



Mode d'emploi

Switches 19" de la série RY-L

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

Switches industriels de la série RY-L

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



Switche 19":**Firmware Release v6.54.3133****Hardware Version 1.01****Switches industriels:****Firmware Release v7.10.1972****Hardware Version v1.01**

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

Éditeur :

barox Kommunikation AG

Im Grund 15

CH-5405 Baden-Daettwil

Suisse

www.barox.ch

Date de publication : Août 2019

Version : 1.3

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	8
3.4	Configuration de la passerelle	9
3.5	Réglage de l'heure	10
3.5.1.	Réglage locale	10
3.5.2.	NTP (Network Time Protocol)	11
3.5.2.1.	Serveur NTP	11
3.5.2.2.	Réglage de l'heure	11
3.6	Configuration des ports	12
3.6.1.	Port SFP	13
3.7	Changer le nom d'utilisateur et le mot de passe	13
3.8	Loop Protection	14
3.9	Configuration en anneau	15
3.9.1.	Ring Master	15
3.9.2.	Configuration des ports	16
3.10	Configuration VLAN	18
3.11	Power over Ethernet (PoE)	18
3.11.1.	Configuration PoE	19
3.11.2.	PoE Power Delay	20
3.11.3.	PoE Schedule	20
3.11.4.	PoE Auto Checking	21
3.11.5.	PoE Chip Reset Schedule	21
3.12	Sauvegarde et chargement de la configuration	22
3.12.1.	Téléchargement de la configuration	22
3.12.2.	Importer la configuration (upload)	22
4	DMS Device Management System	23
4.1	Gestion	23
4.2	Monitoring Graphique	26
4.3	Maintenance	30
5	La gestion des switches au cœur de la sécurité	32
5.1	Gestion et protection au niveau du switch (couches 1 et 2)	32
5.1.1.	Paramètres et limites de la bande passante	32
5.1.2.	Notes sur la prise en compte générale des besoins en bande passante	33
5.1.3.	Protection des ports via les paramètres de configuration MAC	33
5.1.4.	Sécurité des ports avec paramètres de Limit Control	34
5.2	Utilisation et protection des fonctions IP (couche 3)	35
5.2.1.	Serveur DHCP	35
5.2.2.	Protection du DHCP par inspection ARP	38
5.2.3.	IP Source Guard	40
5.3	Protection de la gestion des switches et administration réseau (couches 3-7)	41
5.3.1.	Administration et configuration des utilisateurs	41

5.3.2.	Utilisation et paramétrage de l'authentification au niveau de la gestion des switchs	42
5.3.3.	Gestion des accès et utilisation de HTTPS	44
5.3.4.	Configuration et déploiement de l'accès à la gestion basé sur les certificats	44
5.4	SNMP - Fonction de surveillance et d'administration	45
5.4.1.	Configuration SNMP v2c	45
5.4.2.	Configuration de la Trap SNMP	46
5.4.3.	Informations supplémentaires pour l'envoi de Traps SNMP	49
5.5	Configuration SNMP v3	50
5.5.1.	Activation de la fonction SNMP v3	50
5.5.2.	Configuration de la Trap SNMP	53
5.5.3.	Informations supplémentaires pour l'envoi de Traps SNMP	56
5.6	Lecture des Traps SNMP	57
5.7	Utilisation de fichiers MIB pour la lecture et le contrôle des switchs	60
5.8	Commande des fonctions du switch via SNMP et MIB en utilisant l'opération "SET"	62
6	Mise à niveau du firmware	64
7	Réglages d'usine	65
8	Server Report	66
9	GARANTIE	67

1 INTRODUCTION

Ce mode d'emploi décrit la mise en service des switch 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 www.barox.ch.

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 9.600 octets sont également prises en charge à 100 Mbit/s.

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

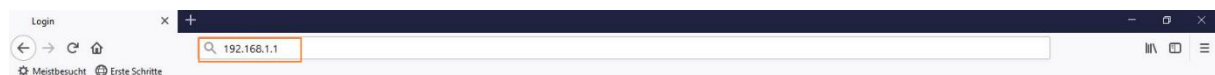
Sinon, les switches peuvent également être configurés via CLI (port console). Cette documentation explique comment configurer le switch à l'aide d'un navigateur Web.

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.

The screenshot shows the web interface of a barox switch. The browser address bar shows 192.168.1.1. The page title is 'RY-LGSP16-10'. The left sidebar has a menu with 'Configuration', 'Monitor', and 'DMS 5'. The 'Monitor' section is expanded, showing 'System', 'IP Status', 'Log', 'Detailed Log', 'Overview', 'Green Ethernet', 'Ports', 'DHCP', 'Security', 'LACP', 'Loop Protection', 'Spanning Tree', 'IPMC', 'LLDP', 'PoE', and 'MAC Table'. The 'System' section is selected, showing 'System Information'. The main content area displays a table of system information with the following data:

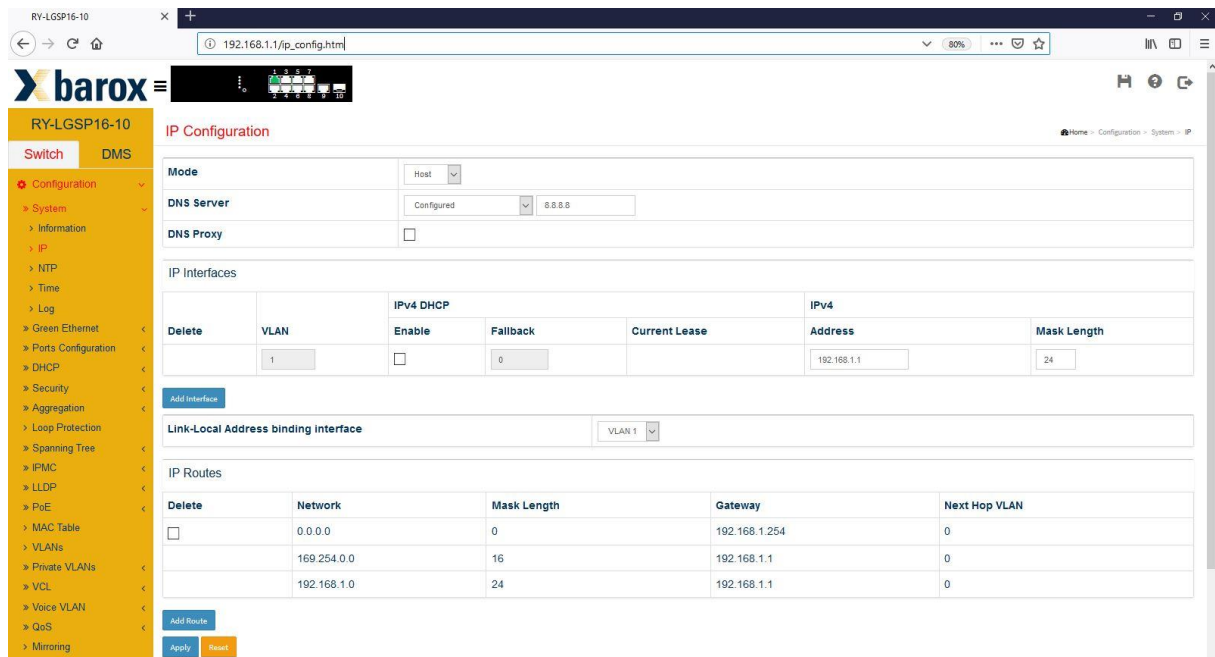
Model Name	RY-LGSP16-10
System Description	10-Port GbE Web Smart+ Managed PoE Switch
Location	Labor
Contact	Labor
System Name	RY-LGSP16-10
System Date	2011-01-01T04:11+01:00
System Uptime	03:31
Bootloader Version	v1.15f
Firmware Version	v6.54.3133 19-04-04
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	C012317AR0300002
MAC Address	38-b8-e8-20-34-62
Memory	Total=85447 KBytes, Free=72268 KBytes, Max=71984 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
CPU Load (100ms, 1s, 10s)	0%, 4%, 2%

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 "Configuration/System/IP" 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 appartient au VLAN 1. Le VLAN 1 est donc le VLAN de gestion.

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 doit être modifié.

DHCP

Si le switch est intégré dans un réseau dans lequel un serveur DHCP attribue les adresses IP, le champ doit être marqué sous "IPv4 DHCP".

Le serveur DHCP 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 :

Débit binaire : 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-LGSP23-26# *show ip interface brief*

➔ 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 Configuration de la passerelle

Si une nouvelle adresse IP a été attribuée au switch, l'adresse de passerelle doit être adaptée en conséquence.

IP Routes				
Delete	Network	Mask Length	Gateway	Next Hop VLAN
☐	0.0.0.0	0	192.168.1.254	0
	169.254.0.0	16	192.168.1.1	0
	192.168.1.0	24	192.168.1.1	0

Add Route

ApplyReset

Pour modifier l'adresse de la passerelle, la ligne doit d'abord être supprimée, puis recrée avec l'adresse correcte. L'adresse réseau doit être réglée sur "0.0.0.0" et la longueur du masque sur "0".

Seule l'adresse de la passerelle doit être réécrite en fonction du réseau.

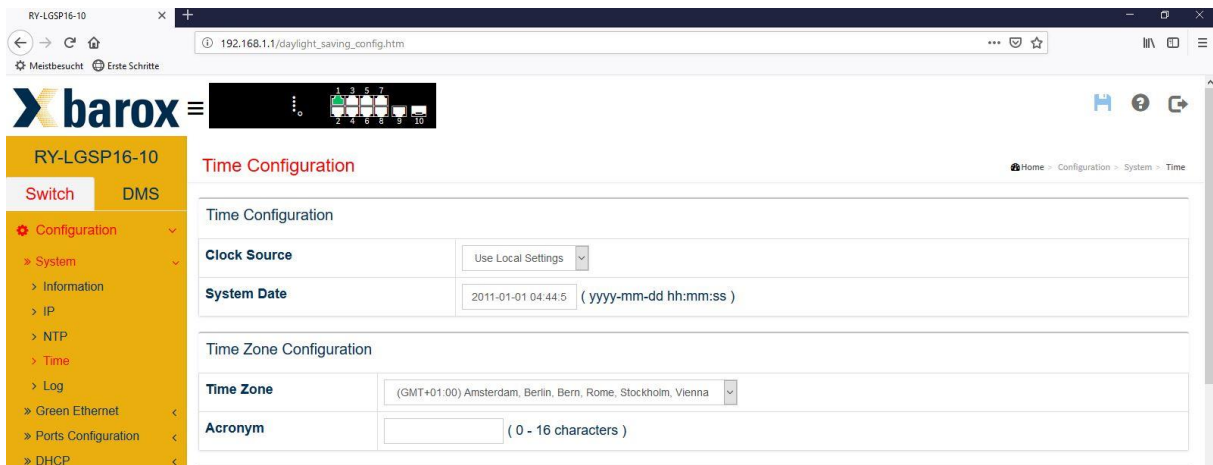
3.5 Réglage de l'heure

L'heure système des switches barox peut être configurée 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.

3.5.1. Réglage locale

Dans le menu "Configuration/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.



The screenshot shows the web interface of a barox switch (RY-LGSP16-10) accessed via a browser at 192.168.1.1/daylight_saving_config.htm. The interface has a left sidebar with a menu: Configuration (expanded), System, Information, IP, NTP, Time, Log, Green Ethernet, Ports Configuration, and DHCP. The main content area is titled "Time Configuration" and contains two sections: "Time Configuration" and "Time Zone Configuration".

Time Configuration

Clock Source	Use Local Settings
System Date	2011-01-01 04:44:5 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Acronym	(0 - 16 characters)

3.5.2. 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.

La configuration s'effectue en deux étapes.

3.5.2.1. Serveur NTP

La première étape consiste à dire au switch où il doit obtenir l'heure.

Si l'heure doit être obtenue directement du serveur DHCP, placez le champ "Automatic" sur "Enabled". L'adresse IP du serveur DHCP est alors affichée dans la ligne en dessous.

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 address 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.

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/>

NTP Configuration	
Automatic	Enabled
Server address via DHCP	
NTP Time-Sync Interval	60
Server address 1	213.209.109.45
Server address 2	
Server address 3	
Server address 4	
Server address 5	

3.5.2.2. Réglage de l'heure

Dans le menu "Configuration/System/Time", sélectionner "Use NTP Server" comme "Clock Source".

Time Configuration	
Clock Source	Use NTP Server
System Date	yyyy-mm-dd hh:mm:ss
Time Zone Configuration	None
Acronym	(0 - 16 characters)

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.

RY-LGSP16-10

barox

RY-LGSP16-10

Switch **DMS**

Configuration

Time Configuration

Time Configuration

Clock Source Use NTP Server

System Date 2019-05-06 14:56:4 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Acronym (0 - 16 characters)

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

3.6 Configuration des ports

Les ports sont réglés en usine en mode Auto. L'autonégociation est une procédure qui permet à deux ports réseau 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".

RY-LGSP16-10

barox

RY-LGSP16-10

Switch **DMS**

Configuration

Ports Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size
		Current	Configured	Current Rx	Current Tx	Configured	
*			<>				9600
1	●	1Gfdx	Auto	⊗	⊗		9600
2	●	Down	Auto	⊗	⊗		9600
3	●	Down	Auto	⊗	⊗		9600
4	●	Down	Auto	⊗	⊗		9600
5	●	Down	Auto	⊗	⊗		9600

3.6.1. 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.

Port	Status	Mode	Speed	Duplex	Flow Control	MTU
9	Down	Auto			☐	9600
10	Down	Auto			☐	9600

Buttons: Apply, Reset

Dropdown for Port 10 Mode:

- Auto
- Disabled
- 100Mbps FDX
- 1Gbps FDX

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>

3.7 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.

barox RY-LGSP16-10

Users Configuration

User Name	Privilege Level
admin	15

Buttons: Add New User

Navigation Menu:

- Configuration
 - System
 - Green Ethernet
 - Ports Configuration
 - DHCP
 - Security
 - Switch
 - Users
 - Privilege Levels
 - Auth Method

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.

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

Dans l'exemple suivant, le technicien 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".

Group Name	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
ACTIVATE	5	10	5	10
Aggregation	5	10	5	10
cloud_management	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Dhcp_Client	5	10	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.

3.8 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 – 604.800 s (7 jours). Si "0" est entré, le port reste désactivé jusqu'à ce que le switch soit redémarré.

RY-LGSP16-10

192.168.1.1/loop_config.htm

barox

RY-LGSP16-10

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Aggregation
- » Loop Protection
- » Spanning Tree
- » IPMC
- » LLD
- » PoE
- » MAC Table
- » VLANs
- » Private VLANs
- » VCL
- » Voice VLAN

Loop Protection Configuration

Global Configuration

Enable Loop Protection: Enable

Transmission Time: 5 seconds

Shutdown Time: 180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☒	<>	<>
1	☒	Shutdown Port	Enable
2	☒	Shutdown Port and Log	Enable
3	☒	Shutdown Port	Enable
4	☒	Shutdown Port	Enable

3.9 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

3.9.1. 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.

RY-LGSP16-10

192.168.1.1/mstp_sys_config.htm

barox

RY-LGSP16-10

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Aggregation
- » Loop Protection
- » Spanning Tree
- » Bridge Settings

STP Bridge Configuration

Basic Settings

Protocol Version: RSTP

Bridge Priority: 32768

Forward Delay: 15

Max Age: 20

Maximum Hop Count: 20

Transmit Hold Count: 6

Ring Master hat Priority "0"

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

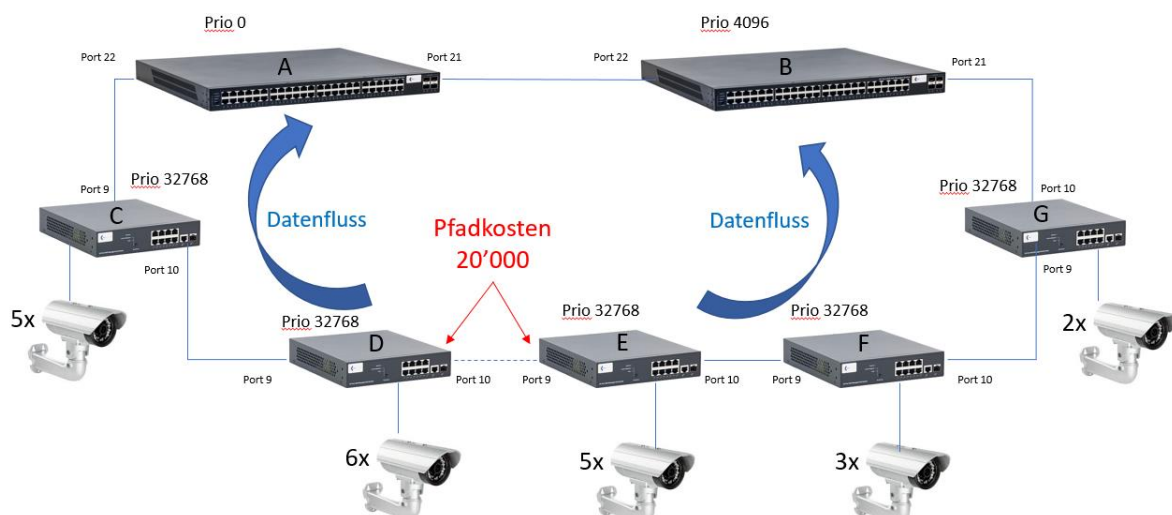
Par défaut, les switches ont la "Bridge Priority" 32768. Si le switch doit agir en tant que Master, la Bridge Priority doit être réglée sur "0". Toutes les autres valeurs peuvent être laissées telles quelles.

3.9.2. Configuration des ports

"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.

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 : RSTP 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.**

3.10 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
*	<>	1	<>	☒	<>	<>	1	
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	
4	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	10	
5	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 VLANs sont autorisés dans la colonne "Allowed VLANs"

3.11 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. Les Powered Devices (par ex. les caméras PoE) peuvent également être surveillés et redémarrés si nécessaire, et la puce PoE de la caméra peut être réinitialisée. Ceci est utile si la caméra est "pingable" mais ne montre pas d'image.

3.11.1. Configuration PoE

The screenshot shows the configuration page for a barox RY-LGSP16-10 switch. The left sidebar contains a navigation menu with options like Configuration, System, Green Ethernet, Ports Configuration, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, IPMC, LLDP, PoE, Configuration, Power Delay, Schedule Profile, Auto Checking, Chip Reset Schedule, MAC Table, and VLANs. The main content area is titled 'Power Over Ethernet Configuration' and includes the following sections:

- Reserved Power determined by:** Radio buttons for Class, Allocation (selected), and LLDP-Med.
- Power Management Mode:** Radio buttons for Actual Consumption (selected) and Reserved Power.
- Capacitor Detection:** A checkbox that is currently unchecked.
- PoE Power Supply Configuration:**
 - PoE Firmware Version:** 012-001
 - Primary Power Supply [W]:** 130 (highlighted with an orange box)
- PoE Port Configuration:** A table with 5 columns: Port, PoE Mode, PoE Schedule, Priority, and Maximum Power [W].

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]
*	Enabled	Profile 1	Low	30
1	Enabled	Profile 1	Low	30
2	Enabled	Profile 2	High	30
3	Enabled	Profile 1	Critical	30

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-LGSP16-10 avec 8 ports PoE+ offre max. 130 W. Cela signifie qu'il est impossible de connecter un terminal de 30 W à chacun des 8 ports, car 240 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	L'alimentation électrique disponible pour le Powered Device	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 (802.3at/Type 2 seulement) ^[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.

3.11.2. 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 de commutation maximale possible 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, les ports 1 et 2 sont activés immédiatement, puis 2 ports de plus toutes les 10 secondes.

Port	Delay Mode	Delay Time(0~300 sec)
*	<>	0
1	Disabled	0
2	Enabled	10
3	Enabled	20
4	Disabled	0
5	Disabled	0
6	Disabled	0
7	Disabled	0
8	Disabled	0

3.11.3. 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, PoE est activé tous les jours de 06h00 à 18h00.







RY-LGSP16-10

Switch DMS

PoE Schedule Profile

Configuration

Home > Configuration > PoE > Schedule Profile

Profile

1

Name

Profile 1

Week Day	Start Time		End Time	
	HH	MM	HH	MM
*	6	0	18	0
Monday	6	0	18	0
Tuesday	6	0	18	0
Wednesday	6	0	18	0
Thursday	6	0	18	0
Friday	6	0	18	0
Saturday	6	0	18	0

3.11.4. 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 192.168.1.25 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-LGSP16-10

Switch DMS

PoE Auto Checking

Configuration

Home > Configuration > PoE > Auto Checking

Ping Check

Enabled

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	192.168.1.41	60	30	3	error=0, total=0	Reboot Remote PD	15
2	192.168.1.42	60	30	3	error=0, total=0	Reboot Remote PD	15
3	192.168.1.43	60	30	3	error=0, total=0	Reboot Remote PD	15
4	0.0.0.0	60	30	3	error=0, total=0	Nothing	15

3.11.5. PoE Chip Reset Schedule

Il arrive que les caméras soient toujours accessibles par ping, mais n'affichent pas d'image.

Dans la plupart des appareils, la commande PoE est sur une puce séparée. Il est possible que le processeur réponde à un ping, mais le flux vidéo n'est pas transmis.

Prophylactiquement, la commande PoE Chip Reset peut être envoyée quotidiennement ou une fois par semaine, par exemple à 03h00.

Cette commande redémarre la puce PoE de la caméra.







RY-LGSP16-10

Switch DMS

PoE Chip Reset Schedule

Configuration

Home > Configuration > PoE > Chip Reset Schedule

Mode

Enabled

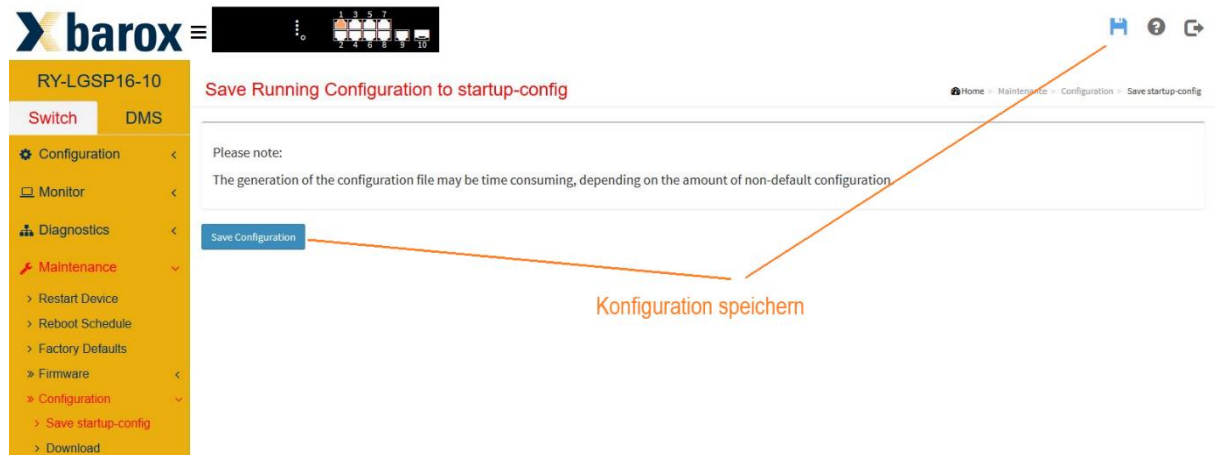
Week Day	PoE Chip Reset Time	
	HH	MM
*	3	0
Monday	3	0
Tuesday	3	0

3.12 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 :

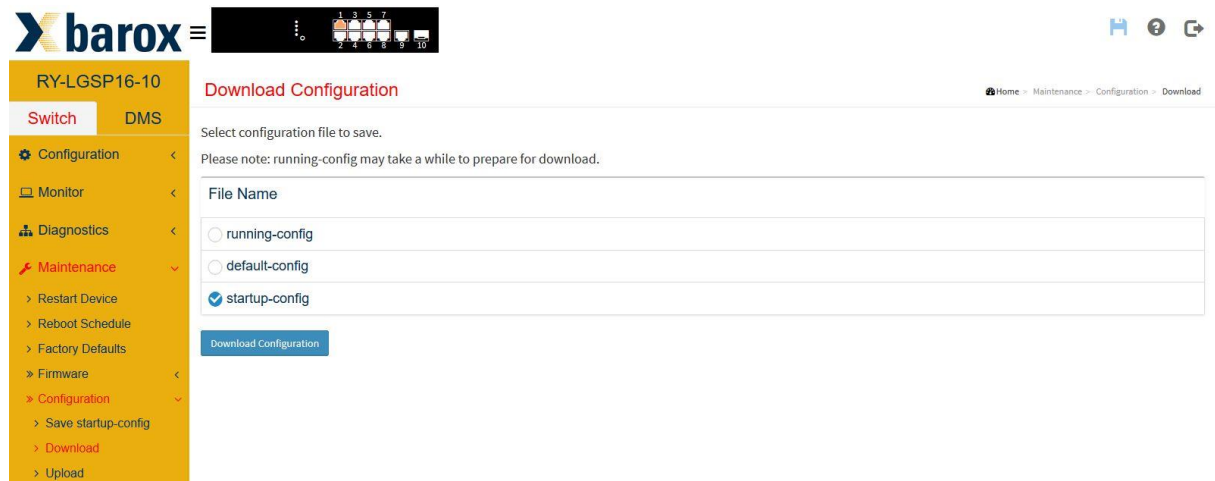
- Le symbole disquette dans chaque masque
- Dans le menu Maintenance/Configuration/Save startup-config



3.12.1. Téléchargement de la configuration

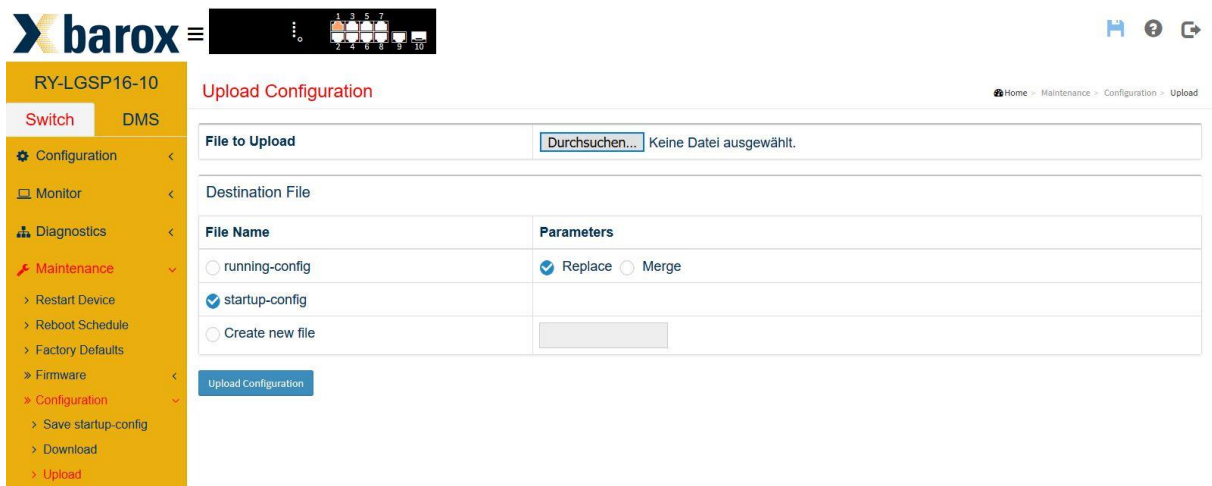
La configuration actuelle du switch peut être téléchargée et sauvegardée séparément. Le fichier de configuration généré peut être importé dans le cas du remplacement d'un switch ou utilisé si plusieurs switches doivent être configurés de manière identique et que seule l'adresse IP doit être modifiée.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

Nous vous recommandons de n'enregistrer que le fichier "startup-config File".



3.12.2. 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 le type de fichier concerné. Il s'agit généralement du fichier "startup-config File".



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.

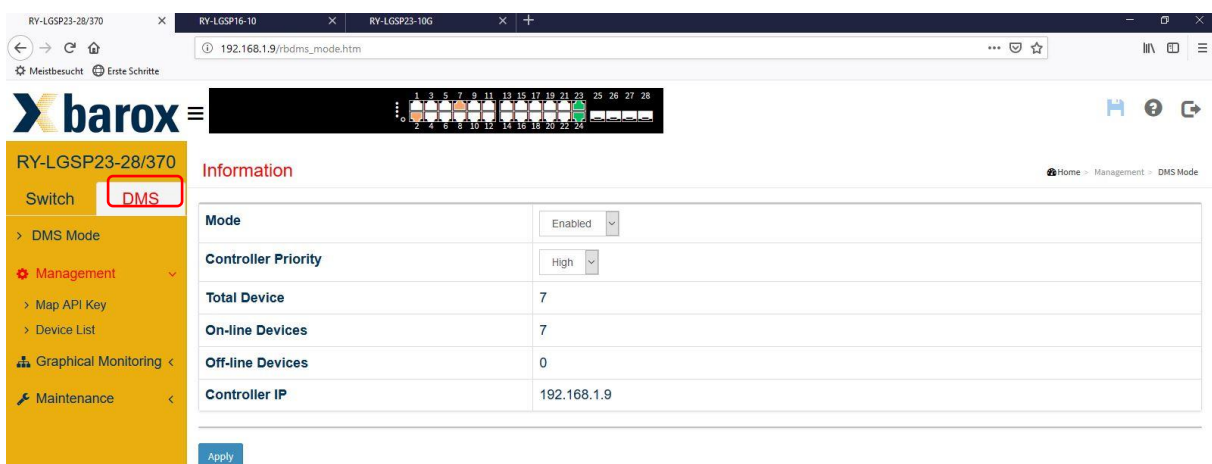
L'aperçu de la topologie du réseau permet une vue d'ensemble rapide de tous les switches et terminaux disponibles sur le réseau, tels que les caméras IP ou les serveurs, avec des détails sur l'adresse IP, le type de périphérique et le nom du périphérique. Les plans d'étage et les plans d'environnement 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 Gestion/DMS), il est possible de voir combien de périphériques ont été détectés dans le réseau, combien d'entre eux sont en ligne (actifs) ou hors ligne (inactifs). Les périphériques 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.



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.

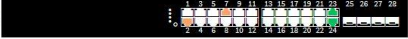
Cette fonction est particulièrement utile lorsqu'un périphérique non configuré est intégré dans le réseau et que l'adresse IP est inconnue.

Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
☐	Online	SWITCH	RY-LGSP16-10	Switch 2	38-B8-EB-20-34-62	192.168.1.1
☐	Online	SWITCH	RY-LGSP23-10G	Switch 3	38-B8-EB-20-38-17	192.168.1.2
☐	Online	SWITCH	RY-LGSP23-28/370	Switch 1	38-B8-EB-20-06-41	192.168.1.9
☐	Online	IP Camera	AXIS P1447-LE	Kamera 1	AC-CC-8E-C7-9C-D5	192.168.1.41
☐	Online	IP Camera	AXIS P1447-LE	Kamera 3	AC-CC-8E-C8-37-3A	192.168.1.42
☐	Online	IP Camera	AXIS P1447-LE	Kamera 2	AC-CC-8E-BB-A6-85	192.168.1.43
☐	Online	PC	General PC	Technik	30-85-A9-6F-31-DE	192.168.1.111

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 à partir du menu "Maintenance/Diagnostics".





RY-LGSP23-28/370

Switch

DMS

> DMS Mode

Management

Graphical Monitoring

Maintenance

> Floor Image

> Diagnostics

> Traffic Monitor

Diagnostics

Home > Maintenance > Diagnostics

Another Try

Show

10

entries

Search:

Select	Status	Model Name	Device Name	MAC	IP Address	Version
☒	Online	AXIS P1447-LE	Kamera 2	AC-CC-8E-BB-A6-85	192.168.1.43	

Showing 1 to 6 of 6 entries

Previous

1

Next

192.168.1.9 38-b8-eb-20-06-41

Connection.....

Cable status.....

192.168.1.1 38-b8-eb-20-34-62

Connection.....

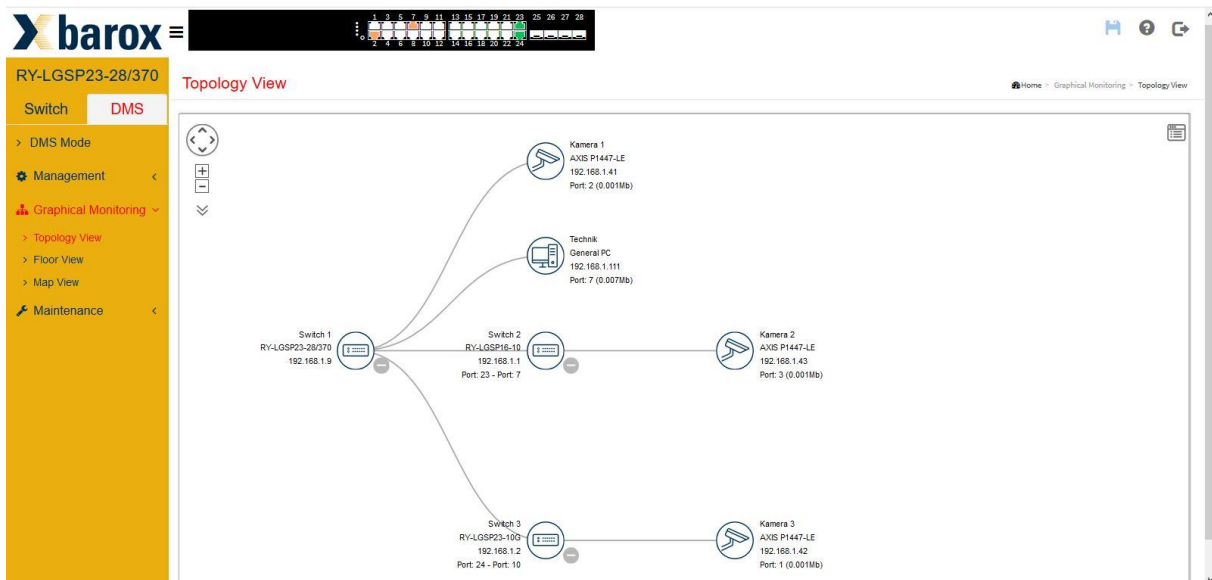
Cable status.....

192.168.1.43 ac-cc-8e-bb-a6-85

4.2 Monitoring Graphique

Vue Topologique

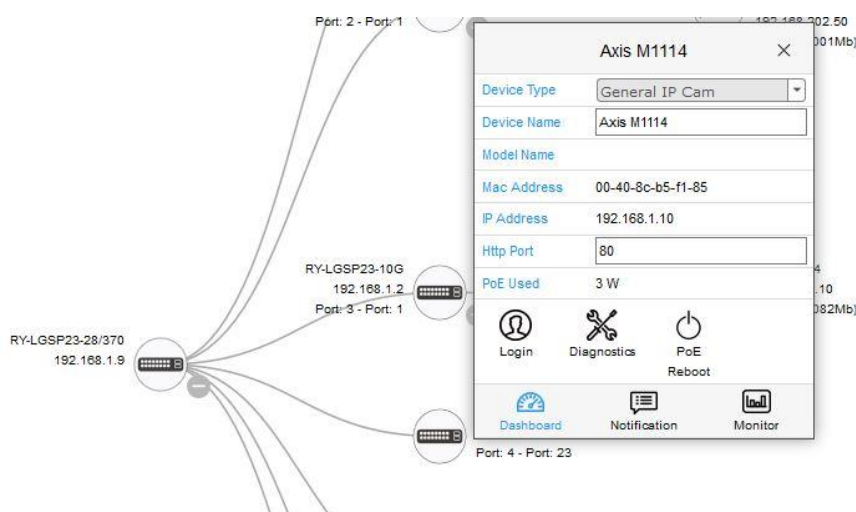
Dans la vue topologique (Topology View), le réseau, y compris tous les terminaux IP connectés, est automatiquement affiché sous forme graphique. Si le terminal est reconnu correctement, le symbole correspondant (caméra, switch, point d'accès, etc.) s'affiche. Toutes les informations telles que le nom 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 périphérique 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.

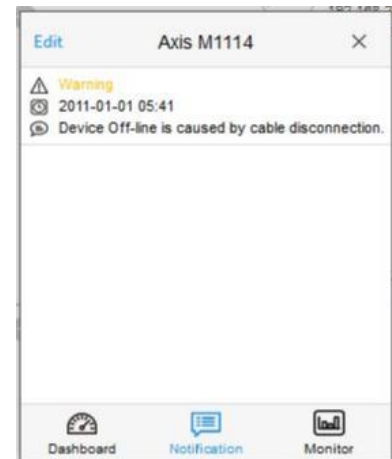
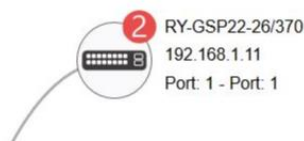


Si un périphérique

- 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.

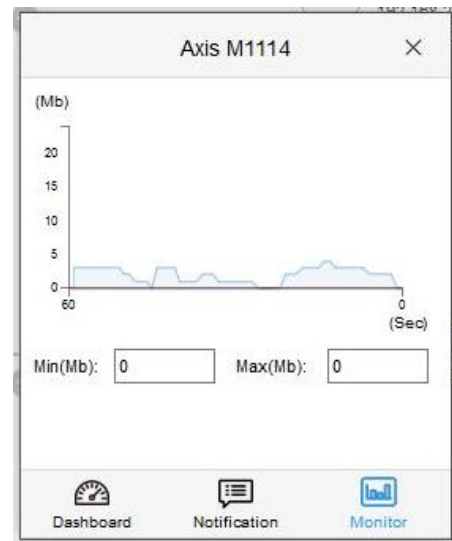
Il faut impérativement cliquer sur "Remove" si, par exemple, une caméra défectueuse doit être remplacée par une nouvelle caméra avec la même adresse IP. Le switch stocke non seulement l'adresse IP mais aussi l'adresse MAC. Si l'ancienne adresse IP n'est pas supprimée via la fonction "Remove", le switch 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.



Autre outil utile : la fonction "Monitor".

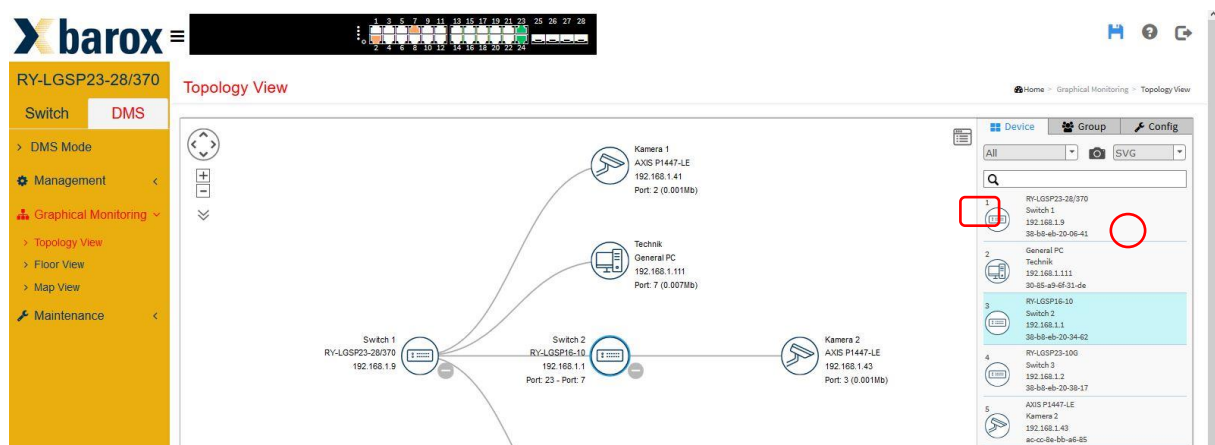
Ici, le flux de données (par ex. d'une caméra) est affiché en temps réel.

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.

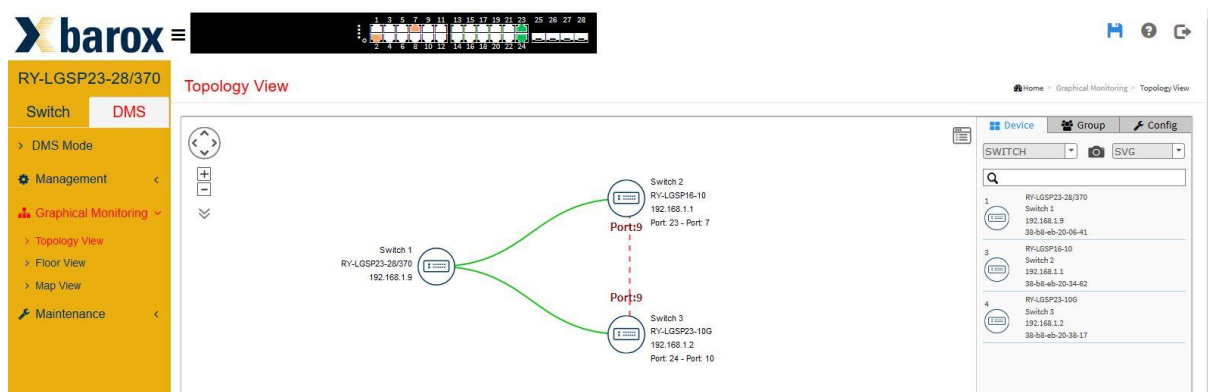


L'outil offre également la possibilité d'imprimer le plan de réseau au format SVG, PNG ou PDF directement depuis la vue topologique. Pour ce faire, il suffit de sélectionner le format désiré puis de cliquer sur l'icône de la caméra.

La vue topologique (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 :

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



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 le périphérique correspondant dans la liste avec un clic de souris et de le placer sur le plan. Rien de plus.

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-LGSP23-28/370

Switch DMS

> DMS Mode

Management

Graphical Monitoring

Maintenance

Floor Image

Diagnostics

Traffic Monitor

Floor Image Management

Home Maintenance Floor Image

Maximum: 30 files Used: 0 file(s) Free: 30 file(s)

Add Floor Image: Stockwerkplan.jpg

Name

Add

Select	No.	File Name	Image
No information found			

Delete

Les plans importés sont listés sur le bas de la page Web. Il est possible d'enregistrer jusqu'à 50 fichiers.

barox RY-LGSP23-28/370

Switch DMS

> DMS Mode

Management

Graphical Monitoring

Maintenance

Floor Image

Diagnostics

Traffic Monitor

Floor Image Management

Home Maintenance Floor Image

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

Add Floor Image: Stockwerkplan.jpg

Name

Add

Select	No.	File Name	Image
☐	1	Stockwerkplan OG (192.168.1.9)	

Delete

Diagnostic

Cette fonction a été décrite et expliquée à la page 23 sous la rubrique "Device List".

Traffic Monitor

ATTENTION : La surveillance du trafic n'est pas supportée par les switches industriels.

Le traffic monitoring (surveillance du trafic) est un autre outil de diagnostic très utile. Le menu "Maintenance" affiche le trafic de chaque port sur 24 heures.

Le graphique à barres sur le haut montre chaque port et toutes les données envoyées et reçues via le port pendant la journée. Il peut être sélectionné par date, par jour ou en vue hebdomadaire.

Si l'on clique maintenant sur la barre d'un port, une échelle de 0 à 23 heures dans le diagramme du bas indique l'heure à laquelle les données ont été transmises, en quelle quantité.

Ceci peut être très utile lors du dépannage, par exemple lorsque l'on remarque qu'à 12h du matin beaucoup de trafic a été généré sur le port 2 et qu'il y avait des problèmes d'enregistrement.



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 (couches 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.

RY-LGSP23-26

Switch **DMS**

⚙️ **Configuration** ▾

» System <

» Green Ethernet <

» **Ports Configuration** ▾

» Ports

» Ports Description

» DHCP <

» Security <

» Aggregation <

» Loop Protection

Ports Configuration

↻

Port	Link	Speed	
		Current	Configured
*			<> ▾
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.

RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» Ports

» Ports Description

» DHCP

» Security

» Aggregation

» Loop Protection

Ports Configuration

Home > Configuration > Ports

↺

Port	Link	Speed		Flow Control			Maximum Frame Si
		Current	Configured	Current Rx	Current Tx	Configured	
*			<>			☐	9600
1	●	Down	Auto	⊘	⊘	☐	9600
2	●	Down	Auto	⊘	⊘	☐	9600
3	●	1Gfdx	Auto	⊘	⊘	☐	9600

! 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.

RY-LGSP23-26

Switch **DMS**

- ⚙️ **Configuration** ▾
- » System <
- » Green Ethernet <
- » Ports Configuration <
- » DHCP <
- » Security <
- » Aggregation <
- > Loop Protection
- » Spanning Tree <
- » IPMC Profile <
- > MVR
- » IPMC <
- » LLDP <
- » PoE <
- > **MAC Table**
- > VLANs
- » Private VLANs <
- » VCL <
- » Voice VLAN <
- » QoS <
- > Mirroring
- > UPnP

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

☐

Aging Time

300 seconds

MAC Table Learning

	Port Members													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Auto	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒
Disable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

	Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
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.

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.

RX-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Network

» Limit Control

» NAS

» ACL

» IP Source Guard

» ARP Inspection

» AAA

» Aggregation

Port Security Limit Control Configuration

Home » Configuration » Security » Network » Limit Control

System Configuration

Mode

Enabled

Aging Enabled

☐

Aging Period

3600

seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open	Sticky	Clear
*	<>	4	<>			<>	
1	Disabled	4	None	Disabled	Reopen	Disabled	Clear
2	Enabled	4	Trap & Shutdown	Disabled	Reopen	Disabled	Clear

5.2 Utilisation et protection des fonctions IP (couche 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

La portée VLAN du service est d'abord définie et le service est généralement activé dans le *Mode* avec le paramètre *Enabled* activé, puis activé avec confirmation comme illustré ci-dessous.

RX-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Server

» Mode

DHCP Server Mode Configuration

VLAN Mode

Delete	VLAN Range	Mode
Delete	10 - 101	Enabled

Add VLAN Range

ApplyReset

Voici les paramètres du pool d'adresses IP qui doit permettre la distribution de 50 adresses dans l'exemple, c'est-à-dire des adresses dans la plage 192.168.10.100 - 192.168.10.150, en spécifiant les adresses ou plages IP environnantes (procédure d'exclusion) aux clients IP dans le VLAN en question.

RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Server

» Mode

» Excluded IP

DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range
Delete	192.168.10.1 - 192.168.10.99
Delete	192.168.10.151 - 192.168.10.254

Add IP Range

ApplyReset

Un nom du service DHCP est ensuite défini et confirmé.

RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Server

» Mode

» Excluded IP

» Pool

DHCP Server Pool Configuration

Home » Configu...

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
Delete	test	-	-	-	1 days 0 hours 0 minutes

Add New Pool

ApplyReset

Une fois le nom défini, on va chercher les réglages en sélectionnant le nom comme indiqué ci-dessous.

RY-LGSP23-26

Switch
DMS

⚙️ Configuration
▼

» System
<

» Green Ethernet
<

» Ports Configuration
<

» DHCP
▼

» Server
▼

> Mode
<

> Excluded IP
<

> Pool
<

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP
☐	test	-	-

Add New Pool

Apply

Reset

Une fois le nom du pool sélectionné, la configuration apparaît comme indiqué ci-dessous.

RY-LGSP23-26

Switch
DMS

⚙️ Configuration
▼

» System
<

» Green Ethernet
<

» Ports Configuration
<

» DHCP
▼

» Server
▼

> Mode
<

> Excluded IP
<

> Pool
<

> Snooping
<

> Relay
<

DHCP Pool Configuration

Pool

Name

test
▼

Setting

Pool Name	test
Type	Network ▼
IP	192.168.10.254
Subnet Mask	255.255.255.0

Pour faciliter l'illustration ou pour la compréhension, seuls les réglages indiqués ci-dessus sont nécessaires et confirmés par la confirmation de la configuration en fin de page.

barox Kommunikation

37

5.2.2. Protection du DHCP par inspection ARP

La protection contre les clients DHCP indésirables peut être réalisée avec l'inspection ARP. Une fois les fonctions activées, les clients DHCP peuvent être gérés 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-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Server

» Snooping

» Relay

» Security

DHCP Snooping Configuration

Snooping Mode

Enabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Untrusted

Les paramètres des ports sont également activés et configurés. Dans l'exemple ci-dessous, l'inspection ARP est activée pour le port 3, le contrôle VLAN est activé et le type de Log est réglé sur "Deny".

RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Network

> Limit Control

> NAS

» ACL

» IP Source Guard

» ARP Inspection

> Port Configuration

ARP Inspection Configuration

Mode

Enabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Enabled	Enabled	Deny
4	Disabled	Disabled	None

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

RY-LGSP23-26

Switch DMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Network

» Limit Control

» NAS

» ACL

» IP Source Guard

» ARP Inspection

» Port Configuration

» VLAN Configuration

VLAN Mode Configuration

Home » Conf

↺

↻

⏪

⏩

Start from VLAN , entries per page.

Delete	VLAN ID	Log Type
Delete	10	None ⌵

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 Layer2 et 3 sont visibles dans le tableau dynamique d'inspection ARP et peuvent ensuite être reportés dans le tableau statique d'inspection ARP.

RY-LGSP23-26

Switch DMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Network

» Limit Control

» NAS

» ACL

» IP Source Guard

» ARP Inspection

» Port Configuration

» VLAN Configuration

» Static Table

» Dynamic Table

Dynamic ARP Inspection Table

Home » Configuration » Security » Network » ARP Inspection »

Auto-refresh ☒

↺

↻

⏪

⏩

Start from

Port 1

 , VLAN , MAC address and IP address , entries p

System Configuration

Port	VLAN ID	MAC Address	IP Address	Translate to static
3	2	5c-9a-d8-5c-98-1c	192.168.11.50	☒

Apply

Reset

Une entrée statique est présentée ci-dessous. L'adresse IP est réservée au client selon le tableau.

RY-LGSP23-26

Switch **DMS**

- ⚙️ Configuration ▾
 - » System <
 - » Green Ethernet <
 - » Ports Configuration <
 - » DHCP <
 - » Security ▾
 - » Switch <
 - » Network ▾
 - > Limit Control
 - > NAS
 - > ACL <
 - > IP Source Guard <
 - » ARP Inspection ▾
 - > Port Configuration
 - > VLAN Configuration
 - > Static Table

Static ARP Inspection Table

Home > Configuration > Security > Network > ARP Inspection

Delete	Port	VLAN ID	MAC Address	IP Address
☐	3	2	5c-9a-d8-5c-98-1c	192.168.11.50

Add New Entry

Apply
Reset

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 source mais aussi l'adresse IP statique des périphériques connectés.

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

RY-LGSP23-26

Switch **DMS**

- ⚙️ Configuration ▾
 - » System <
 - » Green Ethernet <
 - » Ports Configuration <
 - » DHCP <
 - » Security ▾
 - » Switch <
 - » Network ▾
 - > Limit Control
 - > NAS
 - > ACL <
 - » IP Source Guard ▾
 - > Configuration
 - > Static Table

IP Source Guard Configuration

Mode Enabled ▾

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<> ▾	<> ▾
1	Disabled ▾	Unlimited ▾
2	Disabled ▾	Unlimited ▾
3	Enabled ▾	2 ▾
4	Disabled ▾	Unlimited ▾

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

The screenshot shows the 'Static IP Source Guard Table' configuration page. On the left is a navigation menu for 'RY-LGSP23-26' with tabs for 'Switch' and 'DMS'. The 'Configuration' menu is expanded, showing 'IP Source Guard' > 'Static Table'. The main area has a breadcrumb 'Home > Configuration > Security > Netv' and a title 'Static IP Source Guard Table'. Below the title is a table with columns: 'Delete', 'Port', 'VLAN ID', 'IP Address', and 'MAC address'. A single entry is shown with Port 3, VLAN ID 10, IP Address 192.168.10.40, and MAC address A1:00:00:00:00:FF. Below the table are buttons for 'Delete', 'Add New Entry', 'Apply', and 'Reset'.

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.

5.3 Protection de la gestion des switches et administration réseau (couches 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.

The screenshot shows the 'Add User' configuration page. On the left is a navigation menu for 'RY-LGSP23-26' with tabs for 'Switch' and 'DMS'. The 'Configuration' menu is expanded, showing 'Security' > 'Switch' > 'Users'. The main area has a breadcrumb 'Home > Configuration > Security > Netv' and a title 'Add User'. Below the title is a form titled 'User Settings' with fields for 'User Name' (test), 'Password' (masked), 'Password (again)' (masked), and 'Privilege Level' (10). Below the form are buttons for 'Apply', 'Reset', and 'Cancel'.

Paramètres de base des directives et privilèges utilisateur

- Les niveaux de privilèges (Privilege Levels) 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.

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
ACTIVATE	5	10	5	10
Aggregation	5	10	5	10
cloud_management	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	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.

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

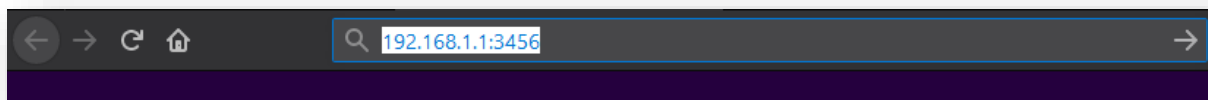
- Il est recommandé d'utiliser le protocole SSH pour l'administration en ligne de commande (CLI), car cette méthode fournit la connexion cryptée.

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 HTTP offre la meilleure protection, car la connexion est cryptée.

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.

RX-LGSP23-26

Switch DMS

Configuration

» System
 » Green Ethernet
 » Ports Configuration
 » DHCP
 » Security
 » Switch
 > Users
 > Privilege Levels
 > Auth Method
 > HTTPS
 > Access Management

Access Management Configuration

Home > Configuration > Security > Switch > Access Management

Mode

Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	192.168.1.10	192.168.1.11	☒	☒	☒
Delete	10	192.168.10.40	192.168.10.41	☐	☒	☐

Add New Entry

Apply Reset

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 barox RY-LGSP23-10G web interface. The left sidebar contains a menu with 'Configuration' expanded, showing 'Switch' and 'DMS' options. The main content area is titled 'Authentication Method Configuration' and shows a table with columns 'Client', 'Methods', and 'Service Port'. The table lists configurations for console, telnet, ssh, http, and https. The 'https' row is highlighted, showing 'local' for the client, 'no' for methods, and '443' for the service port. Below the table are 'Apply' and 'Reset' buttons.

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

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 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.

The screenshot shows the barox RY-LGSP23-26 web interface. The left sidebar contains a menu with 'Configuration' expanded, showing 'Switch' and 'DMS' options. The main content area is titled 'HTTPS Configuration' and shows a 'Certificate Maintain' section with a 'Generate' button. Below this is a 'Certificate Status' section showing 'Switch secure HTTP certificate is presented'. At the bottom are 'Apply' and 'Reset' buttons.

Certificate Maintain	Certificate Status
Generate	Switch secure HTTP certificate is presented

- Génération du certificat pour une utilisation ultérieure, qui peut être téléchargé et installé via le navigateur.

RY-LGSP23-26

Switch **DMS**

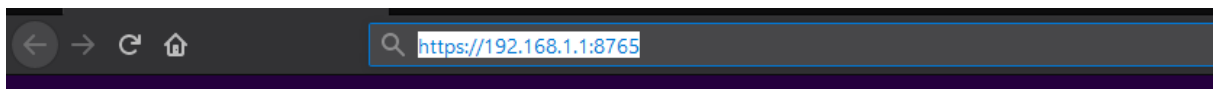
Configuration **HTTPS**

HTTPS Configuration Home > Configuration > Security > Switch > HTTPS

Certificate Maintain	Upload
Certificate Pass Phrase	
Certificate Upload	Web Browser
File Upload	Durchsuchen... Keine Datei ausgewählt.
Certificate Status	Switch secure HTTP certificate is presented

Apply **Reset**

- 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

En principe, le mode doit être activé et la version SNMP v2 doit être sélectionnée dans la configuration SNMP. Les noms des Communities Read and Write sont également définis.



RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Users

» Privilege Levels

» Auth Method

» HTTPS

» Access Management

» SNMP

» System

SNMP System Configuration

Home > Configuration >

Mode	Enabled
Version	SNMP v2c
Read Community	barox
Write Community	barox
Engine ID	800007e5017f000001

ApplyReset

5.4.2. Configuration de la Trap SNMP

Avant de configurer les nouveaux réglages Trap, assurez-vous que le réglage global du mode Trap est désactivé.

RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Users

» Privilege Levels

» Auth Method

» HTTPS

» Access Management

» SNMP

» System

» Trap

Trap Configuration

Home

Global Settings

Mode

Disabled

Trap Destination Configurations

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

Add New Entry

ApplyReset

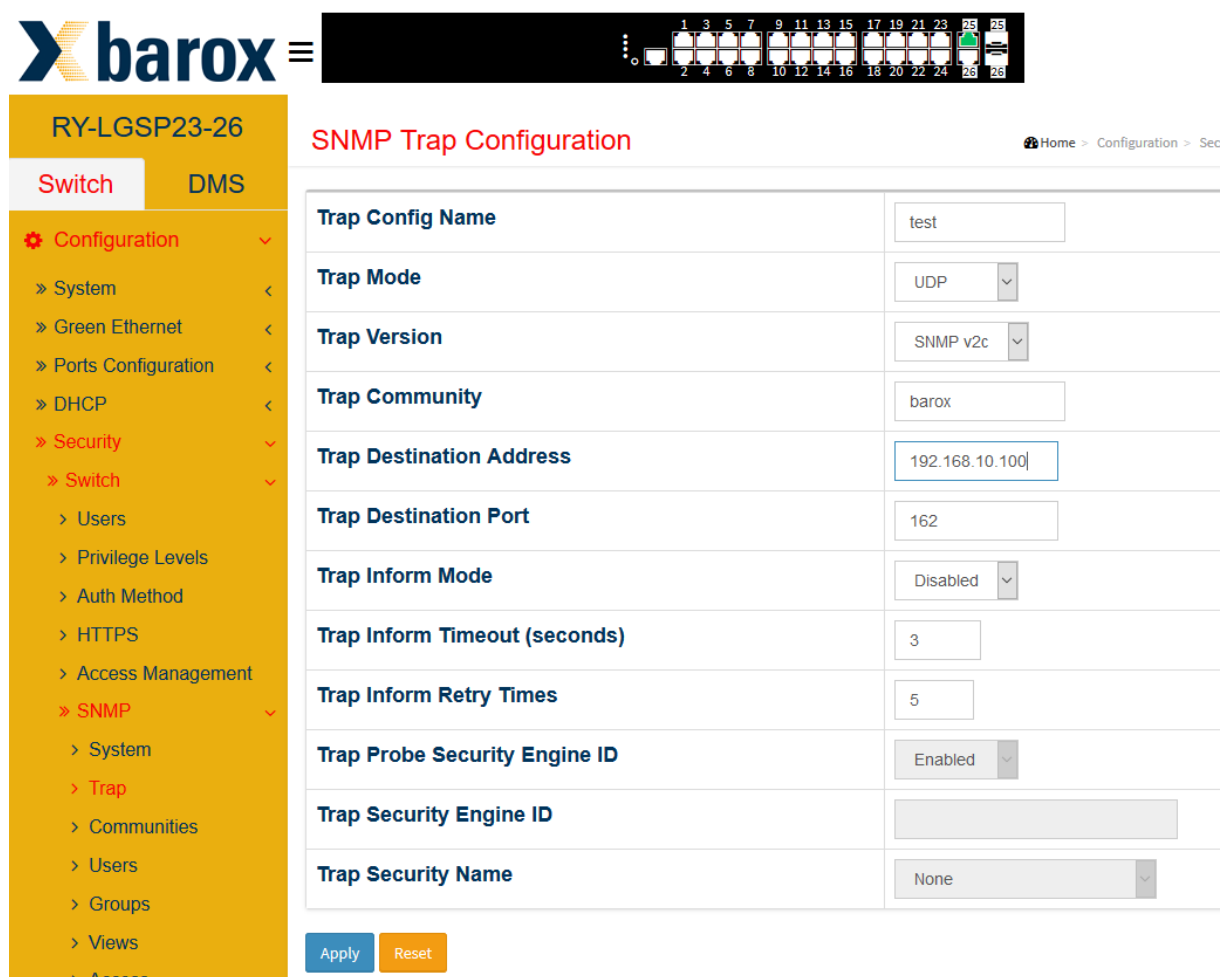
nouvelle configuration s'effectue en 2 étapes :

Étape 1 :

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
- Trap Inform Mode -> Sur "désactivé" dans le présent exemple
- Trap Inform Timeout (seconds) -> La valeur 3 est entrée (standard)
- Trap Inform Retry Times -> 5 (standard)

Les réglages sont ensuite confirmés avec "Apply"



barox RY-LGSP23-26

Home > Configuration > Sec

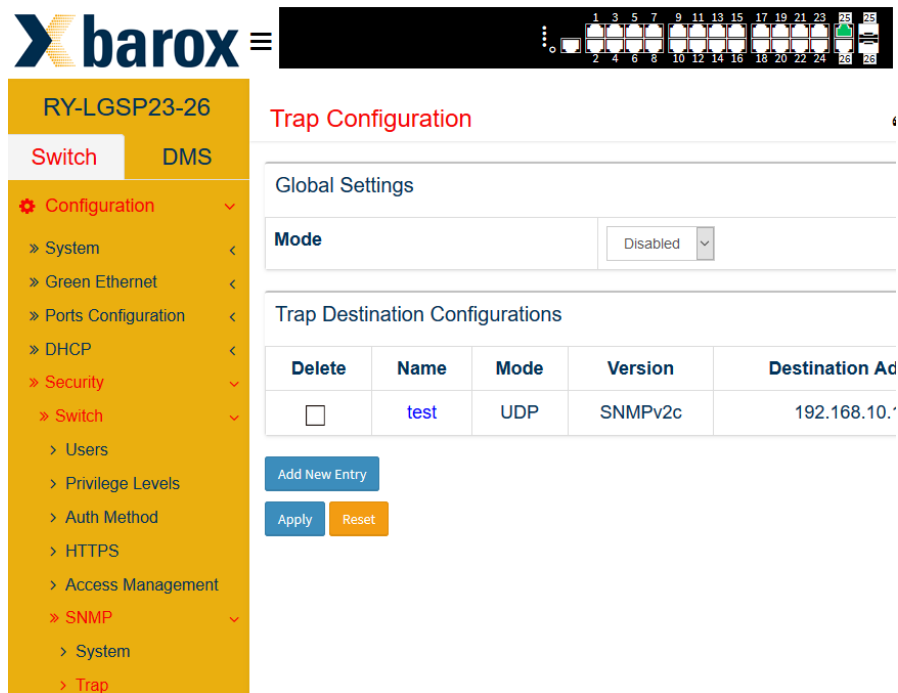
SNMP Trap Configuration

Trap Config Name	test
Trap Mode	UDP
Trap Version	SNMP v2c
Trap Community	barox
Trap Destination Address	192.168.10.100
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

Apply Reset

Étape 2 :

Après avoir créé la nouvelle configuration, on ouvre la configuration en sélectionnant le nom.



barox RY-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Switch
- » Users
- » Privilege Levels
- » Auth Method
- » HTTPS
- » Access Management
- » SNMP
- » System
- » Trap

Trap Configuration

Global Settings

Mode: Disabled

Trap Destination Configurations

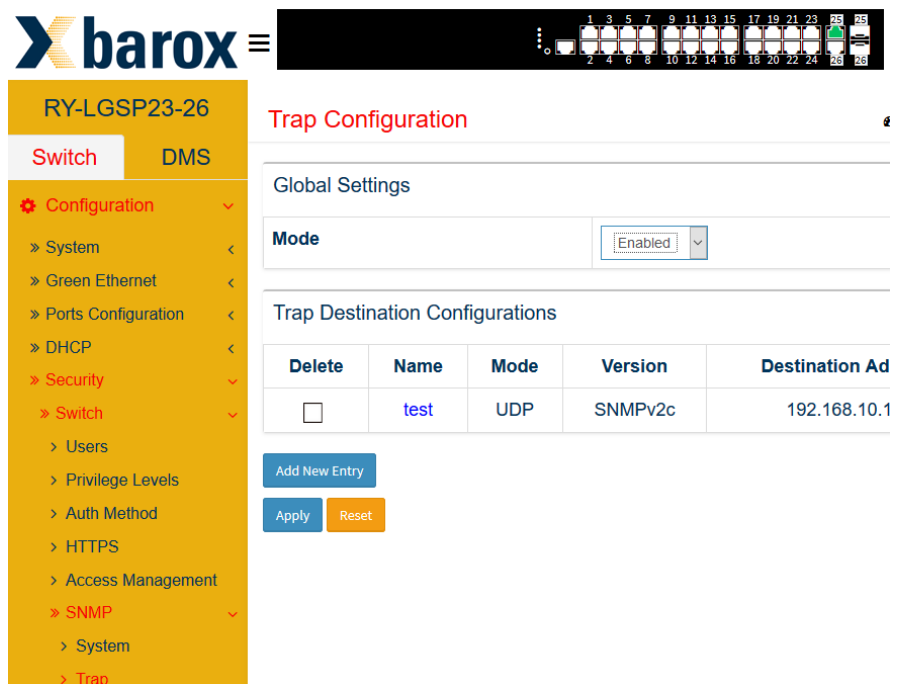
Delete	Name	Mode	Version	Destination Ad
☐	test	UDP	SNMPv2c	192.168.10.1

Add New Entry

Apply Reset

Activation de la fonction Trap SNMP

Une fois la configuration Trap terminée, le mode général doit être activé.



barox RY-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Switch
- » Users
- » Privilege Levels
- » Auth Method
- » HTTPS
- » Access Management
- » SNMP
- » System
- » Trap

Trap Configuration

Global Settings

Mode: Enabled

Trap Destination Configurations

Delete	Name	Mode	Version	Destination Ad
☐	test	UDP	SNMPv2c	192.168.10.1

Add New Entry

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.



RY-LGSP23-26

SwitchDMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Users

» Privilege Levels

» Auth Method

» HTTPS

» Access Management

» SNMP

» System

» Trap

» Communities

» Users

» Groups

» Views

» Access

» Trap Event Severity

Trap Event Severity Configuration

Home > Con

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	☒	☒
Firmware-Upgrade	Info	☒	☒
Import-Export	Info	☒	☒
LACP	Info	☒	☒
Link-Status	Warning	☒	☒
Login	Info	☒	☒
Logout	Info	☒	☒

ATTENTION : Pour les switches industriels, ce réglage se trouve sous Configuration/System/Alarm Notification.

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

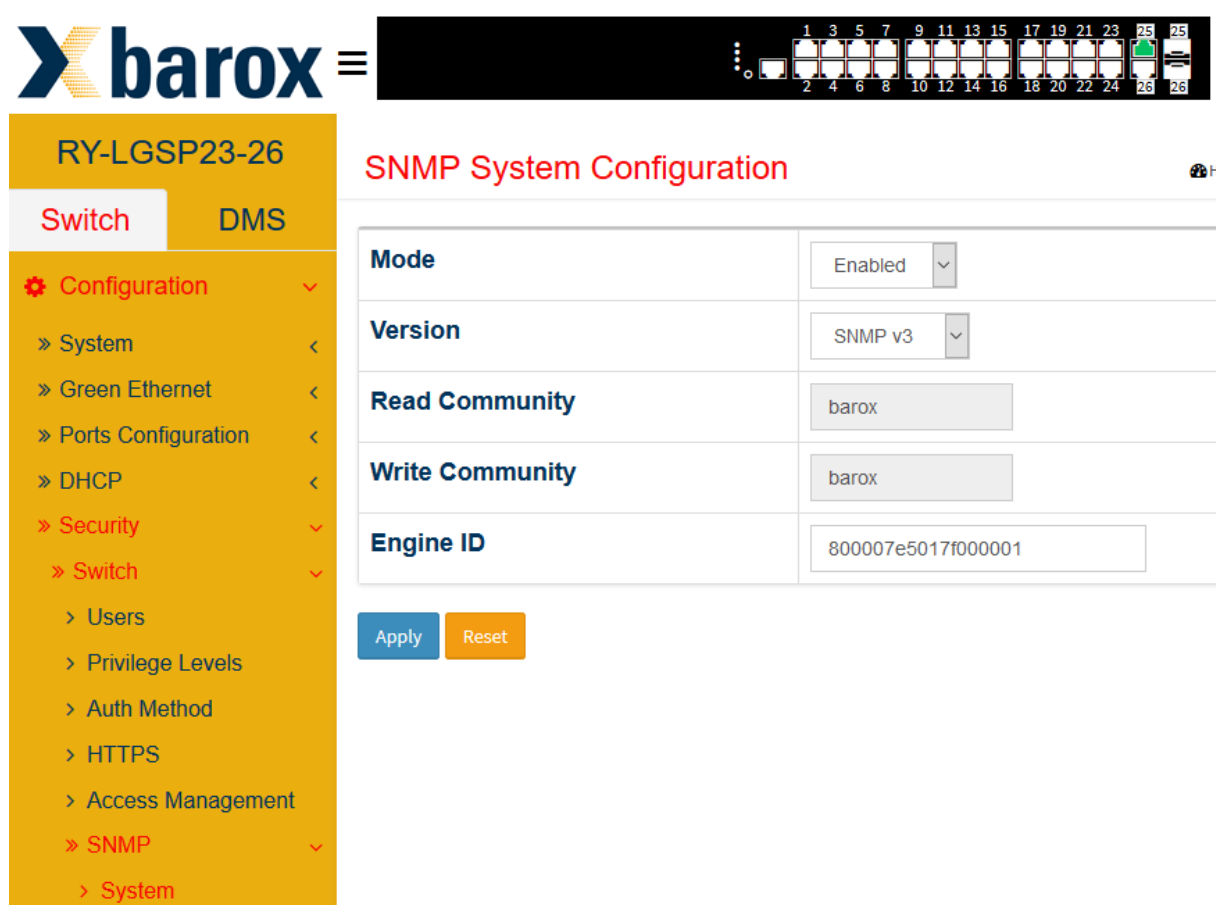
5.5 Configuration SNMP v3

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

En principe, le mode doit être activé et la version SNMP v3 doit être sélectionnée dans la configuration SNMP.



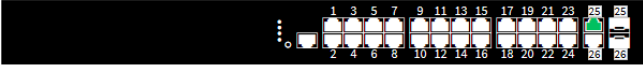
The screenshot shows the web interface of a barox RY-LGSP23-26 switch. The top navigation bar includes the barox logo and a status bar with various indicators. The left sidebar contains a menu with options like Configuration, System, Green Ethernet, Ports Configuration, DHCP, Security, Switch, Users, Privilege Levels, Auth Method, HTTPS, Access Management, SNMP, and System. The main content area is titled "SNMP System Configuration" and contains a table with the following settings:

Parameter	Value
Mode	Enabled
Version	SNMP v3
Read Community	barox
Write Community	barox
Engine ID	800007e5017f000001

At the bottom of the configuration table, there are two buttons: "Apply" and "Reset".

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 et de recevoir des messages SNMP sur plusieurs sous-réseaux.


RY-LGSP23-26

Switch DMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Users

» Privilege Levels

» Auth Method

» HTTPS

» Access Management

» SNMP

» System

» Trap

» Communities

SNMPv3 Community Configuration

Home > Configuration > Security > Switch > SNMP >

Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0
Delete	barox	0.0.0.0	0.0.0.0

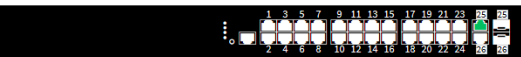
Add New Entry

Apply

Reset

Créer un nouvel utilisateur

Lors de la configuration du nouvel utilisateur, veuillez noter que l'Engine ID doit être ajouté au nouvel objet utilisateur. Celui-ci peut être simplement copié et collé à partir de l'entrée "default_user". 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-LGSP23-26

Switch DMS

Configuration

» System

» Green Ethernet

» Ports Configuration

» DHCP

» Security

» Switch

» Users

» Privilege Levels

» Auth Method

» HTTPS

» Access Management

» SNMP

» System

» Trap

» Communities

» Users

SNMPv3 User Configuration

Home > Configuration > Security > Switch > SNMP > Users

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete	0007e5017f000001	barox	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-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
 - » Switch
 - » Users
 - » Privilege Levels
 - » Auth Method
 - » HTTPS
 - » Access Management
 - » SNMP
 - » System
 - » Trap
 - » Communities
 - » Users
 - » Groups

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Delete usm barox barox

Add New Entry

Apply Reset

Paramétrage de la View Configuration

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-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
 - » Switch
 - » Users
 - » Privilege Levels

SNMPv3 View Configuration

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

Delete barox 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".

RY-LGSP23-26

Switch DMS

Configuration

System

Green Ethernet

Ports Configuration

DHCP

Security

Switch

Users

Privilege Levels

Auth Method

HTTPS

Access Management

SNMP

System

Trap

Communities

Users

Groups

Views

Access

SNMPv3 Access Configuration

Home > Configuration > Security > Switch > SNMP

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
☐	barox	any	Auth, Priv	barox	barox

Add New Entry

Apply Reset

5.5.2. Configuration de la Trap SNMP

Avant de configurer les nouveaux réglages Trap, assurez-vous que le réglage global du mode Trap est désactivé.

RY-LGSP23-26

Switch DMS

Configuration

System

Green Ethernet

Ports Configuration

DHCP

Security

Switch

Users

Privilege Levels

Auth Method

HTTPS

Access Management

SNMP

System

Trap

Trap Configuration

Home > Configuration > Security > Switch > SNMP > Trap

Global Settings

Mode

Disabled

Trap Destination Configurations

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

Add New Entry

Apply Reset

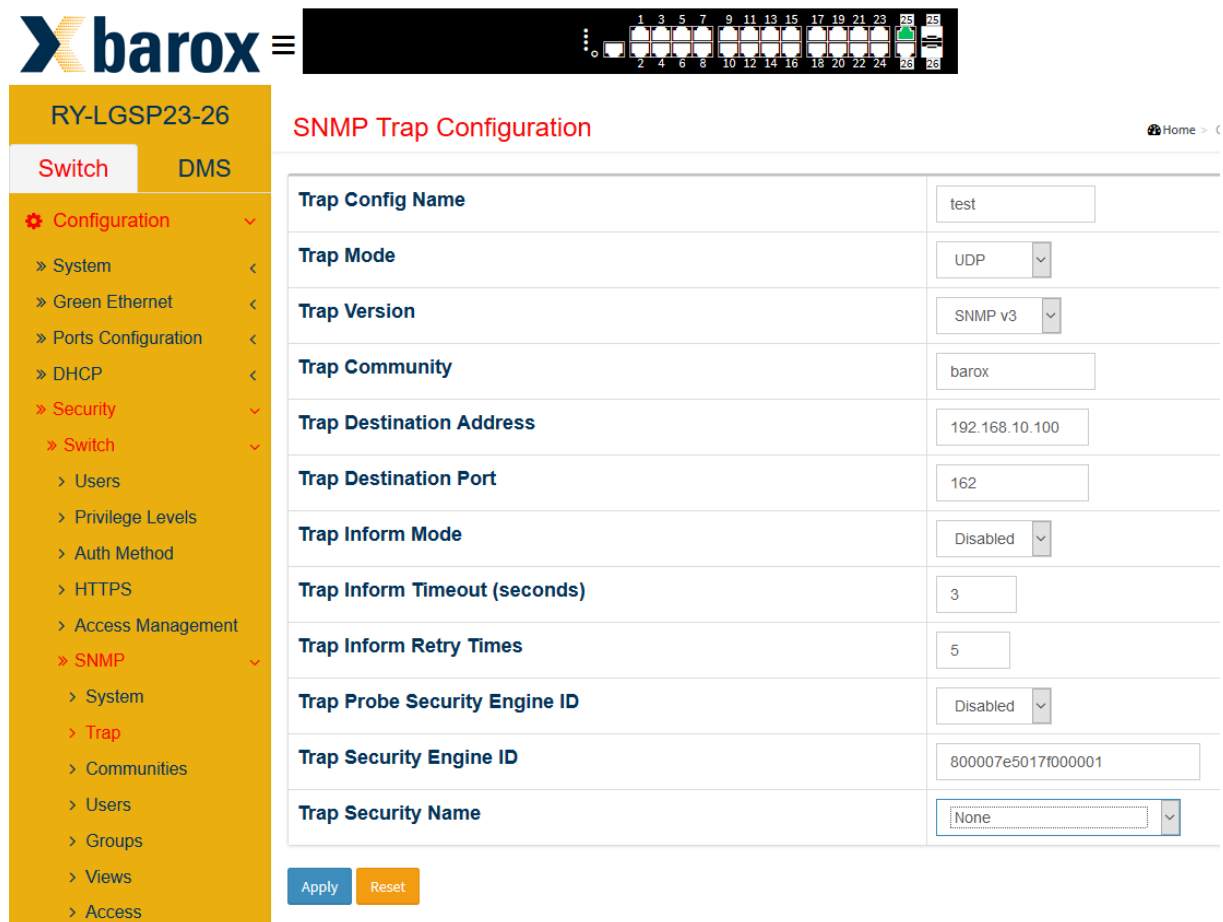
La nouvelle configuration s'effectue en 2 étapes :

Étape 1 :

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 Inform Mode -> Sur "désactivé" dans le présent exemple
- Trap Inform Timeout (seconds) -> La valeur 3 est entrée (standard)
- Trap Inform Retry Times -> 5 (standard)
- Trap Probe Security Engine ID -> Doit être désactivé
- Trap Security Engine ID -> L'Engine ID de l'utilisateur doit être entré ici
- Trap Security Name -> seul "None" peut être sélectionné pour l'instant

Les réglages sont ensuite confirmés avec "Apply"



The screenshot shows the barox web interface for the RY-LGSP23-26 switch. The left sidebar contains a menu with 'Configuration' and 'SNMP' sections. The main content area is titled 'SNMP Trap Configuration' and displays a form with the following fields:

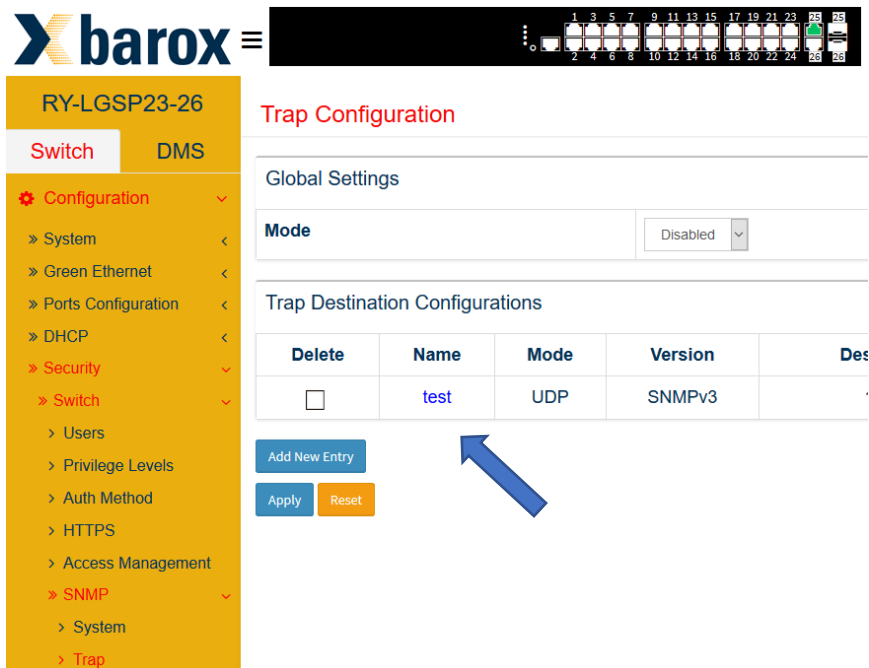
Field	Value
Trap Config Name	test
Trap Mode	UDP
Trap Version	SNMP v3
Trap Community	barox
Trap Destination Address	192.168.10.100
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Disabled
Trap Security Engine ID	800007e5017f000001
Trap Security Name	None

At the bottom of the form, there are 'Apply' and 'Reset' buttons.

Après avoir confirmé la configuration, vous serez informé qu'un Security Name correspondant doit encore être défini. Ceci sera configuré dans la 2ème étape.

Étape 2 :

Après avoir créé la nouvelle configuration, on ouvre la configuration en sélectionnant le nom.



RY-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Switch
- » Users
- » Privilege Levels
- » Auth Method
- » HTTPS
- » Access Management
- » SNMP
- » System
- » Trap

Trap Configuration

Global Settings

Mode: Disabled

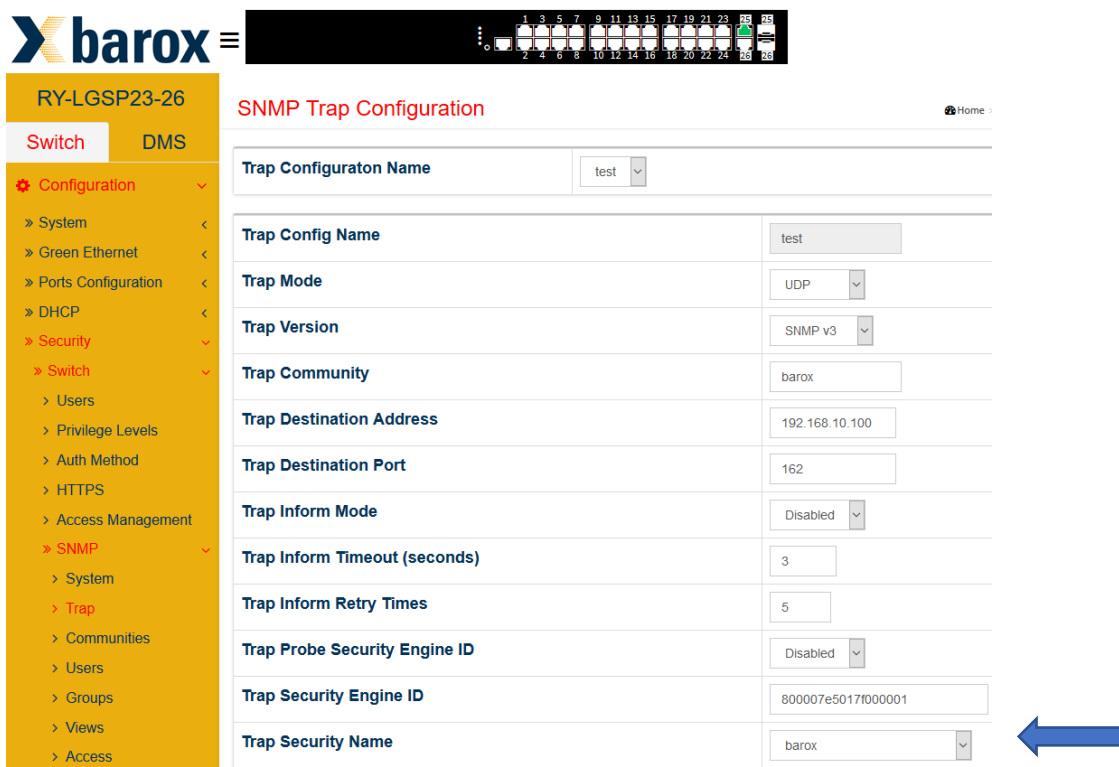
Trap Destination Configurations

Delete	Name	Mode	Version	Des
☐	test	UDP	SNMPv3	

Add New Entry

Apply Reset

L'entrée "Trap Security Name" peut maintenant être réglée sur l'utilisateur SNMP.



RY-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security
- » Switch
- » Users
- » Privilege Levels
- » Auth Method
- » HTTPS
- » Access Management
- » SNMP
- » System
- » Trap
- » Communities
- » Users
- » Groups
- » Views
- » Access

SNMP Trap Configuration

Trap Configuration Name: test

Trap Config Name: test

Trap Mode: UDP

Trap Version: SNMP v3

Trap Community: barox

Trap Destination Address: 192.168.10.100

Trap Destination Port: 162

Trap Inform Mode: Disabled

Trap Inform Timeout (seconds): 3

Trap Inform Retry Times: 5

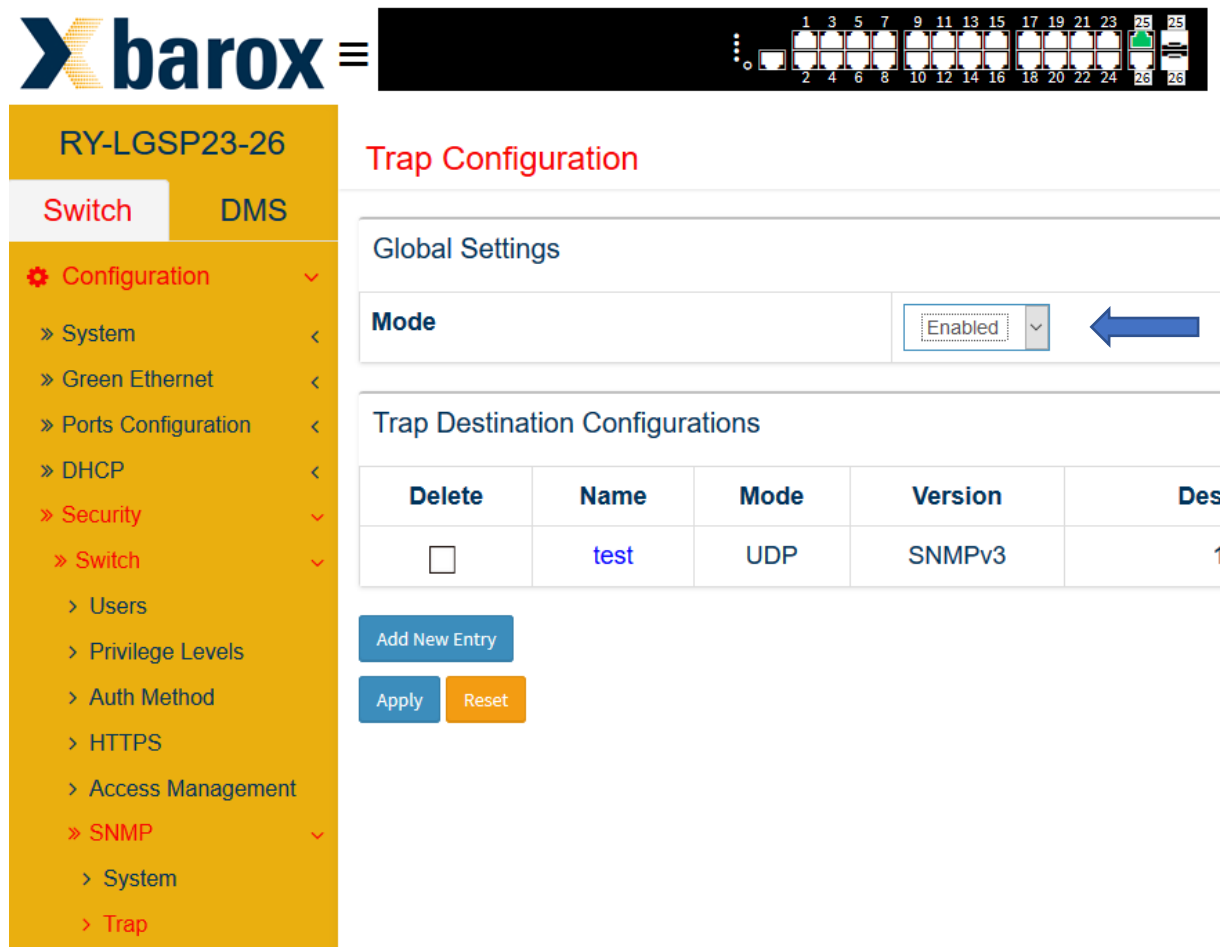
Trap Probe Security Engine ID: Disabled

Trap Security Engine ID: 800007e5017f000001

Trap Security Name: barox

Activation de la fonction Trap SNMP

Une fois la configuration Trap terminée, le mode général doit être activé.



RY-LGSP23-26

Switch DMS

Configuration

- » System
- » Green Ethernet
- » Ports Configuration
- » DHCP
- » Security**
- » Switch
- > Users
- > Privilege Levels
- > Auth Method
- > HTTPS
- > Access Management
- » SNMP**
- > System
- > Trap

Trap Configuration

Global Settings

Mode Enabled

Trap Destination Configurations

Delete	Name	Mode	Version	Des
☐	test	UDP	SNMPv3	1

Add New Entry

Apply Reset

5.5.3. 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.

RY-LGSP23-26

Switch **DMS**

- ⚙️ **Configuration** ▾
- » System ▹
- » Green Ethernet ▹
- » Ports Configuration ▹
- » DHCP ▹
- » **Security** ▾
- » **Switch** ▾
- > Users
- > Privilege Levels
- > Auth Method
- > HTTPS
- > Access Management
- » **SNMP** ▾
- > System
- > Trap
- > Communities
- > Users
- > Groups
- > Views
- > Access
- > **Trap Event Severity**

Trap Event Severity Configuration

🏠 Home > Conf

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 ▾	☒	☒
Firmware-Upgrade	Info ▾	☒	☒
Import-Export	Info ▾	☒	☒
LACP	Info ▾	☒	☒
Link-Status	Warning ▾	☒	☒
Login	Info ▾	☒	☒
Logout	Info ▾	☒	☒

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

5.6 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 :

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 66 bE 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 :

```

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 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

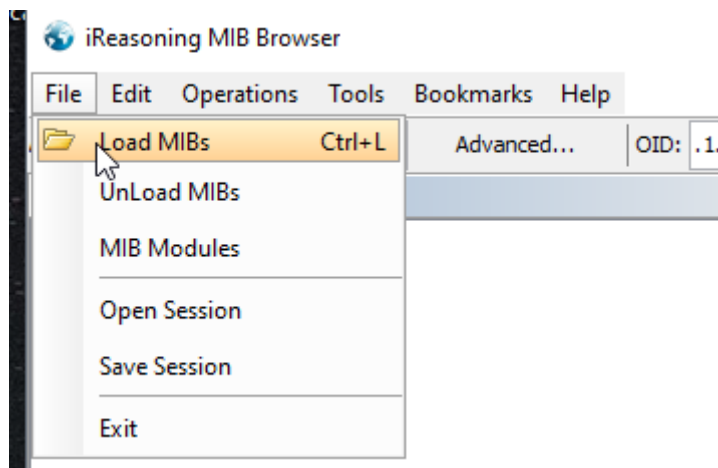
Dans le réseau, le statut des périphériques gérables tels que les switches, les routeurs ou les serveurs peut généralement être interrogé via la fonctionnalité SNMP. Pour des raisons de sécurité ou spécifiques au fabricant, ces fichiers MIB sont souvent nécessaires pour interroger les appareils. Ces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

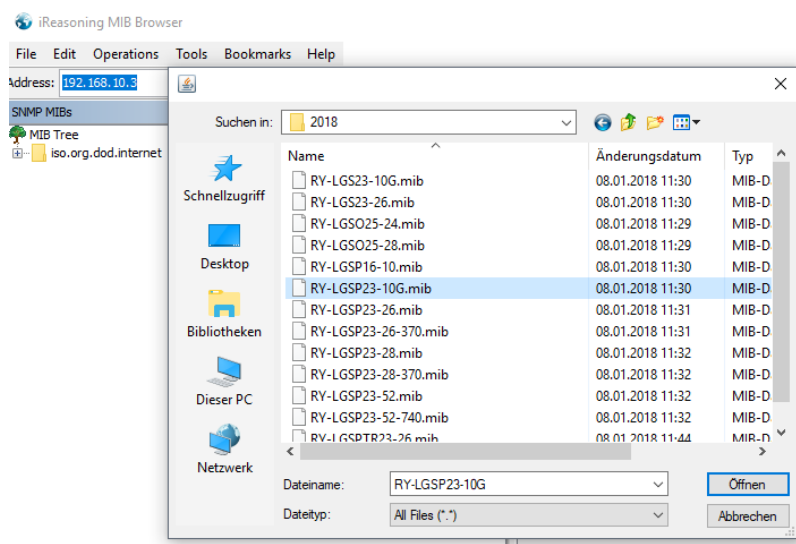
Étape 1 Import du fichier MIB

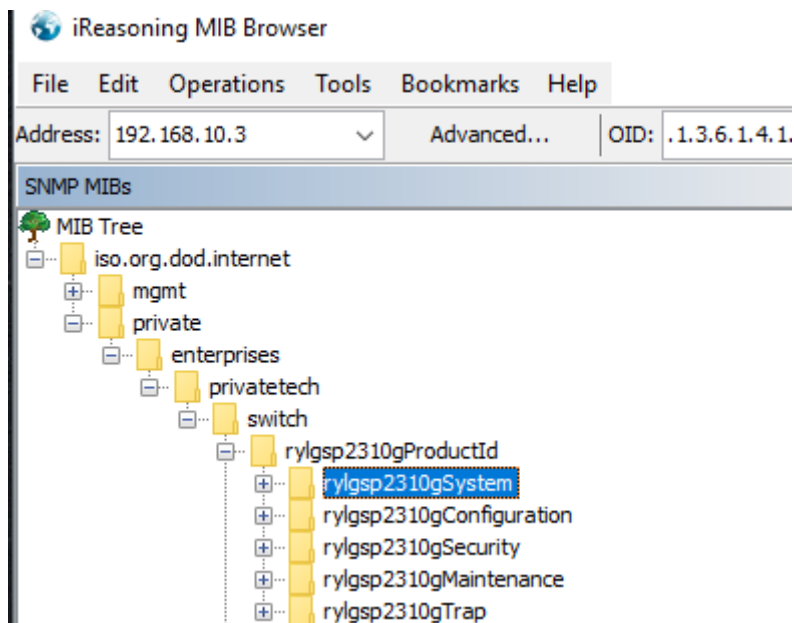
Lors de l'import, assurez-vous que le fichier MIB approprié est sélectionné pour le switch correspondant. Les fichiers MIB requis sont reconnaissables au préfixe ".mib".



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

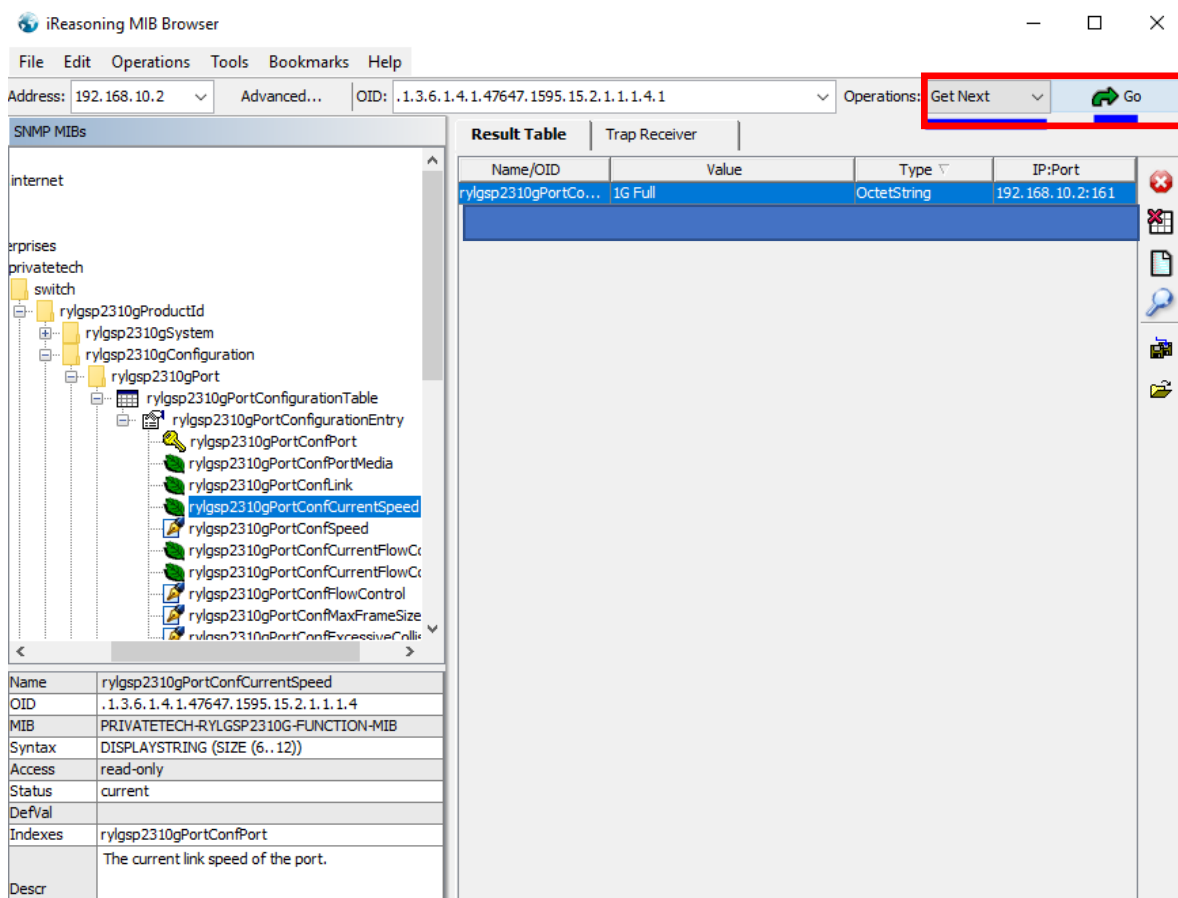
Une fois l'import réussi, les structures MIB sont affichées comme suit.





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"

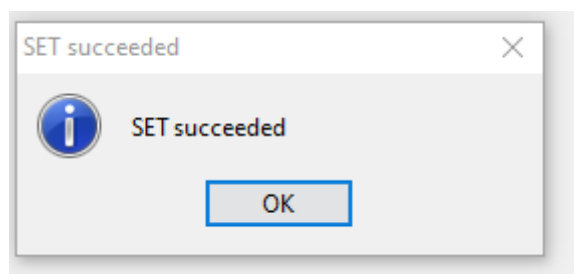
Comme autre méthode de commande des switches barox, il est possible d'effectuer l'opération "SET" via le protocole SNMP. Les configurations SNMP de base sur le switch et le navigateur MIB sont prérequis. Voici un exemple d'utilisation de l'opération SET qui déclenche l'arrêt du port et la reconnexion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

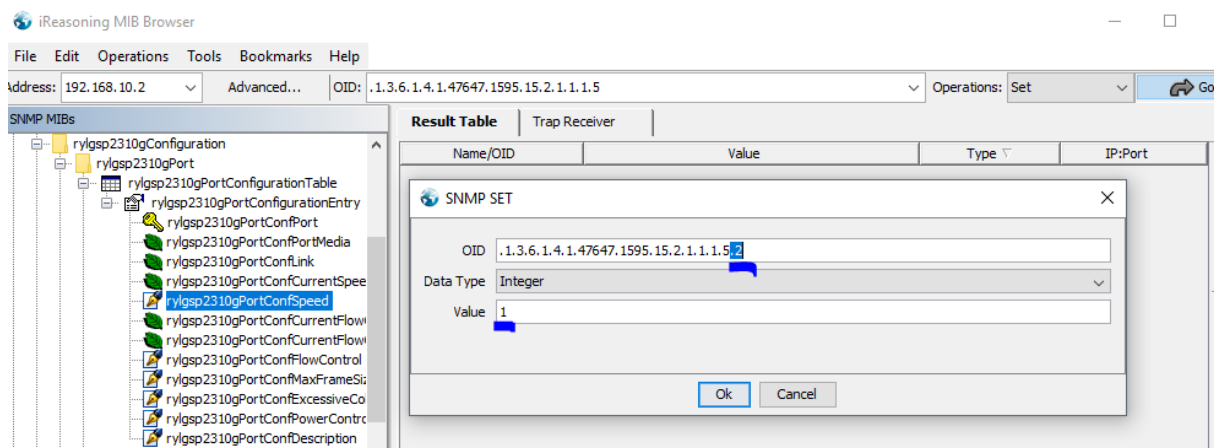
The screenshot shows the iReasoning MIB Browser interface. The left pane displays a tree of SNMP MIBs, with 'rylgsp2310gPortConfSpeed' selected. The right pane shows the 'Result Table' with columns: Name/OID, Value, Type, and IP:Port. Below the table, a table lists details for 'rylgsp2310gPortConfSpeed':

Name	rylgsp2310gPortConfSpeed
OID	.1.3.6.1.4.1.47647.1595.15.2.1.1.1.5
MIB	PRIVATETECH-RYLGSP2310G-FUNCTION-MIB
Syntax	INTEGER32 (0..11)
Access	read-write
Status	current
DefVal	
Indexes	rylgsp2310gPortConfPort
Descr	default: 1, 0:disable state, 1:auto, 2:10 Half, 3:10 Full, 4:100 Half, 5:100 Full, 6:1G full,

An 'SNMP SET' dialog box is open, showing the OID '.1.3.6.1.4.1.47647.1595.15.2.1.1.1.5.2', Data Type 'Integer', and Value '0'. The 'Go' button is visible in the top right of the browser window.



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.

The screenshot shows the barox web interface for device RY-LGSP23-28/370. The left sidebar contains a menu with 'Maintenance' expanded, showing 'Firmware' and 'Firmware Upgrade'. The main content area is titled 'Software Upload' and features a 'Firmware File' input field with a 'Durchsuchen...' button and a status message 'Keine Datei ausgewählt.'. Below this is an 'Upload' button. The top navigation bar includes 'Home', 'Maintenance', 'Firmware', and 'Firmware Upgrade'.

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".

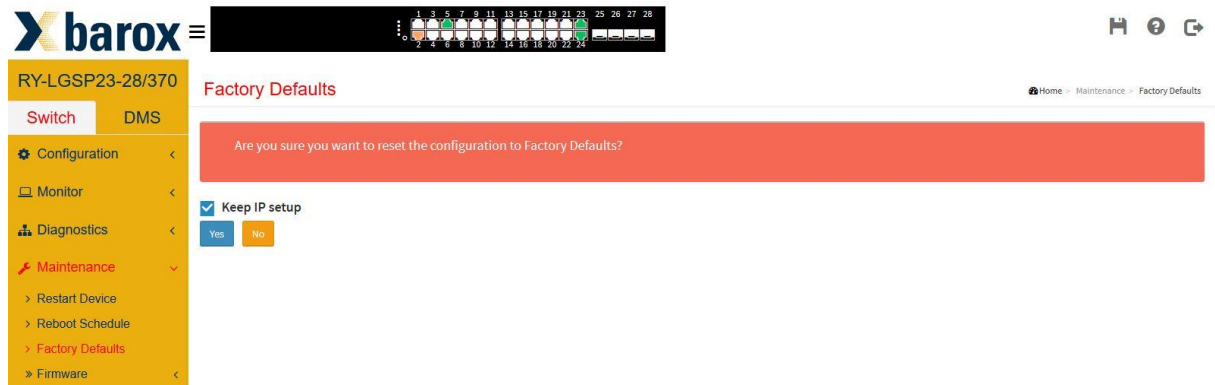
The screenshot shows the barox web interface for device RY-LGSP23-28/370, specifically the 'Software Image Selection' page. The left sidebar shows 'Firmware Selection' selected under the 'Firmware' menu. The main content area displays two sections: 'Active Image' and 'Alternate Image'. The 'Active Image' section shows details for the current firmware: Image (managed), Version (RY-LGSP23-28/370 (standalone) v6.54.3133), and Date (2019-04-04T00:51:35+08:00). The 'Alternate Image' section shows details for a backup firmware: Image (managed.bk), Version (RY-LGSP23-28/370 (standalone) v6.54.2997), and Date (2018-11-01T00:07:09+08:00). At the bottom, there are 'Activate Alternate Image' and 'Cancel' buttons. The top navigation bar includes 'Home', 'Maintenance', 'Firmware', and 'Firmware Selection'.

7 Réglages d'usine

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

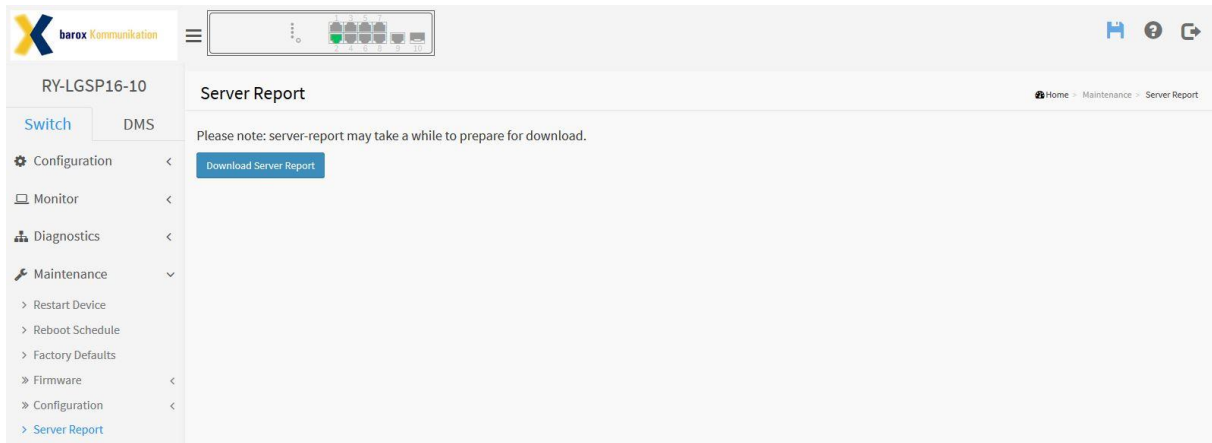
Soit par logiciel via le menu "Maintenance/Factory Defaults", soit en appuyant sur la touche de réinitialisation sur la face avant (plus de 10 secondes).

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 Server Report

Lors de demandes d'assistance, le Server Report doit également être envoyé. Il contient une présentation de l'ensemble de la configuration et d'autres informations utiles pour le technicien d'assistance.



Extrait d'un Server Report

```
server-report - Editor
Datei Bearbeiten Format Ansicht ?

----- System Overview -----

Model Name: RY-LGSP16-10

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

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

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

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

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

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

9 GARANTIE

barox Kommunikation 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.
5. Dommages causés par le transport, la négligence, les fluctuations ou les pannes de l'alimentation électrique, la force majeure ou l'environnement d'exploitation.
6. Dommages dus à l'usure normale
7. Dommages causés par des virus informatiques et autres logiciels
8. 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.