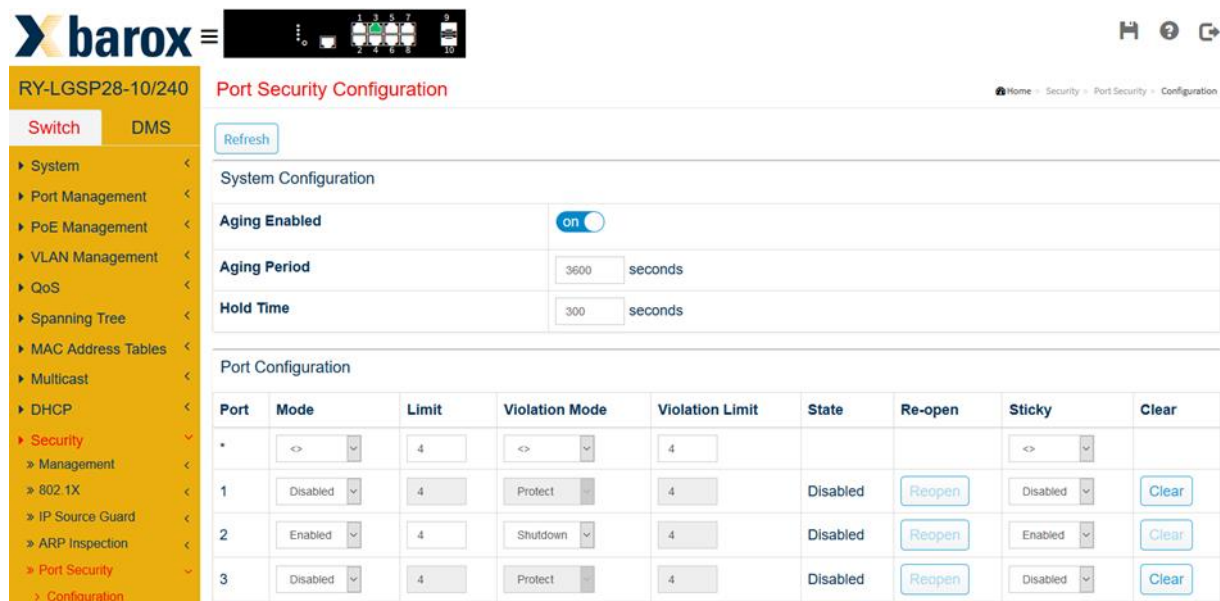
Access Control List Configuration

Auto-refresh ☐ off
 Refresh Clear Remove All

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	1	Any	EType	Permit	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
2	1	Any	EType	Deny	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
3	2	Any	EType	Permit	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
4	2	Any	Any	Deny	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
5	5	Any	IPv4/UDP	Permit	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
6	5	Any	IPv4/UDP 4000	Deny	Disabled	Disabled	Disabled	0	⊕ ⊕ ⊕ ⊕ ⊕
									⊕

5.1.4. Sécurité des ports avec paramètres de Limit Control

Si des switches non gérés avec des terminaux sont connectés au switch barox, il est recommandé d'utiliser le Limit Control. Cette fonction empêche en principe les autres terminaux IP/Ethernet indésirables d'avoir accès à la communication réseau sur les ports libres des switches non gérés. Pour des raisons de planification, il faut déterminer le nombre total de terminaux réseau, y compris le switch non géré connecté au port correspondant du switch barox. Exemple : Si un switch non géré avec 3 autres terminaux réseau est connecté au port 2 du switch barox, le nombre total de la limite est de 4. La configuration doit d'abord être activée. Ensuite, on active le port correspondant, on fixe la limite et on active l'action sélectionnée en cas de dépassement. L'apprentissage des terminaux est activé et rendu possible par la fonction "Sticky". Lors de la configuration, il est nécessaire que les appareils soient physiquement connectés au switch barox au niveau du port à configurer. Vous trouverez ci-dessous une illustration des réglages.



Port	Mode	Limit	Violation Mode	Violation Limit	State	Re-open	Sticky	Clear
*	<>	4	<>	4			<>	
1	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear
2	Enabled	4	Shutdown	4	Disabled	Reopen	Enabled	Clear
3	Disabled	4	Protect	4	Disabled	Reopen	Disabled	Clear

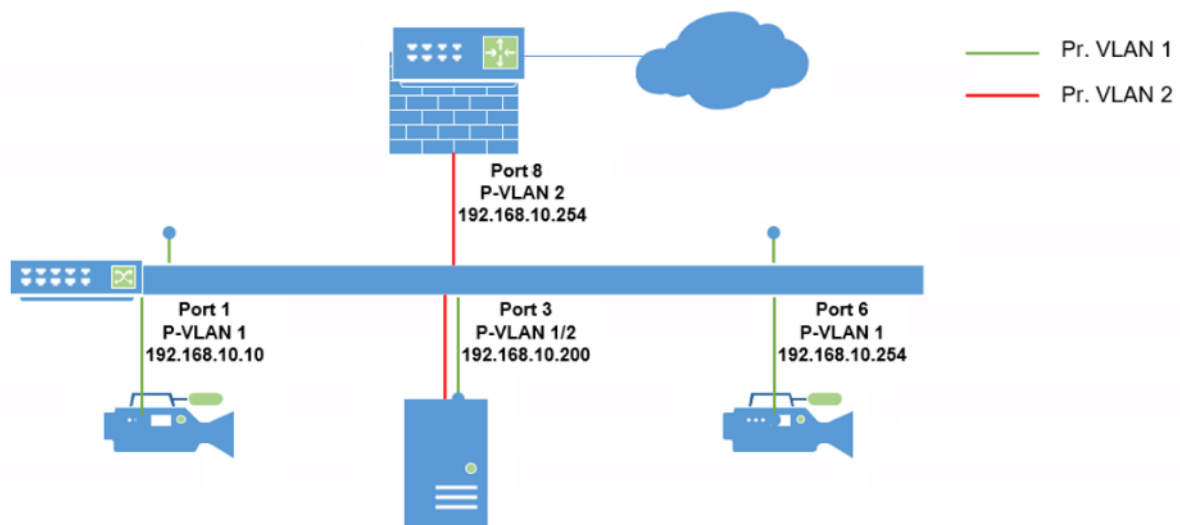
5.1.5. Private VLAN avec Port Isolation

L'utilisation de Port Isolation et Private VLAN convient, par exemple, pour la séparation de terminaux dans un même VLAN. Il empêche un lockup à partir de la layer 2 et permet la communication d'un autre sous-réseau dans le même VLAN. Avec une conception de réseau plate, les ports sélectionnés peuvent communiquer avec d'autres réseaux, par exemple une connexion WAN pour l'accès à distance.

Informations sur la planification de la demande :

- Enregistrement des composants qui communiquent entre eux
- Ajouter la séparation logique (Private VLAN) des composants et des adresses IP à la documentation

Exemple de configuration



Étape 1 :

barox RY-LGSP28-10/240 Private VLAN Membership Configuration

Switch DMS

Auto-refresh ☐ off Refresh

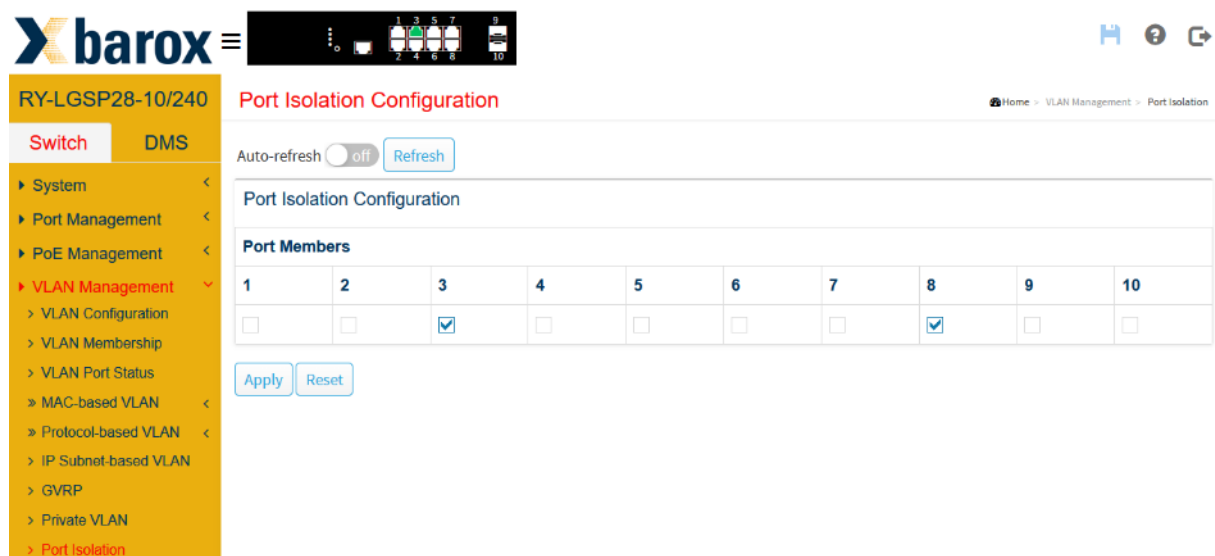
Private VLAN Membership Configuration

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10
☐	1	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒
Delete	2	☐	☐	☒	☐	☐	☐	☐	☒	☐	☐

Add New Private VLAN

Apply Reset

Étape 2 :



barox RY-LGSP28-10/240 **Port Isolation Configuration**

Auto-refresh ☐ off [Refresh](#)

Port Members

1	2	3	4	5	6	7	8	9	10
☐	☐	☒	☐	☐	☐	☐	☒	☐	☐

[Apply](#) [Reset](#)

5.2 Utilisation et protection des fonctions IP (Layer 3)

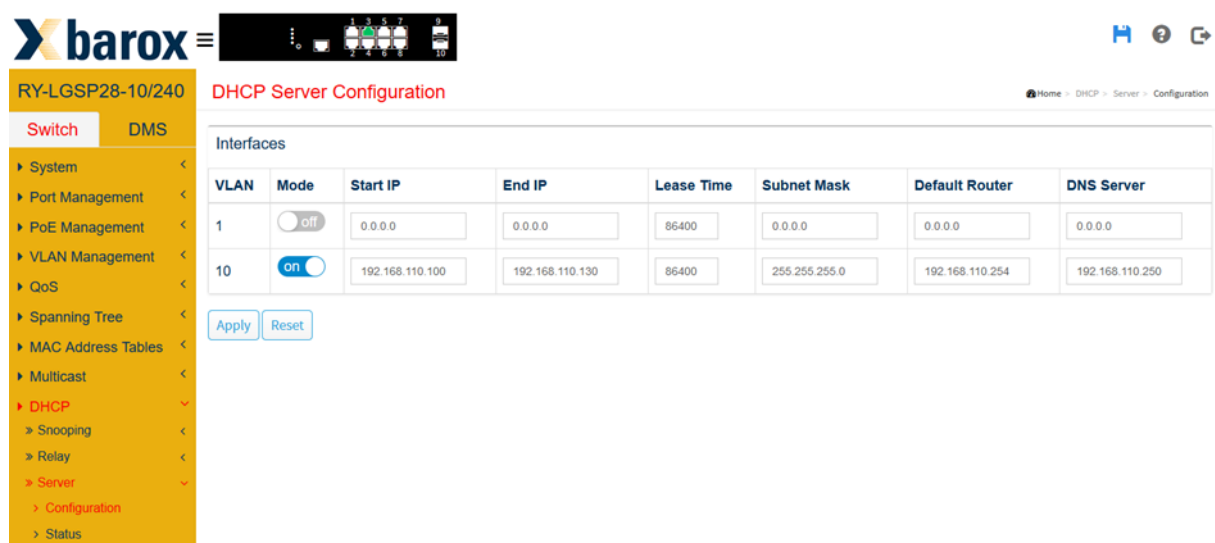
5.2.1. Serveur DHCP

Remarques sur l'utilisation de serveurs DHCP dans les réseaux vidéo

Il est important de vérifier si l'utilisation d'un serveur DHCP est généralement nécessaire du point de vue de la conception du réseau. En plus des avantages de la distribution automatisée de l'information réseau, ce service offre également un large éventail de points d'attaque.

Configuration de base et mise en service du service DHCP à l'aide de l'exemple suivant

En commençant par le VLAN du service, la taille du pool DHCP est définie en spécifiant le début et la fin ainsi que d'autres informations telles que le Lease Time en secondes, le masque de réseau, la passerelle et le serveur DNS pour la transmission du client. Le service est généralement activé dans le mode avec le réglage "On", comme indiqué ci-dessous.



barox RY-LGSP28-10/240 **DHCP Server Configuration**

Interfaces

VLAN	Mode	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
1	☐ off	0.0.0.0	0.0.0.0	86400	0.0.0.0	0.0.0.0	0.0.0.0
10	☒ on	192.168.110.100	192.168.110.130	86400	255.255.255.0	192.168.110.254	192.168.110.250

[Apply](#) [Reset](#)

Voici un aperçu de l'état du service ou des adresses des clients attribuées :



RY-LGSP28-10/240

Switch

DMS

System

Port Management

PoE Management

VLAN Management

QoS

Spanning Tree

MAC Address Tables

Multicast

DHCP

Snooping

Relay

Server

Configuration

Status

DHCP Server Status

Auto-refresh ☒ Refresh

Interfaces

VLAN	Type	Start IP	End IP	Lease Time	Subnet Mask	Default Router	DNS Server
10	Network	192.168.110.100	192.168.110.130	86400	255.255.255.0	192.168.110.254	192.168.110.250

IP Binding Status

IP	VLAN	State	MAC	Expiration
192.168.110.100	10	allocated	5c-9a-d8-5c-98-1c	26 seconds

Home

DHCP

Server

Status

5.2.2. Protection du DHCP par inspection ARP

La protection contre les clients DHCP indésirables ou la protection contre la manipulation du cache ARP peuvent être réalisées avec l'ARP Inspection. Une fois les fonctions activées, les clients DHCP peuvent être entrés statiquement en tant que destinataires dans un tableau. La condition de base pour une sécurité maximale est que la taille du pool d'adresses DHCP soit définie en fonction du nombre de clients.

Tout d'abord, la fonction Snooping est généralement activée dans le menu Snooping Mode, comme illustré ci-dessous. Vous pouvez également sélectionner le degré de confiance pour les ports du switch. Pour la fonction Inspection, le mode doit être réglé sur "Trusted".



RY-LGSP28-10/240

Switch

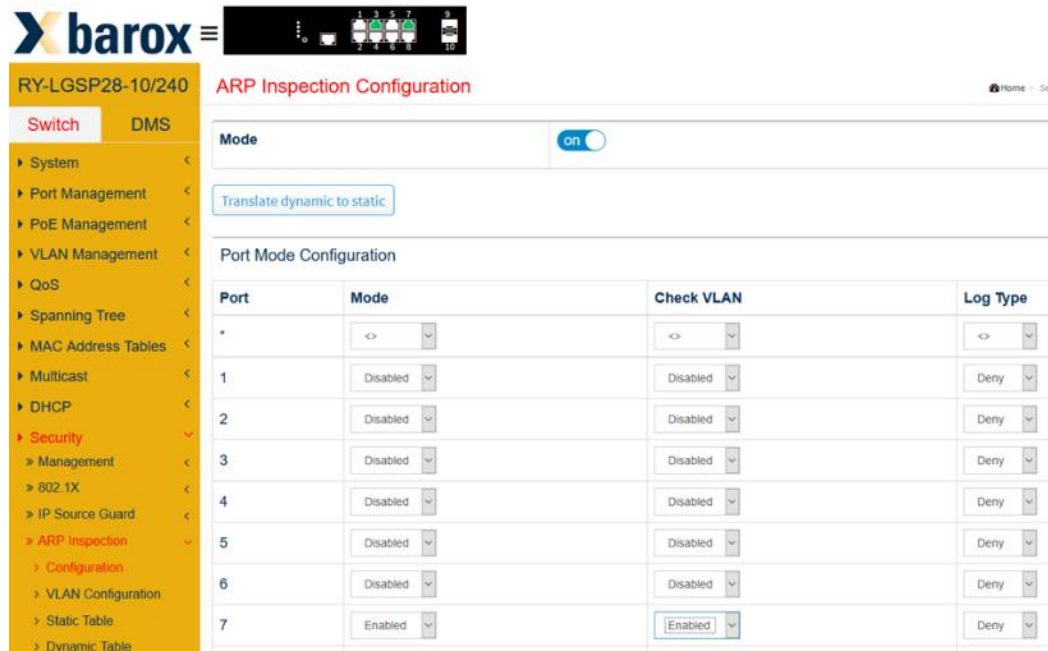
DMS

- ▶ System <
- ▶ Port Management <
- ▶ PoE Management <
- ▶ VLAN Management <
- ▶ QoS <
- ▶ Spanning Tree <
- ▶ MAC Address Tables <
- ▶ Multicast <
- ▶ **DHCP** v
- » Snooping v
- > Configuration

DHCP Snooping Configuration

Snooping Mode		☒ on
Port Mode Configuration		
Port	Mode	
*	<>	
1	Trusted v	
2	Trusted v	
3	Trusted v	
4	Trusted v	

Les paramètres des ports sont également activés et configurés. Dans l'exemple ci-dessous, l'inspection ARP est activée pour le port 7, le contrôle VLAN est activé et le type de Log est configuré.



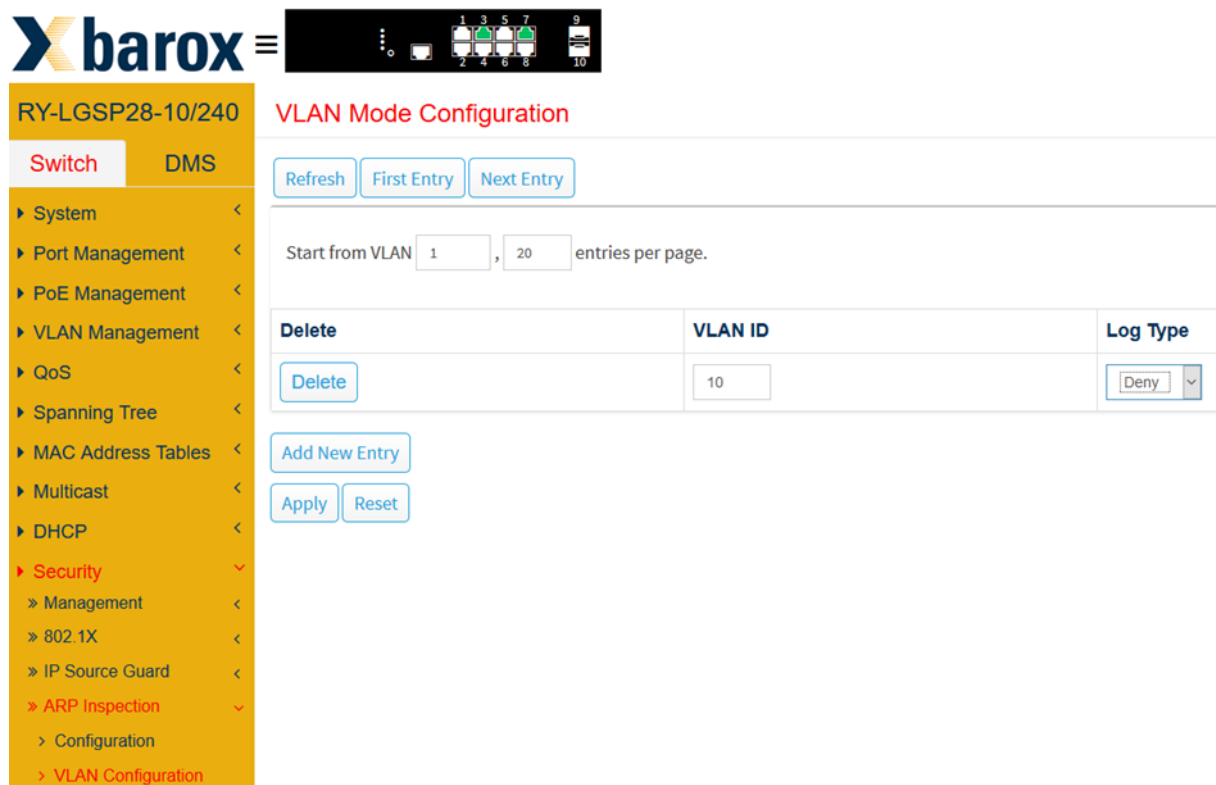
ARP Inspection Configuration

Mode: ☒ on

[Translate dynamic to static](#)

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	Deny
2	Disabled	Disabled	Deny
3	Disabled	Disabled	Deny
4	Disabled	Disabled	Deny
5	Disabled	Disabled	Deny
6	Disabled	Disabled	Deny
7	Enabled	Enabled	Deny

Ensuite, les VLAN à inclure dans le contrôle sont définis et le type de Log (degré de confiance) sont définis comme indiqué ci-dessous.



VLAN Mode Configuration

[Refresh](#) [First Entry](#) [Next Entry](#)

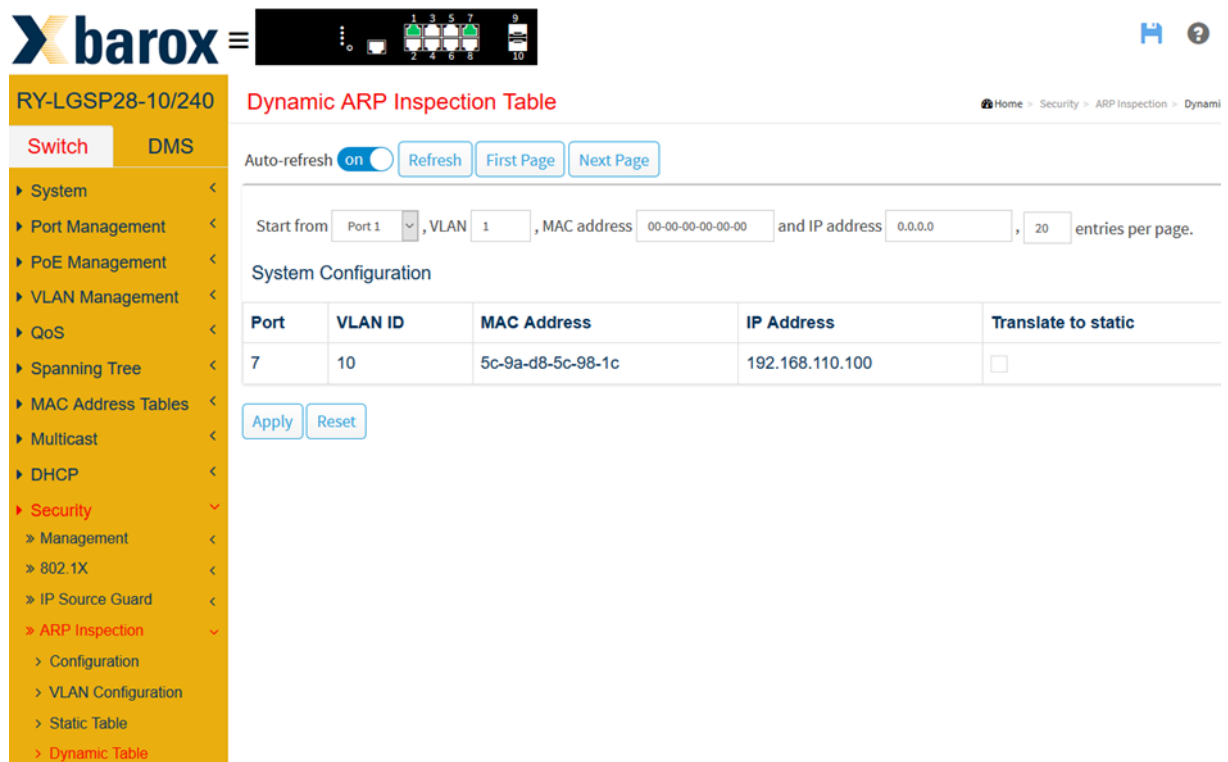
Start from VLAN , entries per page.

Delete	VLAN ID	Log Type
Delete	10	Deny

[Add New Entry](#)

[Apply](#) [Reset](#)

Une fois les réglages effectués, les clients DHCP peuvent être connectés. Une fois que le service DHCP a distribué les adresses IP, les clients ayant des propriétés Layer 2 et 3 sont visibles dans le tableau dynamique d'inspection ARP et peuvent ensuite être reportés dans le tableau statique d'inspection ARP.



The screenshot shows the barox web interface for a RY-LGSP28-10/240 switch. The left sidebar contains a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Management. The 'Security' category is expanded, showing 'ARP Inspection' as a sub-option. The main content area is titled 'Dynamic ARP Inspection Table'. It includes a search filter with fields for 'Start from' (Port 1), 'VLAN' (1), 'MAC address' (00-00-00-00-00-00), and 'IP address' (0.0.0.0), with a '20 entries per page' limit. Below the search filter is a 'System Configuration' table with columns: Port, VLAN ID, MAC Address, IP Address, and Translate to static. The table contains one entry for Port 7, VLAN 10, MAC 5c-9a-d8-5c-98-1c, and IP 192.168.110.100. There are 'Apply' and 'Reset' buttons below the table.

Une entrée statique est présentée ci-dessous. L'adresse IP est renseignée pour le client suivant le tableau.



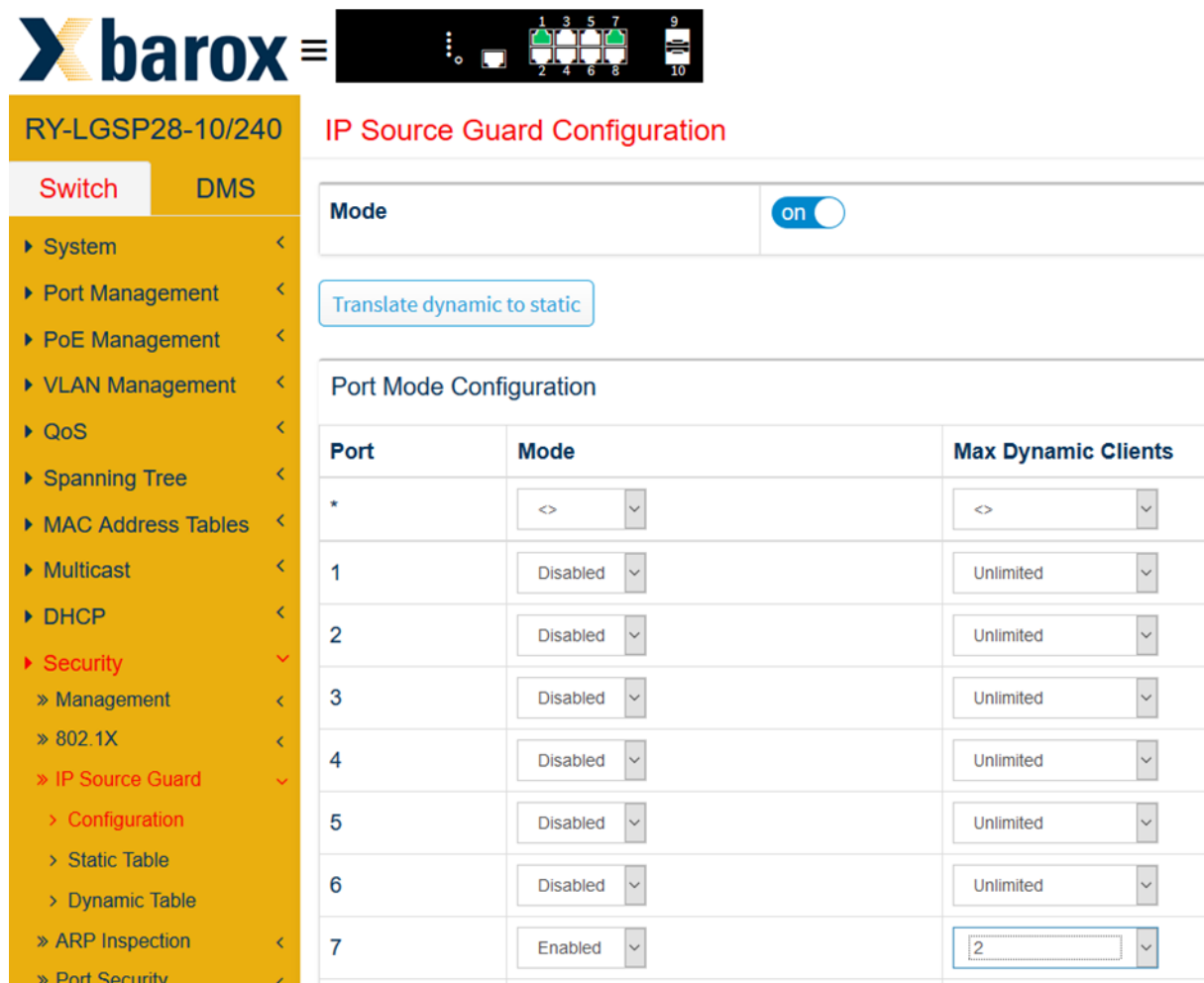
The screenshot shows the barox web interface for a RY-LGSP28-10/240 switch. The left sidebar is the same as the previous screenshot. The main content area is titled 'Static ARP Inspection Table'. It displays a table with columns: Delete, Port, VLAN ID, MAC Address, and IP Address. The table contains one entry for Port 7, VLAN 10, MAC 5c-9a-d8-5c-98-1c, and IP 192.168.110.100. There is a checkbox in the 'Delete' column for this entry.

5.2.3. IP Source Guard

Déploiement et configuration :

L'utilisation de la fonction IP Source Guard représente une fonction étendue pour sécuriser le côté du terminal. Ceci lie non seulement la recherche de l'adresse MAC du terminal mais aussi l'adresse IP statique des périphériques connectés. Elle offre par exemple une protection contre ce qu'on appelle "l'IP spoofing".

Comme indiqué ci-dessous, cette fonction est généralement activée et peut être ajustée pour chaque port.



The screenshot displays the web interface of a barox switch. On the left is a navigation menu with categories like System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Port Security. The 'Security' menu is expanded, showing 'IP Source Guard' as the selected option. The main content area is titled 'IP Source Guard Configuration'. It features a 'Mode' toggle switch set to 'on' and a button labeled 'Translate dynamic to static'. Below this is a 'Port Mode Configuration' table with three columns: 'Port', 'Mode', and 'Max Dynamic Clients'. The table lists ports 1 through 7. Ports 1-6 have 'Disabled' mode and 'Unlimited' clients, while port 7 has 'Enabled' mode and '2' clients. A small diagram of the switch's port layout is shown at the top left of the configuration area.

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Enabled	2

Une fois la fonction mise en marche, la configuration peut être effectuée avec des entrées statiques, tel qu'illustré ci-dessous.





RY-LGSP28-10/240

Switch
DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
 - Management
 - 802.1X
 - IP Source Guard
 - Configuration
 - Static Table

Static IP Source Guard Table

Home > Security > IP Source Guard

Delete	Port	VLAN ID	IP Address	MAC address
Delete	3	10	192.168.110.40	A1:00:00:00:00:FF

L'utilisation d'IP Source Guard permet d'étendre la fonction de sécurité en sécurisant le port avec des adresses MAC et IP. Par rapport à Port Security, où les entrées d'adresse MAC statiques par port sont censées empêcher une éventuelle attaque, l'IP Source Guard, avec des entrées statiques, offre, en plus de l'état du périphérique connecté, une vérification de l'adresse IP. Si les conditions, l'adresse MAC et l'IP assignées sur le port de l'appareil connecté, ne sont pas remplies, le switch bloquera la communication réseau sur le port. Cela signifie que l'attaquant doit connaître l'adresse MAC et l'adresse IP du périphérique pour accéder au réseau.

L'IP Source Guard offre également une autre option pour sécuriser un DHCP configuré sur le switch. Ce type d'utilisation nécessite la fonction de Snooping DHCP qui s'active sous *Switch > DHCP > Snooping > Configuration*. Les clients protégés peuvent être visualisés dans le tableau dynamique comme le montre l'image suivante.





RY-LGSP28-10/240

Switch
DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
 - Management
 - 802.1X
 - IP Source Guard
 - Configuration
 - Static Table
 - Dynamic Table

Dynamic IP Source Guard Table

Home > Security

Auto-refresh ☒ Refresh First Page Next Page

Start from Port 1, VLAN 1 and IP address 0.0.0.0, 20 entries per page.

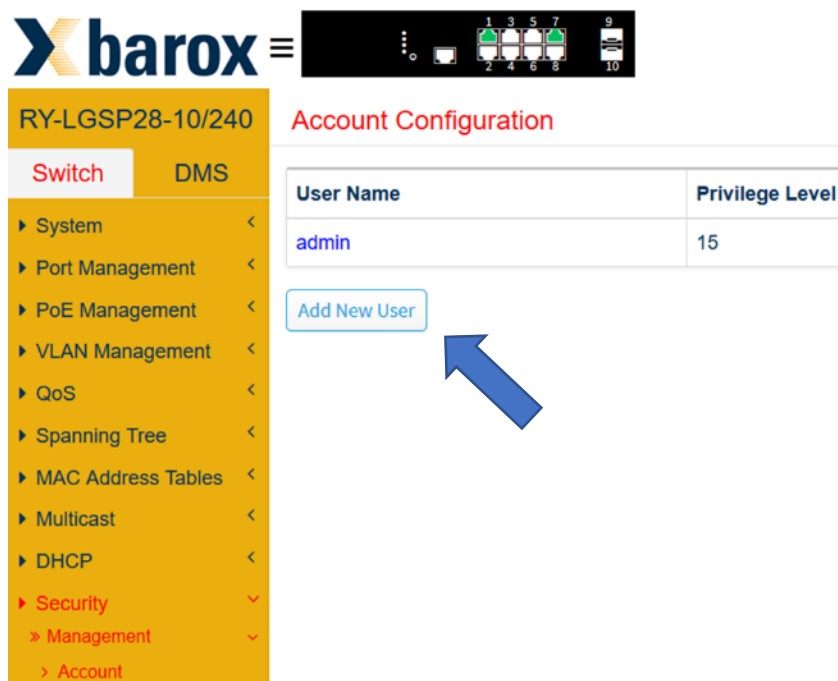
Port	VLAN ID	IP Address	MAC Address
7	10	192.168.110.100	5c-9a-d8-5c-98-1c

5.3 Protection de la gestion des switches et administration réseau (layer 3 – 7)

5.3.1. Administration et configuration des utilisateurs

Créer un utilisateur

Vous trouverez ci-dessous un exemple de création d'un autre utilisateur :

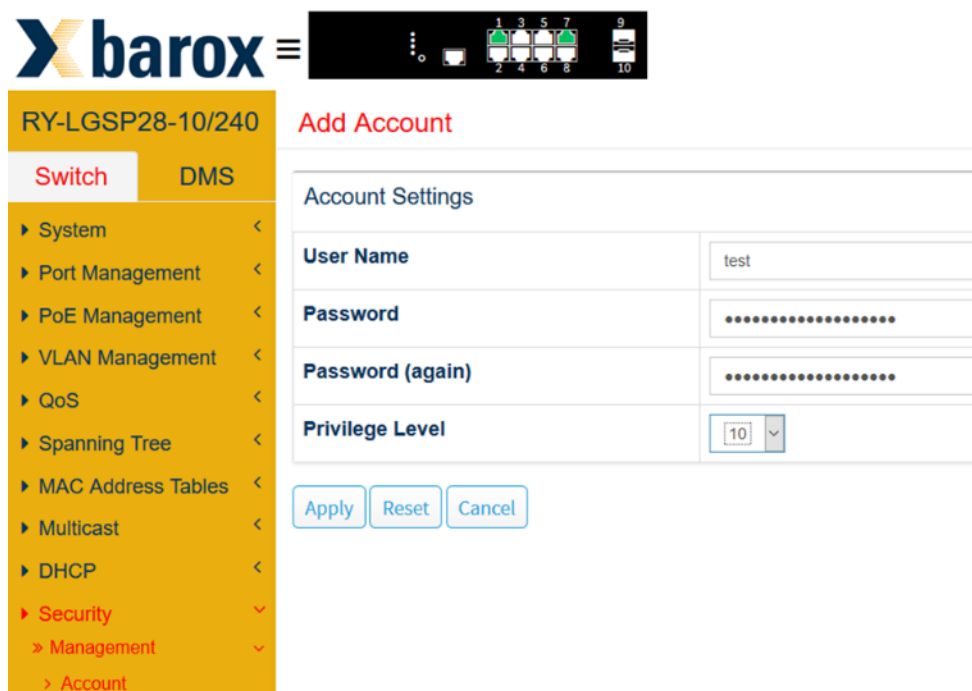


barox RY-LGSP28-10/240

Account Configuration

User Name	Privilege Level
admin	15

[Add New User](#)



barox RY-LGSP28-10/240

Add Account

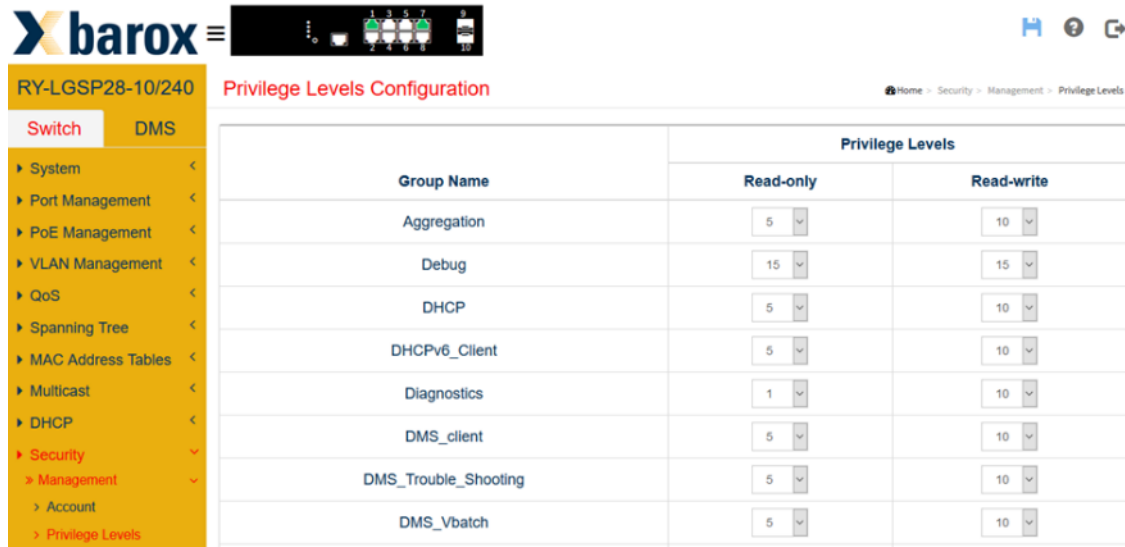
Account Settings

User Name	test
Password	
Password (again)	
Privilege Level	10

[Apply](#) [Reset](#) [Cancel](#)

Paramètres de base des directives et privilèges utilisateur :

- Les niveaux de privilèges (Privilege Level) sont utilisés pour graduer les droits aux paramètres de configuration ou à la lecture et l'écriture des valeurs. Il est recommandé de ne pas modifier les valeurs par défaut, mais de les affecter lors de la création de nouveaux utilisateurs.
- Remarque : Il est utile d'adapter les droits d'un autre utilisateur en fonction de ses habilitations et compétences.



barox RY-LGSP28-10/240 Privilege Levels Configuration

Home > Security > Management > Privilege Levels

Group Name	Privilege Levels	
	Read-only	Read-write
Aggregation	5	10
Debug	15	15
DHCP	5	10
DHCPv6_Client	5	10
Diagnostics	1	10
DMS_client	5	10
DMS_Trouble_Shooting	5	10
DMS_Vbatch	5	10

5.3.2. Utilisation et paramétrage de l'authentification au niveau de la gestion des switches

Protection de l'accès CLI **ssh** vs. **telnet**

Comme indiqué ci-dessous, la méthode d'accès peut être définie ou les fonctions inutilisées peuvent être désactivées. Il est recommandé, si la conception du réseau le permet, de désactiver la fonction d'accès Telnet en général. Les méthodes de configuration peuvent être définies comme indiqué ci-dessous.

barox RY-LGSP28-10/240 Authentication Method Configuration

Home > Security > Management > Auth Method

Switch DMS

System < Port Management < PoE Management < VLAN Management < QoS < Spanning Tree < MAC Address Tables < Multicast < DHCP < Security > Management > Account > Privilege Levels > Auth Method

Client	Methods	Service Port
console	local no no	
telnet	no no no	23
ssh	local no no	22
http	local no no	80
https	no no no	443

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	☐

- Il est recommandé d'utiliser le protocole SSH pour l'administration en ligne de commande (CLI), car cette méthode fournit la connexion cryptée.

Gestion de l'accès à l'interface web (GUI) avec HTTP :

- Il est recommandé de créer un utilisateur séparé pour HTTP
- Modifier le port 80, Remarque : Respecter les spécifications du port lors de l'accès dans le navigateur !
- L'accès HTTPS offre la meilleure protection, car la connexion est cryptée.

barox RY-LGSP28-10/240 Authentication Method Configuration

Home > Security > Management > Auth Method

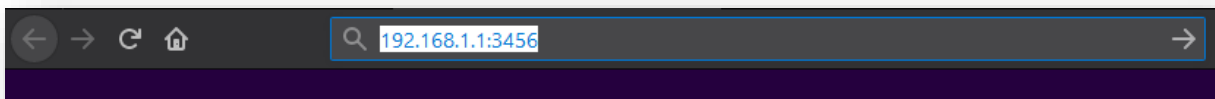
Switch DMS

System < Port Management < PoE Management < VLAN Management < QoS < Spanning Tree < MAC Address Tables < Multicast < DHCP < Security > Management > Account > Privilege Levels > Auth Method

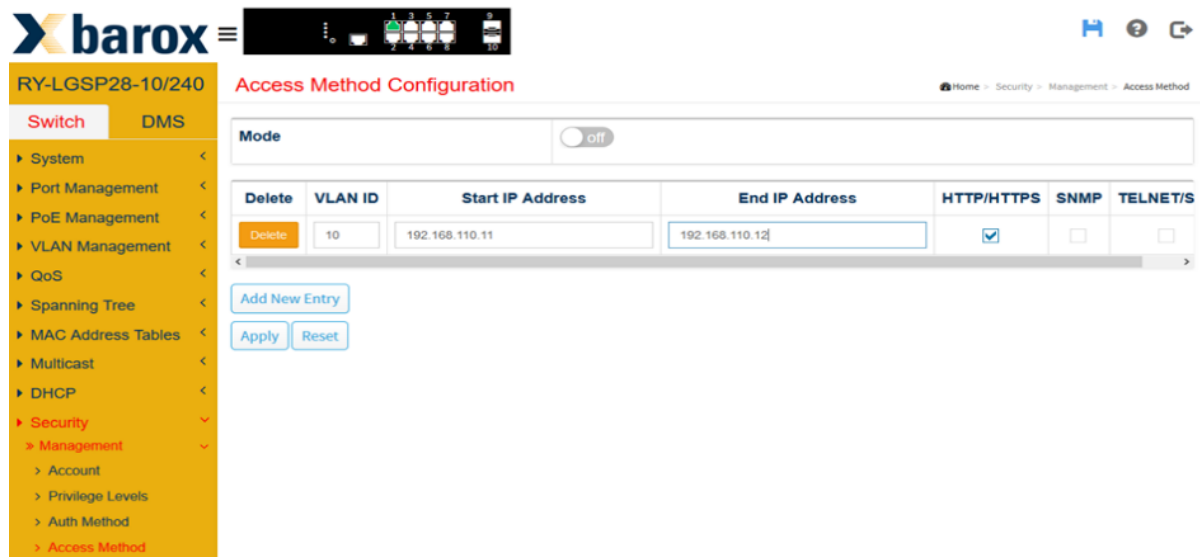
Client	Methods	Service Port
console	local no no	
telnet	local no no	23
ssh	local no no	22
http	local no no	3456
https	no no no	443

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	☐

L'exemple suivant montre la saisie de l'adresse d'administration avec port modifié :



La restriction de l'accès à la gestion et de ses méthodes peut être limitée à certaines plages d'adresses IP et à certains VLAN. Ceci peut être fait dans l'Access Management, comme le montre l'exemple ci-dessous.



! Attention !

Il est obligatoire de choisir une méthode pour chaque entrée. Toutefois, si la méthode en question est généralement désactivée, le switch de ce VLAN ne peut plus être géré ou l'accès à la gestion est exclu. La "mauvaise configuration" peut être annulée en redémarrant l'appareil.

5.3.3. Gestion des accès et utilisation de HTTPS

La possibilité de paramétrage de l'utilisation du protocole HTTPS est également illustrée.

The screenshot shows the web interface of a barox switch. The left sidebar contains a navigation menu with the following items: System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, and Management. The 'Security' and 'Management' items are expanded, showing sub-items: Account, Privilege Levels, and Auth Method. The main content area is titled 'Authentication Method Configuration' and contains two tables.

Authentication Method

Client	local	no	no	Service Port
console	local	no	no	
telnet	local	no	no	23
ssh	local	no	no	22
http	no	no	no	80
https	local	no	no	443

Command Authorization Method

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	☐

Le port normalisé peut également être modifié avec cette méthode.

Si le mode est activé, l'option http doit être désactivée. La GUI du switch est appelée dans le navigateur à l'aide de la phrase de protocole HTTPS [https://192.168.XX\(votreIP de gestion\):1234\(votre port\)](https://192.168.XX(votreIP de gestion):1234(votre port)) dans le champ URL. Une fois définie, la communication du navigateur avec l'interface de gestion est cryptée.

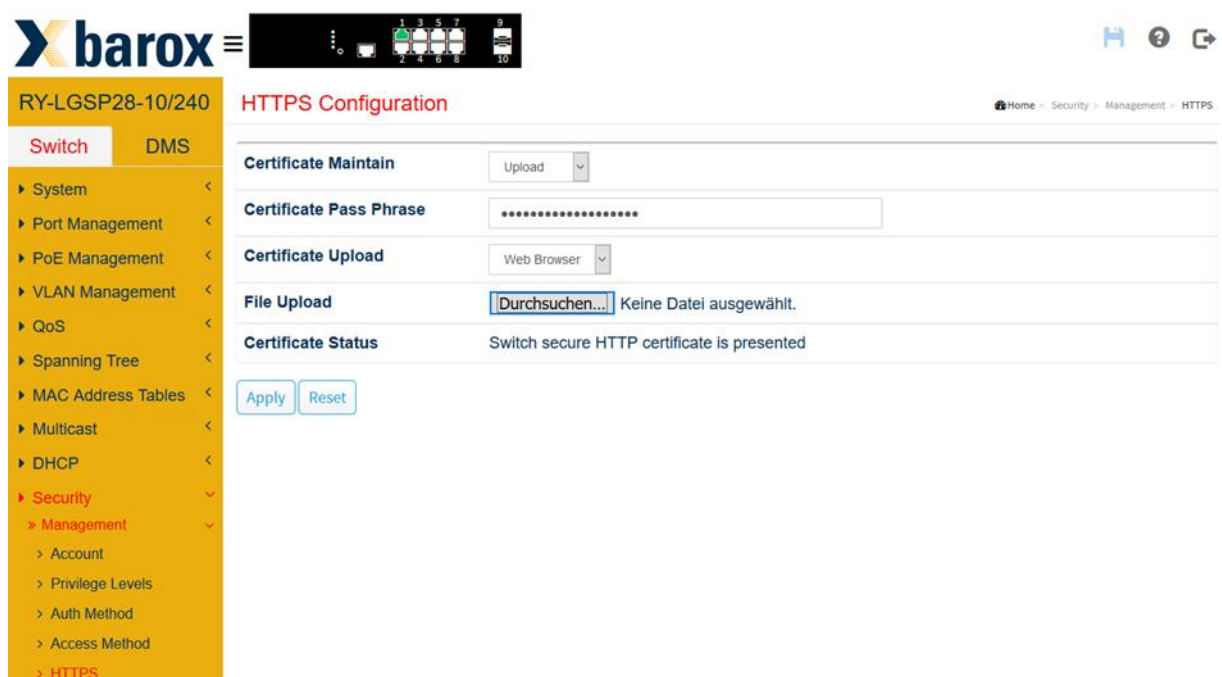
5.3.4. Configuration et déploiement de l'accès à la gestion basé sur les certificats

Brève remarque sur l'utilisation des certificats :

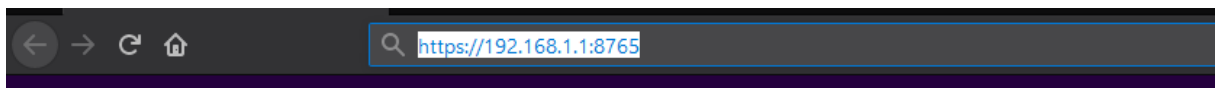
Une connexion basée sur un certificat permet l'un des plus hauts niveaux actuels de protection d'accès pour les services de configuration en réseau. Néanmoins, l'utilisation doit être vérifiée, car la connexion à la gestion ne peut se faire que par l'intermédiaire des supports qui ont intégré le certificat.

Les options et méthodes de réglage sont indiquées ci-dessous.

- Génération du certificat pour une utilisation ultérieure, qui peut être téléchargé et installé via le navigateur.
- Téléchargement d'un certificat généré en externe



- L'accès au navigateur a lieu après l'installation du certificat et la définition de la méthode d'authentification HTTPS via le protocole HTTPS.



5.4 SNMP - Fonction de surveillance et d'administration

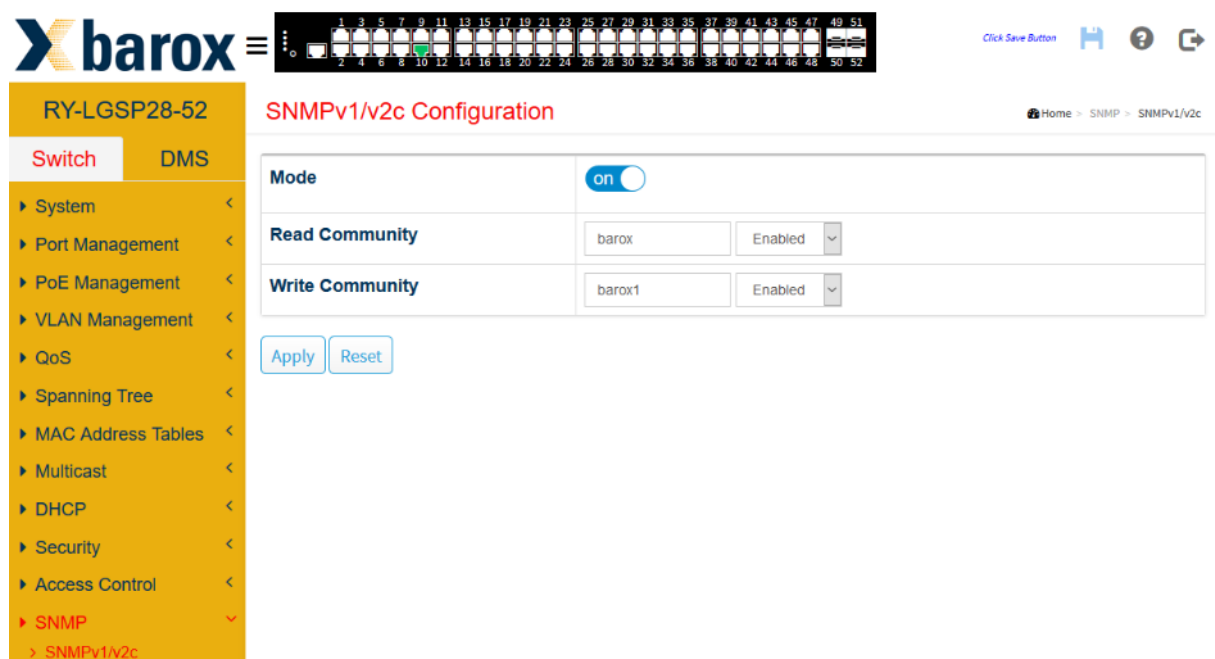
SNMP a été développé par l'IETF (Internet Engineering Task Force) et sert de protocole pour surveiller, contrôler et configurer les éléments du réseau.

5.4.1. Configuration SNMP v2c

Ci-dessous, un exemple décrit une configuration de base SNMP v2 pour l'interrogation de l'état du système ou l'envoi d'événements système via des Traps SNMP. Les étapes suivantes sont destinées à démontrer l'utilisation d'une Community SNMP.

Activation de la fonction SNMP v2

Fondamentalement, le mode doit être activé. Les noms des Communities Read et Write sont également définis et la Community Write est activée.

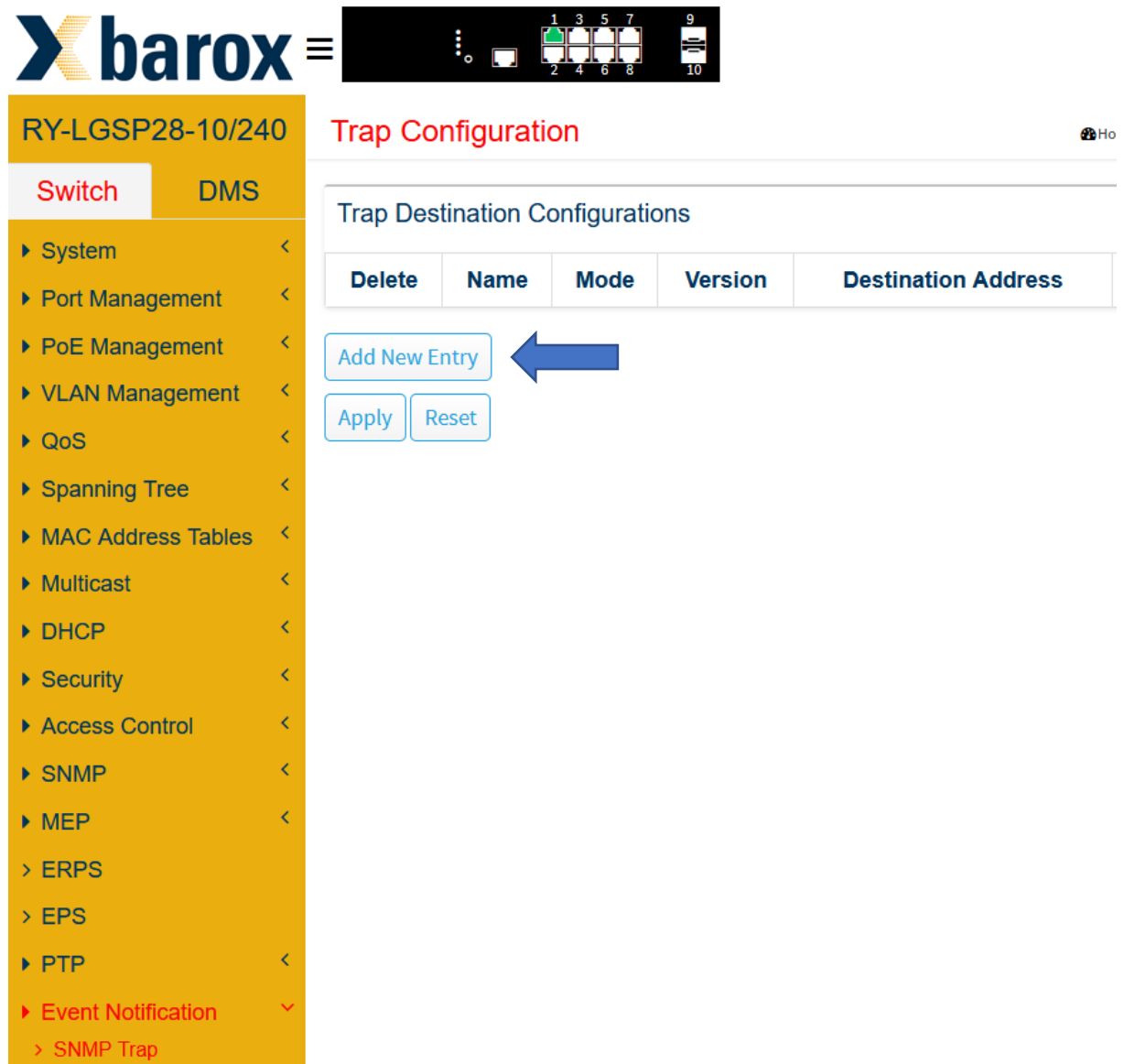


The screenshot displays the barox web interface for the RY-LGSP28-52 device. The top navigation bar features the barox logo and a status bar with 52 ports. The left sidebar shows a menu with 'Switch' and 'DMS' tabs, and a list of configuration categories including System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, and SNMP. The main content area is titled 'SNMPv1/v2c Configuration' and contains a form with fields for Mode (set to 'on'), Read Community (set to 'barox'), and Write Community (set to 'barox1'). There are 'Apply' and 'Reset' buttons at the bottom of the form.

Enfin, il faut enregistrer les changements dans la configuration de démarrage et redémarrer le switch.

5.4.2. Configuration de la Trap SNMP

Pour la réception de messages Trap SNMP, il faut définir les paramètres nécessaires à la connexion avec le destinataire cible. Il faut commencer par la création d'une configuration.



barox RY-LGSP28-10/240

Trap Configuration

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

Trap Destination Configurations

Delete	Name	Mode	Version	Destination Address
--------	------	------	---------	---------------------

Add New Entry

Apply Reset

L'exemple suivant montre comment définir les valeurs suivantes pour une nouvelle configuration :

- Trap Config Name -> Un nom doit être attribué
- Trap Mode -> UDP ou TCP – au début, UDP comme d'habitude
- Trap Version -> Sélection de SNMP v2c
- Trap Community -> Le nom de la Community précédemment créé doit être entré
- Trap Destination Address -> Saisie de l'adresse IP du destinataire Trap
- Trap Destination Port -> Saisie du port pour le destinataire
- D'autres paramètres peuvent être appliqués dans un premier temps à partir paramètres par défaut

Les réglages sont ensuite confirmés avec "Apply"

barox RY-LGSP28-10/240 **SNMP Trap Configuration** Home > Event Notification

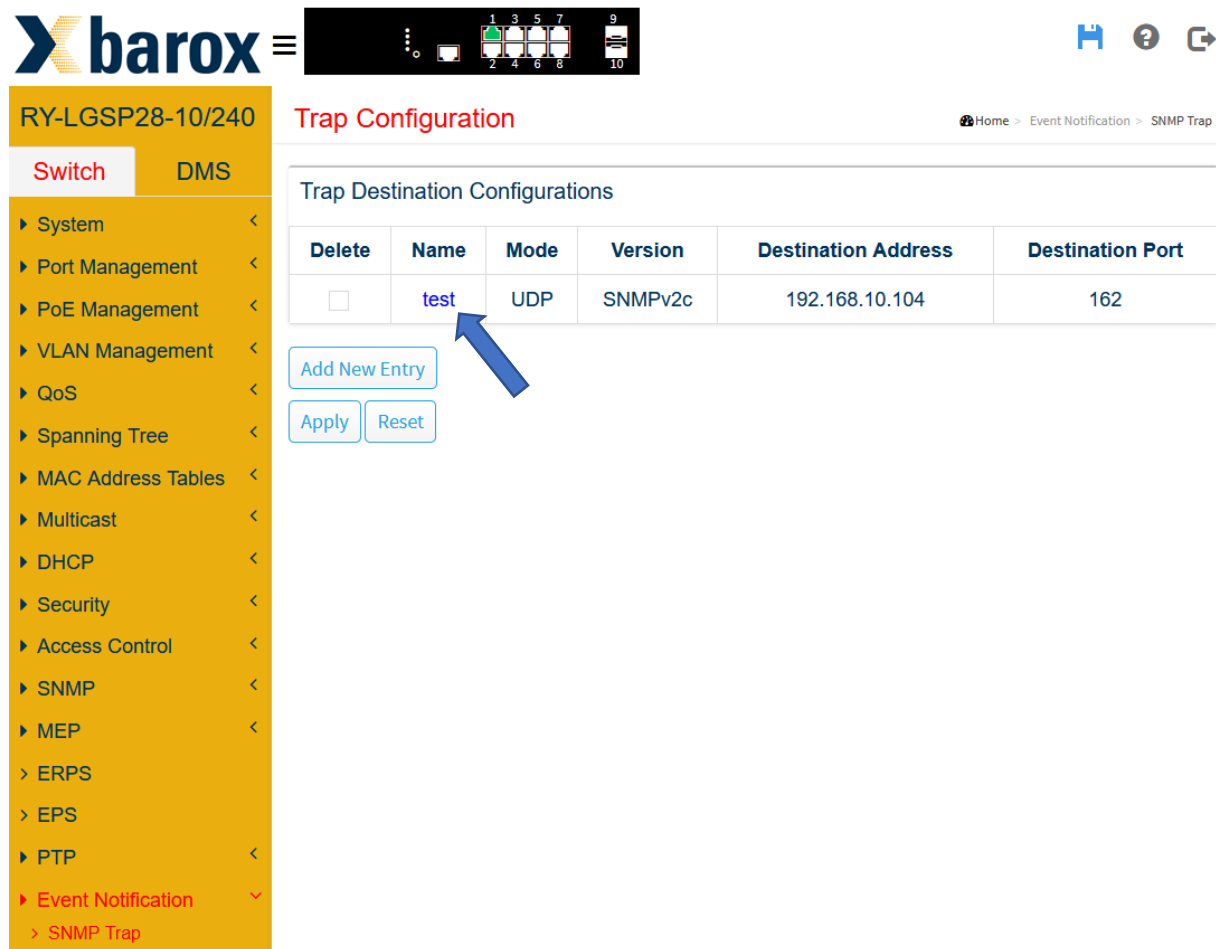
Switch **DMS**

- 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**

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

Une fois la nouvelle configuration créée, elle apparaît dans le niveau supérieur. La configuration peut être ouverte en sélectionnant le nom.



The screenshot displays the barox web interface for the RY-LGSP28-10/240 switch. The left sidebar contains a menu with various configuration categories, including System, Port Management, PoE Management, VLAN Management, QoS, Spanning Tree, MAC Address Tables, Multicast, DHCP, Security, Access Control, SNMP, MEP, ERPS, EPS, PTP, and Event Notification. The Event Notification category is expanded, showing the SNMP Trap option. The main content area is titled 'Trap Configuration' and shows a table of 'Trap Destination Configurations'. The table has columns for Delete, Name, Mode, Version, Destination Address, and Destination Port. A single entry is listed with the name 'test', Mode 'UDP', Version 'SNMPv2c', Destination Address '192.168.10.104', and Destination Port '162'. A blue arrow points to the 'test' name. Below the table are buttons for 'Add New Entry', 'Apply', and 'Reset'.

Delete	Name	Mode	Version	Destination Address	Destination Port
☐	test	UDP	SNMPv2c	192.168.10.104	162

Désactivation de la fonction Trap SNMP

La désactivation peut se faire de deux manières. D'une part, elle peut être désactivée en supprimant la configuration. Si l'envoi de Trap ne doit être utilisé que sporadiquement, il est recommandé de régler la fonction sur "Disabled" dans la configuration.

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 > Event

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

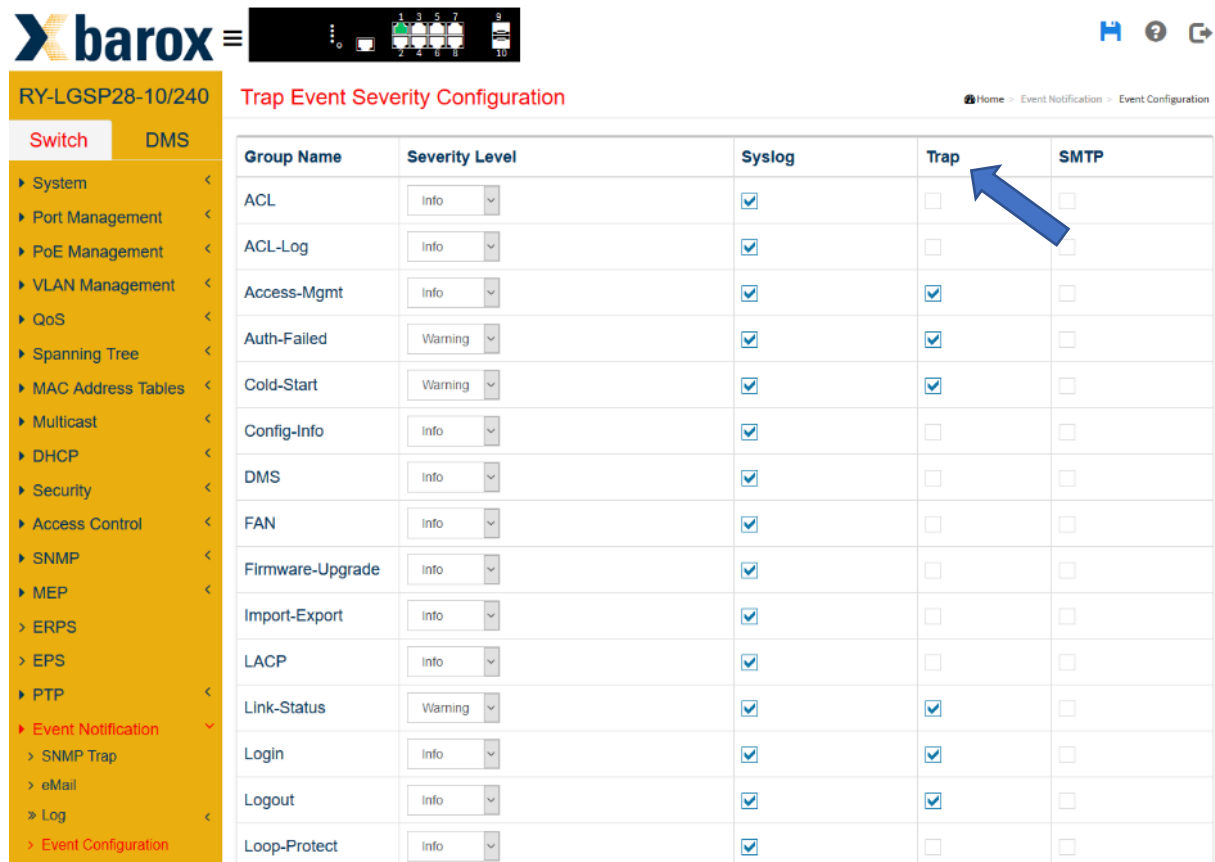
None

Apply

Reset

5.4.3. Informations supplémentaires pour l'envoi de Traps SNMP

Assurez-vous que les événements qui déclenchent une Trap sont configurés en conséquence. Ces réglages peuvent être configurés ailleurs dans le menu de configuration, comme indiqué ci-dessous, en fonction du terminal. Certains événements tels que les Port Events doivent également être définis en conséquence dans la configuration des ports.



The screenshot displays the 'Trap Event Severity Configuration' page in the barox web interface. The left sidebar shows a navigation menu with categories like 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, and Event Configuration. The main content area features a table with columns for Group Name, Severity Level, Syslog, Trap, and SMTP. A blue arrow points to the 'Trap' column header.

Group Name	Severity Level	Syslog	Trap	SMTP
ACL	Info	☒	☐	☐
ACL-Log	Info	☒	☐	☐
Access-Mgmt	Info	☒	☒	☐
Auth-Failed	Warning	☒	☒	☐
Cold-Start	Warning	☒	☒	☐
Config-Info	Info	☒	☐	☐
DMS	Info	☒	☐	☐
FAN	Info	☒	☐	☐
Firmware-Upgrade	Info	☒	☐	☐
Import-Export	Info	☒	☐	☐
LACP	Info	☒	☐	☐
Link-Status	Warning	☒	☒	☐
Login	Info	☒	☒	☐
Logout	Info	☒	☒	☐
Loop-Protect	Info	☒	☐	☐

Vous trouverez de plus amples informations sur la lecture et le test de la configuration au point "5.6 Lecture des Traps SNMP".

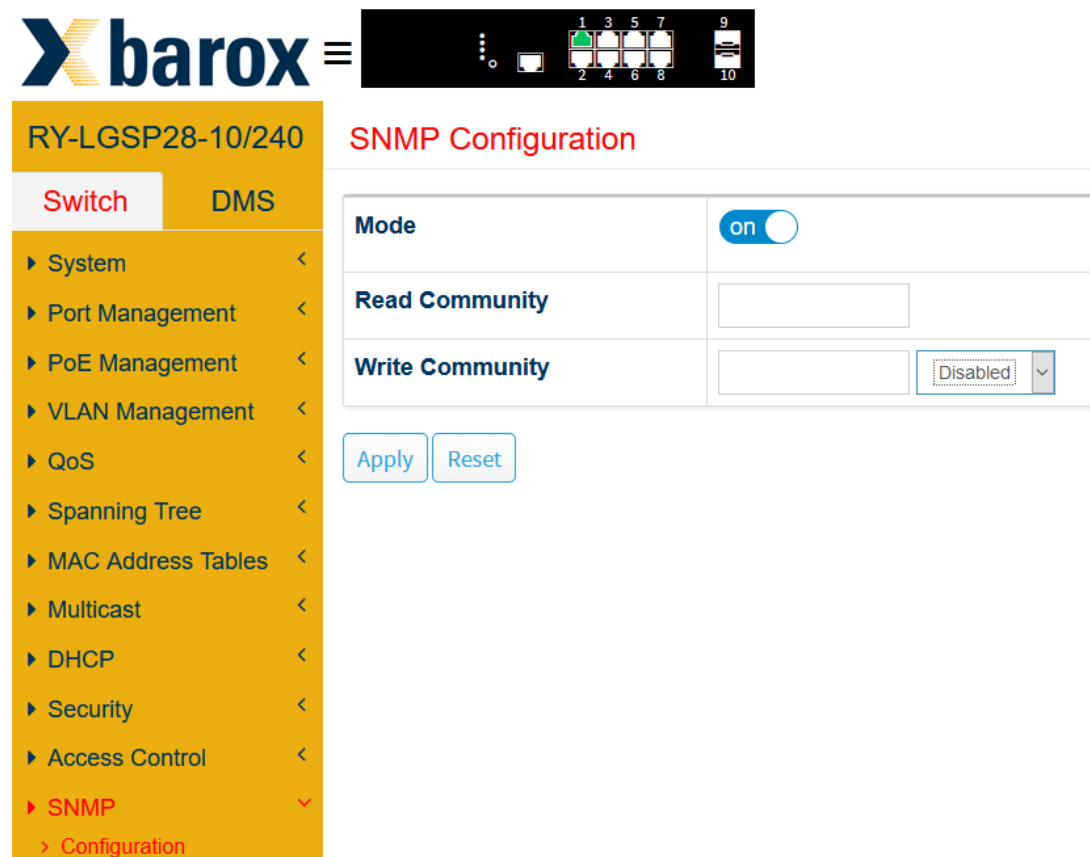
5.5 Configuration SNMP v3

Situation de départ :

Le besoin accru de sécurité dans le réseau se traduit également par des exigences accrues en matière d'administration et de surveillance des composants du réseau. Ceci peut être fait par exemple en utilisant la version 3 de SNMP avec authentification. Ci-dessous, un exemple décrit une configuration de base SNMP v3 pour l'interrogation de l'état du système ou l'envoi d'événements système via des Traps SNMP. Les étapes suivantes visent à démontrer l'utilisation de l'authentification et de la protection par mot de passe.

5.5.1. Activation de la fonction SNMP v3

Fondamentalement, le mode SNMP doit être activé. Les entrées de texte de la Community Read et Write (par défaut "public" et "private") doivent également être supprimées et la Community Write doit être placée sur le statut "Disabled".



barox RY-LGSP28-10/240

Switch **DMS**

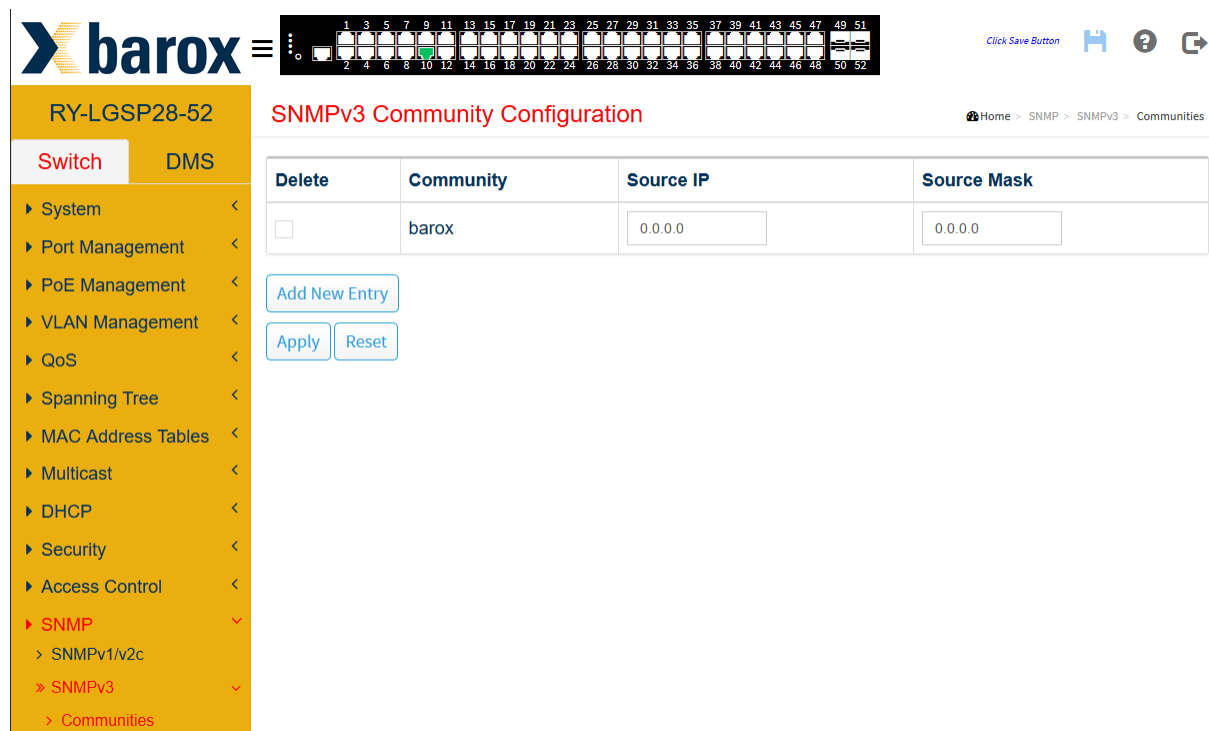
- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
- Access Control
- SNMP**
 - Configuration

SNMP Configuration

Mode	☒ on
Read Community	
Write Community	Disabled

Créer une Community dédiée

Lors de la génération de la Community, l'IP source et le masque peuvent rester tous les deux à 0.0.0.0. Cela permet d'envoyer des messages SNMP également sur plusieurs sous-réseaux.



RY-LGSP28-52

Switch DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
- Access Control
- SNMP**
 - SNMPv1/v2c
 - SNMPv3**
 - Communities**

SNMPv3 Community Configuration

Home > SNMP > SNMPv3 > Communities

Delete	Community	Source IP	Source Mask
☐	barox	0.0.0.0	0.0.0.0

[Add New Entry](#)

[Apply](#) [Reset](#)

Créer un nouvel utilisateur

Lors de la configuration du nouvel utilisateur, veuillez noter que l'Engine ID est ajouté automatiquement au nouvel objet utilisateur. En plus de spécifier le nom d'utilisateur, il faut définir le niveau de sécurité, dans cet exemple "Auth, Priv". Lors de la sélection du protocole d'authentification "MD5" et du protocole de confidentialité DES, veuillez noter que les deux mots de passe doivent comporter au moins 8 caractères (combinaisons de chiffres et de lettres).



RY-LGSP28-52

Switch DMS

- System
- Port Management
- PoE Management
- VLAN Management
- QoS
- Spanning Tree
- MAC Address Tables
- Multicast
- DHCP
- Security
- Access Control
- SNMP**
 - SNMPv1/v2c
 - SNMPv3**
 - Users**

SNMPv3 User Configuration

Home > SNMP > SNMPv3 > Users

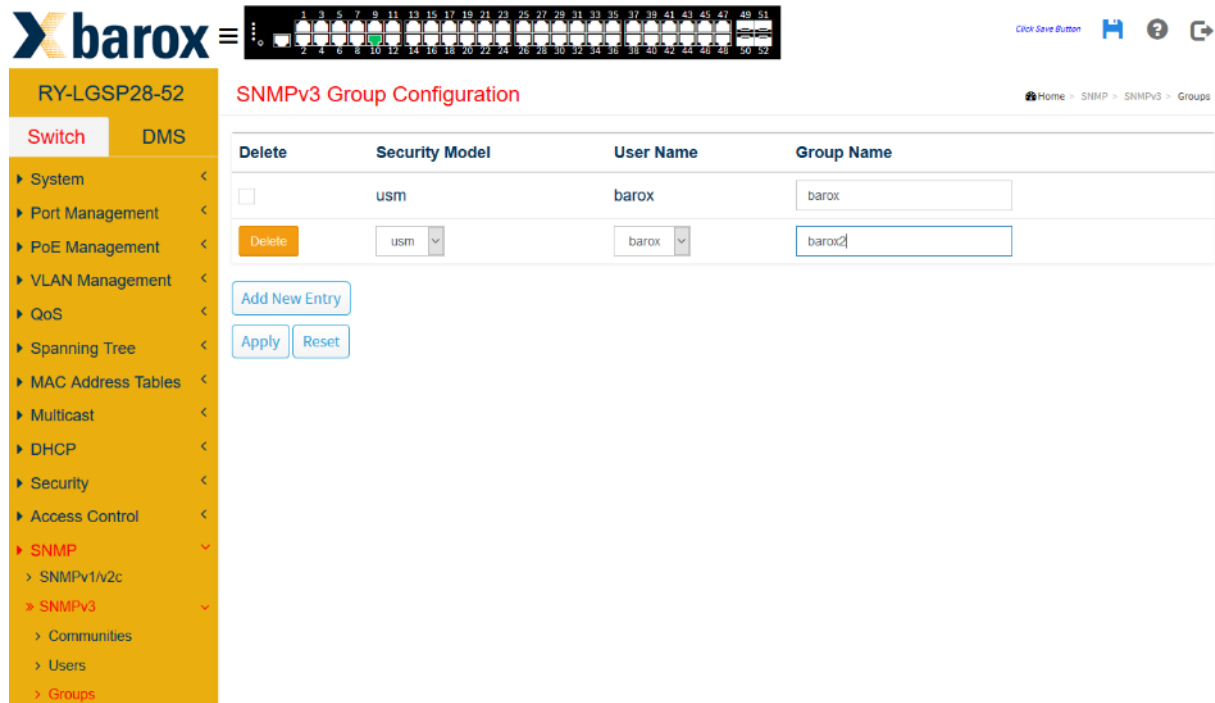
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800014550338b8eb22e828	barox	Auth, Priv	MD5	*****	DES	*****
Delete	800014550338b8eb22e82	barox2	Auth, Priv	MD5		DES	

[Add New Entry](#)

[Apply](#) [Reset](#)

Créer un groupe

Pour configurer un nouveau groupe dans SNMP v3, sélectionner "*usm*" comme modèle de sécurité. Sélectionner le nom d'utilisateur précédemment créé comme "*Security Name*" et lui attribuer un nom de groupe.



RY-LGSP28-52

Switch DMS

System < Port Management < PoE Management < VLAN Management < QoS < Spanning Tree < MAC Address Tables < Multicast < DHCP < Security < Access Control < **SNMP** > SNMPv1/v2c > **SNMPv3** > Communities > Users > Groups

SNMPv3 Group Configuration

Home > SNMP > SNMPv3 > Groups

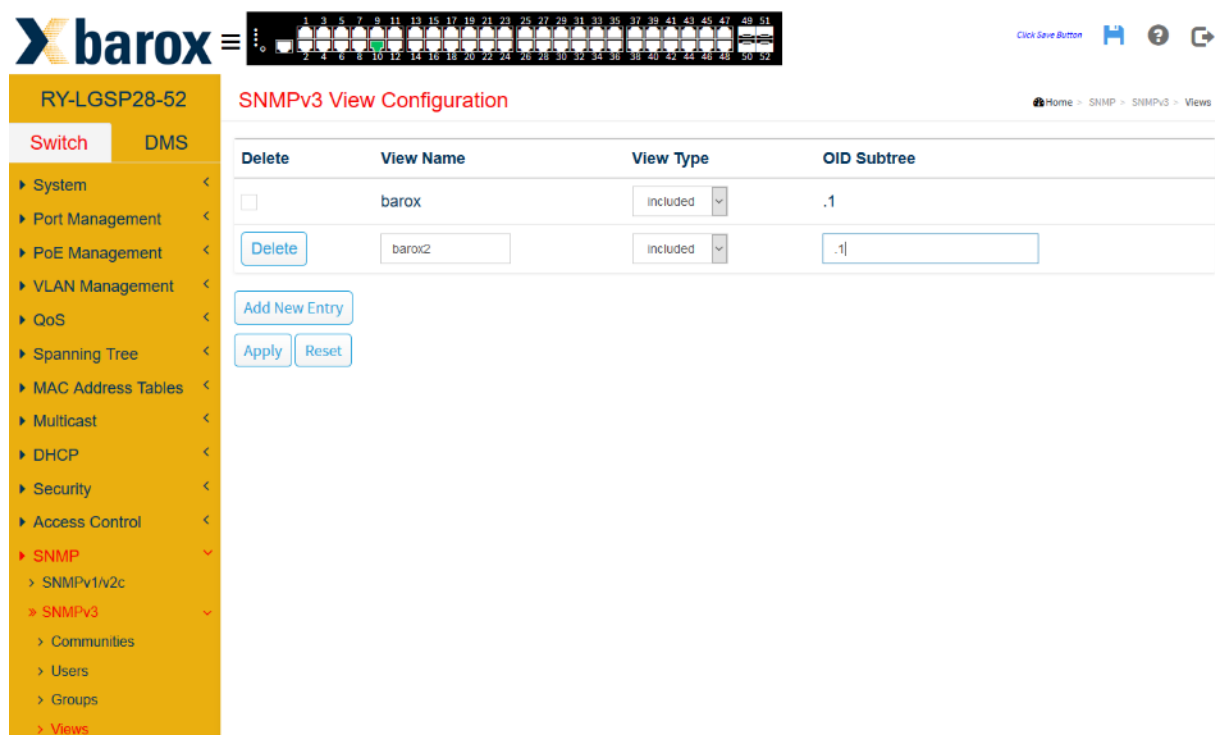
Delete	Security Model	User Name	Group Name
☐	usm	barox	barox
Delete	usm	barox	barox2

Add New Entry

Apply Reset

Paramétrage de la configuration View

On définit d'abord le View Name. Si tous les messages SNMP pertinents sont visibles, il est recommandé de régler l'OID sur la valeur ".1". Ceci permet d'avoir une vue complète de tous les OID ramifiés.



RY-LGSP28-52

Switch DMS

System < Port Management < PoE Management < VLAN Management < QoS < Spanning Tree < MAC Address Tables < Multicast < DHCP < Security < Access Control < **SNMP** > SNMPv1/v2c > **SNMPv3** > Communities > Users > Groups > **Views**

SNMPv3 View Configuration

Home > SNMP > SNMPv3 > Views

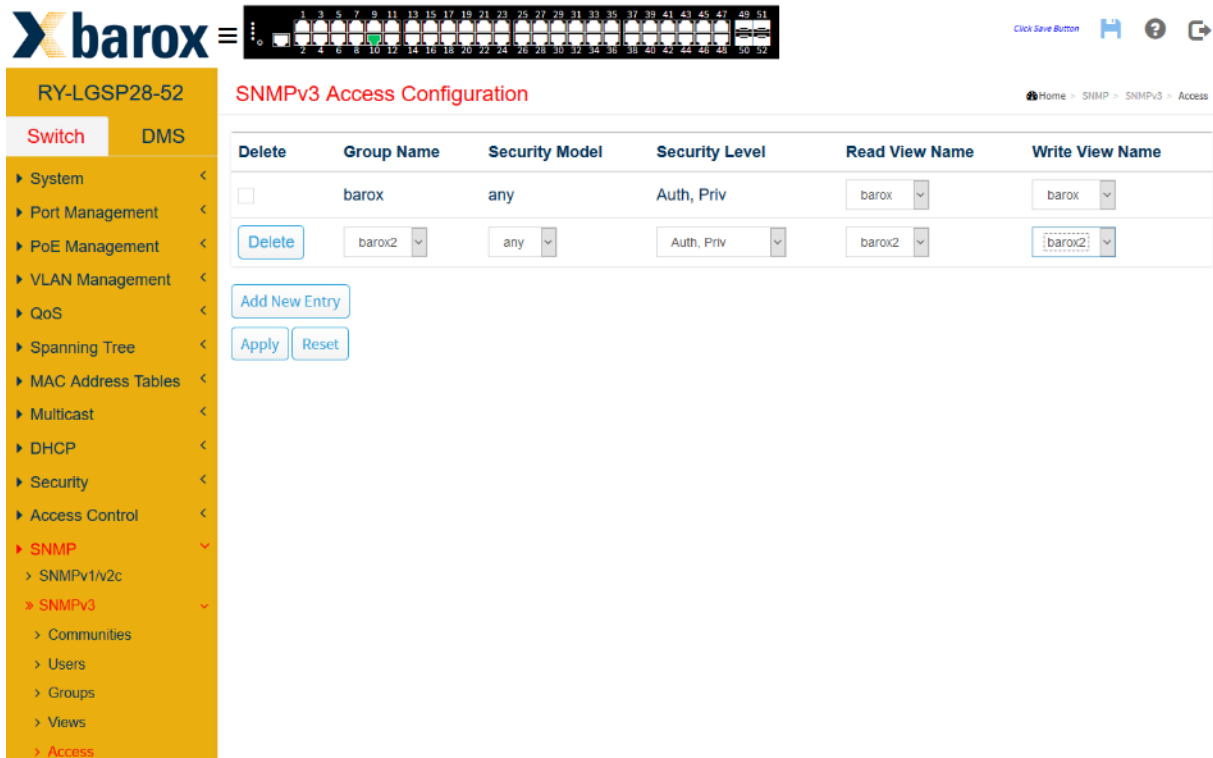
Delete	View Name	View Type	OID Subtree
☐	barox	included	.1
Delete	barox2	included	.1

Add New Entry

Apply Reset

Configuration de la méthode d'accès

Pour ce faire, une nouvelle entrée avec la méthode d'authentification et de privatisation doit être générée. Sélectionner d'abord le groupe précédemment créé sous "Group Name". Le groupe se voit ensuite attribuer le "Security Model" – "usm" et le "Security Level" – "Auth, Priv". Enfin, pour la lecture et l'écriture, les Views précédemment créées sont sélectionnées sous "Read View Name" et "Write View Name".



The screenshot displays the barox RY-LGSP28-52 web interface. The top status bar shows a bar chart with 52 bars, each labeled with a number from 1 to 52. The sidebar menu on the left lists various configuration options, with "SNMPv3" highlighted in red. The main content area is titled "SNMPv3 Access Configuration" and features a table with the following columns: Delete, Group Name, Security Model, Security Level, Read View Name, and Write View Name. The table contains two entries: one for "barox" and one for "barox2". The "barox2" entry is selected, and its "Write View Name" is set to "barox2". Below the table, there are buttons for "Delete", "Add New Entry", "Apply", and "Reset".

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	barox	any	Auth, Priv	barox	barox
Delete	barox2	any	Auth, Priv	barox2	barox2

Buttons:

5.5.2. Configuration de la Trap SNMP

L'exemple suivant montre comment définir les valeurs suivantes pour une nouvelle configuration :

- Trap Config Name -> Un nom doit être attribué
- UDP ou TCP – Au début, UDP comme d'habitude
- Trap Version -> Sélection de SNMP v3
- Trap Community -> Le nom de la Community précédemment créé doit être entré
- Trap Destination Address -> Saisie de l'adresse IP du destinataire Trap
- Trap Destination Port -> Saisie du port pour le destinataire
- Trap Security Engine ID -> L'Engine ID de l'utilisateur est saisi à cet endroit.
- Trap Security Name -> Sélection du USM User en question
- Les réglages sont ensuite confirmés avec "Apply"



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

Trap Config Name	test2
Trap Mode	UDP ▾
Trap Version	SNMP v3 ▾
Trap Community	barox2
Trap Destination Address	192.168.10.104
Trap Destination Port	162
Trap Security Engine ID	80001455030040c71cdd09
Trap Security Name	barox2 ▾

Désactivation de la fonction Trap SNMP

La désactivation peut se faire de deux manières. D'une part, elle peut être désactivée en supprimant la configuration. Si l'envoi de Trap ne doit être utilisé que sporadiquement, il est recommandé de régler la fonction sur "Disabled" dans la configuration.

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

Trap Configuraton Name

test2 ▼

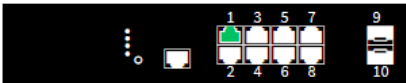
Trap Config Name	test2
Trap Mode	Disabled ▼
Trap Version	SNMP v3 ▼
Trap Community	barox2
Trap Destination Address	192.168.10.104
Trap Destination Port	162
Trap Security Engine ID	80001455030040c71cdd09
Trap Security Name	barox2 ▼

Apply

Reset

5.5.3 Informations complémentaires pour l'envoi de Traps SNMP

Assurez-vous que les événements qui déclenchent l'envoi d'une Trap sont configurés en conséquence. Ces réglages peuvent être configurés ailleurs dans le menu de configuration, comme indiqué ci-dessous, en fonction du terminal. Certains événements tels que les Port Events doivent également être définis en conséquence dans la configuration des ports.

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
- > eMail
- >> Log <
- > Event Configuration

Trap Event Severity Configuration

Home > Event

Group Name	Severity Level	Syslog	Trap
ACL	Info ▼	☒	☐
ACL-Log	Info ▼	☒	☐
Access-Mgmt	Info ▼	☒	☒
Auth-Failed	Warning ▼	☒	☒
Cold-Start	Warning ▼	☒	☒
Config-Info	Info ▼	☒	☐
DMS	Info ▼	☒	☐
FAN	Info ▼	☒	☐
Firmware-Upgrade	Info ▼	☒	☐
Import-Export	Info ▼	☒	☐
LACP	Info ▼	☒	☐
Link-Status	Warning ▼	☒	☒
Login	Info ▼	☒	☒
Logout	Info ▼	☒	☒

5.6 Lecture des Traps SNMP

Différents paramètres des configurations des switches barox peuvent être lus ou réglés via le protocole SNMP. Pour ce faire, des "navigateurs SNMP/MIB" sont nécessaires. Un logiciel d'enregistrement / renifleur de réseau peut également être utilisé pour lire les transmissions SNMP.

La lecture d'une Trap SNMP v2 vous est expliquée brièvement dans l'exemple suivant :

Situation de départ :

Une caméra PoE est débranchée puis rebranchée sur le port Ethernet 3 du switch. Un PC du réseau est configuré pour recevoir des traps SNMP. Pour la lecture, on utilise le logiciel Wireshark (<https://www.wireshark.org>) et pour un affichage ergonomique, le "MIB Browser d'iReasoning" (<http://www.ireasoning.com/mibbrowser.shtml>).

La caméra PoE est déconnectée / appareil PD hors ligne :

Aperçu des informations envoyées par le switch :

No.	Time	Source	Destination	Protocol	Length	Info
347	10.600913	192.168.10.3	192.168.10.100	SNMP	169	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1
408	11.703519	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

> Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.100
> User Datagram Protocol, Src Port: 1297, Dst Port: 162
▼ Simple Network Management Protocol
 version: v2c (1)
 community: barox
 ▼ data: snmpV2-trap (7)
 ▼ snmpV2-trap
 request-id: 104244592
 error-status: noError (0)
 error-index: 0
 ▼ variable-bindings: 3 items
 > 1.3.6.1.2.1.1.3.0: 3760014107
 > 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)
 ▼ 1.3.6.1.4.1.43665.2.138.5.2.1: 506f7274203320506f45205044206f6666
 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): 506f7274203320506f45205044206f6666

0000 b4 b6 86 e1 3b 78 38 b8 eb 21 5a 61 08 00 45 00 ...;x8··!Za·E·
0010 00 9b 05 9a 00 00 40 11 df 00 c0 a8 0a 03 c0 a8 ...·@·
0020 0a 64 05 11 00 a2 00 87 06 ed 30 82 00 7b 02 01 ·d·...·0·{·
0030 01 04 05 62 61 72 6f 78 a7 82 00 6d 02 04 06 36 ··barox··m··6
0040 a5 70 02 01 00 02 01 00 30 82 00 5d 30 82 00 11 ·p·...·0·]0·
0050 06 08 2b 06 01 02 01 01 03 00 43 05 00 e0 1d 43 ·+·...·C·...C
0060 1b 30 82 00 1d 06 0a 2b 06 01 06 03 01 01 04 01 ·0·...+
0070 00 06 0f 2b 06 01 04 01 82 d5 11 02 81 0a 05 01 ··+·...
0080 00 05 30 82 00 23 06 0e 2b 06 01 04 01 82 d5 11 ··0·#·· +
0090 02 81 0a 05 02 01 04 11 50 6f 72 74 20 33 20 50Port 3 P
00a0 6f 45 20 50 44 20 6f 66 66oE PD of f

* Lors de l'utilisation du logiciel, veuillez respecter les conditions de licence respectives des fournisseurs de logiciels.

Affichage des informations dans le navigateur SNMP :

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				

La caméra PoE est reconnectée / appareil PD en ligne :

Aperçu des informations envoyées par le switch :

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

Affichage des informations dans le navigateur SNMP :

En plus des OID (identifiants d'objets pour les unités d'information) correspondants des Traps, une valeur pour la lecture ou l'interprétation du statut du message SNMP est généralement ajoutée. Dans cet exemple, la dernière ligne est marquée à des fins illustration.

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 Utilisation de fichiers MIB pour la lecture et le contrôle des switches

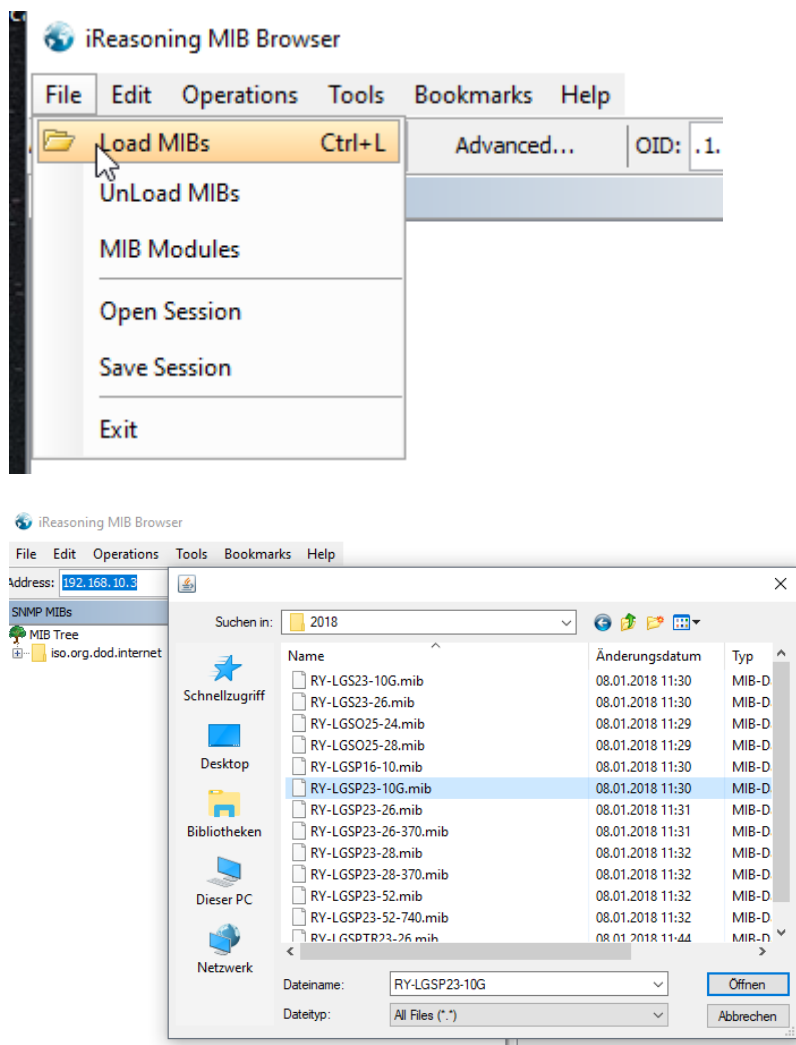
Dans le réseau, le statut des périphériques gérables tels que les switches, les routeurs ou les serveurs peut généralement être interrogé via la fonctionnalité SNMP. Pour des raisons de sécurité ou spécifiques au fabricant, ces fichiers MIB sont souvent nécessaires pour interroger les appareils. Ces fichiers contiennent les informations relatives aux indicatifs d'identification des fonctions.

Interrogation des fonctions d'état du switch via SNMP à l'aide de fichiers MIB

L'utilisation d'un navigateur MIB est recommandée pour l'introduction. Dans l'exemple, on utilise le "MIB Browser d'iReasoning" (<http://www.ireasoning.com/mibbrowser.shtml>) pour sa vue ergonomique. Le navigateur doit également être configuré avec les paramètres SNMP appropriés pour se connecter au switch correspondant.

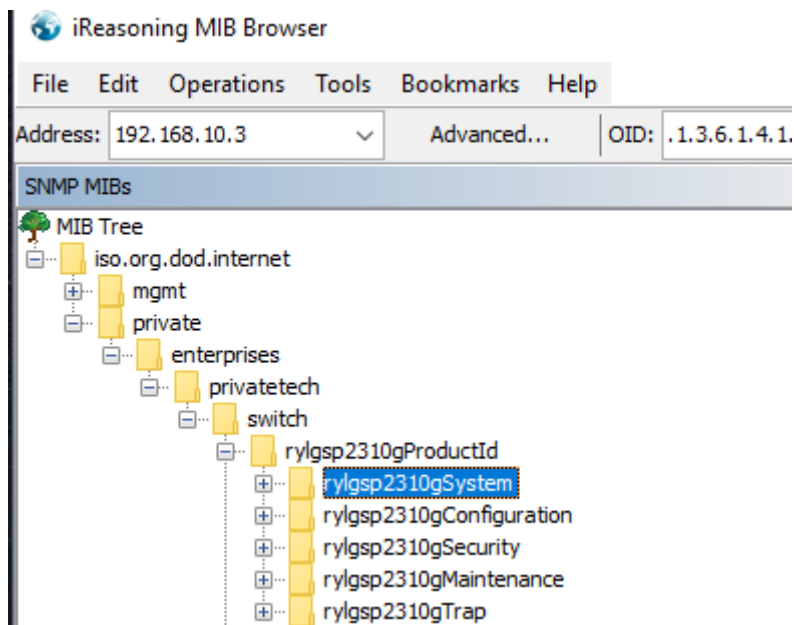
Étape 1 : Import du fichier MIB

Lors de l'import, assurez-vous que le fichier MIB approprié est sélectionné pour le switch correspondant. Les fichiers MIB requis sont reconnaissables au préfixe ".mib".



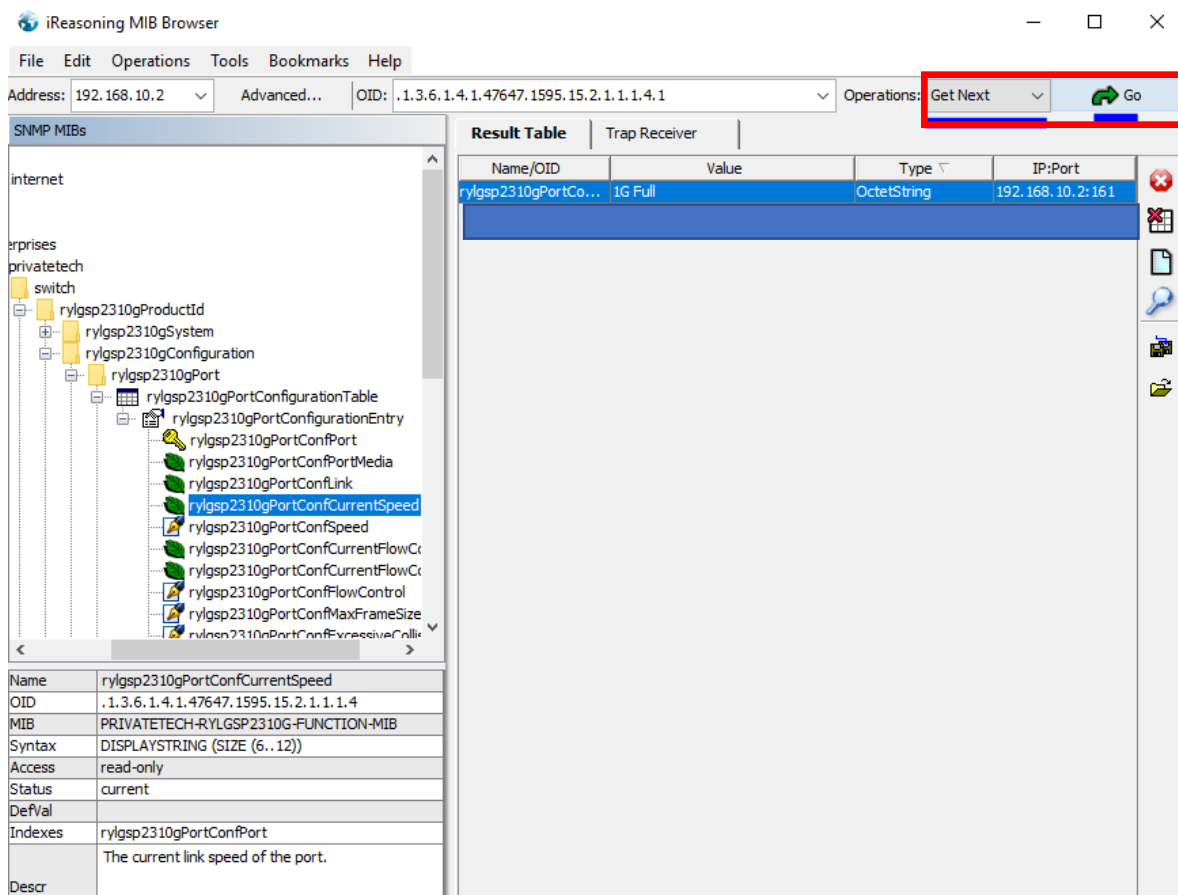
* Lors de l'utilisation du logiciel, veuillez respecter les conditions de licence respectives des fournisseurs de logiciels !

Une fois l'import réussi, les structures MIB sont affichées comme suit.



Étape 2 : Générer des requêtes

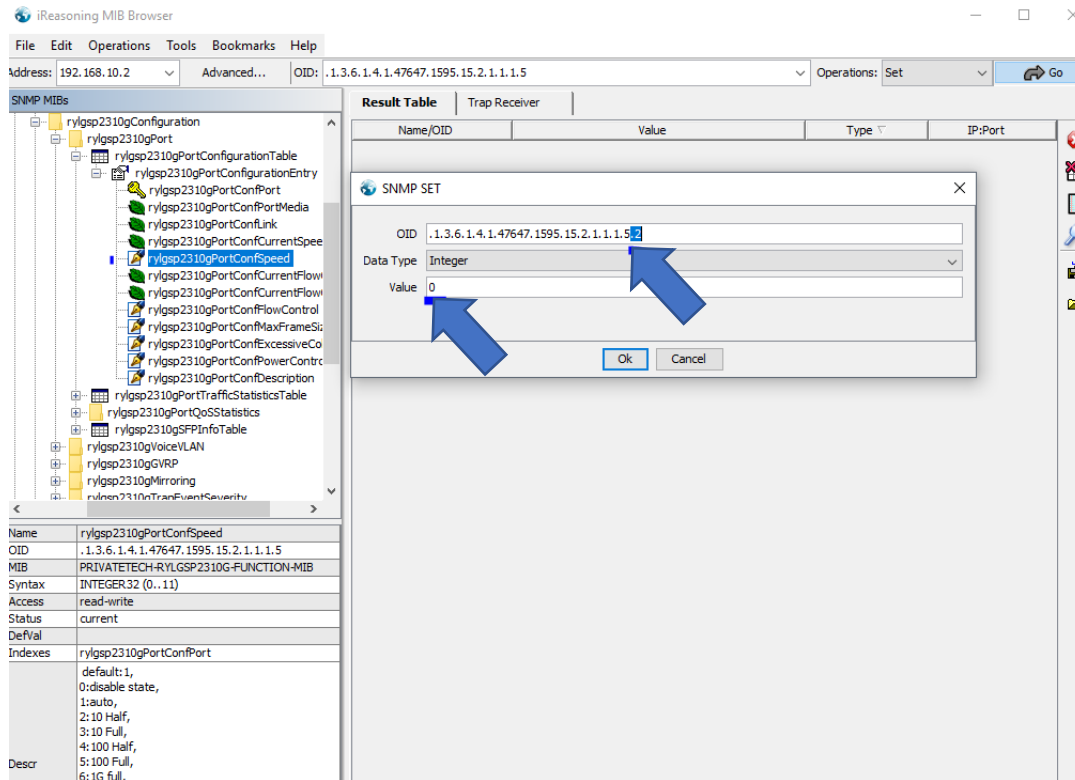
Pour générer une requête, sélectionner d'abord l'état désiré, effectuer l'opération "Get Next" et cliquer sur "Go" pour générer la requête. Après une requête réussie, les informations sur le statut apparaissent dans le tableau des résultats comme indiqué dans l'exemple ci-dessous.



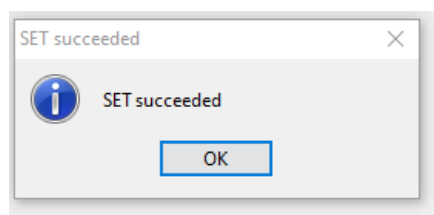
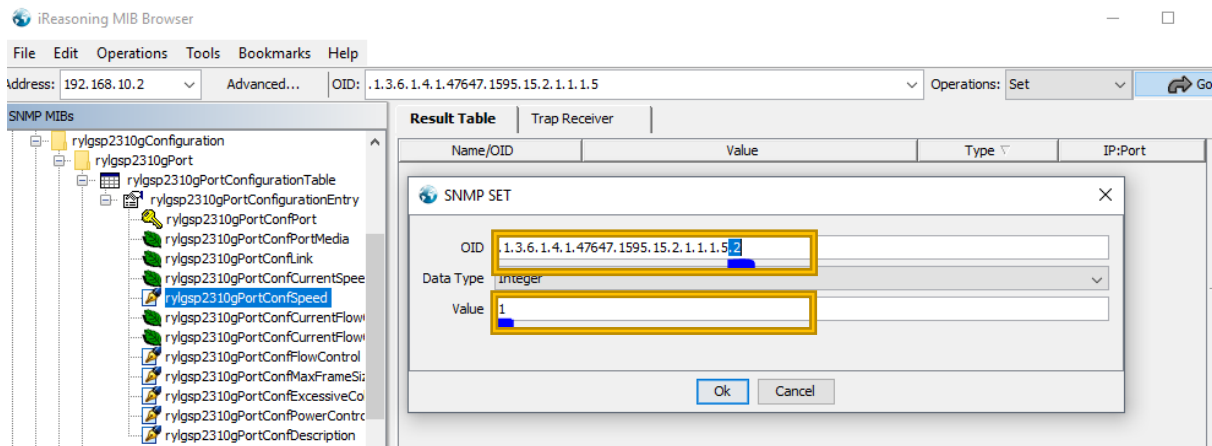
5.8 Commande des fonctions du switch via SNMP et MIB en utilisant l'opération "SET"

Comme autre méthode de commande des switches barox, il est possible d'effectuer l'opération "SET" via le protocole SNMP. Les configurations SNMP de base sur le switch et le navigateur MIB sont prérequis. Voici un exemple d'utilisation de l'opération SET qui déclenche l'arrêt du port et la reconnexion au switch.

Pour désactiver le port 2 au niveau du switch, on recherche la configuration des ports dans le répertoire MIB. Veuillez pour cela vous assurer d'avoir sélectionné le bon bloc d'informations avec la fonction d'écriture. L'opération Set s'ouvre en cliquant sur "Go" et l'entrée OID doit se terminer par ".2" (identification du port 2). En outre, on entre la valeur "0" (pour désactiver) et on confirme par "OK". Après une opération réussie, un message de confirmation est généré en conséquence.



Pour activer le port 2 au niveau du switch, on recherche la configuration des ports dans le répertoire MIB. Veuillez pour cela vous assurer d'avoir sélectionné le bon bloc d'informations avec la fonction d'écriture. L'opération Set s'ouvre en cliquant sur "Go" et l'entrée OID doit se terminer par ".2" (identification du port 2). En outre, on entre la valeur "1" (pour activer) et on confirme par "OK". Après une opération réussie, un message de confirmation est généré en conséquence.

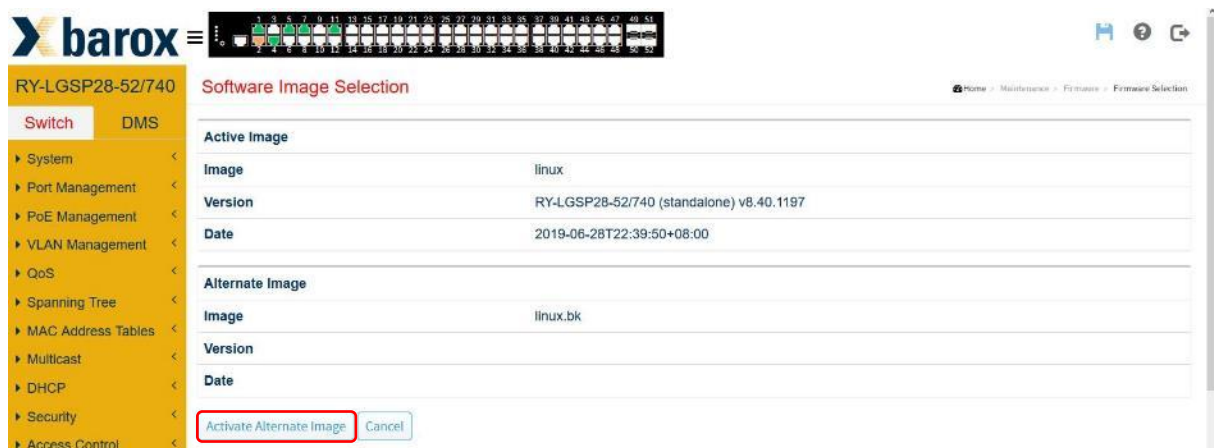


6 Mise à niveau du firmware

En raison des mises à jour régulières du logiciel pour le dépannage et l'introduction de nouvelles fonctionnalités, il est recommandé de mettre à jour le firmware de temps en temps.



Le nouveau firmware est disponible immédiatement après l'upgrade. Si, pour une raison quelconque, l'ancien firmware devait être à nouveau installé, vous pouvez le réactiver très simplement dans le menu "Firmware Selection".



7 Réglages d'usine

Les switches peuvent être réinitialisés à tout moment aux réglages d'usine.

Soit par logiciel via le menu "Maintenance/Factory Defaults", soit en appuyant sur la touche de réinitialisation sur la face avant (plus de 10 secondes).

En cochant la case "Keep IP setup", le switch conserve l'adresse IP configurée tandis que tout le reste est réinitialisé aux réglages d'usine.



8 GARANTIE

barox Kommunikation garantit que le produit est exempt de défauts de matériaux et de fabrication pendant toute la durée de la période de garantie spécifique au pays. La garantie de barox Kommunikation est indépendante de l'obligation de garantie du vendeur découlant du contrat d'achat avec le client final et ne l'affecte d'aucune façon.

barox Kommunikation réparera gratuitement les défauts du produit qui sont dus à un défaut de matériau et/ou de fabrication et qui sont signalés à barox Kommunikation pendant la période de garantie. barox Kommunikation décidera, à sa seule discrétion, de la mesure à prendre pour réparer le défaut. La garantie pour les pièces réparées ou remplacées est donnée pour le reste de la période de garantie.

Le programme de garantie ne s'applique pas aux produits dont le numéro de série a été retiré, masqué ou modifié. La garantie ne couvre pas non plus les dommages suivants :

1. Dommages dus à un accident ou à une utilisation incorrecte ou incorrecte, en particulier le non-respect des instructions d'utilisation du produit.
2. Dommages causés par l'utilisation de pièces non fabriquées ou distribuées par barox Kommunikation.
3. Dommages causés par des modifications effectuées sans l'accord écrit préalable de barox Kommunikation.
4. Dommages résultant de services non fournis par barox Kommunikation ou par des représentants autorisés de barox Kommunikation.
Dommages causés par le transport, la négligence, les fluctuations ou les pannes de l'alimentation électrique, la force majeure ou l'environnement d'exploitation.
5. Dommages dus à l'usure normale.
6. Dommages causés par des virus informatiques et autres logiciels.
7. Dommages causés par la configuration ou la reconfiguration des mots de passe.

Pour les prestations fournies par barox Kommunikation dans le cadre de la réparation de tels défauts ou dommages imputables à l'un des motifs d'exclusion énumérés ci-dessus, des frais supplémentaires seront facturés pour l'exécution du travail, le transport et les pièces. Des frais supplémentaires seront facturés pour la réinstallation du logiciel d'origine.